



Wireless ADSL2/2+ Modem Router

User Manual

KM-4150NR

V1.0

Contents

Wizard	9
Internet Setup	16
Wireless Setup	18
Local Network	20
Time and Date	22
Logout	23
Advanced Wireless	24
Port Forwarding	33
DMZ	35
Parental Control	36
Filtering Options	41
QoS Config	47
Firewall Settings	51
DNS	52
Dynamic DNS	53
Network Tools	56
Routing	66
Schedules	70
Logout	71
System Management	72
Firmware Update	74
Access Controls	74
Diagnostics	78
Log Configuration	79
Logout	80
Device Info	80
Wireless Clients	82
DHCP Clients	82
Logs	83
Statistics	83
Route info	84
Logout	85

1 Introduction

The KM-4150NR supports multiple line modes. It provides four 10/100 base-T Ethernet interfaces at the user end. The device provides high-speed ADSL broadband connection to the Internet or Intranet for high-end users, such as net bars and office users. It provides high performance access to the Internet, downstream up to 24 Mbps and upstream up to 1 Mbps.

The device supports WLAN access, such as WLAN AP or WLAN device, to the Internet. It complies with IEEE 802.11,802.11b/g specifications, WEP, WPA, and WPA2 security specifications.

1.1 Package List

- 1 x KM-4150NR
- 1 x external splitter
- 1 x power adapter
- 2 x telephone cables (RJ-11, more than 1.8m)
- 1 x Ethernet cable (RJ-45, more than 1.8m)
- 1 x user manual
- 1 x quality guarantee card
- 1 x certificate of quality

1.2 Safety Cautions

Follow the following instructions to prevent the device from risks and damage caused by fire or electric power:

- Use volume labels to mark the type of power.
- Use the power adapter packed within the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to

avoid damage caused by overheating to the device. The long and thin holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.

- Do not put this device close to a place where a heat source exits or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where it is over damp or watery. Do not spill any fluid on this device.
- Do not connect this device to any PCs or electronic products, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause power or fire risk.
- Do not place this device on an unstable surface or support.

1.3 LEDs and Interfaces

Front Panel



Figure 1

Front panel

The following table describes the LEDs of the device.


LED	Color	Status	Description
Power	Green	Off	The power is off.
		On	The power is on and the initialization is normal.
	Red	On	The device is initiating.
		Blinks	The firmware is upgrading.
Status	Green	Off	No IP is connected.
		Blinks	IP traffic is detected.
LAN 1/2/3/4	Green	Off	No LAN link.
		Blinks	Data is being transmitted through the LAN interface.
		On	The connection of LAN interface is normal.
WLAN	Green	Off	No WLAN connection.
WLAN	Green	Blinks	Data is transmitted through the WLAN interface.
		On	The connection of WLAN interface is normal.
DSL	Green	Off	Initial self-test is failed.
		Blinks	The device is detecting itself.
		On	Initial self-test of the unit has passed and is ready.
Internet	Green	Off	The device is under the Bridge mode, DSL connection is not present, or the power is off.
		On	IP is connected.
	Red	On	The device is attempted to become IP connected, but failed.

Rear Panel



Figure 2 Rear panel

The following table describes the interface of the device.

Interface/Button	Description
DSL	RJ-11 interface that connects to the telephone set through the telephone cable.
LAN1/2/3/4	Ethernet RJ-45 interfaces that connect to the Ethernet interfaces of computers or Ethernet devices.
Power	Interface that connects to the power adapter.
Reset	Reset to the factory defaults. To restore factory defaults, keep the device powered on and push a paper clip into the hole. Press down the button for over 5 seconds and release.
WPS	Wi-Fi Protected Setup
	Power on or off.

1.4 Features

The device supports the following features:

- Various line modes
- External PPPoE dial-up access
- Internal PPPoE and PPPoA dial-up access
- Leased line mode
- Zero installation PPP bridge mode (ZIPB)
- 1483B, 1483R, and MER access
- Multiple PVCs (eight at most) and these PVCs can be isolated from each other
- A single PVC with multiple sessions

- Multiple PVCs with multiple sessions
- Binding of ports with PVCs
- 802.1Q and 802.1P protocol
- DHCP server
- NAT and NAT
- Static route
- Firmware upgrade: Web, TFTP and FTP
- Reset to the factory defaults
- DNS relay
- Virtual server
- DMZ
- Two-level passwords and user names
- Web user interface
- Telnet CLI
- System status display
- PPP session PAP and CHAP
- IP filter
- IP QoS
- Remote access control
- Line connection status test
- Remote management (telnet and HTTP)
- Backup and restoration of configuration file
- Ethernet interface supports crossover detection, auto-correction and polarity correction
- UPnP

Error! Style not defined.

2 Hardware Installation

Step 1 Connect the DSL port of the device and the Modem port of the splitter with a telephone cable. Connect the phone to the Phone port of the splitter through a telephone cable. Connect the incoming line to the Line port of the splitter.

The splitter has three ports:

- Line: Connect to a wall phone port (RJ-11 jack).
- Modem: Connect to the DSL port of the device.
- Phone: Connect to a telephone set.

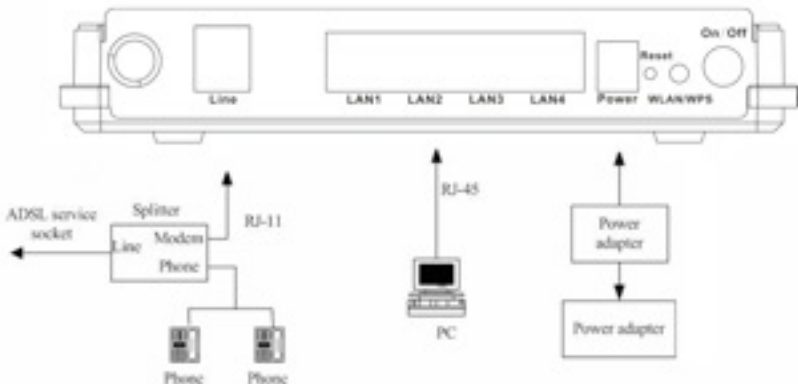
Step 2 Connect the LAN port of the device to the network card of the PC through an Ethernet cable (MDI/MDIX).

Note:

Use twisted-pair cables to connect with the Hub or switch.

Step 3 Plug one end of the power adapter to the wall outlet and connect the other end to the Power port of the device.

Connection 1: Figure 3 displays the application diagram for the connection of the device, PC, splitter and telephone sets, when no telephone set is placed before the splitter.



Wireless ADSL2/2+ Modem Router

Figure 3 Connection diagram (without telephone sets before the splitter)

Connection 2: Figure 4 displays the application diagram for the connection of the device, PC, splitter and telephone sets when a telephone set is placed before the splitter.

As illustrated in the following figure, the splitter is installed close to the device.

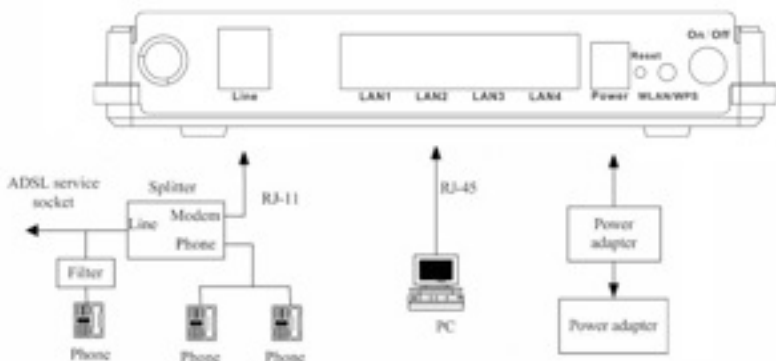


Figure 4 Connection diagram (with a telephone set before the splitter)
Connection 1 is recommended.

Note:

When connection 2 is used, the filter must be installed close to the telephone cable. See Figure 4. Do not use the splitter to replace the filter.

Installing a telephone directly before the splitter may lead to failure of connection between the device and the central office, or failure of Internet access, or slow connection speed. If you really need to add a telephone set before the splitter, you must add a microfilter before a telephone set. Do not connect several telephones before the splitter or connect several telephones with the microfilter.

3 About the Web Configurator

This chapter describes how to configure the device by using the Web-based configuration utility.

3.1 Access the Device

The following is the detailed description of accessing the device for the first time.

Step 4 Open the Internet Explorer (IE) browser and enter <http://192.168.1.1>.

Step 5 The **Login** page shown in the following figure appears. Enter the user name and password.

- The user name and password of the super user are **admin** and **admin**.
- The user name and password of the normal user are **user** and **user**.



Input username and password

UserName

Password

If you log in as the super user successfully, the page shown in the following figure appears.



3.2 Setup

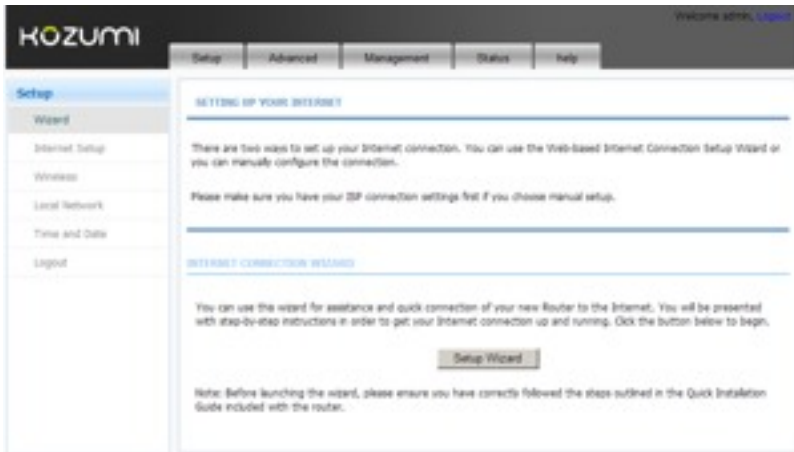
3.2.1 Wizard

Wizard enables fast and accurate configuration of Internet connection and other important parameters. The following sections describe these various configuration parameters.

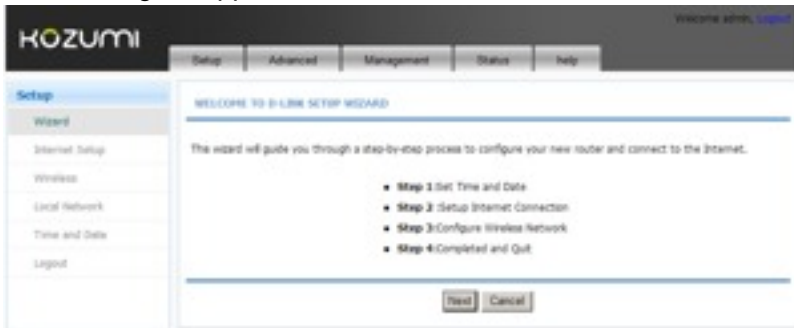
When subscribing to a broadband service, you should be aware of the method, by which you are connected to the Internet. Your physical WAN device can be Ethernet, DSL, or both. Technical information about the properties of your Internet connection is provided by your Internet service provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, or the protocol, such as PPPoA or PPPoE, that you use to communicate over the Internet.

Step 6 Choose **Setup** > **Wizard**. The page shown in the following figure appears.

Wireless ADSL/2+ Modem Router



Step 7 Click **Setup Wizard**. The page shown in the following figure appears.



Step 8 There are four steps to configure the device. Click **Next** to continue.

Step 9 Set the time and date.

The screenshot shows the Kozumi router's web interface. The top navigation bar includes 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The left sidebar lists 'Setup' (selected), 'Wizard', 'Internet Setup', 'Wireless', 'Local Network', 'Time and Date', and 'Logout'. The main content area is titled 'STEP 1 - SET TIME AND DATE'. It contains a descriptive paragraph about time configuration, a 'TIME SETTINGS' section with a checked option for 'Automatically synchronize with Internet time servers' and two input fields for '1st NTP time server' and '2nd NTP time server', and a 'TIME CONFIGURATION' section with a 'Time Zone' dropdown menu, an unchecked 'Enable Daylight Saving' checkbox, and two rows of time selection fields (Hour, Min, Sec) for 'Daylight Saving Start' and 'Daylight Saving End'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

Step 10 Setup the Internet connection.

Select the country and ISP. Set the VPI and VCI. If you fail to find the country and ISP from the drop-down lists, select **Others**. Click **Next**. If the **Protocol** is **PPPoE** or **PPPoA**, the page shown in either of the two following figures appears.

Wireless ADSL2/2+ Modem Router

The screenshot shows the Kozumi router's web interface. The top navigation bar includes 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The left sidebar lists 'Setup' (selected), 'Wizard', 'Internet Setup', 'Wireless', 'Local Network', 'Time and Date', and 'Logout'. The main content area is titled 'STEP 2: SETUP INTERNET CONNECTION'. It instructs the user to select an ISP and shows the following configuration: Protocol: PPPoE, Encapsulation Mode: LLC, VPI: 0 (range 0-255), VCI: 35 (range 0-4095), and Encapsulation Mode: Scan. Below this, it asks for Username and Password, with a 'Confirm Password' field. 'Back', 'Next', and 'Cancel' buttons are at the bottom.

Set the user name and password.

If the **Protocol** is **Dynamic IP**, the page shown in the following figure appears.

This screenshot is identical to the one above, but the 'Protocol' dropdown menu is set to 'Dynamic IP'. The rest of the configuration options (Encapsulation Mode: LLC, VPI: 0, VCI: 35, Encapsulation Mode: Scan) and the Username/Password fields remain the same.

If the **Protocol** is **Bridge**, the page shown in the following figure appears.

Wireless ADSL2/2+ Modem Router

The screenshot shows the Kozumi router's web interface. The top navigation bar includes 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The 'Setup' menu is expanded, showing 'Wizard', 'Internet Setup', 'Wireless', 'Local Network', 'Time and Date', and 'Logoff'. The main content area is titled 'STEP 2: SETUP INTERNET CONNECTION'. It instructs the user to select an ISP from the list below. The form includes a 'Protocol' dropdown menu set to 'Bridge', an 'Encapsulation Mode' dropdown set to 'LLC', and two input fields for 'VPI' (set to 0) and 'VCI' (set to 35). Below these are 'Encapsulation Mode' buttons for 'Scan' and 'Static'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

If the **Protocol** is **Static IP**, the page shown in the following figure appears.

The screenshot shows the 'STATIC IP' configuration page. It states: 'You have selected STATIC IP Internet connection. Please enter the appropriate information below as provided by your ISP. The Auto PVC Scan feature will not work in all cases so please enter the VPI/VCI numbers if provided by the ISP. Click Next to continue.' The form contains four input fields: 'IP Address', 'Subnet Mask', 'Default Gateway', and 'Primary DNS Server'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

Enter the **IP Address**, **Subnet Mask**, **Default Gateway**, and **Primary DNS Server**. Click **Next**. The page shown in the following page appears.

Wireless ADSL2/2+ Modem Router

The screenshot shows the Kozumi router's web interface. The top navigation bar includes 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The left sidebar lists configuration categories: 'Wizard', 'Internet Setup', 'Wireless', 'Local Network', 'Time and Date', and 'Logout'. The main content area is titled 'STEP 3: CONFIGURE WIRELESS NETWORK' and contains the following sections:

- Enable Your Wireless Network:** A radio button is selected for 'Enabled'. Text below explains that wireless is enabled by default and can be disabled.
- Wireless Network Name (SSID):** A text input field contains the value 'room_1'.
- Visibility Status:** Radio buttons are selected for 'Visible' and 'Invisible'. Text explains that 'Visible' allows discovery by clients, while 'Invisible' requires manual SSID entry.
- Security Level:** A table lists four options: 'None', 'WEP', 'WPA-PSK', and 'WPA2-PSK'. The 'None' option is selected.
- Security Mode/Options:** A text input field is present with the instruction: 'Select the option if you do not want to activate any security features.'

At the bottom of the configuration area are three buttons: 'Back', 'Next', and 'Cancel'.

Step 11 Configure the wireless network. Enter the information and click **Next**.

STEP 6: COMPLETED AND RESTART

Setup complete. Click "Back" to review or modify settings.

If your Internet connection does not work, you can try the Setup Wizard again with alternative settings or use Manual Setup instead if you have your Internet connection details as provided by your ISP.

STEP SUMMARY

Below is a detailed summary of your settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Time Settings :	1
NTP Server 1:	192.168.2.10
NTP Server 2:	192.168.2.100
Time Zone:	-08:00
Daylight Saving Time (1)	0
VPI/VCI :	0/35
Protocol :	Static IP
Connection Type :	LLC
IP Address 1 :	
Subnet Mask :	
Default Gateway :	
Primary DNS Server :	
Wireless Network Name (SSID) :	Kozumi_
Visibility Status :	0
Encryption :	None
Pre-Shared Key :	
WEP Key :	

Back Apply Cancel

Step 12 When the settings are complete, click **Apply** to apply the settings and reboot the device.

Rebooting...

System is rebooting... Please wait for a moment

Please relogin after reboot

11%

Note:

In each step of the Wizard page, you can click **Back** to review or

modify the previous settings. Click **Cancel** to exit the wizard page.

3.2.2 Internet Setup

Choose **Setup > Internet Setup**. The page shown in the following figure appears. In this page, you can configure the WAN interface of the device.



Click **Add**. The page shown in the following figure appears.

Wireless ADSL2/2+ Modem Router

The screenshot shows the configuration interface for a Kozumi Wireless ADSL2/2+ Modem Router. The main content area is titled "INTERNET SETUP" and contains the following sections:

- INTERNET SETUP:** A introductory text stating, "This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category."
- ATM PVC CONFIGURATION:** This section contains several input fields:
 - VPI: 0 (range 0-255)
 - VCI: 35 (range 32-65535)
 - Service Category: UBR With PCR (dropdown menu)
 - Peak Cell Rate: 0 (range 0-64K)
 - Sustainable Cell Rate: 0 (range 0-1K)
 - Maximum Burst Size: 0 (range 0-6K)
- CONNECTION TYPE:** This section contains:
 - Protocol: Bridging (dropdown menu)
 - Encapsulation Mode: L2L (dropdown menu)
 - VDSL2 QoS PLAN ID: 0 (range 0-4096)
- NETWORK ADDRESS TRANSLATION SETTINGS:** This section contains:
 - Enable Bridge Service:
 - Service Category: N, D, S, L, P (dropdown menu)

At the bottom of the configuration area, there are "Apply" and "Cancel" buttons.

The table describes the parameters in this page.

Field	Description
ATM PVC CONFIGURATION	
VPI	Virtual Path Identifier (VPI) is the virtual path between two points in an ATM network. Its value range is from 0 to 255.
VCI	Virtual Channel Identifier (VCI) is the virtual channel between two points in an ATM network. Its value range is from 32 to 65535 (0 to 31 is reserved for local management of ATM traffic).
Service Category	Select UBR with PCR , UBR without PCR , CBR , Non Realtime VBR , or Realtime VBR from the drop-down list.

Wireless ADSL2/2+ Modem Router

Field	Description
Peak Cell Rate	Set the maximum transmission rate of the cell in ATM transmission.
Sustainable Cell Rate	Set the minimum transmission rate of the cell in ATM transmission.
Maximum Burst Size	Set the maximum burst size of the cell in ATM transmission.
CONNECTION TYPE	
Protocol	Select PPP over ATM (PPPoA) , PPP over Ethernet (PPPoE) , MAC Encryption Routing (MER) , IP over ATM(IPOA) , or Bridging from the drop-down list.
Encapsulation Mode	Select LLC or VCMUX from the drop-down list. Usually, you can select LLC .
NETWORK ADDRESS TRANSLATION SETTINGS	
Enable Bridge Service	Select or deselect the check box to enable or disable the WAN connection.
Service Category	The name to identify the WAN connection. You need not modify it.

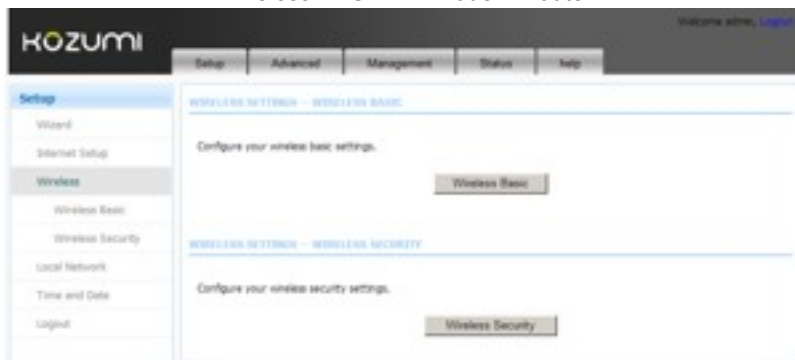
Click **Apply** to save the current settings and reboot the device.

3.2.3 Wireless Setup

This section describes the wireless LAN and some basic configuration. Wireless LANs can be as simple as two computers with wireless LAN cards communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN cards communicating through access points which bridge network traffic to wired LAN.

Choose **Setup > Wireless**. The **Wireless Setup** page shown in the following figure appears.

Wireless ADSL/2+ Modem Router



3.2.3.1 Wireless Basics

In the **Wireless Setup** page, click **Wireless Basics**. The page shown in the following figure appears. In this page, you can configure the parameters of wireless LAN clients that may connect to the device.



Click **Apply** to save the settings.

3.2.3.2 Wireless Security

In the **Wireless Setup** page, click **Wireless Security**. The page shown in the following figure appears. Wireless security is vital to your network to protect the wireless communication among wireless stations, access points and wired network.



Click **Apply** to save the settings.

3.2.4 Local Network

You can configure the LAN IP address according to the actual application. The preset IP address is 192.168.1.1. You can use the default settings and DHCP service to manage the IP settings for the private network. The IP address of the device is the base address used for DHCP. To use the device for DHCP on your LAN, the IP address pool used for DHCP must be compatible with the IP address of the device. The IP address available in the DHCP IP address pool changes automatically if you change the IP address of the device.

You can also enable the secondary LAN IP address. The two LAN IP addresses must be in different networks.

Choose **Setup > Local Network**. The **Local Network** page shown in the following figure appears.

Wireless ADSL2/2+ Modem Router

Kozumi

Welcome admin, Logout

Setup Advanced Management Status Help

Setup

- Wizard
- Internet Setup
- Wireless
- Local Network**
- Time and Date
- Logout

LOCAL NETWORK

This section allows you to configure the local network settings of your router. Please note that this section is optional and you should not need to change any of the settings here to get your network up and running.

ROUTER SETTINGS

Use this section to configure the local network settings of your router. The Router IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Domain Name: kozumi.com

Configure the second IP Address and Subnet Mask for LAN

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

By default, **Enable DHCP Server** is selected for the Ethernet LAN interface of the device. DHCP service supplies IP settings to workstations configured to automatically obtain IP settings that are connected to the device through the Ethernet port. When the device is used for DHCP, it becomes the default gateway for DHCP client connected to it. If you change the IP address of the device, you must also change the range of IP addresses in the pool used for DHCP on the LAN. The IP address pool can contain up to 253 IP addresses.

DHCP SERVER SETTINGS (OPTIONAL)

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

Enable DHCP Server

DHCP IP Address Range: 192.168.1.2 to 192.168.1.254

DHCP Lease Time: 100 (seconds)

Apply Cancel

Click **Apply** to save the settings.

In the **Local Network** page, you can assign IP addresses on the LAN to specific individual computers based on their MAC addresses.

DHCP RESERVATIONS LIST

Status	Computer Name	MAC Address	IP Address
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

Click **Add** to add static DHCP (optional). The page shown in the following figure appears.

ADD DHCP RESERVATION (OPTIONAL)

Enable :

Computer Name :

IP Address :

MAC Address :

Select **Enable** to reserve the IP address for the designated PC with the configured MAC address.

The **Computer Name** helps you to recognize the PC with the MAC address. For example, Father's Laptop.

Click **Copy Your PC's MAC Address** to obtain the MAC address from the PC you are using.

Click **Apply** to save the settings.

After the DHCP reservation is saved, the DHCP reservations list displays the configuration.

If the DHCP reservations list table is not empty, you can select one or more items and click **Edit** or **Delete**.

The **NUMBER OF DYNAMIC DHCP CLIENTS** page shows the current DHCP clients (PC or Laptop) connected to the device and the detailed information of the connected computer (s).

NUMBER OF DYNAMIC DHCP CLIENTS : 1

Computer Name	MAC Address	IP Address	Expire Time
GD211H	00:1e:65:22:ee:2c	192.168.1.2	70

3.2.5 Time and Date

Choose **Setup > Time and Date**. The page shown in the following figure appears.

The screenshot shows the Kozumi router's configuration interface. The top navigation bar includes 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The left sidebar has 'Setup' selected, with sub-options for 'Wizard', 'Internet Setup', 'Wireless', 'Local Network', 'Time and Date', and 'Logout'. The main content area is titled 'TIME AND DATE' and contains the following elements:

- A descriptive paragraph: "The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From the section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed."
- A section titled 'TIME SETTINGS' with a checkbox for 'Automatically synchronize with Internet time servers' which is checked.
- Two text input fields for NTP servers: 'Set NTP time server:' and '2nd NTP time server:', both containing the IP address '192.168.2.10'.
- A section titled 'TIME CONFIGURATION' showing:
 - 'Current Local Time:' as '2009-01-01 00:11:02'.
 - 'Time Zone:' as a dropdown menu showing 'GMT+08:00 Beijing, Hong Kong'.
 - A checked checkbox for 'Enable Daylight Saving'.
 - Two rows of date pickers for 'Daylight Saving Start' and 'Daylight Saving End', each with fields for Year, Month, Day, Hour, Min, and Sec.
 - 'Apply' and 'Cancel' buttons at the bottom.

In the **Time and Date** page, you can configure, update, and maintain the correct time on the internal system clock. You can set the time zone that you are in and the network time protocol (NTP) server. You can also configure daylight saving to automatically adjust the time when needed.

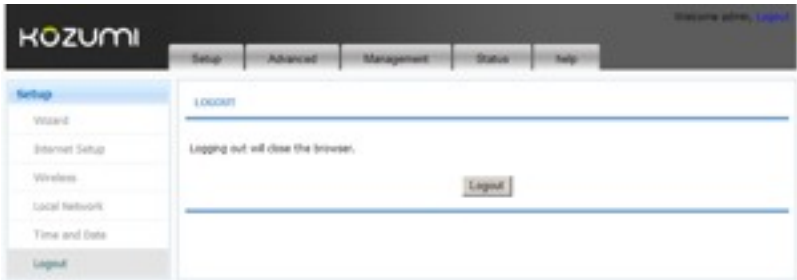
Select **Automatically synchronize with Internet time servers**. Select the specific time server and the time zone from the corresponding drop-down lists.

Select **Enable Daylight Saving** if necessary and set the daylight saving dates.

Click **Apply** to save the settings.

3.2.6 Logout

Choose **Setup > Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page.



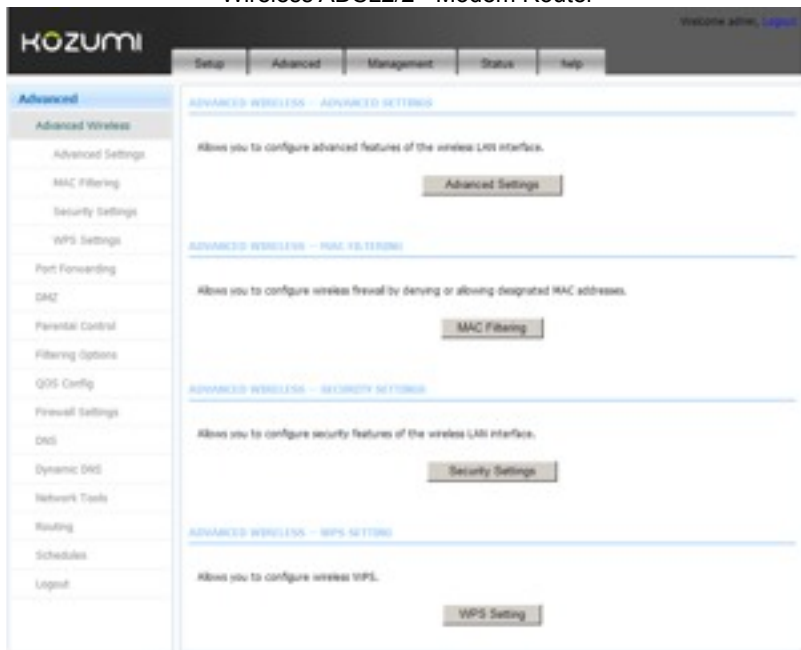
3.3 Advanced

This section includes advanced features used for network management, security and administrative tools to manage the device. You can view status and other information that are used to examine performance and troubleshoot.

3.3.1 Advanced Wireless

This function is used to modify the standard 802.11g wireless radio settings. It is recommend not to change the default settings, because incorrect settings may impair the performance of your wireless radio. The default settings provide the best wireless radio performance in most environments.

Choose **ADVANCED > Advanced Wireless**. The page shown in the following figure appears.



3.3.1.1 Advanced Settings

Select **Advanced Settings**. The page shown in the following figure appears.

Wireless ADSL/2+ Modem Router

The screenshot shows the Kozumi router's web interface. The top navigation bar includes 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The left sidebar lists various configuration options, with 'Advanced Wireless' selected. The main content area is titled 'ADVANCED SETTINGS' and contains a warning about changing default settings. Below this, the 'ADVANCED WIRELESS SETTINGS' section is visible, showing various parameters like Transmission Rate, Multicast Rate, Transmit Power, Beacon Period, RTS Threshold, Fragmentation Threshold, DTX Interval, and Fragmentation Type. The 'WLAN' section is partially visible at the bottom, showing 'Enable Wireless' checked, SSID 'Wlan_3', and other wireless-related options.

Kozumi Wireless ADSL/2+ Modem Router

Setup | **Advanced** | Management | Status | Help

Advanced

- Advanced Wireless
 - Advanced Settings**
 - MAC Filtering
 - Security Settings
 - WPS Settings
 - Port Forwarding
 - DNS
 - Parental Control
 - Filtering Options
 - QoS Config
 - Firewall Settings
 - DNS
 - Dynamic DNS
 - Network Tools
 - Routing
 - Schedules
 - Logout

ADVANCED SETTINGS

These options are for users that wish to change the behaviour of their 802.11g wireless radio from the standard setting. We does not recommend changing these settings from the factory default. Incorrect settings may impair the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.

ADVANCED WIRELESS SETTINGS

Transmission Rate: Auto
Multicast Rate: Lower
Transmit Power: 100%
Beacon Period: 100 (20 - 1024)
RTS Threshold: 2345 (0 - 2347)
Fragmentation Threshold: 2340 (256 - 2346)
DTX Interval: 100 (1 - 255)
Fragmentation Type: long

WLAN

Enable Wireless:
SSID: Wlan_3
Visibility Status: Visible Invisible
User Selection:
Disable WMM Admission:
Max Clients: 15 (0 - 32)

These settings are only for more technically advanced users who have sufficient knowledge about wireless LAN. Do not change these settings unless you know the effect of changes on the device.

Wireless ADSL2/2+ Modem Router

SSID-1

Enable Wireless Guest Network:

SSID:

Visibility Status: Visible Invisible

User Isolation:

Double WMM Advertise:

Max Clients: (0 - 32)

SSID-2

Enable Wireless Guest Network:

SSID:

Visibility Status: Visible Invisible

User Isolation:

Double WMM Advertise:

Max Clients: (0 - 32)

SSID-3

Enable Wireless Guest Network:

SSID:

Visibility Status: Visible Invisible

User Isolation:

Double WMM Advertise:

Max Clients: (0 - 32)

Click **Apply** to save the settings.

3.3.1.2 MAC Filtering

Select **MAC Filtering**. The page shown in the following figure appears.

Wireless ADSL2/2+ Modem Router

The screenshot shows the Kozumi router's web interface. The top navigation bar includes 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The left sidebar lists various settings categories, with 'Advanced Wireless' selected. The main content area is titled 'BLOCK MAC ADDRESS' and contains the following text:

Time of Day Restrictions – A maximum of 16 entries can be configured

This page adds a time of day restriction to a special LAN device connected to the router. The "Current PC" 's MAC Address automatically displays the MAC address of the LAN device where the browser is running. To restrict another LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows-based PC, open a command prompt window and type "ipconfig /all".

Below the text is a table with the following header:

Username	MAC	Schedule
----------	-----	----------

At the bottom of the table area are three buttons: 'Add', 'Edit', and 'Delete'.

Click **Add**. The page shown in the following figure appears.

The screenshot shows the 'ADD SCHEDULE RULE' configuration page. It contains the following fields and options:

- User Name:** [Text input field]
- Current PC 's MACAddress:** [Text input field with value: 00:22:BD:58:DE:69]
- Other MAC Address:** [Text input field]
- Schedule:** [Dropdown menu with 'Always' selected] [View Available Schedules](#)
- Manual Schedule:**
 - Day(s): All Week Select Day(s)
 - Days: Sun Mon Tue Wed Thu Fri Sat
 - All Day - 24 hrs:
 - Start Time: [Hour] : [Minute] (hour:minute, 24 hour time)
 - End Time: [Hour] : [Minute] (hour:minute, 24 hour time)

At the bottom are 'Apply' and 'Cancel' buttons.

Click **Apply** to save the settings.

3.3.1.3 Security Settings

Select **Security Settings**. The page shown in the following figure appears.



Select the SSID that you want to configure from the drop-down list.

Select the encryption type from the **Security Mode** drop-down list. You can select **None**, **WEP**, **AUTO (WPA or WPA2)**, **WPA Only**, or **WPA2 Only**.

If you select **WEP**, the page shown in the following figure appears.

Wireless ADSL2/2+ Modem Router

WEP

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**.

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length:

Choose WEP Key:

WEP Key1:

WEP Key2:

WEP Key3:

WEP Key4:

Authentication:

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

If you select **AUTO (WPA or WPA2)**, **WPA Only**, or **WPA2 Only**, the page shown in the following figure appears.

Wireless ADSL2/2+ Modem Router

WPA

Use **WPA** or **WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(128) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode :

Group Key Update Interval :

PRE-SHARED KEY

Pre-Shared Key :

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Click **Apply** to save the settings.

3.3.1.4 WPS Settings

Select **WPS Setting**. The page shown in the following figure appears.



- **Enabled:** The WPS service is enabled by default.

Note:

Ensure that the network card supports the WPS function.

You can use one of the following three methods to use WPS authentication:

- Press the **WPS** button on the side panel for 3 seconds.
- In the **WIRELESS WPS** page, click PBC. It has the same function of the **WPS** button on the side panel. This is an optional method on wireless clients.

Note:

You need a Registrar when using the PBC method in a special case in which the PIN is all zeros.

- In the **WIRELESS WPS** page, enter the **PIN** code provided by the station and click **PIN**. PIN entry is a

Wireless ADSL2/2+ Modem Router
mandatory method of setup for all WPS certified devices.

Note:

If you are using the PIN method, you need a Registrar, either an access point or a wireless router, to initiate the registration between a new device and an active access point or a wireless router.

3.3.2 Port Forwarding

This function is used to open ports in your device and re-direct data through those ports to a single PC on your network (WAN-to-LAN traffic). It allows remote users to access services on your LAN, such as FTP for file transfers or SMTP and POP3 for e-mail. The device accepts remote requests for these services at your global IP address. It uses the specified TCP or UDP protocol and port number, and redirects these requests to the server on your LAN with the LAN IP address you specify. Note that the specified private IP address must be within the available range of the subnet where the device is in. Choose **ADVANCED > Port Forwarding**. The page shown in the following figure appears.

The screenshot shows the Kozumi router's web interface. The top navigation bar includes 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The left sidebar is titled 'Advanced' and lists various settings: Advanced Wireless, Port Forwarding (selected), DNS, Firewall Control, Filtering Options, QoS Config, Firewall Settings, DNS, Dynamic DNS, Network Tools, Routing, Schedules, and Logout. The main content area is titled 'PORT FORWARDING' and contains the following text: 'Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port) to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.' Below this text is a section titled 'PORT FORWARDING LIST' which contains a table with the following columns: Server Name, External Port Start, External Port End, Protocol, Internal Port Start, Internal Port End, Server IP Address, Schedule, and Remote IP. At the bottom of the table are three buttons: 'Add', 'Edit', and 'Delete'.

Click **Add** to add a virtual server.

Wireless ADSL2/2+ Modem Router

PORT FORWARDING SETUP

Remaining number of entries that can be configured: 32

WAN Connection(s)

Server Name:

Select a Service:

Custom Server:

Schedule: [View Available Schedules](#)

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remote Ip
<input type="text"/>	<input type="text"/>	<input type="button" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="button" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Select a service for a preset application, or enter a name in the **Custom Server** field.

Enter an IP address in the **Server IP Address** field, to appoint the corresponding PC to receive forwarded packets.

The Ports show the ports that you want to open on the device.

The **TCP/UDP** means the protocol type of the opened ports.

Click **Apply** to save the settings. The page shown in the following figure appears. A virtual server is added.

The screenshot shows the Kozumi web interface for a Wireless ADSL/2+ Modem Router. The 'Advanced' tab is selected, and the 'Port Forwarding' sub-tab is active. The page title is 'PORT FORWARDING'. Below the title, there is a descriptive paragraph: 'Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port) to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.' Below this is a note: 'Select the service name, and enter the server IP address and click "Apply" to forward IP packets for the service to the specified server. Note: Modifying the Internal Port Start or Internal Port End is not recommended. If the External Port Start or the External Port End changes, the Internal Port Start or Internal Port End automatically changes accordingly.'

Below the text is a table titled 'PORT FORWARDING SETUP'. The table has the following columns: Server Name, External Port Start, External Port End, Protocol, Internal Port Start, Internal Port End, Server IP Address, Schedule, and Remote IP. There is one entry in the table with the following values: Server Name: 'HTTP', External Port Start: '80', External Port End: '80', Protocol: 'tcp', Internal Port Start: '103', Internal Port End: '103', Server IP Address: '192.168.1.29', Schedule: 'Always', and Remote IP: (empty). Below the table are three buttons: 'Add', 'Edit', and 'Delete'.

3.3.3 DMZ

Since some applications are not compatible with NAT, the device supports the use of a DMZ IP address for a single host on the LAN. This IP address is not protected by NAT and it is visible to agents on the Internet with the correct type of software. Note that any client PC in the DMZ is exposed to various types of security risks. If you use the DMZ, take measures (such as client-based virus protection) to protect the remaining client PCs on your LAN from possible contamination through DMZ.

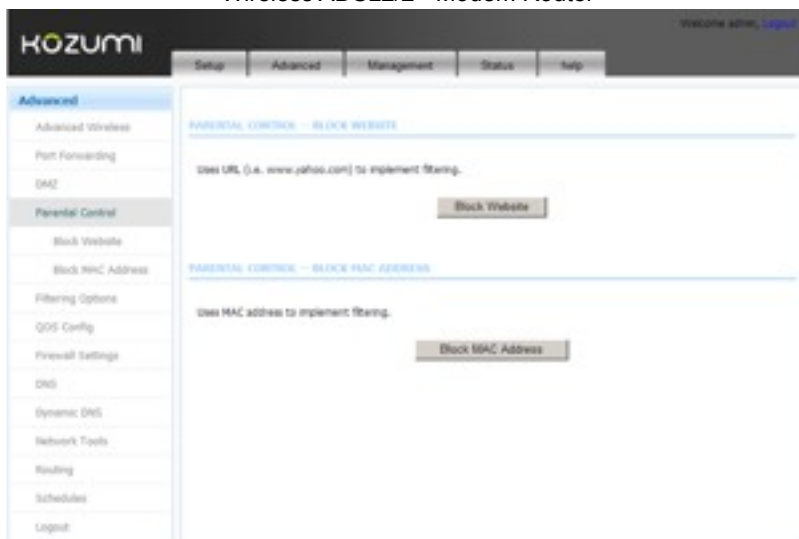
Choose **ADVANCED > DMZ**. The page shown in the following figure appears.



Click **Apply** to save the settings.

3.3.4 Parental Control

Choose **ADVANCED > Parental Control**. The **Parent Control** page shown in the following figure appears.



This page provides two useful tools for restricting the Internet access. **Block Websites** allows you to quickly create a list of all websites that you wish to stop users from accessing. **Block MAC Address** allows you to control when clients or PCs connected to the device are allowed to access the Internet.

3.3.4.1 Block Website

In the **Parent Control** page, click **Block Website**. The page shown in the following figure appears.

Wireless ADSL2/2+ Modem Router

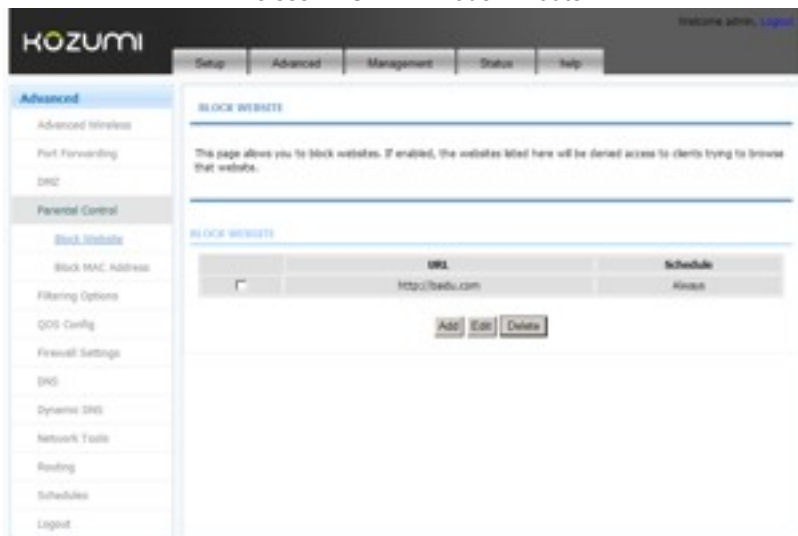
The screenshot shows the Kozumi router's web interface. The top navigation bar includes 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The left sidebar lists various configuration options, with 'Block Website' selected. The main content area is titled 'BLOCK WEBSITE' and contains a descriptive paragraph: 'This page allows you to block websites. If enabled, the websites listed here will be denied access to clients trying to browse that website.' Below the text is a table with two columns: 'URL' and 'Schedule'. At the bottom of the table are three buttons: 'Add', 'Edit', and 'Delete'.

Click **Add**. The page shown in the following page appears.

The screenshot shows the 'ADD SCHEDULE RULE' configuration page. It features a 'URL' field with 'http://' entered. Below it is a 'Schedule' dropdown menu set to 'Always', with a link to 'View Available Schedules'. There is also a 'Manual Schedule' section with radio buttons for 'All Week' and 'Select Day(s)'. Under 'Select Day(s)', there are checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat. An 'All Day - 24 hrs:' checkbox is also present. At the bottom, there are 'Start Time' and 'End Time' fields, each with a dropdown for hours and minutes, and a label '(hour:minute, 24 hour time)'. 'Apply' and 'Cancel' buttons are at the bottom.

Enter the website in the **URL** field. Select the **Schedule** from drop-down list, or select **Manual Schedule** and select the corresponding time and days.

Click **Apply** to add the website to the **BLOCK WEBSITE Table**. The page shown in the following figure appears.



3.3.4.2 Block MAC Address

In the **Parent Control** page, click **Block MAC Address**. The page shown in the following figure appears.

Wireless ADSL2/2+ Modem Router

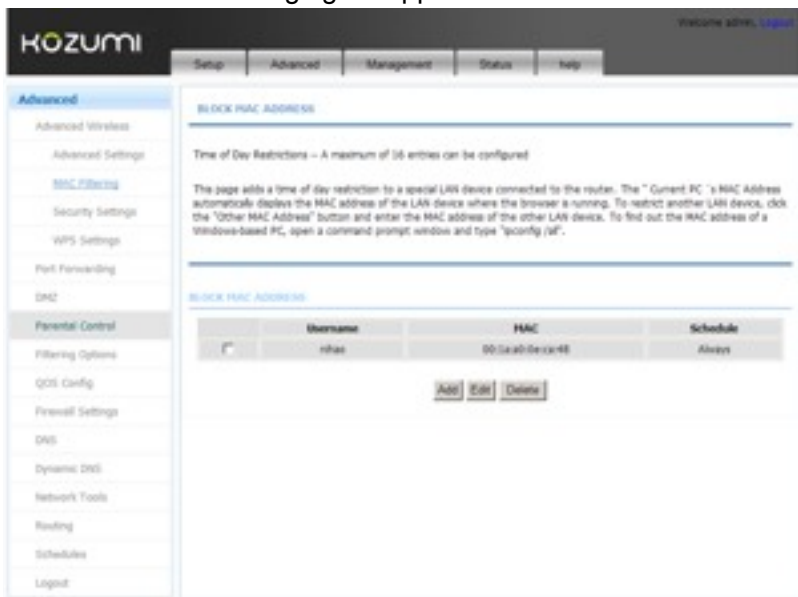
The screenshot shows the Kozumi router's web interface. The top navigation bar includes 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The 'Advanced' tab is selected, and the 'BLOCK MAC ADDRESS' section is active. The page title is 'BLOCK MAC ADDRESS'. Below the title, there is a sub-section 'Time of Day Restrictions - A maximum of 24 entries can be configured'. A paragraph explains that this page allows adding time-of-day restrictions to a LAN device. It notes that the 'Current PC's MAC Address' is automatically displayed, and to restrict another LAN device, the user should click the 'Other MAC Address' button and enter the MAC address of the other LAN device. To find the MAC address of a Windows-based PC, the user is instructed to open a command prompt and type 'ipconfig /all'. Below this text is a table with three columns: 'Username', 'MAC', and 'Schedule'. The table is currently empty. Below the table are three buttons: 'Add', 'Edit', and 'Delete'.

Click **Add**. The page shown in the following figure appears.

The screenshot shows the 'ADD SCHEDULE RULE' configuration page. It contains several input fields and options: 'User Name:' with an empty text box; 'Current PC's MACAddress:' with the value '00:22:80:68:DE:69'; 'Other MAC Address:' with an empty text box; 'Schedule:' with a dropdown menu set to 'Always' and a link 'View Available Schedules'; 'Manual Schedule:' with a radio button selected; 'Day(s):' with radio buttons for 'All Week' (selected) and 'Select Day(s)', and checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat; 'All Day - 24 hrs:' with a checked checkbox; 'Start Time:' and 'End Time:' with time selection boxes and '(hour:minute, 24 hour time)' labels; and 'Apply' and 'Cancel' buttons at the bottom.

Enter the use name and MAC address and select the corresponding time and days. Click **Apply** to add the MAC

Wireless ADSL2/2+ Modem Router
address to the **BLOCK MAC ADDRESS** Table. The page shown in the following figure appears.



3.3.5 Filtering Options

Choose **ADVANCED > Filtering Options**. The **Filtering Options** page shown in the following figure appears.



3.3.5.1 Inbound IP Filtering

By default, all incoming IP traffic that does not originate from the internal network is blocked when the firewall is enabled. Normal outgoing Internet requests created by web browsing, email and other software you run, work as usual as the requests originated from your internal network. The inbound filter allows you to create a filter rule to allow incoming IP traffic by specifying a filter name and you need to select at least one condition.

In the **Filtering Options** page, click **Inbound IP Filtering**. The page shown in the following figure appears.

Wireless ADSL2/2+ Modem Router

The screenshot shows the Kozumi web interface for a Wireless ADSL2/2+ Modem Router. The top navigation bar includes 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The left sidebar lists various configuration options, with 'Advanced' selected and 'Inbound IP Filtering' highlighted. The main content area is titled 'INBOUND IP FILTERING' and contains the following text:

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below.

Packets matched the rule will be discarded.

Below this text is a table with the following columns: Name, WFL/WCE, Protocol, Source Address, Source Port, Dest. Address, Dest. Port, and Schedule Rule. The table is currently empty. At the bottom of the table area are three buttons: 'Add', 'Edit', and 'Delete'.

Click **Add** to add an inbound IP filter. The page shown in the following figure appears.

INCOMING IP FILTERING

Filter Name :

Protocol : Any ▾

Source IP Type : Any ▾

Source IP Address :

Source Subnet Mask :

Source Port Type : Any ▾

Source Port : (port or port/port)

Destination IP Type : Any ▾

Destination IP Address :

Destination Subnet Mask :

Destination Port Type : Any ▾

Destination Port : (port or port/port)

Schedule : Always ▾ [View Available Schedules](#)

WAN Interfaces (Configured in Routing mode and with firewall enabled only)

WWAN Interfaces :

Enter the **Filter Name** and specify at least one of the following criteria: protocol, source/destination IP address, subnet mask, and source/destination port.

Click **Apply** to save the settings.

Note:

The settings only apply when the firewall is enabled.

The **ACTIVE INBOUND FILTER** shows detailed information about each created inbound IP filter. Click **Remove** to remove an IP filter (only appears when an IP filter exists).

3.3.5.2 Outbound IP Filtering

By default, all outgoing IP traffic from the LAN is allowed. The outbound filter allows you to create a filter rule to block outgoing IP traffic by specifying a filter name and at least one condition.

Wireless ADSL2/2+ Modem Router

In the **Filtering Options** page, click **Outbound IP Filtering**. The page shown in the following figure appears.



Click **Add** to add an outbound IP filter. The page shown in the following figure appears.

OUTGOING IP FILTERING

Filter Name :

Protocol: Any ▾

Source IP Type : Any ▾

Source IP Address :

Source Subnet Mask :

Source Port Type : Any ▾

Source Port : (port or port:port)

Destination IP Type: Any ▾

Destination IP Address :

Destination Subnet Mask :

Destination Port Type : Any ▾

Destination Port : (port or port:port)

Schedule : Always ▾ [View Available Schedules](#)

Enter the **Filter Name** and specify at least one of the following criteria: protocol, source/destination IP address, subnet mask, and source/destination port. Click **Apply** to save the settings.

The **ACTIVE OUTBOUND IP FILTER** shows detailed information about each created outbound IP filter. Click **Remove** to remove an IP filter (only appears when an IP filter exists).

3.3.5.3 Bridge Filtering

In the **Filtering Options** page, click **Bridge Filtering**. The page shown in the following figure appears. This page is used to configure bridge parameters. In this page, you can change the settings or view some information of the bridge and its attached ports.

Advanced

- Advanced Wireless
- Port Forwarding
- DNS
- Parental Control
- Filtering Options**
 - Inbound IP Filtering
 - Outbound IP Filtering
 - Bridge Filtering**
 - QoS Config
 - Firewall Settings
 - DNS
 - Dynamic DNS
 - Network Tools
 - Routing
 - Schedules
 - Logout

BRIDGE FILTER

Bridge Filtering is only effective on ATR-PVDS configured in Bridge mode. ALLOW means that all MAC layer frames will be ALLOWED except those matching with any of the specified rules in the following table. DENY means that all MAC layer frames will be DENIED except those matching with any of the specified rules in the following table.

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

WARNING : Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Bridge Filtering Global Policy:

ALLOW all packets but DENY those matching any of specific rules listed.

DENY all packets but ALLOW those matching any of specific rules listed.

Apply Cancel

DISPLAY LIST

VPI/VCI	protocol	DMAC	SMAC	DIR	TIME
Add Edit Delete					

Click **Add** to add a bridge filter. The page shown in the following figure appears.

ADD BRIDGE FILTER

Protocol Type :

Destination MAC Address :

Source MAC Address :

Frame Direction:

Time schedule: [View Available Schedules](#)

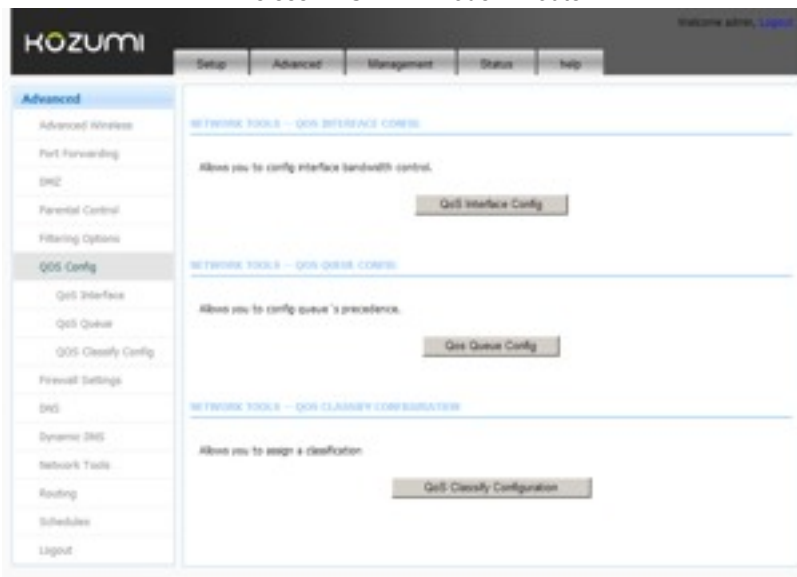
WWan interface:

Apply Cancel

Click **Apply** to save the settings.

3.3.6 QoS Config

Choose **ADVANCED > QoS Config**. The **QoS Config** page shown in the following figure appears.



3.3.6.1 QoS Interface Config

Choose **ADVANCED** > **QoS Config** and click **QoS Interface Config**. The page shown in the following figure appears.



In this table, you could config each interface with up stream bandwidth and down stream bandwidth. When configed, the stream rate will be limited to that rate.

QOS INTERFACE CONFIG

Interface :

Enable :

Up Stream : (Kbps)

Down Stream : (Kbps)

Click **Apply** to save the settings.

3.3.6.2 QoS Queue Config

This page will help you to config priority queue, only three priority are support now, high, medium, low, the high queue will transport all packet cache in its buf, and then medium, and then low.

Choose **ADVANCED > QoS Config** and click **QoS Queue Config**. The page shown in the following figure appears.

QOS QUEUE CONFIG

This is queue precedence configuration, the packets with high precedence will pass before medium and low precedence.

LISTS

Queue Name	Queue Priority	State
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>		

Click **Add**. The page shown in the following figure appears.

QOS QUEUE CONFIG

Queue Enable:

Queue Priority:

Associated Interface:

Click **Apply** to save the settings.

3.3.6.3 QoS Classify Configuration

This page allows you to config various classification, the classification include two class, the one is L1&L2, the other is L3&L4. you could assign classification to a queue, make dscp, or mark 802.1p.

QoS CLASSIFY CONFIGURATION

This page allows you to assign a classification, the classification may assign to a queue that you can limit the bandwidth or assign precedence, the classification can also be marked such as 802.1p, dscp.

LIST

Classification Result					
Class Name	Associated Queue	DSCP Mark	802.1P Mark	state	Details
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>					

Click **Add**. The page shown in the following figure appears.

QoS CLASSIFY CONFIGURATION

Traffic Class Name :

Enable Classification :

SPECIFY TRAFFIC CLASSIFICATION RULES

Classification Type : L1&L2 ▾

Physical Lan Port : any ▾

Source MAC Address :

Source MAC Mask :

Destination MAC Address :

Destination MAC Mask :

Ethernet Type : Any ▾

802.1p Priority : no match ▾

SPECIFY TRAFFIC CLASSIFICATION RESULT

Assign Classification Queue : no assign ▾

Mark DSCP : no assign ▾

Mark 802.1p Priority : no assign ▾

3.3.7 Firewall Settings

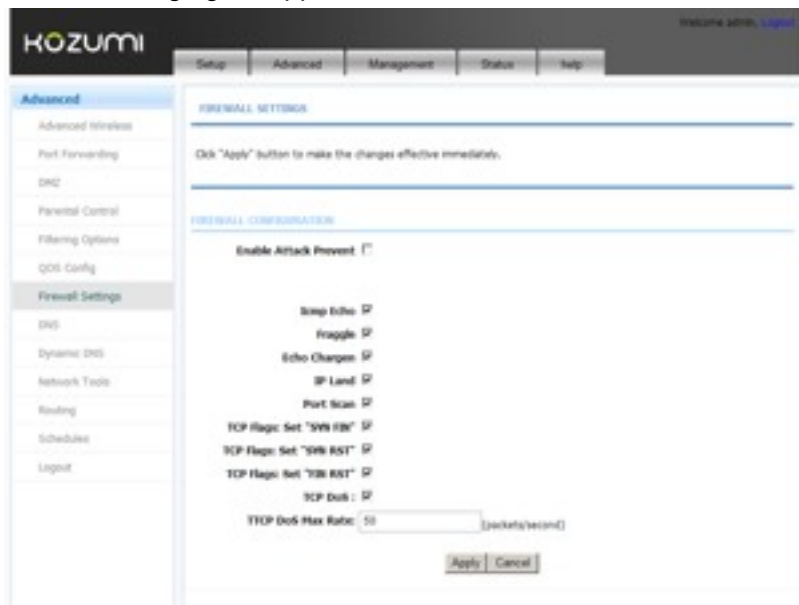
A denial-of-service (DoS) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include the following

- The attackers attempt to flood a network, thereby preventing legitimate network traffic
- The attackers attempt to disrupt connections between two machines, thereby preventing access to a service
- The attackers attempt to prevent a particular individual from accessing a service
- The attackers attempt to disrupt service to a specific system or person.

Wireless ADSL2/2+ Modem Router

Port scan protection is designed to block attempts to discover vulnerable ports or services that might be exploited in an attack from the WAN.

Choose **ADVANCED > Firewall Settings**. The page shown in the following figure appears.



Click **Apply** to save the settings.

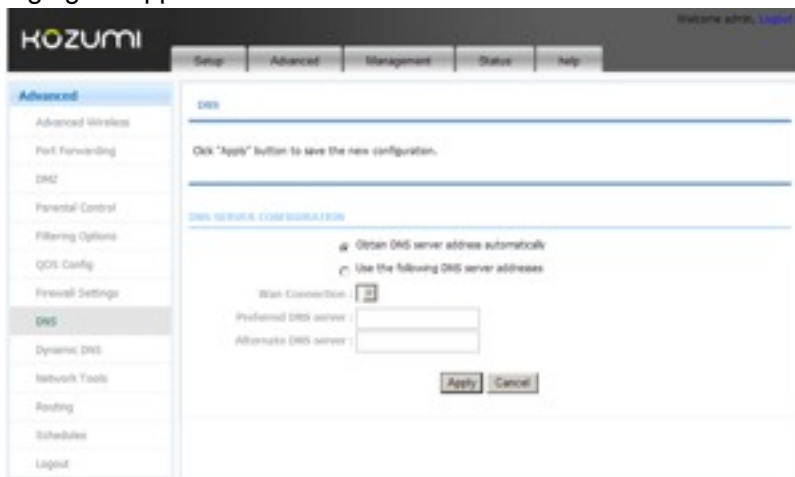
3.3.8 DNS

Domain name system (DNS) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. The Internet, however, is actually based on IP addresses. Each time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name `www.example.com` might be translated to `198.105.232.4`.

Wireless ADSL2/2+ Modem Router

The DNS system is, in fact, its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Choose **ADVANCED > DNS**. The page shown in the following figure appears.



DNS SERVER CONFIGURATION

If you are using the device for DHCP service on the LAN or if you are using DNS servers on the ISP network, select **Obtain DNS server address automatically**.

If you have DNS IP addresses provided by your ISP, enter these IP addresses in the available entry fields for the preferred DNS server and the alternate DNS server.

Click **Apply** to save the settings.

3.3.9 Dynamic DNS

The device supports dynamic domain name service (DDNS). The dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, and allows access to a specified host from various

Wireless ADSL2/2+ Modem Router

locations on the Internet. Click a hyperlinked URL in the form of hostname.dyndns.org and allow remote access to a host. Many ISPs assign public IP addresses using DHCP, so locating a specific host on the LAN using the standard DNS is difficult. For example, if you are running a public web server or VPN server on your LAN, DDNS ensures that the host can be located from the Internet even if the public IP address changes. DDNS requires that an account be set up with one of the supported DDNS service providers (DynDNS.org or TZO or GnuDIP).

Choose **ADVANCED > Dynamic DNS**. The page shown in the following page appears.



Click **Add** to add dynamic DNS. If **DDNS provider** is DynDNS.org, the page shown in the following figure appears.

Wireless ADSL2/2+ Modem Router

The screenshot shows a web form titled "ADD DYNAMIC DNS". The "DDNS provider:" dropdown menu is set to "DynDNS.org". Below it are four input fields: "Hostname:", "Interface:" (a dropdown menu), "Username:", and "Password:". At the bottom right of the form are two buttons: "Apply" and "Cancel".

- **Host Name:** Enter the host name that you registered with DynDns.org.
- **Interface:** Select one of the Wan connection from the down-list drop.
- **Username:** Enter the user name for your DDNS account.
- **Password:** Enter the password for your DDNS account.

If **DDNS provider** is TZO, the page shown in the following figure appears.

The screenshot shows a web form titled "ADD DYNAMIC DNS". The "DDNS provider:" dropdown menu is set to "TZO". Below it are four input fields: "Hostname:", "Interface:" (a dropdown menu), "Email:", and "Key:". At the bottom right of the form are two buttons: "Apply" and "Cancel".

- **Host Name:** Enter the host name that you registered with TZO.
- **Interface:** Select one of the Wan connection from the down-list drop.
- **Email:** Enter the email address that registered with TZO.
- **Key:** Enter the email key that registered with TZO.

If **DDNS provider** is GnuDIP, the page shown in the following figure appears.

ADD DYNAMIC DNS

DDNS provider: GnuDIP

Hostname:

Interface:

DDNS Server:

Username:

Password:

Apply Cancel

- **Host Name:** Enter the host name that you registered with GnuDIP.
- **Interface:** Select one of the Wan connection from the down-list drop.
- **DDNS Server** Enter the IP address of DDNS server.
- **Username:** Enter the user name for your DDNS account.
- **Password:** Enter the password for your DDNS account.

Click **Apply** to save the settings.

3.3.10 Network Tools

Choose **ADVANCED > Network Tools**. The page shown in the following figure appears.

Wireless ADSL2/2+ Modem Router

The screenshot displays the configuration interface for a Kozumi Wireless ADSL2/2+ Modem Router. The top navigation bar includes 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The 'Advanced' section is active, and the 'Network Tools' menu item is selected in the left sidebar. The main content area lists several network tools, each with a brief description and a corresponding button:

- PORT MAPPING**: Port Mapping supports multiple port to IP and bridging groups. Each group will perform as an independent network. Button: [Port Mapping](#)
- DMZ PROXY**: Transmission of identical content, such as multimedia, from a source to a number of recipients. Button: [DMZ Proxy](#)
- DMZ SNOOPING**: Transmission of identical content, such as multimedia, from a source to a number of recipients. Button: [DMZ Snooping](#)
- DMZ**: Allow you to enable or disable DMZ. Button: [DMZ](#)
- ACL**: Allow you to configure advanced settings for ACL. Button: [ACL](#)
- DMZ**: Network Tools - DMZ. Button: [DMZ](#)
- TR-069**: Allow you to configure TR-069 protocol. Button: [TR-069](#)
- CERTIFICATES**: Allow you to manage certificates used with TR-069. Button: [Certificates](#)
- PROFILES**: Allow you to manage profile. Button: [Profiles](#)

3.3.10.1 Port Mapping

Choose **ADVANCED** > **Network Tools** and click **Port Mapping**. The page shown in the following figure appears. In this page, you can bind the WAN interface and the LAN interface to the same group.

PORT MAPPING

Port Mapping - A maximum 5 entries can be configured

Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and VLAN interfaces using the "Add" button. The "Delete" button will remove the grouping and add the ungrouped interfaces to the Default group.

PORT MAPPING SETUP

Group Name	Interfaces
<input type="checkbox"/> lan1	ethernet1, ethernet2, ethernet3, ethernet4, wan0, wan0-vap0, wan0-vap1, ...

Click **Add** to add port mapping. The page shown in the following figure appears.

Wireless ADSL2/2+ Modem Router

ADD PORT MAPPING

To create a new mapping group:

1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
2. Click "Apply" button to make the changes effective immediately.

PORT MAPPING CONFIGURATION

Group Name:

Grouped Interfaces

Available Interfaces

- ethernet1
- ethernet2
- ethernet3
- ethernet4
- wlan0
- wlan0-vap0
- wlan0-vap1
- wlan0-vap2

Apply Cancel

The procedure for creating a mapping group is as follows:

Step 13 Enter the group name.

Step 14 Select interfaces from the **Available Interface** list and click the <- arrow button to add them to the grouped interface list, in order to create the required mapping of the ports. The group name must be unique.

Step 15 Click **Apply** to save the settings.

3.3.10.2 IGMP Proxy

Choose **ADVANCED > Network Tools** and click **IGMP Proxy**. The page shown in the following figure appears.

IGMP PROXY

IGMP proxy enables the system to issue IGMP host messages on behalf of

IGMP PROXY CONFIGURATION

Enable IGMP Proxy

WAN Connection :

LAN Connection :

Apply Cancel

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts after you enable it.

Click **Apply** to save the settings.

3.3.10.3 IGMP Snooping

Choose **ADVANCED** > **Network Tools** and click **IGMP Snooping**. The page shown in the following figure appears.

IGMP

Transmission of identical content, such as multimedia, from a source to a number of recipients.

IGMP SETUP

Enable IGMP Snooping

Apply Cancel

3.3.10.4 UPnP

Choose **ADVANCED** > **Network Tools** and click **UPnP**. The page shown in the following figure appears.

Wireless ADSL2/2+ Modem Router

UPnP

Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.

UPnP SETUP

Enable UPnP

WAN Connection:

LAN Connection:

Apply Cancel

In this page, you can configure universal plug and play (UPnP). The system acts as a daemon after you enable UPnP. UPnP is used for popular audio visual software. It allows automatic discovery of your device in the network. If you are concerned about UPnP security, you can disable it. Block ICMP ping should be enabled so that the device does not respond to malicious Internet requests.

Click **Apply** to save the settings.

3.3.10.5 ADSL Settings

Choose **ADVANCED > Network Tools** and click **ADSL**. The page shown in the following figure appears.

ADSL SETTINGS

The page is used to configure the ADSL settings of your ADSL router.

ADSL SETTINGS

- G.Dmt Enabled
- G.Lite Enabled
- T1.413 Enabled
- ADSL2 Enabled
- AnnexL Enabled
- ADSL2+ Enabled
- AnnexM Enabled

Capability

- Bitswap Enable
- SRA Enable

In this page, you can select the DSL modulation. Normally, you can remain this factory default setting. The device supports the following modulations: G.lite, G.Dmt, T1.413, ADSL2, ADSL2+, AnnexL, and AnnexM. The device negotiates the modulation mode with DSLAM.

Click **Apply** to save the settings.

3.3.10.6 SNMP

Choose **ADVANCED > Network Tools** and click **SNMP**. The page shown in the following figure appears. In this page, you can set SNMP parameters.

SNMP CONFIGURATION

This page is used to configure the SNMP protocol.

SNMP CONFIGURATION

Enable SNMP Agent

Read Community: public

Set Community: private

Trap Manager IP:

Trap Manager IP: public

Trap Version: v2c

Apply Cancel

- **Read Community:** The network administrator must use this password to read the information of this device.
- **Set Community:** The network administrator must use this password to configure the information of this device.
- **Trap Manager IP:** The trap information is sent to this host.

Click **Apply** to save the settings.

3.3.10.7 TR069

Choose **ADVANCED** > **Network Tools** and click **TR069**. The page shown in the following figure appears. In this page, you can configure the TR069 CPE.

Wireless ADSL2/2+ Modem Router

TR-069

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration. Select the desired values and click "Apply" to configure the TR-069 client options.

TR-069 CLIENT - CONFIGURATION

Inform: Disabled Enabled

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

Connection Request: Authentication

Click **Apply** to save settings.

3.3.10.8 Certificates

Choose **ADVANCED > Network Tools** and click **Certificates**. The **Certificates** page shown in the following figure appears.

CERTIFICATES - TRUSTED CA

Trusted CA certificates are used by you to verify peers' certificates.

In the **Certificates** page, click **Trused CA**. page shown in the following figure appears.

Wireless ADSL2/2+ Modem Router

CERTIFICATES -- TRUSTED CA

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Only one certificate can be stored. Notice you have to synchronize your time when use certificate

TRUSTED-CA (CERTIFICATE AUTHORITY) CERTIFICATES

Name	Subject	Type	Action
------	---------	------	--------

Click **Input Certificate**. The page shown in the following figure appears.

IMPORT CA CERTIFICATE

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----
<Import CA certificate Here>
-----END CERTIFICATE-----
```

- **Certificate Name:** Enter certificate name.
- **Certificate:** Enter certificate's content.

Click **Apply** to save the settings.

3.3.10.9 Printer

This page allows you to config network printer, if you have an USB interface.

DISPLAY LIST

This page allows you to enable/disable printer support.

Enable

Printer Name:

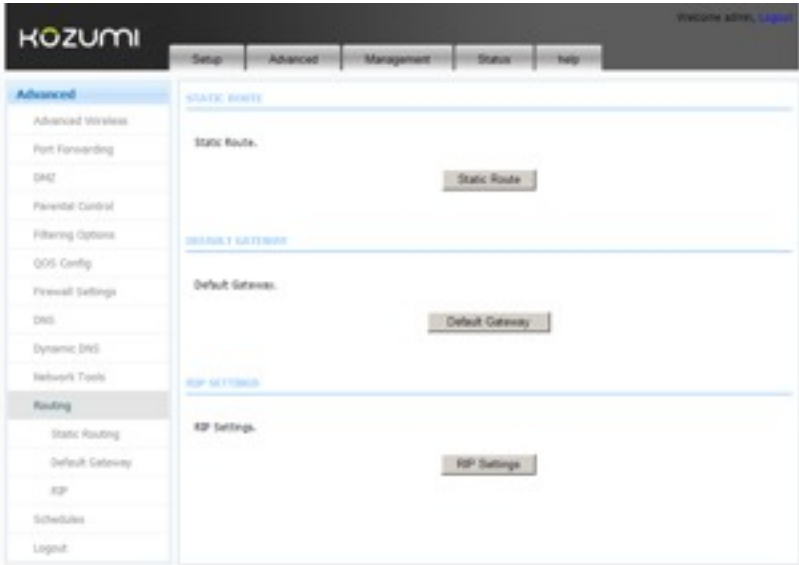
URL:

DISPLAY LIST

Manufacturer	Model	CMD	Firmware Version
--------------	-------	-----	------------------

3.3.11 Routing

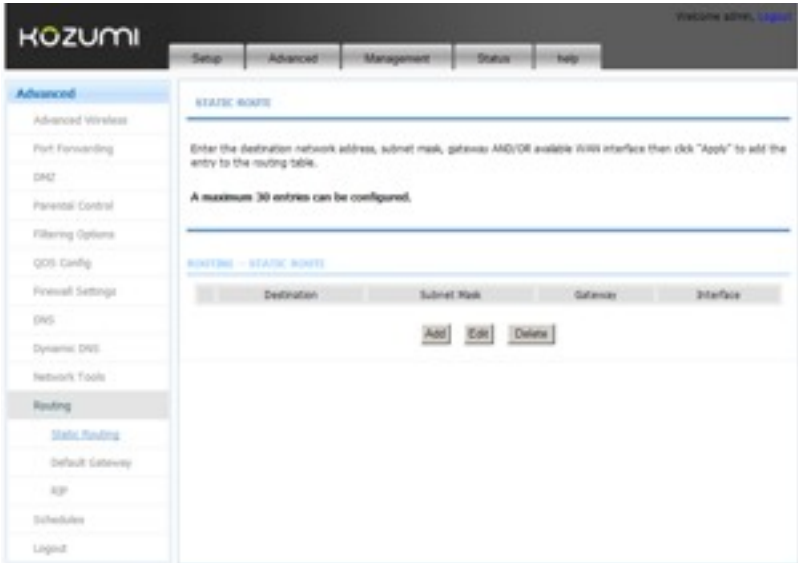
Choose **ADVANCED** > **Routing**. The page shown in the following page appears.



3.3.11.1 Static Route

Choose **ADVANCED** > **Routing** and click **Static Route**. The page shown in the following figure appears. This page is used to configure the routing information. In this page, you can add or delete IP routes.

Wireless ADSL2/2+ Modem Router



Click **Add** to add a static route. The page shown in the following figure appears.

The screenshot shows the 'STATIC ROUTES ADD' form. It contains four input fields: 'Destination Network Address', 'Subnet Mask', 'Use Gateway IP Address', and 'Use Interface'. The 'Use Interface' dropdown menu is set to 'LAN Group1'. 'Apply' and 'Cancel' buttons are at the bottom.

- **Destination Network Address:** The destination IP address of the router.
- **Subnet Mask:** The subnet mask of the destination IP address.
- **Use Gateway IP Address:** The gateway IP address of the router.
- **User Interface:** The interface name of the router output port.

You can only choose **Use Gateway IP Address** or **User Interface**.

Click **Apply** to save the settings.

3.3.11.2 Default Gateway

Choose **ADVANCED > Routing** and click **Default Gateway**. The page shown in the following figure appears.



Click **Apply** to save the settings.

3.3.11.3 RIP Settings

Choose **ADVANCED > Routing** and click **RIP Settings**. The page shown in the following figure appears. This page is used to select the interfaces on your device that use RIP and the version of the protocol used.

The screenshot shows the Kozumi web interface. The top navigation bar includes 'Setup', 'Advanced', 'Management', 'Status', and 'help'. The left sidebar lists various settings categories: Advanced Wireless, Port Forwarding, DMZ, Parental Control, Filtering Options, QoS Config, Firewall Settings, DNS, Dynamic DNS, Network Tools, Routing (highlighted), Static Routing, Default Gateway, RIP (highlighted), Schedules, and Logout. The main content area is titled 'RIP CONFIGURATION' and contains the following text:

To activate RIP for the device, select the "Enabled" checkbox for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the "Enabled" checkbox for the interface. Click the "Apply" button to save the configuration, and to start or stop RIP based on the Global RIP Mode selected.

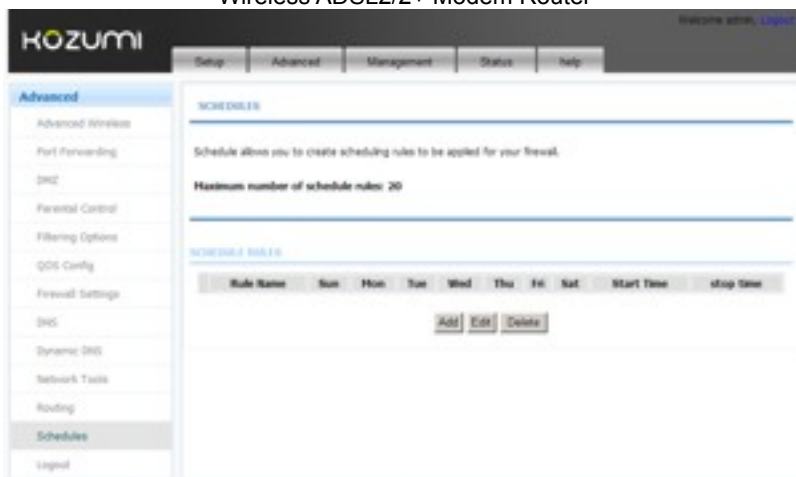
Below the text is a table for configuring RIP on individual interfaces:

Interface	VRF/VCI	Version	Operation	Enabled
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

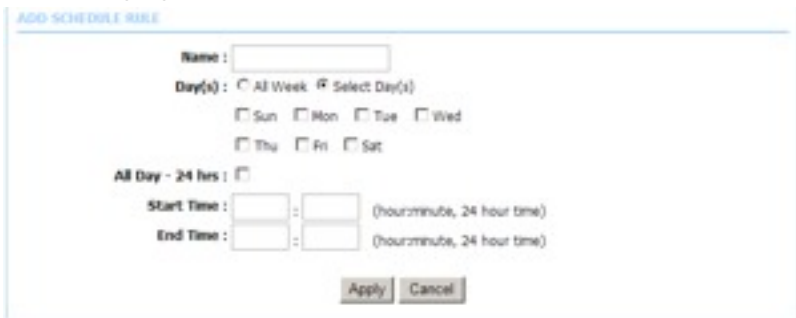
If you are using this device as a RIP-enabled device to communicate with others using the routing information protocol, enable RIP and click **Apply** to save the settings.

3.3.12 Schedules

Choose **ADVANCED** > **Schedules**. The page shown in the following figure appears.



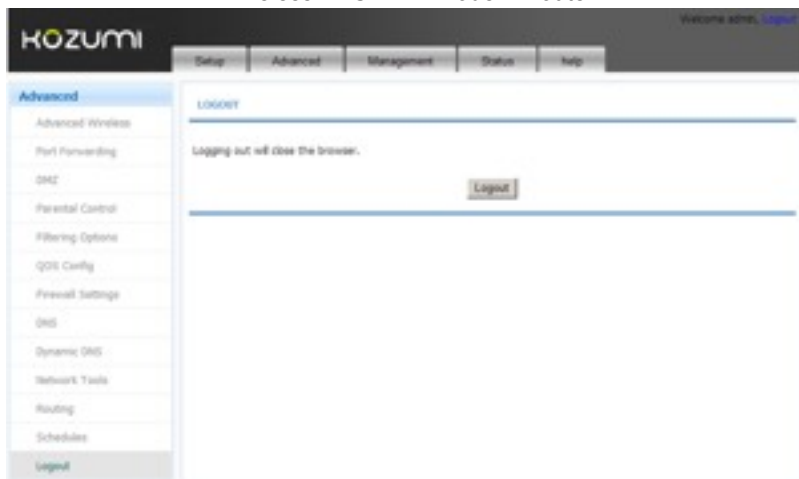
Click **Add** to add schedule rule. The page shown in the following figure appears.



Click **Apply** to save the settings.

3.3.13 Logout

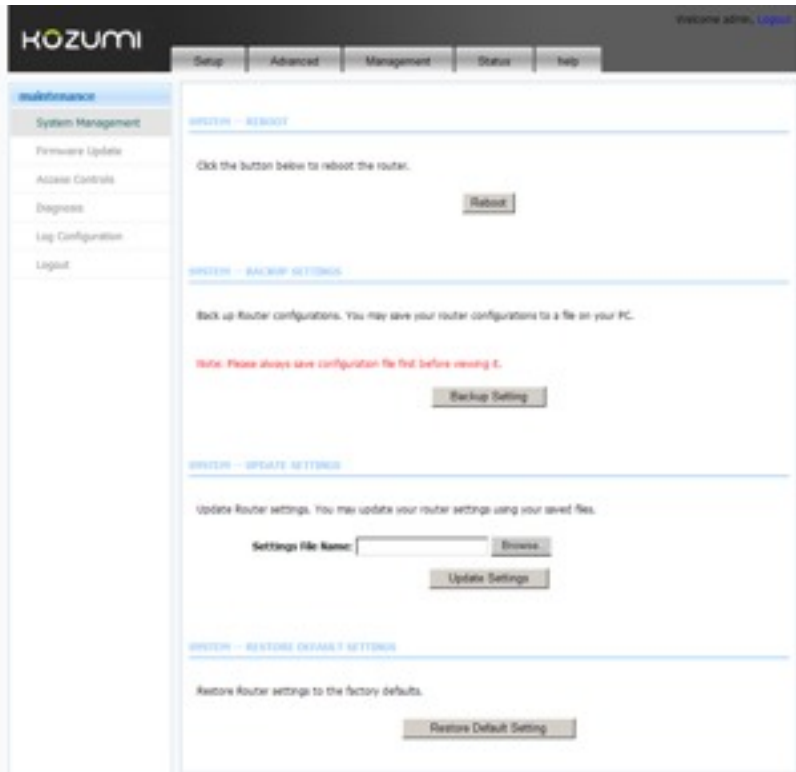
Choose **ADVANCED > Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page.



3.4 Management

3.4.1 System Management

Choose **MAINTENANCE > System Management**. The **System** page shown in the following figure appears.



In this page, you can reboot device, back up the current settings to a file, restore the settings from the file saved previously, and restore the factory default settings.

The buttons in this page are described as follows:

Reboot: Reboot the device.

Backup Setting: Save the settings to the local hard drive. Select a location on your computer to back up the file. You can name the configuration file.

Update Settings: Click **Browse** to select the configuration file of device and click **Update Settings** to begin restoring the device configuration..

Restore Default Setting: Reset the device to default settings.

Notice: Do not turn off your device or press the **Reset** button while an operation in this page is in progress.

3.4.2 Firmware Update

Choose **MAINTENANCE > Firmware Update**. The page shown in the following figure appears. In this page, you can upgrade the firmware of the device.



The procedure for updating the firmware is as follows:

Step 16 Click **Browse...** to search the file.

Step 17 Click **Update Firmware** to copy the file.

The device loads the file and reboots automatically.

Notice: Do not turn off your device or press the reset button while this procedure is in progress.

3.4.3 Access Controls

Choose **MAINTENANCE > Access Controls**. The **Access Controls** page shown in the following figure appears. The page contains **Account Password**, **Services**, and **IP Address**.



3.4.3.1 Account Password

In the **Access Controls** page, click **Account Password**. The page shown in the following figure appears. In this page, you can change the password of the user and set time for automatic logout.

Kozumi Wireless ADSL2/2+ Modem Router

Setup | Advanced | Management | Status | Help

Subinterface

- System Management
- Firmware Update
- Access Controls**
 - User Management
 - Services
 - IP Address
 - Diagnosis
 - Log Configuration
 - Logout

ACCOUNT PASSWORD

Access to your DSL Router is controlled through three user accounts: admin, support, and user.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics. The user name can not be used in local.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as update the router's firmware.

Use the fields below to enter up to 36 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

ACCOUNT PASSWORD

Username:

Current Password:

New Password:

Confirm Password:

WEB SITE TIME OUT SETTINGS

Web Site Time Out: (3 - 30 minutes)

You should change the default password to secure your network. Ensure that you remember the new password or write it down and keep it in a safe and separate location for future reference. If you forget the password, you need to reset the device to the factory default settings and all configuration settings of the device are lost.

Select the **Username** from the drop-down list. You can select **admin**, **support**, or **user**.

Enter the current and new passwords and confirm the new password, to change the password.

Click **Apply** to apply the settings.

3.4.3.2 Services

In the **Access Controls** page, click **Services**. The page shown in the following figure appears.



In this page, you can enable or disable the services that are used by the remote host. For example, if telnet service is enabled and port is 23, the remote host can access the device by telnet through port 23. Normally, you need not change the settings.

Select the management services that you want to enable or disable on the LAN or WAN interface.

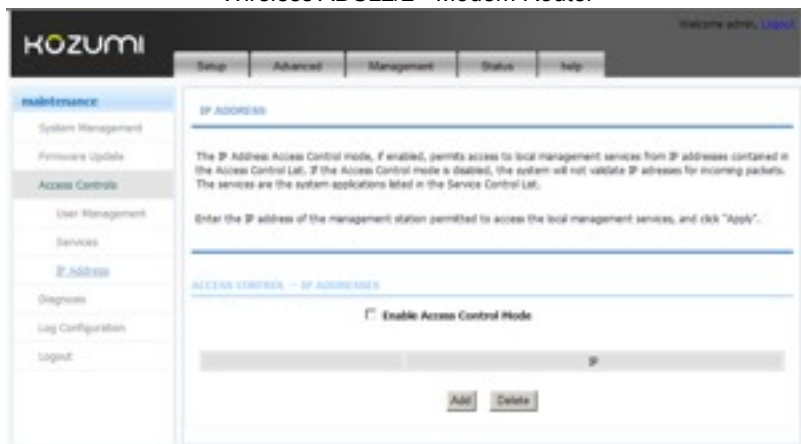
Click **Apply** to apply the settings.

Note:

If you disable HTTP service, you cannot access the configuration page of the device any more.

3.4.3.3 IP Address

In the **Access Controls** page, click **IP Address**. The page shown in the following figure appears.



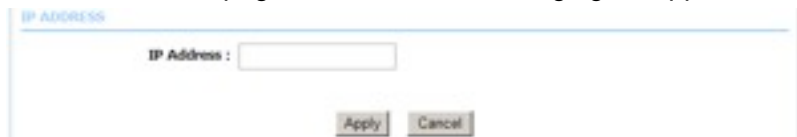
In this page, you can configure the IP address for access control list (ACL). If ACL is enabled, only devices with the specified IP addresses can access the device.

Select **Enable Access Control Mode** to enable ACL.

Note:

If you enable the ACL capability, ensure that IP address of the host is in ACL list.

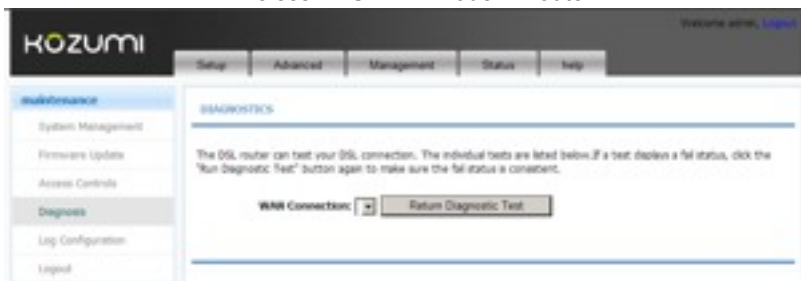
Click **Add**. The page shown in the following figure appears.



Click **Apply** to apply the settings.

3.4.4 Diagnostics

Choose **MAINTENANCE > Diagnostic**. The page shown in the following figure appears. In this page, you can test the device.



Click **Return Diagnostics Test** to run diagnostics.

3.4.5 Log Configuration

Choose **MAINTENANCE >Log Configuration**. The **System Log** page shown in the following figure appears.



This page displays event log data in the chronological manner. You can read the event log from the local host or send it to a system log server. Available event severity levels are as follows: Emergency, Alert, Critical, Error, Warning, Notice, Informational and Debugging. In this page, you can enable or disable the system log function.

Wireless ADSL2/2+ Modem Router

The procedure for logging the events is as follows:

Step 18Select **Enable Log**.

Step 19Select the display mode from the **Mode** drop-down list.

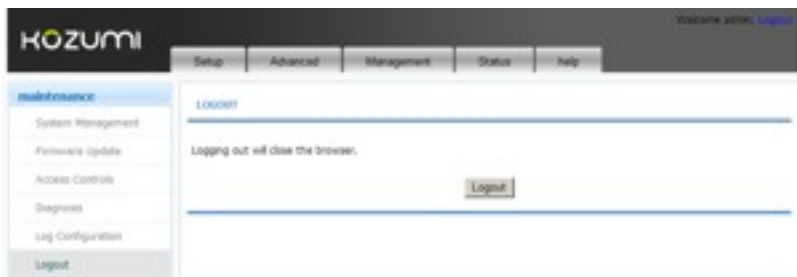
Step 20Enter the **Server IP Address** and **Server UDP Port** if the **Mode** is set to **Both** or **Remote**.

Step 21Click **Apply** to apply the settings.

Step 22Click **View System Log** to view the detail information of system log.

3.4.6 Logout

Choose **MAINTENANCE** > **Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page.



3.5 Status

You can view the system information and monitor performance.

3.5.1 Device Info

Choose **STATUS** > **Device Info**. The page shown in the following figure appears.

Wireless ADSL2/2+ Modem Router

The screenshot displays the status page of a Kozumi Wireless ADSL2/2+ Modem Router. The page is organized into several sections:

- DEVICE INFO:** Provides an overview of the WAN connection status.
- WAN INFO:** Displays key WAN statistics:

Modem Name :	GM41509R
Time and Date :	2000-01-01 01:22:30
Firmware Version :	V1.0
- INTERNET INFO:** Shows Internet connection status and configuration:

Internet Connection Status:	Down
Internet Connection Status:	
Default Gateway:	
Preferred DNS Server:	
Alternate DNS Server:	
Downstream Line Rate (Kbps):	0
Upstream Line Rate (Kbps):	0
- ENABLED WAN CONNECTIONS:** A table listing active connections:

VPI/VCI	Service Name	Protocol	SNMP	QoS	IP Address
- WIRELESS INFO:** Shows wireless network configuration for the selected interface (Wlan_0):

MAC Address :	00:14:33:01:0F:53
Status :	Enable
Network Name (SSID):	Wlan_0
Visibility:	Visible
Security Mode:	WPA
- LOCAL NETWORK INFO:** Shows local network configuration:

MAC Address:	00:14:33:01:0F:04
IP Address :	192.168.2.1
Subnet Mask :	255.255.255.0
DHCP Server :	Enable

The page displays the summary of the device status. It includes the information of firmware version, upstream rate, downstream rate, uptime and Internet configuration (both wireless and Ethernet statuses).

3.5.2 Wireless Clients

Choose **STATUS > Wireless Clients**. The page shown in the following page appears. The page displays authenticated wireless stations and their statuses.

The screenshot shows the Kozumi router's web interface. The top navigation bar includes 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The left sidebar has a 'Status' menu with options: Device Info, Wireless Clients (selected), DHCP Clients, Logs, Statistics, Route Info, and Logout. The main content area is titled 'WIRELESS CLIENTS' and contains the text: 'This page shows authenticated wireless stations and their status.' Below this is a section titled 'WIRELESS - AUTHENTICATED STATIONS' with a table:

Mac	Associated	Authorized	SSID	Interface
88-1e-85-22-4e-2c	Connected	None	Wlan_0	wlan0

A 'Refresh' button is located at the bottom of the table.

3.5.3 DHCP Clients

Choose **STATUS > DHCP Clients**. The page shown in the following page appears.

The screenshot shows the Kozumi router's web interface. The top navigation bar includes 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The left sidebar has a 'Status' menu with options: Device Info, Wireless Clients, DHCP Clients (selected), Logs, Statistics, Route Info, and Logout. The main content area is titled 'DHCP CLIENTS' and contains the text: 'This information reflects the current DHCP client of your modem.' Below this is a section titled 'DHCP LEASES' with a table:

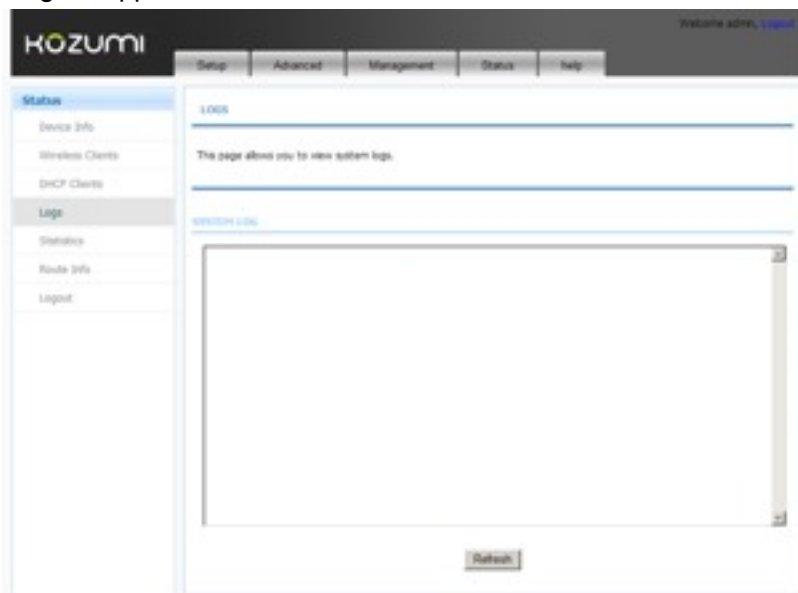
Hostname	MAC Address	IP Address	Expires In
----------	-------------	------------	------------

A 'Refresh' button is located at the bottom of the table.

This page displays all client devices that obtain IP addresses from the device. You can view the host name, IP address, MAC address and time expired(s).

3.5.4 Logs

Choose **STATUS** > **Logs**. The page shown in the following figure appears.



This page displays the system log. Click **Refresh** to refresh the system log shown in the table.

3.5.5 Statistics

Choose **STATUS** > **Statistics**. The page shown in the following figure appears.

The screenshot shows the Kozumi web interface with the 'Status' tab selected. The left sidebar contains navigation options: Status, Device Info, Wireless Clients, DHCP Clients, Logs, Statistics, Route Info, and Logout. The main content area is titled 'DEVICE INFO' and contains a message: 'This information reflects the current status of your DSL connection.' Below this is a section for 'LOCAL NETWORK & WIRELESS' with a table showing interface statistics. The table has columns for Interface, Received (Bytes, Pkts, Errs, Rx drop), and Transmitted (Bytes, Pkts, Errs, Tx drop). The data rows are LAN and Eth_0. Below this is a 'SERVICES' table with columns for Service, VPL/VCI, Protocol, Received (Bytes, Pkts, Errs, Drops), and Transmitted (Bytes, Pkts, Errs, Drops). The Services table is currently empty. At the bottom is an 'ADSL' section with a table of parameters: Mode, Type, Line Coding, Status, SNR Margin, Attenuation, Output Power, Attainable Rate, Rate, D, Delay, FEC Errors, OOB Errors, LCD Errors, and Total ER.

DEVICE INFO

This information reflects the current status of your DSL connection.

LOCAL NETWORK & WIRELESS

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Rx drop	Bytes	Pkts	Errs	Tx drop
LAN	204144	3626	0	0	1123795	3726	0	0
Eth_0	26254665	231632	0	0	26254665	72916	0	0

SERVICES

Service	VPL/VCI	Protocol	Received				Transmitted				
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops	

ADSL

Mode:		0
Type:		0
Line Coding:		Enable
Status:		ACTIVTBAL
	Downstream	Upstream
SNR Margin (dB):	0.0	0.0
Attenuation (dB):	04	0.0
Output Power (dBm):	0.0	0.0
Attainable Rate (Kbps):	0	0
Rate (Kbps):	0	0
D (Discrete depth):	0	0
Delay (ms):	0	0
FEC Errors:	0	0
OOB Errors:	0	0
LCD Errors:	0	0
Total ER:	0	0

This page displays the statistics of the network and data transfer. This information helps technicians to identify if the device is functioning properly. The information does not affect the function of the device.

3.5.6 Route info

Choose **STATUS > Route Info**. The page shown in the following figure appears.

ROUTE INFO

Flag: I-IPv4, F-reject, G-gateway, H-host, R-remote, D-dynamic (redirect), R-modified (redirect)

DEVICE INFO - ROUTE

Destination	Gateway	Subnet Mask	Flags	Metric	Service	Interface
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	br1
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	br1

The table shows a list of destination routes commonly accessed by the network.

3.5.7 Logout

Choose **STATUS** > **Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page.

LOGOUT

Logging out will close the browser.

Logout