



KW5212 Wireless VDSL Router User Manual

Kasda Networks Inc.

深圳市宏成数字科技股份有限公司

NOTICE

This document contains proprietary information protected by copyright, and this Manual and all the accompanying hardware, software, and documentation are copyrighted. All rights are reserved. No part of this document may be photocopied or reproduced by mechanical, electronic, or other means in any form.

The manufacturer does not warrant that the hardware will work properly in all environments and applications, and makes no warranty or representation, either expressed or implied, with respect to the quality, performance, merchantability, or fitness for a particular purpose of the software or documentation. The manufacturer reserves the right to make changes to the hardware, software, and documentation without obligation to notify any person or organization of the revision or change.

All brand and product names are the trademarks of their respective owners.

© Copyright 2014

All rights reserved.

Content

1	OVERVIEW.....	1
1.1	FEATURES.....	1
1.1.1	Data Rate.....	1
1.1.2	VDSL Compliant.....	1
1.1.3	Wireless.....	1
1.1.4	Network Protocol & Features.....	1
1.1.5	ATM Capabilities.....	2
1.1.6	FIREWALL.....	2
1.1.7	Management Support.....	3
1.1.8	Operating System Support.....	3
1.1.9	Environmental.....	3
1.2	PACKET CONTENTS.....	3
1.3	SYSTEM REQUIREMENTS.....	3
1.4	FACTORY DEFAULTS.....	4
1.5	WARNINGS AND CAUTIONS.....	4
2	HARDWARE DESCRIPTION.....	5
3	HARDWARE INSTALLATION.....	7
4	PC CONFIGURATION GUIDE.....	8
4.1	LOCAL PC CONFIGURATION IN WINDOWS 95, 98, ME, XP,7.....	8
4.2	LOCAL PC CONFIGURATION IN WINDOWS 2000.....	8
5	WEB-BASED MANAGEMENT GUIDE.....	9
5.1	LAN SETTING PAGE.....	9
5.2	INTERNET ACCESS CONFIGURATION.....	10
5.2.1	ADSL Setup.....	10
5.2.2	VDSL Setup.....	15
5.2.3	Router Mode Setup.....	19
5.2.4	LAN Settings.....	25
5.3	WIRELESS SETTING.....	27
5.3.1	Basic.....	27
5.3.2	Security.....	28
5.4	PRINTER SERVER INSTALLATIONS.....	31
6.	QOS SETUP.....	33
	APPENDIX : FREQUENT ASKED QUESTIONS.....	43

1 Overview

Thank you for choosing our product. The product is a Wireless VDSL router combining an VDSL modem, an 802.11n wireless router ,a 4-port switch and an USB port in one unit, bringing high-speed wireless Internet connection to a home or office.

1.1 Features

1.1.1 Data Rate

- Downstream data rate up to 100 Mbps
- Upstream data rate up to 50Mbps

1.1.2 VDSL Compliant

- ITU G.992.1 (G.DMT)
- ITU G.993.2 (G.vdsl2) (Profile 8a, 8b, 8c, 8d, 12a,12b and 17a)
- ITU G.992.2 (G.Lite)
- ITU G.994.1 (G.hs)
- ITU G.992.3 (G.DMT.BIS)
- ITU G.992.4 (G.lite.bis)
- ITU G.992.5
- Compatible with all T1.413 issue 2 (full rate DMT over analog POTS), and CO DSLAM equipment

1.1.3 Wireless

- Fully IEEE 802.11n compatible.
- Wireless data rate up to 300Mbps
- Operating in the unlicensed 2.4 GHz ISM band
- Multi-SSID
- Supports 64/128 bits WEP security and user authentication

1.1.4 Network Protocol & Features

- Ethernet to ADSL Self-Learning Transparent Bridging
- Internet Control Message Protocol (ICMP)

- IP Static Routing
- Routing Information Protocol (RIP, RIPv2)
- Network Address Translation (NAT)
- Virtual Server, Port Forwarding
- Dynamic Host Configuration Protocol (DHCP)
- DNS Relay, DDNS
- IGMP Proxy
- Simple Network Time Protocol (SNTP)
- VPN pass-through (IPSec/PPTP/L2TP)
- Parent control

1.1.5 ATM Capabilities

- RFC 1483 Multi-protocol over ATM “Bridged Ethernet” compliant
- RFC 2364 PPP over ATM compliant
- RFC 2516 PPP over Ethernet compliant
- ATM Forum UNI3.1/4.0 PVC – Support up to 16 PVCs
- VPI Range: 0-255
- VCI Range: 32-65535
- UNI 3.0 & 3.1 Signaling
- ATM AAL5 (Adaption Layer type 5)
- OAM F4/F5

1.1.6 FIREWALL

- Built-in NAT
- MAC Filtering
- Packet Filtering
- Stateful Packet Inspection (SPI)
- Denial of Service Prevention (DoS)

- DMZ

1.1.7 Management Support

- Web Based GUI
- Upgrade or update via FTP/HTTP
- Command Line Interface via Telnet
- Diagnostic Test
- Firmware upgradeable for future feature enhancement

1.1.8 Operating System Support

- WINDOWS 98/98 SE/ME/2000/XP/VISTA/7
- Macintosh
- LINUX

1.1.9 Environmental

- Operating humidity: 10%-90% non-condensing
- Non-operating storage humidity: 5%-95% non-condensing

1.2 Packet Contents

The packet contents are as the following:

- VDSL ROUTER x 1
- External Splitter x 1
- Power Adapter x 1
- Telephone Line x 1
- Ethernet Cable x 1
- Antenna x 2
- Base x 1
- CD x 1

1.3 System Requirements

Before using this ROUTER, verify that you meet the following requirements:

- Subscription for ADSL service. Your ADSL service provider should provide you with at least one valid IP address (static assignment or dynamic assignment via dial-up connection).
- One or more computers, each contains an Ethernet 10/100M Base-T network interface card (NIC).
- A hub or switch, if you are connecting the device to more than one computer.
- For system configuration using the supplied web-based program: A web browser such as Internet Explorer v5.0 or later, or Netscape v4.7 or later.

1.4 Factory Defaults

The device is configured with the following factory defaults:

- IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0
- Encapsulation: RFC 2516 LLC
- VPI/VCI: According to local information

1.5 Warnings and Cautions

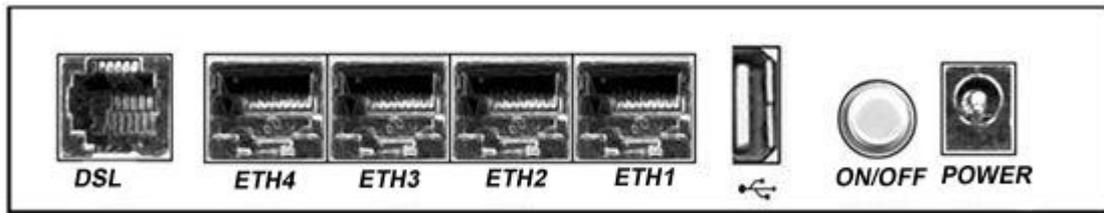
- Never install telephone wiring during storm. Avoid using a telephone during an electrical storm. There might be a risk of electric shock from lightning.
- Do not install telephone jacks in wet locations and never use the product near water.
- To prevent dangerous overloading of the power circuit, be careful about the designed maximum power load ratings. Not to follow the rating guideline could result in a dangerous situation.
- Please note that telephone line on modem must adopt the primary line that directly outputs from junction box. Do not connect Router to extension phone. In addition, if your house developer divides a telephone line to multi sockets inside the wall of house, please only use the telephone that has connected with the splitter of ADSL Router when you access the Internet.

2 Hardware Description

Front Panel

	LED	Color	Function
		Green	On: Power on Off: No power
   		Green	On: LAN link established and active via LAN port Blinking: DSL data activity occurs Off: No LAN link via LAN port
	WLAN	Green	On: The wireless module is ready and idle Blinking: Data transmitting or receiving over WLAN Off: The wireless function is off
	DSL	Green	On: DSL link established and active Quick Blinking: DSL is trying to establish a connection Slow Blinking: No DSL link
	INET	Green	On: IP connected Blinking: IP connected and IP traffic is passing through this device Off: ADSL connection is not present

Rear panel



Port	Function
DSL	Connect the device to an DSL telephone jack or splitter using a RJ-11 telephone cable
ETH1,2,3,4	Connect the device to your PC's Ethernet port, or to the uplink port on your hub/switch, using a RJ-45 cable
	Connect the device to a printer
ON/OFF	Switch it on or off
POWER	Connect to the supplied power adapter

Side panel

WIFI button: Enable or disable wireless function.

Reset button: System reset or reset to factory defaults.

WPS button: A convenient way for WPS set.

3 Hardware Installation

This chapter shows you how to connect Router. Meanwhile, it introduces the appropriate environment for the Router and installation instructions.

- Using a telephone line to connect the **DSL** port of ROUTER to the **MODEM** port of the splitter, and using a other telephone line connect your telephone to the **PHONE** port of the splitter, then connect the wall phone jack to the **LINE** port of the splitter.

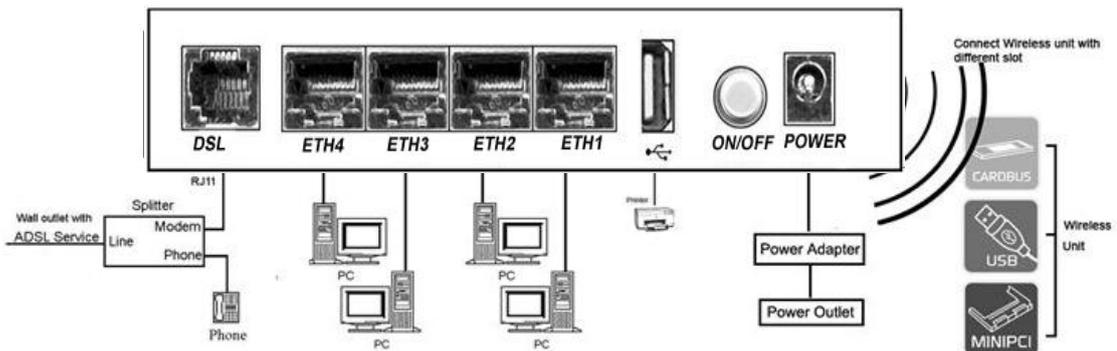
The splitter comes with three connectors as below:

LINE: Connects to a wall phone jack (RJ-11 jack)

MODEM: Connects to the DSL jack of ROUTER

PHONE: Connects to a telephone set

- Using an Ethernet Cable to connect the LAN port of the ROUTER to your LAN or a PC with network card installed.
- Connect the power cable to the PWR connector on ROUTER, then plug in the power adapter to the power outlet, and then press the on-off button.



Notes: Without the splitter and certain situation, transient noise from telephone can interfere with the operation of the Router, and the Router may introduce noise to the telephone line. To prevent this from happening, a small external splitter must be connected to each telephone.

4 PC Configuration Guide

4.1 Local PC Configuration in Windows 95, 98, ME, XP,7

1. In the Windows task bar, click the “Start” button, point to “Settings”, and then click “Control Panel”.
2. Double-click the “Network” icon.
3. On the “Configuration” tab, select the TCP/IP network associated with your network card and then click “Properties”.
4. In the “TCP/IP Properties” dialog box, click the “IP Address” tab. Set the IP address as 192.168.1.x (x can be a decimal number from 2 to 254.) like 192.168.1.2, and the subnet mask as 255.255.255.0.
5. On the “Gateway” tab, set a new gateway as 192.168.1.1, and then click “Add”.
6. Configure the “DNS” tab if necessary. For information on the IP address of the DNS server, please consult with your ISP.
7. Click “OK” twice to confirm and save your changes.
8. You will be prompted to restart Windows. Click “Yes”.

4.2 Local PC Configuration in Windows 2000

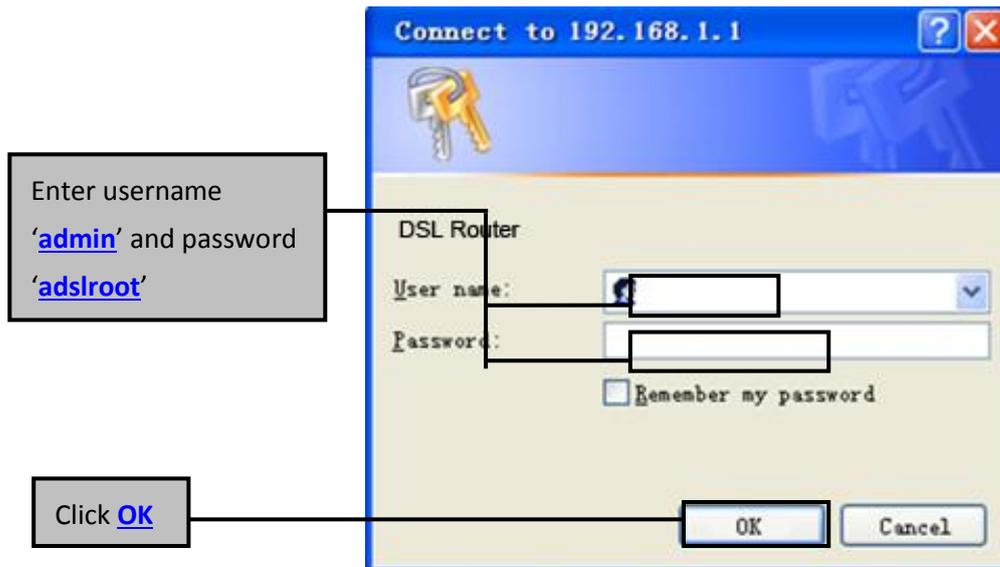
1. In the Windows task bar, click the “Start” button, point to “Settings”, and then click “Control Panel”.
2. Double-click the “Network and Dial-up Connections” icon.
3. In the “Network and Dial-up Connections” window, right-click the “Local Area Connection” icon, and then select “Properties”.
4. Highlight “Internet Protocol (TCP/IP)”, and then click “Properties”.
5. In the “Internet Protocol (TCP/IP) Properties” dialog box, set the IP address as 192.168.1.x (x can be a decimal number from 2 to 254.), and the subnet mask as 255.255.255.0 and the default gateway as 192.168.1.1. Then click “OK”.
6. Configure the “DNS” tab if necessary. For information on the IP address of the DNS server, please consult with your ISP.
7. Click “OK” twice to confirm and save your changes.

5 Web-based Management Guide

In order to use the web-based management software it will be necessary to use a computer that occupies the same subnet as the Router. The simplest way to do this for many users will be to use DHCP server that is enabled by default on the Router.

5.1 LAN setting page

Launch a web browser, such as Internet Explorer, and then use <http://192.168.1.1> to log on to the setting pages.



After log on ,you will see the following screen :

Please select Wizard or Advanced mode

The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router or if you need to make basic configuration changes.

Use Advanced mode if you need access to more advanced features not included in Wizard mode.

- Go to Wizard setup**
- Go to Advanced setup**
- Click here to always start with the Advanced setup.**

Apply

Exit

We can select wizard setup or advanced setup mode to setup KW5212. the wizard set up will guide us for a basic setting, and the advanced setup will guide us to home page for more detailed setup.

5.2 Internet Access Configuration

5.2.1 ADSL Setup

From home page, you can find **Advanced Setup** option on the left router configuration page.

1. From **Layer2 Interface**, click **ATM Interface**. you can set it up according to the following steps. You Choose **Add**, or **Remove** to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate (cells/s)	Sustainable Cell Rate(cells/s)	Max Burst Size (bytes)	Link Type	Conn Mode	IP QoS	MPAAL Prec/Alg/Wght	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>												

2. Click **Add** to configure PVC identifier, select DSL latency and select connection mode according to your local occasion. After the configuration, you need to click **Apply/Save**.

VPI: [0-255]

VCI: [32-65535]

Select DSL Latency

Path0

Path1

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

EoA

PPPoA

IPoA

Select Connection Mode

Default Mode - Single service over one connection

VLAN MUX Mode - Multiple Vlan service over one connection

Encapsulation Mode:

Service Category:

3. Click **WAN Service** from the left menu.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit
-----------	-------------	------	-----------	-----------	------	-----	----------	--------	------

- Click **Add** to select a layer 2 interface for this service and then click **Next**.

atm0/ (0_0_35) ▼

- Choose WAN service type, just choose PPPoE for example here. You can enter your own service description here if you want and then click **Next**.

Select WAN service type:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description:

- Input **PPP Username** & **PPP Password** and then click **Next**. The user interface allows a maximum of 256 characters in the user name and a maximum of 32 characters in the password.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: 

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Use Static IPv4 Address

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

Enable IGMP Multicast Proxy

No Multicast VLAN Filter

PPPoE service name can be blank unless your Internet Service Provider gives you a value to enter.

Authentication method is default to **Auto**. It is recommended that you leave the **Authentication method** in **Auto**, however, you may select **PAP** or **CHAP** if necessary. The default value for MTU (Maximum Transmission Unit) is **1500** for PPPoA and **1492** for PPPoE. Do not change these values unless your ISP asks you to.

Enable Full Cone NAT: In full cone NAT, all requests from the same private IP address and port are mapped to the same public source IP address and port. Someone on the Internet only needs to know the mapping scheme in order to send packets to a device behind the VDSL Device.

The gateway can be configured to disconnect if there is no activity for a specific period of time by selecting the **Dial on demand** check box and entering the **Inactivity timeout**. The entered value must be between 1 minute and 4320 minutes.

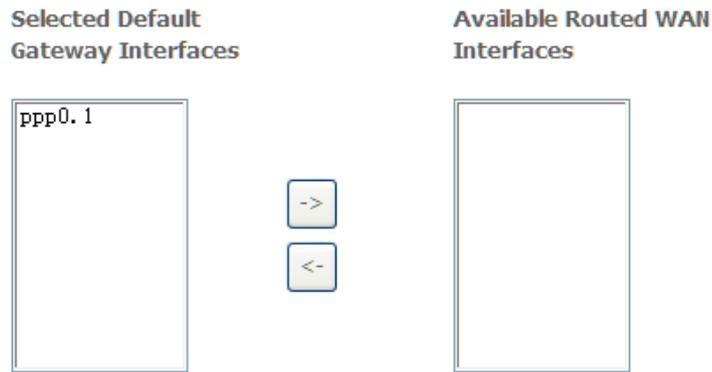
Use Static IPv4 address: If the ISP gave you a static (fixed) IP address, select this option and enter it in the IP Address field. If the ISP did not give you a static IP address, clear the Use Static IP Address option. The ISP automatically assigns the WAN connection an IP address when it connects.

Enable PPP Debug Mode: Select this to turn on the debug mode for the PPP connection.

Bridge PPPoE Frames Between WAN and Local Ports: In addition to the VDSL Device's built-in PPPoE client, you can enable this to pass PPPoE through in order to allow LAN hosts to use PPPoE client software on their computers to connect to the ISP via the VDSL Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for applications where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.

The **PPP IP Extension** is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it. If you need to select it, the PPP IP Extension supports the following conditions:

- It allows only one computer on the LAN.
 - The public IP address assigned by the remote using the PPP/PCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the computer's LAN interface through DHCP. Only one system on the LAN can be connected to the remote, since the DHCP server within the ADSL gateway has only a single IP address to assign to a LAN device.
 - NAPT and firewall are disabled when this option is selected.
 - The gateway becomes the default gateway and DNS server to the computer through DHCP using the LAN interface IP address.
 - The gateway extends the IP subnet at the remote service provider to the LAN computer. That is, the PC becomes a host belonging to the same IP subnet.
 - The ADSL gateway bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the gateway's LAN IP address.
7. Select a preferred wan interface as the system default gateway.



8. Get DNS server information from the selected WAN interface or enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces Available WAN Interfaces

The diagram shows the selection of a DNS server interface. On the left, a box labeled "Selected DNS Server Interfaces" contains the text "ppp0.1". On the right, a box labeled "Available WAN Interfaces" is empty. Between the two boxes are two buttons: a right-pointing arrow (->) and a left-pointing arrow (<-).

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

9. Make sure that the settings below match the settings provided by your ISP. Click on the **Apply/Save** button to save your configurations.

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

5.2.2 VDSL Setup

From home page, you can find **Advanced Setup** option on the left router configuration page.

1. From **Layer2 Interface**, click **PTM Interface**. you can set it up according to the following steps. You Choose **Add**, or **Remove** to configure DSL PTM interfaces.

Interface	DSL Latency	PTM Priority	Conn Mode	IP QoS	Remove
-----------	-------------	--------------	-----------	--------	--------

2. Click **Add** to configure **PTM Priority**, select DSL latency and select connection mode according to your local occasion. After the configuration, you need to click **Apply/Save**.

Select DSL Latency

Path0 (Fast)

Path1 (Interleaved)

Select Scheduler for Queues of Equal Precedence as the Default Queue

Weighted Round Robin

Weighted Fair Queuing

Default Queue Weight: [1-63]

Default Queue Precedence: [1-8] (lower value, higher priority)

Default Queue Shaping Rate: [Kbits/s] (blank indicates no shaping)

Default Queue Shaping Burst Size: [bytes] (shall be >=1600)

3. Click **WAN Service** from the left menu.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit
-----------	-------------	------	-----------	-----------	------	-----	----------	--------	------

4. Click **Add** to select a layer 2 interface for this service and then click **Next**.

▼

5. Choose WAN service type, just choose PPPoE for example here. You can enter your own service description here if you want and then click **Next**.

Select WAN service type:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description:

6. Input **PPP Username** & **PPP Password** and then click **Next**. The user interface allows a maximum of 256 characters in the user name and a maximum of 32 characters in the password.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: ▼

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Use Static IPv4 Address

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

Enable IGMP Multicast Proxy

No Multicast VLAN Filter

PPPoE service name can be blank unless your Internet Service Provider gives you a value to enter.

Authentication method is default to **Auto**. It is recommended that you leave the **Authentication method** in **Auto**, however, you may select **PAP** or **CHAP** if necessary. The default value for MTU (Maximum Transmission Unit) is **1500** for PPPoA and **1492** for PPPoE. Do not change these values unless your ISP asks you to.

Enable Full Cone NAT: In full cone NAT, all requests from the same private IP address and port are mapped to the same public source IP address and port. Someone on the Internet only needs to know the mapping scheme in order to send packets to a device behind the VDSL Device.

The gateway can be configured to disconnect if there is no activity for a specific period of time by selecting the **Dial on demand** check box and entering the **Inactivity timeout**. The entered value must be between 1 minute and 4320 minutes.

Use Static IPv4 address: If the ISP gave you a static (fixed) IP address, select this option and enter it in the IP Address field. If the ISP did not give you a static IP address, clear the Use Static IP Address option. The ISP automatically assigns the WAN connection an IP address when it connects.

Enable PPP Debug Mode: Select this to turn on the debug mode for the PPP connection.

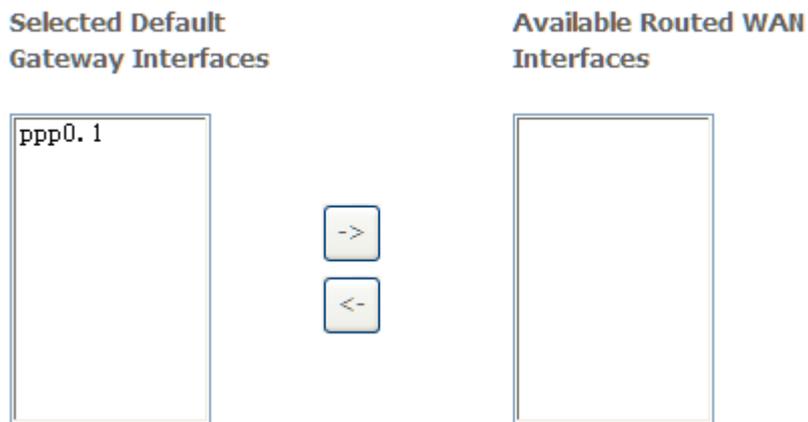
Bridge PPPoE Frames Between WAN and Local Ports: In addition to the VDSL Device's built-in PPPoE client, you can enable this to pass PPPoE through in order to allow LAN hosts to use PPPoE client software on their computers to connect to the ISP via the VDSL Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for applications where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.

The **PPP IP Extension** is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it. If you need to select it, the PPP IP Extension supports the following conditions:

- It allows only one computer on the LAN.
- The public IP address assigned by the remote using the PPP/PCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the computer's LAN interface through DHCP. Only one system on the

LAN can be connected to the remote, since the DHCP server within the ADSL gateway has only a single IP address to assign to a LAN device.

- NAPT and firewall are disabled when this option is selected.
 - The gateway becomes the default gateway and DNS server to the computer through DHCP using the LAN interface IP address.
 - The gateway extends the IP subnet at the remote service provider to the LAN computer. That is, the PC becomes a host belonging to the same IP subnet.
 - The ADSL gateway bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the gateway's LAN IP address.
7. Select a preferred wan interface as the system default gateway.



8. Get DNS server information from the selected WAN interface or enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server
Interfaces

Available WAN Interfaces

ppp0.1	<input type="button" value="->"/> <input type="button" value="<-"/>	
--------	--	--

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

9. Make sure that the settings below match the settings provided by your ISP. Click on the **Apply/Save** button to save your configurations.

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

5.2.3 Router Mode Setup

- From **Advanced Setup**, click **Layer2 Interface** and select **ETH Interface**. Before you configure ETH WAN interface, you'd better remove all PVC settings from **ATM interface**.

Interface/(Name)	Connection Mode	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>		

- Click **Add** and you'll see the following screen.

ETH WAN Configuration

This screen allows you to configure a ETH port .

Select a ETH port:

eth0/eth0 ▼

Back Apply/Save

3. Select a ETH port as you will. You can select ENET1, ENET2, ENET3 or ENET4 port as the WAN interface and Default mode as connection mode.

eth0/eth0 ▼

eth0/eth0
eth1/eth1
eth2/eth2
eth3/eth3

4. Click **Apply/Save** and you'll see the following screen.

Interface/(Name)	Connection Mode	Remove
eth2/eth2	VlanMuxMode	<input type="checkbox"/>

Remove

5. From **Advanced Setup**, click **WAN Service** to configure a WAN service over the interface you selected.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit
-----------	-------------	------	-----------	-----------	------	-----	----------	--------	------

Add Remove

6. Click **Add** and you'll see the following screen.

eth2/eth2 ▼

Back Next

7. Click **Next** and you'll see the following screen. Select PPPoE as WAN service type for example. Click **Next**.

WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Network Protocol Selection:(IPV6 Only not support)

▼

8. Enter the user name and password that your ISP has provided to you. Click **Next**.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: 

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Use Static IPv4 Address

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

Enable IGMP Multicast Proxy

No Multicast VLAN Filter

PPPoE service name can be blank unless your Internet Service Provider gives you a value to enter.

Authentication method is default to **Auto**. It is recommended that you leave the **Authentication method** in **Auto**, however, you may select **PAP** or **CHAP** if necessary. The default value for MTU (Maximum Transmission Unit) is **1500** for PPPoA and **1492** for PPPoE. Do not change these values unless your ISP asks you to.

Enable Full Cone NAT: In full cone NAT, all requests from the same private IP address and port are mapped to the same public source IP address and port. Someone on the Internet only needs to know the mapping scheme in order to send packets to a device behind the VDSL Device.

The gateway can be configured to disconnect if there is no activity for a specific period of time by selecting the **Dial on demand** check box and entering the **Inactivity timeout**. The entered value must be between 1 minute and 4320 minutes.

Use Static IPv4 address: If the ISP gave you a static (fixed) IP address, select this option and enter it in the IP Address field. If the ISP did not give you a static IP address, clear the Use Static IP Address option. The ISP automatically assigns the WAN connection an IP address when it connects.

Enable PPP Debug Mode: Select this to turn on the debug mode for the PPP connection.

Bridge PPPoE Frames Between WAN and Local Ports: In addition to the VDSL Device's built-in PPPoE client, you can enable this to pass PPPoE through in order to allow LAN hosts to use PPPoE client software on their computers to connect to the ISP via the VDSL Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for applications where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.

The **PPP IP Extension** is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it. If you need to select it, the PPP IP Extension supports the following conditions:

- It allows only one computer on the LAN.
- The public IP address assigned by the remote using the PPP/PCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the computer's LAN interface through DHCP. Only one system on the LAN can be connected to the remote, since the DHCP server within the ADSL gateway has only a single IP address to assign to a LAN device.
- NAT and firewall are disabled when this option is selected.

- The gateway becomes the default gateway and DNS server to the computer through DHCP using the LAN interface IP address.
- The gateway extends the IP subnet at the remote service provider to the LAN computer. That is, the PC becomes a host belonging to the same IP subnet.
- The ADSL gateway bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the gateway's LAN IP address.

9. Select WAN interface as the system default gateway. Click **Next**.

Selected Default Gateway Interfaces

ppp0.1

->

<-

Available Routed WAN Interfaces

10. Get DNS server information from the selected WAN interface or enter static DNS server IP addresses. Click **Next**.

 **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces

ppp0.1

->

<-

Available WAN Interfaces

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

11. Make sure that the settings below match the settings provided by your ISP. Click on the **Apply/Save** button to save your configurations and reboot the ADSL router.

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

5.2.4 LAN Settings

From **LAN**, Configure the DSL Router's IP Address and Subnet Mask for LAN interface. In this page, you can use DHCP (Dynamic Host Configuration Protocol) to control the assignment of IP addresses on your local network (LAN only). KW5212 support IPv4 /IPv6 dual stack.

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName Default 

IP Address:
 Subnet Mask:

Enable IGMP Snooping

Standard Mode

Blocking Mode

Enable LAN side firewall

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
<input type="button" value="Add Entries"/> <input type="button" value="Remove Entries"/>		

Enable DHCP Server Relay

DHCP Server IP Address:

Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

Item	Description
IP address	This is the IP address that other devices on your local network will use to connect to the modem.
Subnet mask	This defines the size of your network. The default is 255.255.255.0 .
Enable IGMP snooping	IGMP Snooping is a method that actually “snoops” or inspects IGMP traffic on a switch. When enabled, the switch will watch for IGMP messages passed between a host and a router, and will add the necessary ports to its multicast table, ensuring that only the ports that require a given multicast stream actually receive it.
Disable / Enable DHCP server	The DHCP server assigns an IP addresses from a pre-set pool of addresses upon request from DHCP client (e.g. your computer). Do not disable the DHCP server unless you wish to let another device handle IP address issuance on the local network.
Start / end IP address	This is the beginning and ending range for the DHCP server addresses.
Lease time	The amount of time before the IP address is refreshed by the DHCP server.
Enable DHCP server relay	If NAT is disabled and the PVC is the IPoA or static MER type, this item allows you to inform the router of another DHCP server on your LAN. To do this, disable the DHCP server on the gateway. Then input the IP address of the current DHCP server. Click Apply and restart the gateway.
Configure the second IP address and...	Use this feature to create a public network on your local LAN, accessible from the Internet. By assigning an address to this interface and then statically setting your LAN clients to the same network, the LAN clients are accessible from the public network (e.g. FTP or HTTP servers).

5.3 Wireless setting

5.3.1 Basic

Enable Wireless
 Hide Access Point
 Clients Isolation
 Disable WMM Advertise
 Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID: 00:0E:F4:E7:FF:B6

Country:

Max Clients:

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
<input type="checkbox"/>	<input type="text" value="wl0_Guest1"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wl0_Guest2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wl0_Guest3"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A

Option	Description
Enable wireless	A checkbox that enables or disables the wireless LAN interfaces. The default is to enable wireless communications.
Hide Access Point	<p>Select Hide Access Point to protect the ADSL route access point from detection by wireless active scans. If you do not want the access point to be automatically detected by a wireless station, this checkbox should be deselected.</p> <p>The station will not discover this access point. To connect a station to the access point, the station must manually add this access point name in it's wireless configuration.</p> <p>In Windows XP, go to the Network>Properties function to view all of the available access points. You can also use other software programs such as NetStumbler to view available access points.</p>
Clients isolation	Enable this item if you don't want your wireless clients to communicate with each other.
Network name	Enter a name for user's wireless network here. SSID stands for Service Set Identifier. This name must be between 1 and 32 characters long. The default name is

(SSID)	KASDAxxxx (xxxx means the mac address of KW5212 with uppercase and without colon) . All wireless clients must either detect the gateway or be configured with the correct SSID to access the Internet.
BSSID	Displays the gateway's wireless MAC address. (User may need this address if user is using WDS or multiple gateways.) Click Apply to save changes.
Country	Drop-down menu that allows selection of specific channel.

5.3.2 Security

This page allows you to configure security features of the wireless LAN interface. You may set up configuration manually or through WiFi Protected Setup(WPS)

1.Click **Security** of **Wireless** item and you'll see the following page.

- Enable Wireless
- Hide Access Point
- Clients Isolation
- Disable WMM Advertise
- Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID: 00:0E:F4:D7:55:66

Country: ▼

Max Clients:

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
<input type="checkbox"/>	<input type="text" value="w0_Guest1"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="w0_Guest2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A

2.Configure WPA Pre-shared key as below and click **Apply/Save**.

WPS Setup

Enable **WPS** ▼

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless ne. Click "Apply/Save" when done.

Select SSID: ▼

Network Authentication: ▼

WEP Encryption: ▼

3.Enable WPS as below. click **Save/Apply**

WPS Setup

Enable **WPS** ▼

Add **Client** (This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)

Enter STA PIN Use AP PIN

Set **WPS AP Mode** ▼

Setup **AP** (Configure all security settings with an external registrar)

Device **PIN** [Help](#)

4.. Now you can use a wireless adaptor with WPS function and the WPS button to connect KW5212 to access the Internet.

5. To configure security features for the Wireless interface, please open Security item from Wireless menu. This web page offers nine authentication protocols for user to secure user's data while connecting to networks. There are four selections including Open, Shared, 802.1X,WPA, WPA-PSK, WPA2, WPA2-PSK, Mixed WPA-WPA2, Mixed WPA-WPA2-PSK. Different item leads different web page settings. Please read the following information carefully.

The wireless security page allows user to configure the security features of user's wireless network.

Set **WPS AP Mode** ▼

Setup **AP** (Configure all security settings with an external registrar)

Device PIN [Help](#)

Manual Setup AP

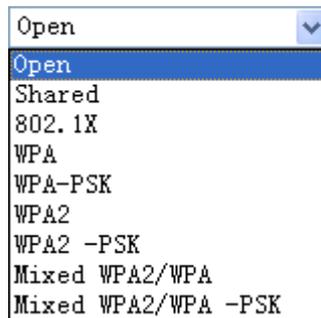
You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID: ▼

Network Authentication: ▼

WEP Encryption: ▼

There are several security methods to choose from, depending on user's needs and the capabilities of user's wireless machines.



- **WEP open** and **WEP shared** —WEP is an encryption scheme that is used to protect user's wireless data communications. WEP uses a combination of 64-bit keys or 128-bit keys to provide access control to user's network and encryption security for every data transmission. To decode a data transmission, each wireless client on the network must use an identical 64-bit or 128-bit key. WEP is an older wireless encryption method that is not as hard to break as the more-recent WPA.
- **802.1x** — In 802.1x (also known as RADIUS), a separate machine called an authentication server receives a user ID and password. It grants or denies access based on whether the ID and password match any entries in its account list. User can optionally enable WEP encryption with this option. Because it requires a separate machine acting as the authentication server, 802.1x is most often used in business environments.

- **WPA** — WPA is a more recent encryption method that addresses many of the weaknesses in WEP. Any client capable of WPA encryption should use it instead of WEP.
- **WPA (PSK)** — This is WPA encryption combined with a *pre-shared key (PSK)*, which is a text string known only to the gateway and authorized wireless clients. The gateway rejects the login if the client's PSK does not match.
- **WPA2** — WPA2 is a more advanced encryption method than WPA. Because it is a more recent standard, some of user's wireless devices might not be able to use it.
- **WPA2 (PSK)** — This option uses WPA2 with a pre-shared key.
- **WPA2 and WPA** — This option supports WPA2/WPA encryption for devices capable of one or the other standard. The gateway automatically detects whether a particular device can use WPA2 or WPA.
- **WPA2 AND WPA (PSK)** — This has WPA2 or WPA encryption based on client abilities, as well as a pre-shared key.

After making changes, click **Apply** to save.

5.4 Printer Server Installations

1. Click “Advanced setup⇒Print Server” and then Check “**Enable on-board printer server**” and key in “**Printer name**”, “**Make and model**” .

Print Server settings

This page allows you to enable / disable printer support.

Enable on-board print server.

Printer name

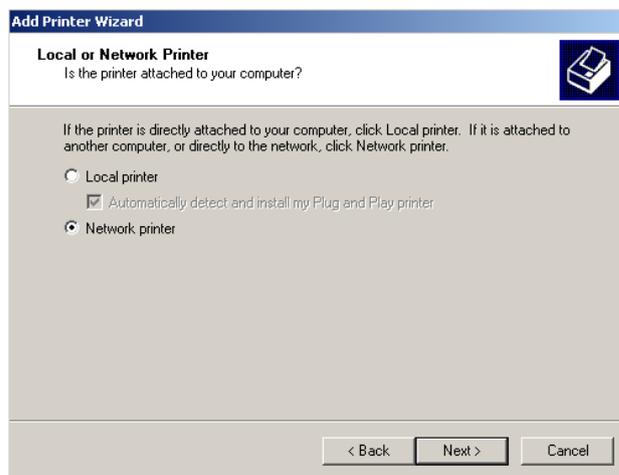
Make and model

Save/Apply

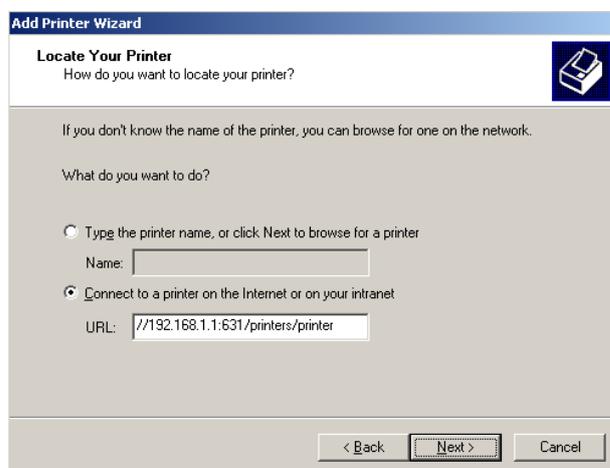
2. Click on Add a printer from **Control Panel** of the Windows computer and click “Next”.



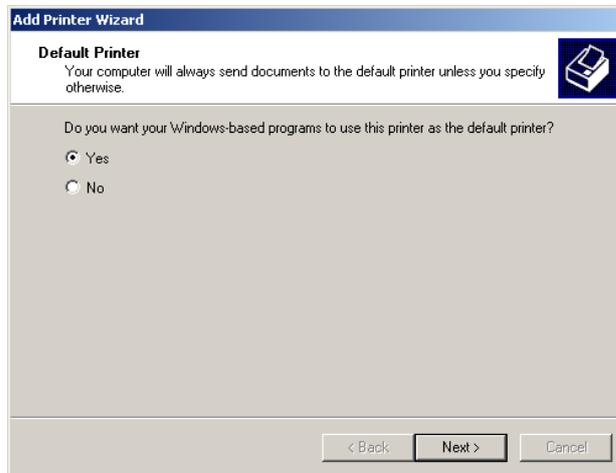
3. Select “Network Printer” and click “Next”.



4. Select Connect to a printer on the Internet, type “**http://192.168.1.1:631/printers/printer**” and click “Next”. **The printer name “Printer” must be the same name entered in the ADSL router “print server setting” as in step 1.**



5. Select driver file directory on CD-ROM or in your hard disk and click “OK”.
6. Choose “Yes” or “No” for default printer setting and click “Next”.

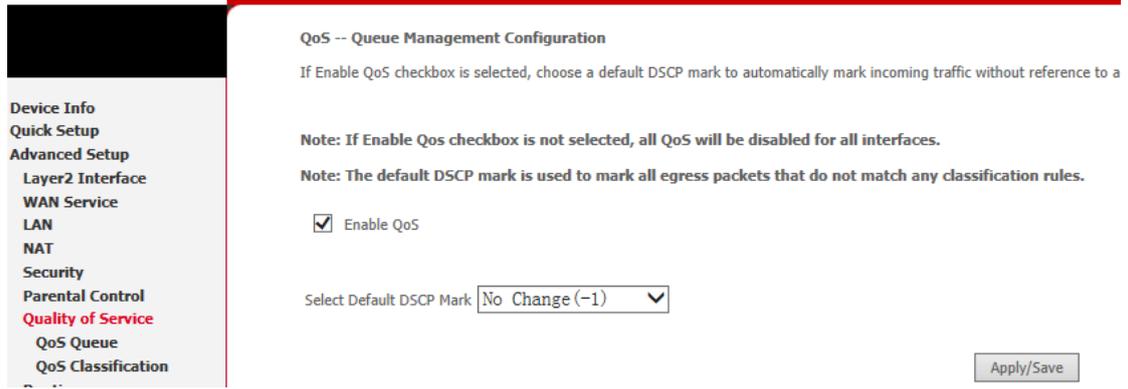


7. Click “Finish”.



6. QoS setup

QoS helps you to control the data upload traffic of each application from LAN (Ethernet) to WAN (Internet). It facilitates you the features to control the quality and speed of throughput for each application when the system is running with full upstream load.



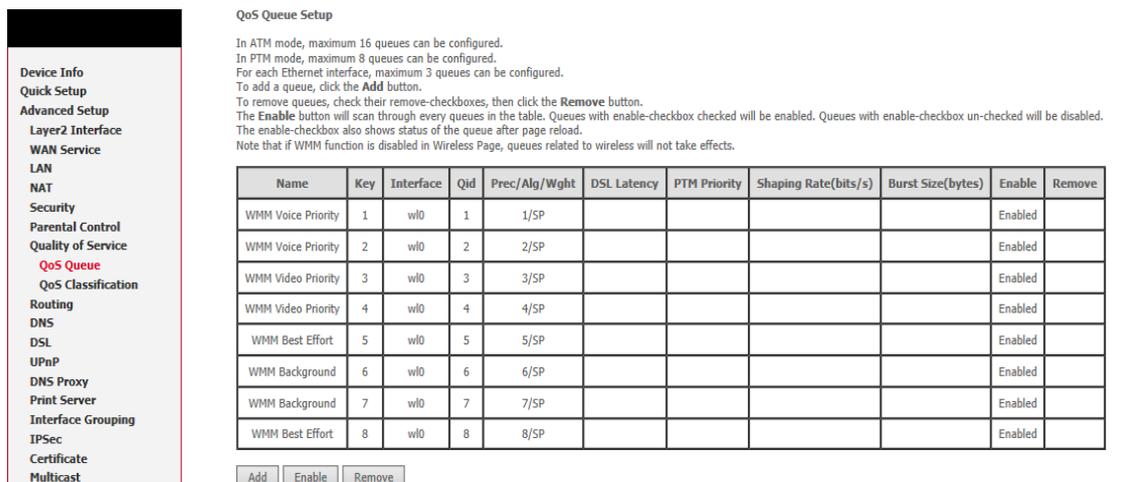
Quality of Service: Check to activate this function and the following field will be available.

Select Default DSCP Mark: Select the default DSCP mark from the list-box. Differentiated Services Code Point (DSCP) is the first 6 bits in the ToS byte. DSCP Mark allows users to classify the traffic of the application to be executed according to the DSCP value. The default DSCP mark is used to mark all egress packets that do not match any classification rules.

DSCP indicates three kinds of service, Class Selector (CS), Assured Forwarding (AF) and Expedited Forwarding (EF). AF1, AF2, AF3 and AF4 are four kinds of assured forwarding services. Each AF has three different packet loss priorities from high, medium, to low. Also, CS1-CS7 indicates the IP precedence.

☞ Note: Before configuring Queue config and QoS Classification section, you must enable QoS function, for the reason that the queues' activation will depend on this, the classification will also depend on this.

✧ QoS queue setup



Name: the queue name.

Key: the item number.

Interface: the queue interface.

Scheduler Algorithm: the QoS Scheduler Algorithm, SP(Strict Priority) or WFQ(Weight Fair Queuing)

Precedence: the priority identification.

Weight: the weight value, 1-63. the highest is 63.

PTM Priority: the PTM priority, normal or high.

Enable: check the enable check-box, then press Enable to activate the queue. If you want to disable this queue, you can uncheck the corresponding check-box and press Enable, the queue will be disabled.

To add a queue, click the Add button, you will see the following page.

QoS Queue Configuration

This screen allows you to configure a QoS queue and add it to a selected layer2 interface.

Name:

Enable: Enable

Interface:
 eth0
 eth1
 eth2
 eth3

Queue Precedence: (lower value, higher priority)

- The precedence list shows the scheduler algorithm for each precedence level.
- Queues of equal precedence will be scheduled based on the algorithm.
- Queues of unequal precedence will be scheduled based on SP.

Apply/Save

Input a queue name as you want and select a interface depending your need. decide the priority of the interface. (lower value, higher priority). click apply/save button.

✧ QoS Classification Setup

You can add or remove a rule.

QoS Classification Setup -- maximum 32 rules can be configured.

To add a rule, click the **Add** button.

To remove rules, check their remove-checkboxes, then click the **Remove** button.

The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the rule after page reload.

If you disable WMM function in Wireless Page, classification related to wireless will not take effects

CLASSIFICATION CRITERIA													CLASSIFICATION RESULTS					
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	Rate Limit (kbps)	Enable	Remove
<input type="button" value="Add"/> <input type="button" value="Enable"/> <input type="button" value="Remove"/>																		

Click add button you will see the following page.

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

Specify Classification Criteria (A blank criterion indicates it is not used for classification.)

Class Interface:

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Specify Classification Results (A blank value indicates no operation.)

Specify Class Queue (Required):

- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
 - Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
 - Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
 - Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Set Rate Limit: [Kbits/s]

Parameters

Traffic Class Name: Assign a name for this class to uniquely identify the others among multiple classes.

Rule Order: Select the priority for this class rule.

Rule Status: Select Enable to activate this class rule.

Specify Classification Criteria

The following parameters are to be classification rule. Enter or select appropriate parameters on the following fields. A blank criterion indicates it is not used for classification.

Class Interface: select the interface you want to be the one aspect of the classification criteria. Here "LAN" and "WAN" can be viewed as IP QoS, the others can be viewed as ported based QoS, which means that control the QoS of certain port such. For example, if you select ETH0 port, then criteria applies to this port, that is ported-based QoS.

Entry Type: select the application type.

Source/destination MAC Address: enter the source and destination MAC address as the QoS

Classification Criteria. The format should be xx:xx:xx:xx:xx:xx

Source/destination MAC Mask: MAC mask is similar to IP mask, and the format also should be xx:xx:xx:xx:xx:xx. It is used to hide some information of the MAC address. '1', means needed and '0' means ignored. For example, MAC address e0:3b:4a:c2:ca:e2 and MAC mask ff:ff:ff:00:00:00, that is whatever MAC address while matches e0:3b:4a:XX:XX:XX, will be accepted.

Specify Classification Results

Enter or select appropriate parameters you want for the packets matched the above classification criteria in the following fields. You have to choose a classification queue. A blank mark or tag value means no change.

Specify Classification Queue: assign classification queue from the drop-down box. If you want to select the queue, you should make sure the specific queue is enabled in Queue Config section.

Mark Differentiated Service Code Point (DSCP): select the DSCP you want to be the new DSCP for the packets which matched the above classification criteria.

Mark 802.1p priority: it is a LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization. It is interoperable with IEEE 802.1Q. 802.1p has 8 kinds of priority.

☞ Note: 802.1p/vlan tag feature be supported only when in bridge mode, DSL WAN interface.

➤ IP QoS

● LAN to WAN IP QoS

1. It is a QoS controlling the traffic from LAN to WAN. So first make sure there is at least one WAN queue. If you have configured WAN interface and it will appeared as a default queue, you can also add other queues of the specific interface. See Queue Config.

Here we have a atm0 (WAN interface), the interface has a default queue. Make sure to enable the queue.

Name	Key	Interface	Scheduler Alg	Precedence	Weight	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	SP	1				Enabled	
WMM Voice Priority	2	wl0	SP	2				Enabled	
WMM Video Priority	3	wl0	SP	3				Enabled	
WMM Video Priority	4	wl0	SP	4				Enabled	
WMM Best Effort	5	wl0	SP	5				Enabled	
WMM Background	6	wl0	SP	6				Enabled	
WMM Background	7	wl0	SP	7				Enabled	
WMM Best Effort	8	wl0	SP	8				Enabled	
Default Queue	33	atm0	SP	8		Path0		<input checked="" type="checkbox"/>	

2. In QoS Classification Setup page, Click Add to add a QoS Classification.

QoS Classification Setup -- A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.

If you disable WMM function in Wireless Page, classification related to wireless will not take effects

		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS					
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Enable	Remove

Then in the appeared Add Network Traffic Class Rule page, enter the information to set up a rule.

1) Specify the rule name, rule order, and rule status.

Traffic Class Name:

Rule Order:

Rule Status:

2) Specify the classification criteria. Here you can set every parameter to strictly control the specific traffic or you can set several parameters to let them be the key elements to control the traffic. A blank criterion indicates it is not used for classification.

Specify Classification Criteria

A blank criterion indicates it is not used for classification.

Class Interface:	LAN
Ether Type:	IP (0x800)
Source MAC Address:	00:0e:f4:23:45:12
Source MAC Mask:	ff:ff:ff:00:00:00
Destination MAC Address:	00:23:22:23:22:22
Destination MAC Mask:	ff:ff:ff:ff:ff:ff
Source IP Address[/Mask]:	192.168.1.12
Destination IP Address[/Mask]:	12.63.23.22
Differentiated Service Code Point (DSCP) Check:	AF11 (001010)
Protocol:	TCP
UDP/TCP Source Port (port or port:port):	80
UDP/TCP Destination Port (port or port:port):	80

3) Specify the classification results. Here you must Assign Classification Queue. Whether the following parameters are needed is according to your needs. If you do not want to change the original information, please leave it empty. The queues listed here in the Assign Classification Queue are WAN interface queues set in Queue Config section. Select the needed queue. If you find none queues here, turn back to check whether you have configured a queue and enable it.

Specify Classification Results

Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:	ppp0&atm0&Path0&Key33&Pre8
Mark Differentiated Service Code Point (DSCP):	
Mark 802.1p priority:	
Tag VLAN ID [0-4094]:	

3. Click Apply to save your settings. The added rule will listed as below.

QoS Classification Setup -- A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.

If you disable WMM function in Wireless Page, classification related to wireless will not take effects

		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS					
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Enable	Re
upstream	1	LAN	IP	00:0e:f4:23:45:12/ ff:ff:ff:00:00:00	00:23:22:23:22:22/ ff:ff:ff:ff:ff:ff	192.168.1.12	12.63.23.22	TCP	80	80	AF11		33				<input checked="" type="checkbox"/>	

● WAN to LAN IP QoS

1. Here we take WAN to LAN (ETH1) QoS for example. Make sure there are enabled port ETH1 based queues here. LAN queues need your configuration. You can enable wireless to enable WMM queues by default or add ETH0-ETH4 ported based queues manually.

LAN	34	eth1	SP	1				<input checked="" type="checkbox"/>	<input type="checkbox"/>
-----	----	------	----	---	--	--	--	-------------------------------------	--------------------------

2. In QoS Classification Setup page, Click Add to add a QoS Classification.

QoS Classification Setup -- A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.

If you disable WMM function in Wireless Page, classification related to wireless will not take effects

		CLASSIFICATION CRITERIA										CLASSIFICATION RESULTS					
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Enable
upstream	1	LAN	IP	00:0e:f4:23:45:12/ff:ff:ff:00:00:00	00:23:22:23:22:22/ff:ff:ff:ff:ff:ff	192.168.1.12	12.63.23.22	TCP	80	80	AF11		33				<input checked="" type="checkbox"/>

Then in the Add Network Traffic Class Rule page, enter the information to set up a rule.

Traffic Class Name:

Rule Order:

Rule Status:

Specify Classification Criteria

A blank criterion indicates it is not used for classification.

Class Interface:

Ether Type:

Source MAC Address:

Source IP Address[/Mask]:

Destination IP Address[/Mask]:

Differentiated Service Code Point (DSCP) Check:

Protocol:

UDP/TCP Source Port (port or port:port):

UDP/TCP Destination Port (port or port:port):

Specify Classification Results

Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:

Mark Differentiated Service Code Point (DSCP):

3. Click Apply to save your settings. The added rule will be listed as below.

QoS Classification Setup -- A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.

If you disable WMM function in Wireless Page, classification related to wireless will not take effects

		CLASSIFICATION CRITERIA										CLASSIFICATION RESULTS				
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag
upstream	1	LAN	IP	00:0e:f4:23:45:12/ff:ff:ff:00:00:00	00:23:22:23:22:22/ff:ff:ff:ff:ff:ff	192.168.1.12	12.63.23.22	TCP	80	80	AF11		33			
downstream	2	WAN	IP	00:0c:12:1a:11:11		13.36.25.11/8	192.168.1.23/24	TCP	80	80	AF13		34			

➤ Port based QoS

Take port ETH0 to WAN QoS for example.

1. First make sure there is at least a WAN queue and it is enabled.

Name	Key	Interface	Scheduler Alg	Precedence	Weight	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	SP	1				Enabled	
WMM Voice Priority	2	wl0	SP	2				Enabled	
WMM Video Priority	3	wl0	SP	3				Enabled	
WMM Video Priority	4	wl0	SP	4				Enabled	
WMM Best Effort	5	wl0	SP	5				Enabled	
WMM Background	6	wl0	SP	6				Enabled	
WMM Background	7	wl0	SP	7				Enabled	
WMM Best Effort	8	wl0	SP	8				Enabled	
Default Queue	33	atm0	SP	8		Path0		<input checked="" type="checkbox"/>	
LAN	34	eth1	SP	1				<input checked="" type="checkbox"/>	<input type="checkbox"/>
ETH	35	eth0	SP	1				<input checked="" type="checkbox"/>	<input type="checkbox"/>

2. In QoS Classification Setup page, Click Add to add a QoS Classification.

QoS Classification Setup -- A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.

If you disable WMM function in Wireless Page, classification related to wireless will not take effects

CLASSIFICATION CRITERIA														CLASSIFICATION RESULTS			
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	
upstream	1	LAN	IP	00:0e:f4:23:45:12/ff:ff:ff:00:00:00	00:23:22:23:22:22/ff:ff:ff:ff:ff:ff	192.168.1.12	12.63.23.22	TCP	80	80	AF11		33				
downstream	2	WAN	IP	00:0c:12:1a:11:11		13.36.25.11/8	192.168.1.23/24	TCP	80	80	AF13		34				

Add Enable Remove

Then in the Add Network Traffic Class Rule page, enter the information to set up a rule to your needs. To Assign Classification queue, select the needed WAN queue.

Traffic Class Name:

Rule Order:

Rule Status:

Specify Classification Criteria
 A blank criterion indicates it is not used for classification.

Class Interface:

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Specify Classification Results
 Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:

Tag VLAN ID [0-4094]:

3. Click Apply to save your settings and the added rule will be listed as below.

CLASSIFICATION CRITERIA														CLASSIFICATION RESULTS			
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	
upstream	1	LAN	IP	00:0e:f4:23:45:12/ff:ff:ff:00:00:00	00:23:22:23:22:22/ff:ff:ff:ff:ff:ff	192.168.1.12	12.63.23.22	TCP	80	80	AF11		33				
downstream	2	WAN	IP	00:0c:12:1a:11:11		13.36.25.11/8	192.168.1.23/24	TCP	80	80	AF13		34				
ETH0-WAN	3	eth0	PPPoE_DISC	00:23:22:ae:12:22/ff:ff:ff:00:00:00	12:11:11:21:a1:1a/ff:ff:ff:00:00:00								33	AF12	1	200	

Add Enable Remove

Appendix : Frequent Asked Questions

Q: None of the LEDs are on when you power on the ADSL router?

A: Please make sure what you use is the power adaptor attached with the ADSL router package and checks the connection between the AC power and ADSL router.

Q: DSL LED does not turn on after connect telephone line?

A: Please make sure what you use is the standard telephone line (as attached with the package), make sure the line is connected correctly and check whether there is poor contact at each interface. Wait for 30 seconds to allow the ADSL router establishes connection with you ADSL operator.

Q: DSL LED is in the circulation of slow-flashing and fast-flashing after connecting telephone line?

A: This situation means the ADSL router is in the status of failing to establish connection with Central Office. Please check carefully and confirm whether the ADSL router has been installed correctly.

Q: LAN LED does not turn on after connect Ethernet cable?

A: Please make sure Ethernet cable is connected hub/PC and ADSL router correctly. Then please make sure the PC/hub have been power on.

Please make sure that you use parallel network cable to connect UpLink port of hub, or use parallel network cable to connect PC. If connect normal port of hub (not UpLink port), you must use cross-cable. Please make sure that your network cables meet the networking requirements above.

Q: PC cannot access the Router?

A: Please make sure that all devices communicating with the device must use the same channel (and use the same SSID). Otherwise your PC will not find the wireless Router.

Q: PC cannot access the Internet?

A: First check whether PC can ping the interface Ethernet IP address of this product successfully (default value is 192.168.1.1) by using ping application. If ping application fails, please check the connection of Ethernet cable and check whether the states of LEDs are in gear.

If the PC uses private IP address that is set manually (non-registered legal IP address), please check:

1. Whether IP address of the PC gateway is legal IP address. Otherwise please use the right gateway, or set the PC to Obtain an IP address automatically.
2. Please confirm the validity of DNS server appointed to the PC with ADSL operator. Otherwise please use the right DNS, or set the PC to Obtain an IP address automatically.
3. Please make sure you have set the NAT rules and convert private IP address to legal IP address. IP address range of the PC that you specify should meet the setting range in NAT rules.
4. Central Office equipment may have problem.
5. The country or the wireless network type you selected is wrong.

Q: PC cannot browse Internet web page?

A: Please make sure DNS server appointed to the PC is correct. You can use ping application program to test whether the PC can connect to the DNS server of the ADSL operator.

Q: Initialization of the PVC connection failed?

A: Be sure that cable is connected properly from the DSL port to the wall jack. The DSL LED on the front panel of the ADSL router should be on. Check that your VPI, VCI, type of encapsulation and type of multiplexing setting are the same as what you collected from your service provider, Re-configure ADSL router and reboot it. If you still cannot work it out, you may need to verify these variables with the service provider.

If the cause is not given above, please contact your local service provider!