1532a ADSL Wireless N
Router User Manual

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.

Content

1 Overview

Thank you for choosing our product. The 1532a ADSL Wireless N router combining an ADSL modem, an 802.11n wireless router and a 4-port switch in one unit, bringing high-speed wireless Internet connection to a home or an office.

1.1 Features

1.1.1 Data rate

- Downstream data rate up to 24Mbps,

- Upstream data rate up to 1Mbps

1.1.2 ADSL Compliant

- ITU G.992.1 (G.DMT)

- 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 802.11b & IEEE 802.11g compatible.

- IEEE 802.11n draft 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 - 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:

- ADSL ROUTER   x 1

- Antenna   x 2

- Base   x 1

- External Splitter   x 1

- Power Adapter   x 1

- Telephone Line   x 1

- Ethernet Cable   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

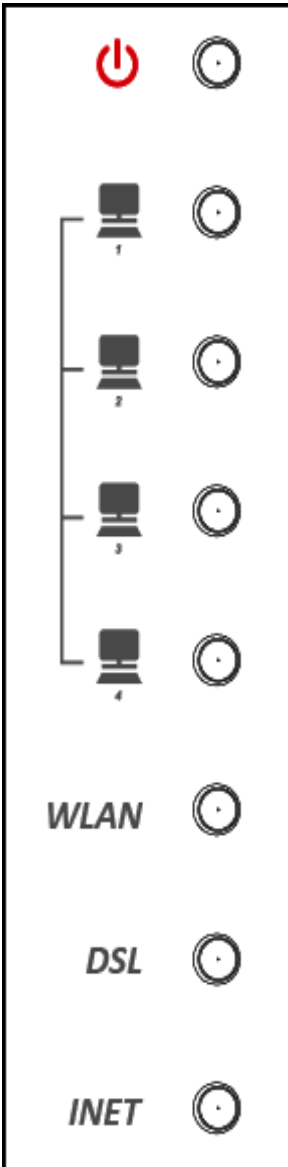The device is configured with the following factory defaults:

- 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 lightening.

- 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
PWR	Solid Green	Power on
	Off	Power off
LAN1,2,3,4	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	Solid Green	IP connected
	Off	Modem power off, modem in bridged mode or ADSL connection not present
	Flickering Green	IP connected and IP Traffic is passing thru the device

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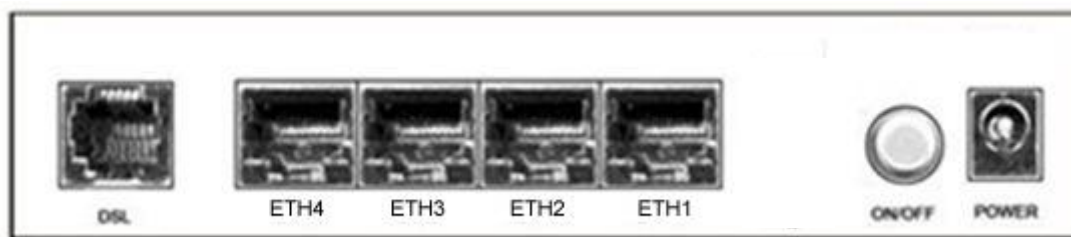
Port	Function
DSL	Connect the device to an ADSL telephone jack or splitter using a RJ-11 telephone cable
ETH1,2,3,4	Connect the device to your PC's Ethernet port, or to the uplink port on your hub/switch, using a RJ-45 cable
ON/OFF	Switch it on or off
POWER	Connect to the supplied power adapter

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.

1. 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
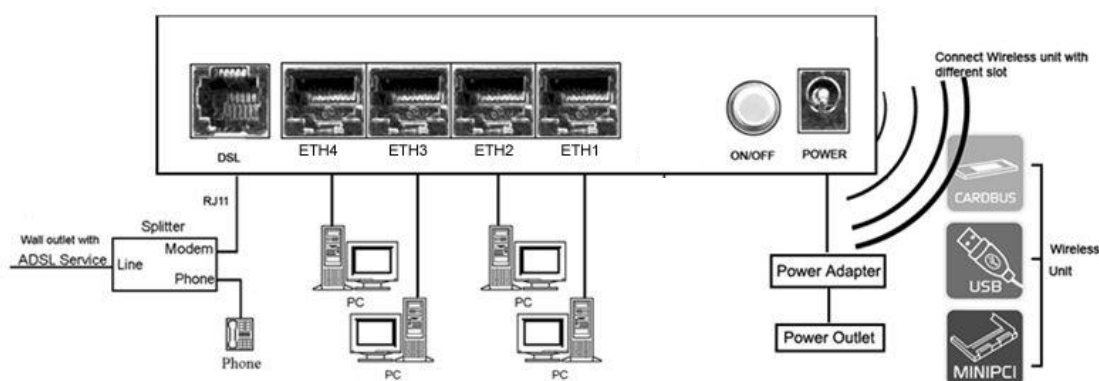   **LINE** port of the splitter.

    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

2. Using an Ethernet Cable to connect the LAN port of the ROUTER to your
    LAN or a PC with network card installed.

3. Connect the power cable to the PWR connector on ROUTER, then plug in
    the AC power adapter to the AC 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

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 page.

Enter username '**admin**' and password '**adslroot**'

Click **OK**
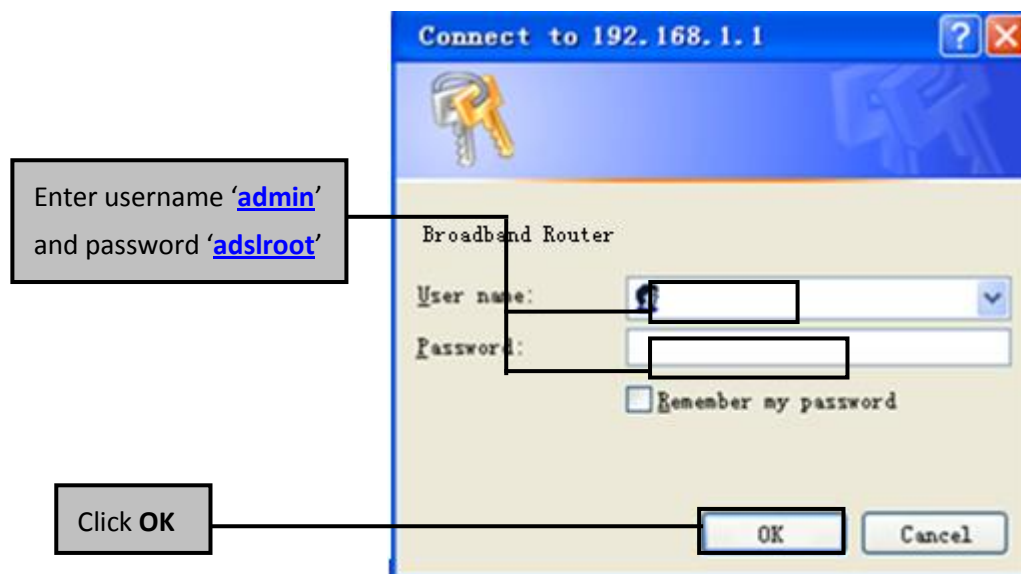
After log on ,you will see the following screen :

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 1532a. 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 Mode 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 can choose **Add**, or **Remove** to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove

Add 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]   0

VCI: [32-65535] 35

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: LLC/SNAP-BRIDGING ▾

Service Category: UBR Without PCR ▾

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

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit

Add   Remove

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

atm0/(0_0_35) ▾

Back   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: pppoe_0_0_35

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: [AUTO   ▼]

☐ 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

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.

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.

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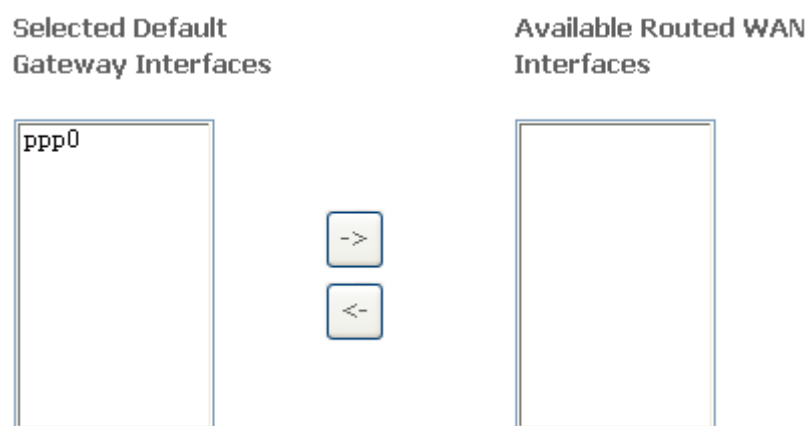
8. Get DNS server information from the selected WAN interface or enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

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:	Disabled

5.2.2 Router Mode Setup

1. 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

Add   Remove

15

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

Select a ETH port:

eth0/ENET1 ▾

Select Connection Mode
◉ Default Mode - Single service over one connection
○ VLAN MUX Mode - Multiple Vlan service over one connection

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 MSC mode as connection mode.

eth0/ENET1 ▾
eth0/ENET1
eth2/ENET3
eth3/ENET4
eth1/ENET2

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

Interface/(Name)	Connection Mode	Remove
eth1/ENET2	DefaultMode	☐

Remove

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

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit

Add   Remove

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

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

eth1/ENET2

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

Enter Service Description: pppoe_eth1

Back   Next

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: AUTO

☐ 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

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.

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.

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:

a) It allows only one computer on the LAN.

b) The public IP address assigned by the remote using the PPP/IPCP 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.

c) NAPT and firewall are disabled when this option is selected.

d) The gateway becomes the default gateway and DNS server to the computer through DHCP using the LAN interface IP address.

e) 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.

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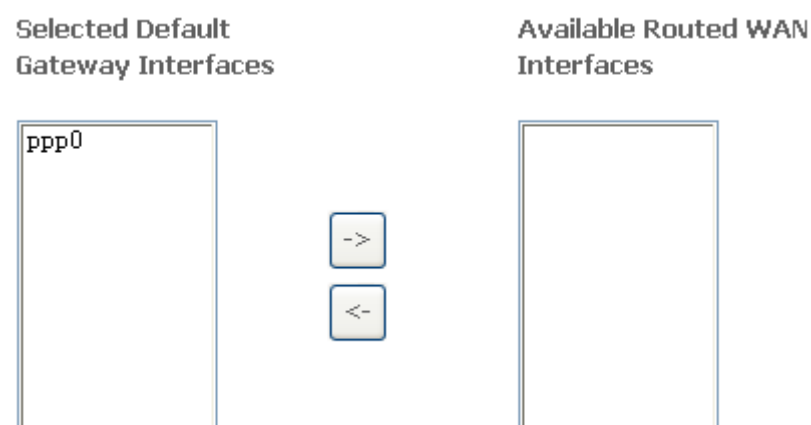
10. Get DNS server information from the selected WAN interface or enter static DNS server IP addresses. Click **Next**.

⊙ Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces   Available WAN Interfaces

ppp0		

->

<-

○ 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:	Disabled

5.2.3 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).

Local Area Network (LAN) Setup

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

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

☐ Enable IGMP Snooping

☐ Enable LAN side firewall

○ Disable DHCP Server
◉ Enable DHCP Server
   Start IP Address: 192.168.1.2
   End IP Address: 192.168.1.254
   Leased Time (hour): 24
   Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove

   [Add Entries]   [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.
Leased 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).

Note: If you want to cancel all modification that you do on the Router, please select from "Management⇨Setting⇨Restore Default Settings" to restore factory default settings.

5.3 Wireless setting

5.3.1 Basic

☑ Enable Wireless

☐ Hide Access Point

☐ Clients Isolation

☐ Disable WMM Advertise

☐ Enable Wireless Multicast Forwarding (WMF)

SSID: KasdaD3FC6A

BSSID: 00:0E:F4:D3:FC:6B

Country: UNITED STATES

Max Clients: 16

Option	Description
Enable wireless	A check box that enables or disables the wireless LAN interfaces. The default is to enable wireless communications.
Hide Access Point	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. 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. 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.
Clients isolation	Enable this item if you don't want your wireless clients to communicate with each other.
Network name (SSID)	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. 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 Advanced Settings

This page is where user specifies a number of advanced settings for wireless communications.

Note: After making any changes, click **Apply** to save.

Warning: The settings shown above are default settings. Changes made to these items can cause wireless communication problems.

Field	Description
Band	This is the range of frequencies the gateway will use to communicate with

	user's wireless devices.
Channel	Drop-down menu that allows selection of specific channel.
54g^{TM} Rate	This drop-down list lets user specify the wireless communication rate, which can be **Auto** (uses the highest rate when possible, or else a lower rate) or a fixed rate between 1 and 54 Mbps.
Multicast rate	This drop-down list lets user specify the wireless communication rate for multicast packets, which are sent to more than one destination at a time. The value can be **Auto** (uses the highest rate when possible, or else a lower rate) or a fixed rate between 1 and 54 Mbps.
Basic rate	User has the option of supporting all rates listed in **Rate** above or using the 1-, 2-Mbps rates, which support only older 802.11b implementations.
Fragmentatio n threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 connection, packets that are larger the fragmentation threshold are split into smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between **256** and **2346**. If user experience a high packet error rate, try to increase this value slightly. Setting the fragmentation threshold too low may result in poor performance.
RTS threshold	This is number of bytes in the packet size beyond which the gateway invokes its RTS/CTS (request to send, clear to send) mechanism. Packets larger than this threshold trigger the RTS/CTS mechanism, while the gateway transmits smaller packets without using RTS/CTS. The default setting of **2347**, which is the maximum, disables the RTS threshold mechanism.
DTIM interval	A delivery traffic indication message (DTIM), also known as a beacon, is a countdown informing wireless clients of the next window for listening to broadcast and multicast messages. When the gateway has broadcast or multicast messages for its clients, it sends its next DTIM message with this DTIM interval value. The clients hear the beacons and awaken as needed to receive the broadcast and multicast messages.
Beacon interval	The amount of time (in milliseconds) between beacon transmissions, each of which identifies the presence of an access point. By default, wireless

	clients passively scan all radio channels, listening for beacons coming from access points. Before a client enters power-save mode, it needs the beacon interval to determine when to wake up for the next beacon (and learn whether the access point has any messages for it). User can enter any value between **1** and **65535**, but the recommended range is **1 - 1000**.
XPress™ Technology	**XPress™ Technology** is a feature in which two of our devices can communicate with each other at twice the normal rate. 54g+ is a technology that achieves higher throughput with frame-bursting. With 54g+ enabled, aggregate throughput (the sum of the individual throughput of each network client) improves by up to 25% in 802.11g-only networks, and up to 75% in mixed networks containing both 802.11g and 802.11b equipment.

5.3.3 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.

WPS Setup

Enable **WPS**   Disabled ▾

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
Click "Apply/Save" when done.

Select SSID: KasdaD3FC6A ▾

Network Authentication: Open ▾

WEP Encryption: Disabled ▾

Apply/Save

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

WPS Setup

Enable **WPS**   Disabled

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
Click "Apply/Save" when done.

Select SSID: KasdaD3FC6A

Network Authentication: WPA-PSK

WPA/WAPI passphrase: ●●●●●●●●●●   Click here to display

WPA Group Rekey Interval: 0

WPA/WAPI Encryption: TKIP+AES

WEP Encryption: Disabled

Apply/Save

3.Enable WPS as below.

WPS Setup

Enable **WPS**   Enabled

Add **Client** (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)
            ⦿ Push-Button ○ Enter STA PIN ○ Use AP PIN   Add Enrollee

Set **WPS AP Mode**   Configured

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

Device PIN   16870635   Help

Config AP

4.Set WPS AP mode as **Unconfigured** and click **Config AP**.

WPS Setup

Enable **WPS**   Enabled ▼

Add **Client** (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)
⦿ Push-Button ◯ Enter STA PIN ◯ Use AP PIN   Add Enrollee

Set **WPS AP Mode**   Unconfigured ▼

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

Device PIN   16870635   Help

Config AP

5. Set WPS AP mode as **configured** and click **Save/Apply.**

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

7. 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.

Select SSID: KasdaD3FC6A ▼

Network Authentication: Open ▼

WEP Encryption: Enabled ▼
Encryption Strength: 128-bit ▼
Current Network Key: 1 ▼
Network Key 1:   1234567890123
Network Key 2:   1234567890123
Network Key 3:   1234567890123
Network Key 4:   1234567890123
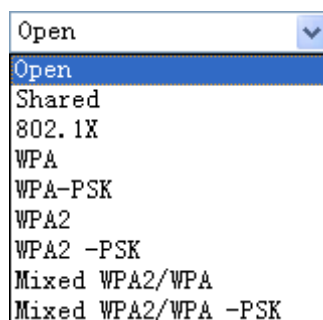   Enter 13 ASCII characters or 26 hexadecima
                              Enter 5 ASCII characters or 10 hexadecimal

Apply/Save

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 Management

5.4.1 Remote Access

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

1. Select Advanced Setup=>Security=>IP Filtering=>Incoming and Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove

Add   Remove

2.Click Add to add rules. If you want to do remote ping test, please select protocol as ICMP; If you want to do Http or Telnet test, please select protocol as TCP/UDP. If you want only Http remote access, you can set destination port as 80; If you want only Telnet remote access, you can set destination port as 23; If you want both, you can set destination port as blank.

Filter Name:

IP Version: IPv4
Protocol:
Source IP address[/prefix length]:
Source Port (port or port:port):
Destination IP address[/prefix length]:
Destination Port (port or port:port):

3.Click Apply/Save and select Device Info=>WAN. You can see the IP address of WAN interface

Interface	Description	Type	VlanMuxId	Igmp	NAT	Firewall	Status	IPv4 Address
atm0	ipoe_0_1_35	IPoE	Disabled	Disabled	Disabled	Disabled	Connecting	0.0.0.0

4. Now you can access the ADSL router remotely using username **support** and password **support**. You can input http://x.x.x.x/ for Http and input telnet x.x.x.x for Telnet.

5.4.2 TR-069 Client

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Inform	⦿ Disable ◯ Enable
Inform Interval:	300
ACS URL:	
ACS User Name:	admin
ACS Password:	•••••
WAN Interface used by TR-069 client:	Any_WAN ▾
Display SOAP messages on serial console	⦿ Disable ◯ Enable
☑ Connection Request Authentication	
Connection Request User Name:	admin
Connection Request Password:	•••••
Connection Request URL:	

[Apply/Save]   [GetRPCMethods]

Inform: Whether or not the CPE must periodically send CPE information to Server using the Inform method call.

Inform Interval: The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method if Inform is enabled.

ACS URL: URL for the CPE to connect to the ACS using the CPE WAN Management Protocol.

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

ACS Password: Password used to authenticate an ACS making a Connection Request to the CPE. When read, this parameter returns an empty string, regardless of the actual value.

WAN Interface used by TR-069 client: Remember to choose the interface of PVC used for TR069

Connection Request User Name: Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for authentication of the CPE.

Connection Request Password: Password used to authenticate the CPE when

making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for authentication of the CPE.

GetRPCMethods: Used by a CPE or ACS to discover the set of methods supported by the ACS or CPE it is in communicate with.

5.4.3 Printer Server Installations

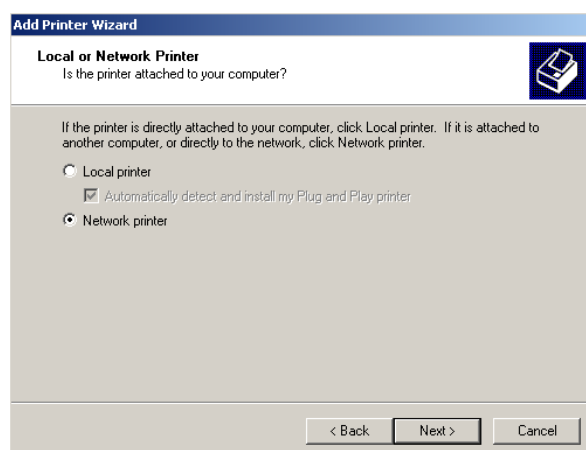1. Click "Advanced setup⇨Print Server" and then Check "**Enable on-board printer server**" and key in "**Printer name**", "**Make and model**"
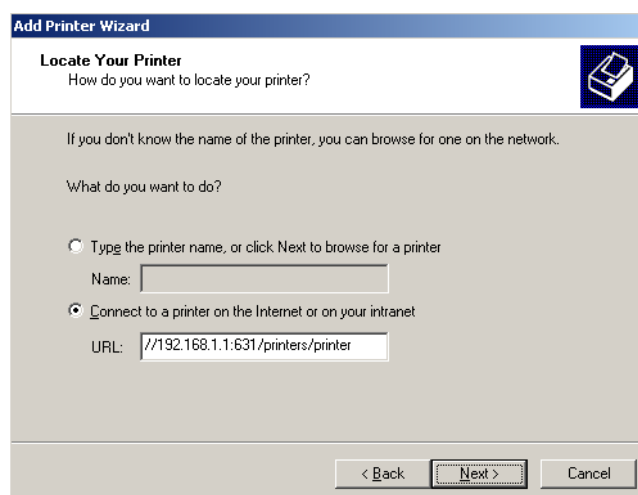

2. Click on Add a printer from **Control Panel** of the Windows computer and click "Next".
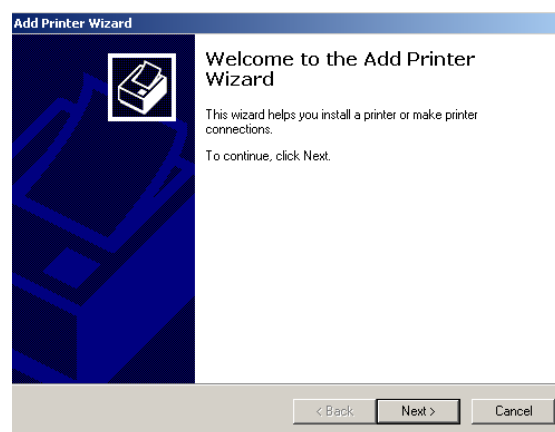
3. Select "Network Printer" and click "Next".

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".
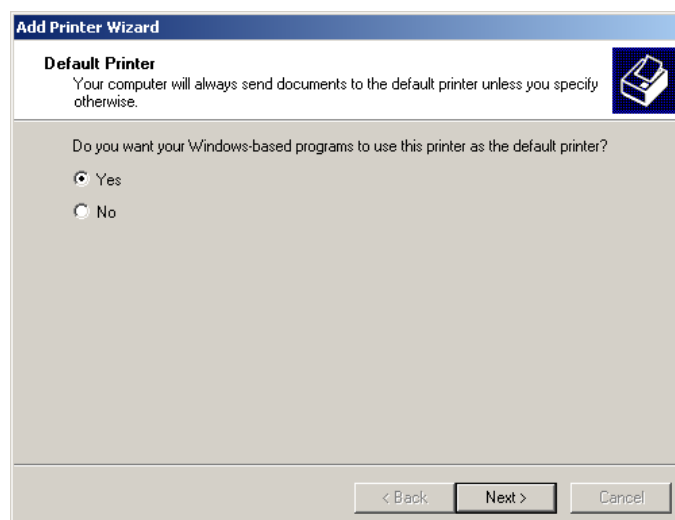
7.   Click "Finish".

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!

RF exposure information: To maintain compliance with FCC RF exposure requirements, use handset that maintain a 20cm separation distance between the user's body and the host. MPE limit for RF exposure at prediction frequency is 0.161mW/cm^2. It satisfy RF exposure compliance.

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

NOTE: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
 - Reorient or relocate the receiving antenna.
 - Increase the separation between the equipment and receiver.
 -Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
 -Consult the dealer or an experienced radio/TV technician for help