



User Manual

**CDD530AM-003/ CDD531AM-U03
WiFi ADSL2/2+ RG**

Copyright

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

Trademarks

All products, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

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

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

FCC Part 15.21 information for user

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B.

FCC Part 15.19 Caution:

1. 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
2. This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.
3. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment. **IMPORTANT NOTE:** FCC Radiation Exposure Statement: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

FCC Radiation Exposure Statement:

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




TABLE OF CONTENTS

Copyright	2
Chapter 1 Introduction.....	5
Chapter 2 Getting Started	10
Chapter 3 Making Configuration.....	18
Chapter 4 Troubleshooting	82

Chapter 1 . Introduction

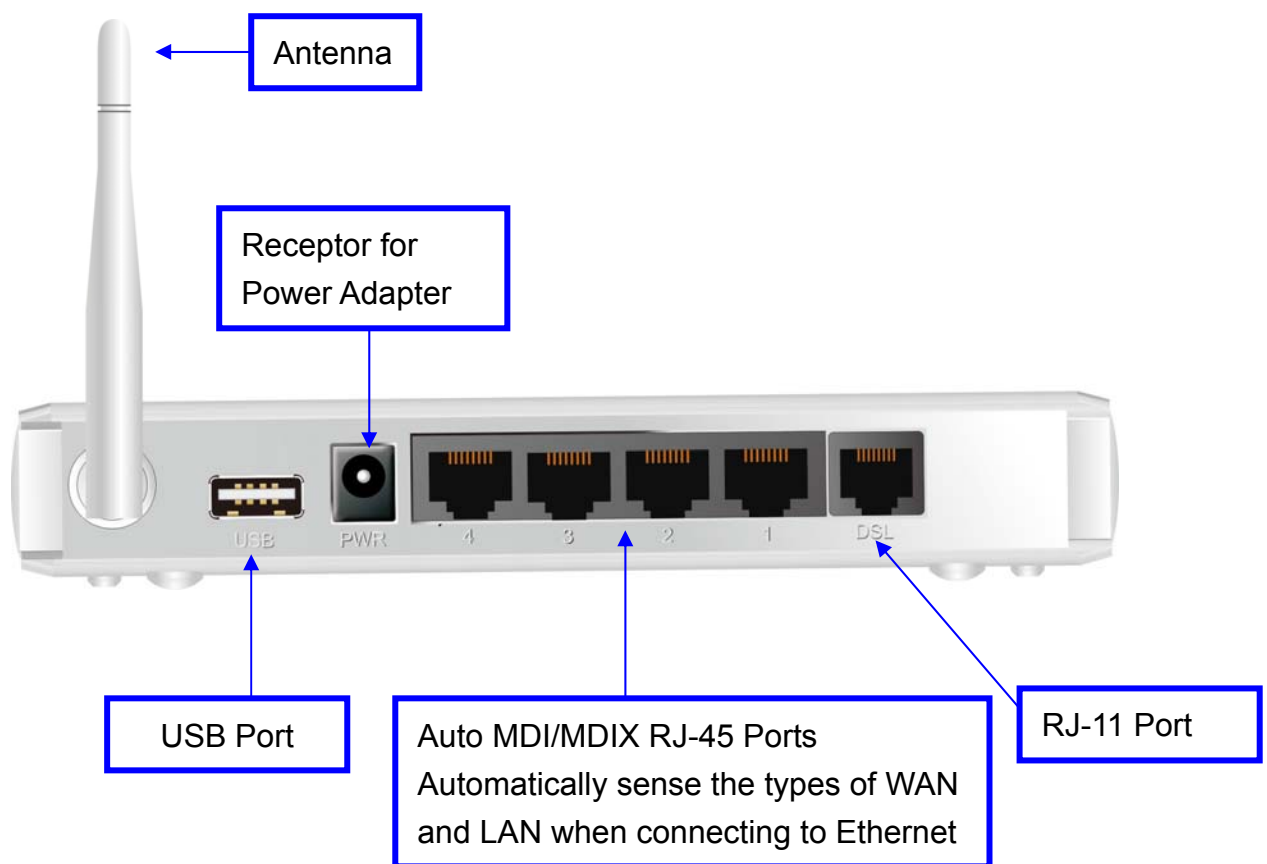
Congratulations on your purchase of this outstanding product: CDD531AM-U03 WiFi ADSL RG. This residential gateway is specifically designed for those who need to have the data, voice, video and file sharing services beyond his home and office. It provides a complete solution for Internet surfing and broadband sharing. Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read this manual carefully for fully exploiting the functions of this product.

1.1 Package List

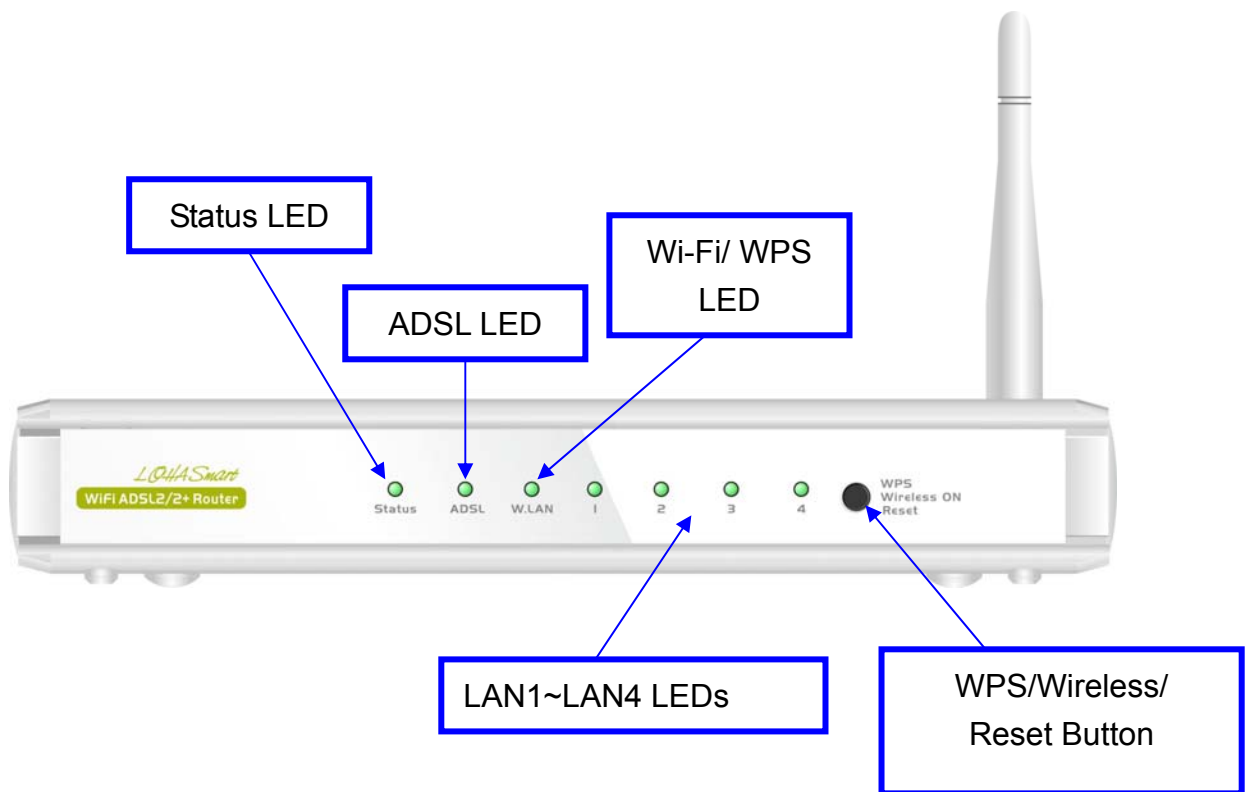
Items	Description	Contents	Quantity
1	WiFi ADSL RG		1
2	Power adapter		1
3	CD		1

1.2 Hardware Installation

1.2.1 Hardware configuration



Note : CDD530-003 without USB Port



1.2.2 LED indicators

	LED Status	Description
Status (USB)	Green in flash	power is on
	Green in fast flash	Reset mode
	Green	USB storage attached (only for CDD531-U03)
	Green in flash	Data access
ADSL	Green in flash	xDSL connection is established
	Green in fast flash	Data packet transferred via DSL Line
WLAN	Green	WiFi is on.
	Green in flash	Data access
LAN	Green	RJ45 cable is plugged, and Ethernet connection is established.
	Green in flash	Data access

How to Operate

Step 1.

Plug the RJ45 cable into LAN port 1~4 and connect with your PC or NB.



Step 2.

Plug your RJ-11 into the DSL port and connect with your xDSL modem.



Step 3.

Plug the power jack into it.



Step 4

Prepare a USB Storage or 3G dongle, and then plug into the USB port.



Chapter 2 Getting Started

Please use windows EZ setup utility or Web UI wizard to enter the setup process.

2.1 Easy Setup by Windows Utility

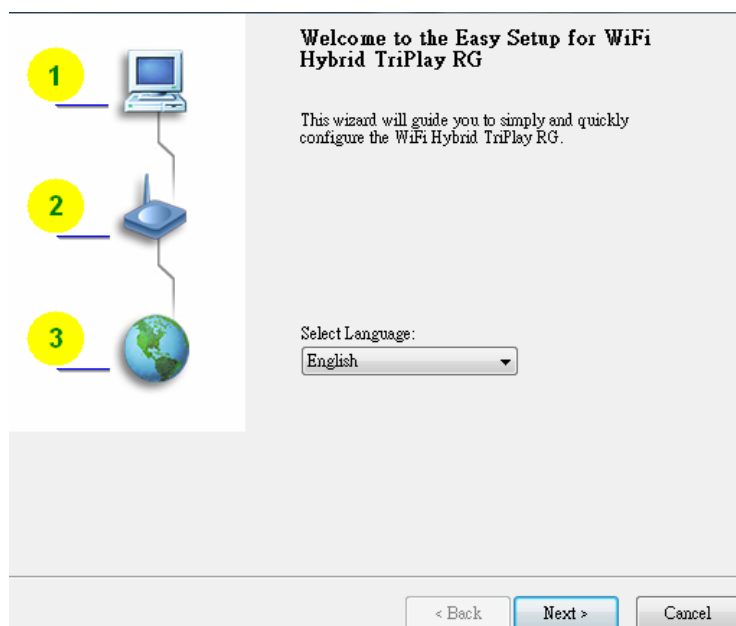
Step 1.

Install the Easy Setup Utility from the provided CD then follow the steps to configure the device.



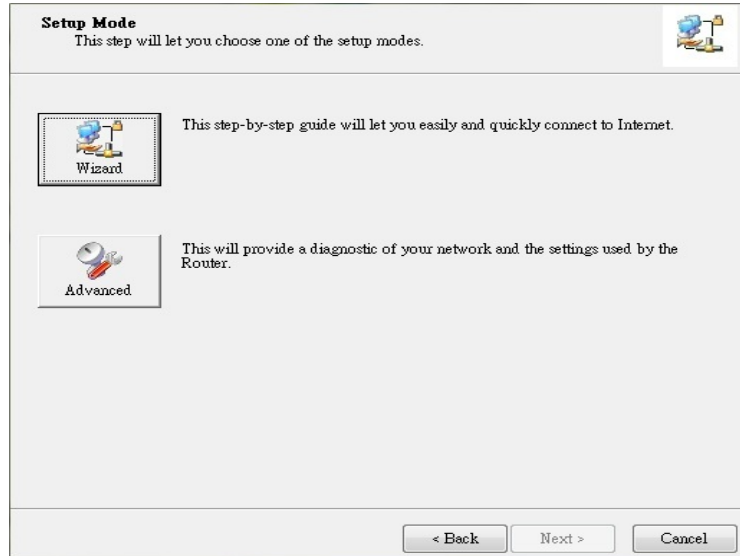
Step 2.

Select Language then click "Next" to continue.



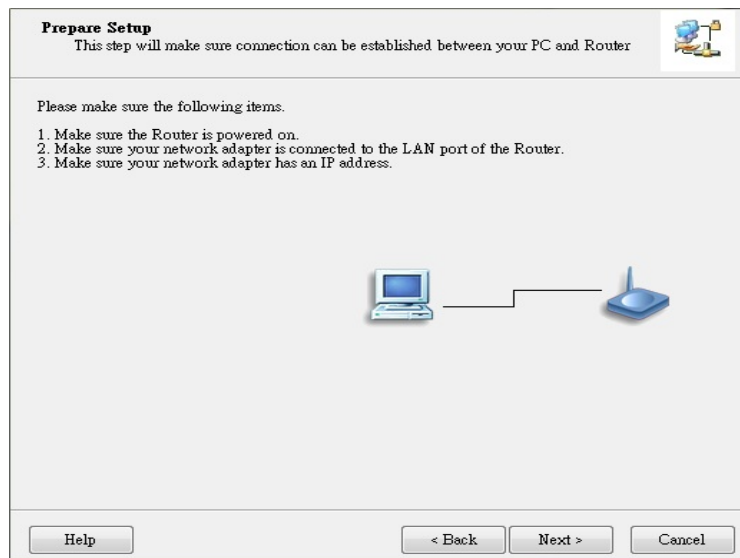
Step 3.

Then click the "Wizard" to continue.



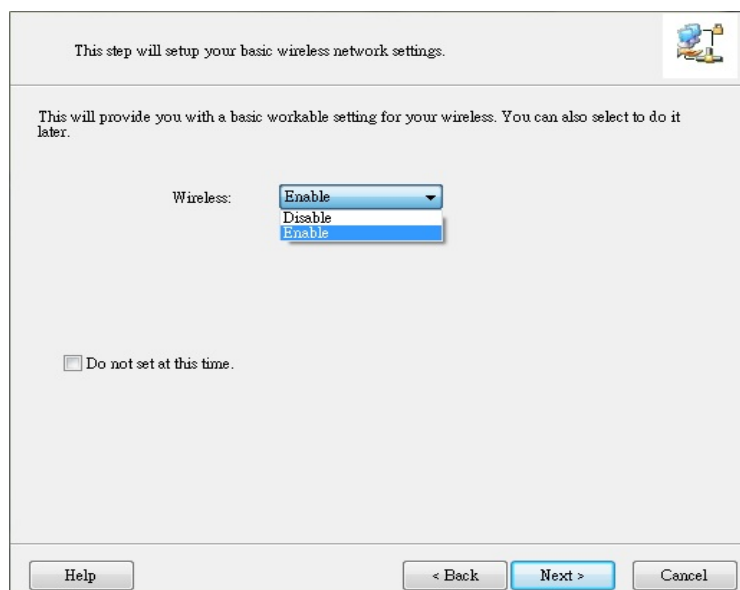
Step 4.

Click "Next" to continue.



Step 6.

Select Wireless Enable, and then click "Next" to continue.



Step 7.

Enter SSID, Channel and Security options, and then click "Next" to continue.

This step will setup your basic wireless network settings.

Please assign the parameters to your wireless networking. If you need more settings, please login to the Router's configuration page.

SSID: default
Channel: 6
Security: WEP
Key: ●●●●●●●●


Help < Back Next > Cancel

Step 8.

Select Auto Detect WAN service.

Auto Detect WAN Service
This step will automatically detect one suitable WAN service for Router

Please make sure the WAN cable connection is working between your Router and broadband modem.
You can ignore the WAN cable connection, but the WAN service will not be checked later.
You can set it manually if you know your WAN service type.



Let me select WAN service by myself

Help < Back Next > Cancel

Step 9.

Save the setting.

Save Settings

The settings will be saved to the Router and reboot at the next step.

Wireless Setting
Wireless Mode: AP Only Mode
SSID: default
Channel: 6
Security: Disable

WAN Setting (Dynamic IP Service)

Modify Settings

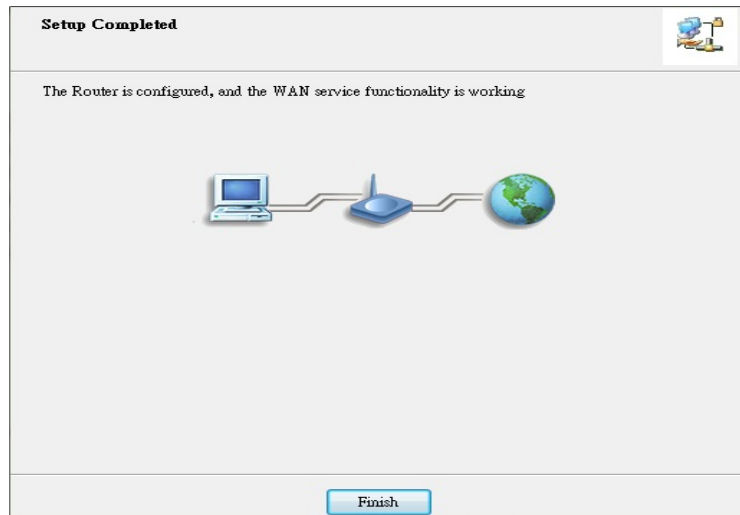
Help < Back Next > Cancel

Step 10.

Congratulations!

Setup is completed.

Now you have already
connected to Internet
successfully.

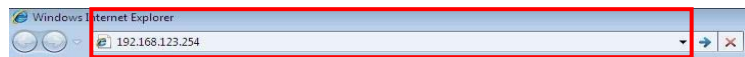


2.3 Easy Setup by Configuring Web UI

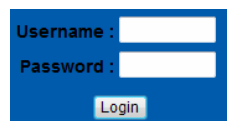
You can also browse UI of the web to configure the device.

Browse to Activate the Setup Wizard

Type in the IP Address
(<http://192.168.123.254>)



Type the default
Username and password
'admin' in the System
Password and then click
'login' button.

A blue login form with two input fields labeled "Username :" and "Password :". Below the fields is a "Login" button.

Select your language.

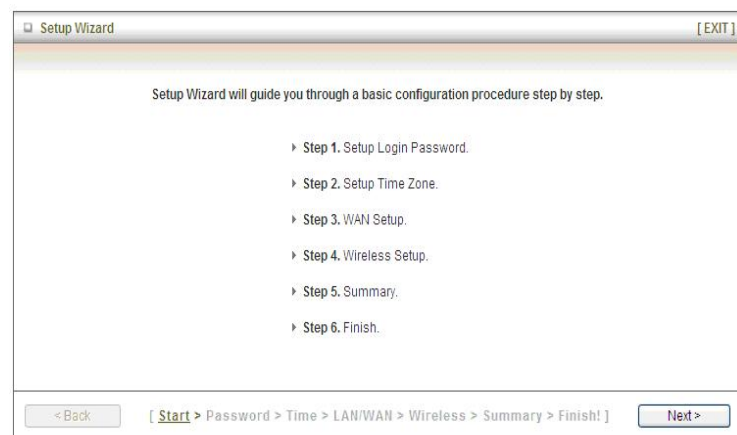


Select "Wizard" for basic
settings in a simple way.



Or, you can go to
basic/advance/application
/system to setup the
configuration by your own
selection.

Press "Next" to start the
Setup Wizard.



Configure with the Setup Wizard

Step 1

You can change the password of administrator here.

The screenshot shows a window titled "Setup Wizard - Setup Login Password" with an "[EXIT]" button in the top right corner. The main area contains three labeled input fields: "Old Password", "New Password", and "Reconfirm", each with a corresponding text box. At the bottom, there is a navigation bar with a "< Back" button, a breadcrumb trail "[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]", and a "Next >" button.

Step 2

Select Time Zone.

The screenshot shows a window titled "Setup Wizard - Setup Time Zone" with an "[EXIT]" button in the top right corner. The main area features a dropdown menu displaying "(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi". Below the dropdown is a "Detect Again" button. At the bottom, there is a navigation bar with a "< Back" button, a breadcrumb trail "[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]", and a "Next >" button.

Step 3

You can select Auto detecting WAN type or setup WAN type manually.

The screenshot shows a window titled "Setup Wizard - Select WAN Type" with an "[EXIT]" button in the top right corner. The main area contains two radio button options: "Auto Detecting WAN Type" (which is selected) and "Setup WAN Type Manually". At the bottom, there is a navigation bar with a "< Back" button, a breadcrumb trail "[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]", and a "Next >" button.

Step 4

The system will detect the WAN type if you choose to let the system detect automatically.

The screenshot shows a window titled "Setup Wizard - Auto Detecting WAN type" with an "[EXIT]" button in the top right corner. The main area displays the text "Please wait a few second...". At the bottom, there is a navigation bar with a "< Back" button, a breadcrumb trail "[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]", and a "Next >" button.

Step 5

Type in Host name and ISP registered MAC address. (if no such information, you can go next)



Setup Wizard - Dynamic IP Address [EXIT]

▶ LAN IP Address: 192.168.123.254

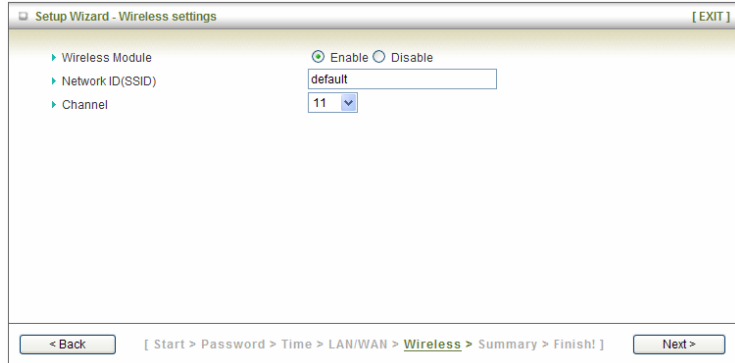
▶ Host Name: [] (optional)

▶ ISP registered MAC Address: [] Clone

< Back [Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!] Next >

Step 5-1

Wireless setting.



Setup Wizard - Wireless settings [EXIT]

▶ Wireless Module: Enable Disable

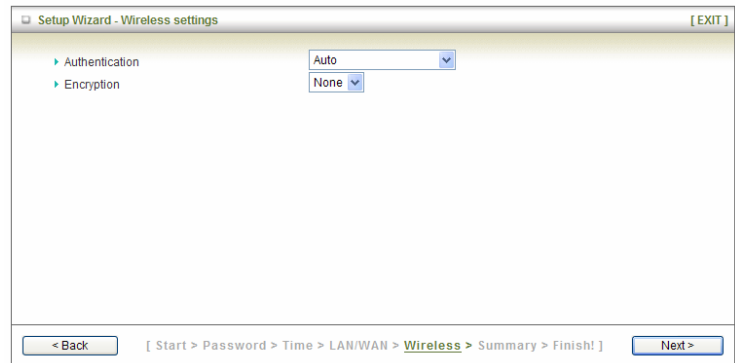
▶ Network ID(SSID): default

▶ Channel: 11

< Back [Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!] Next >

Step 5-2

Wireless authentication and encryption.



Setup Wizard - Wireless settings [EXIT]

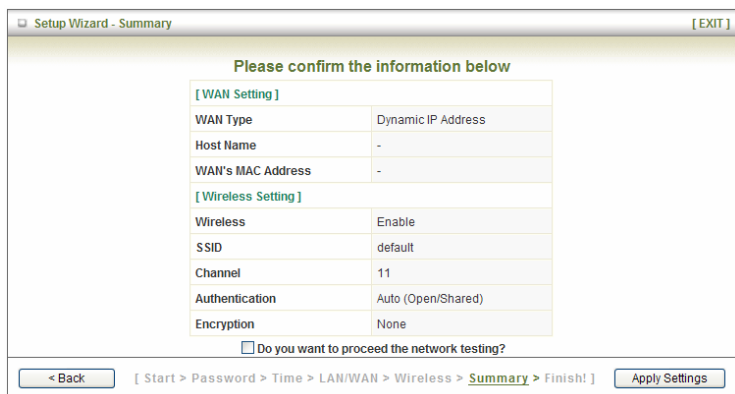
▶ Authentication: Auto

▶ Encryption: None

< Back [Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!] Next >

Step 6

Check the information again.



Setup Wizard - Summary [EXIT]

Please confirm the information below

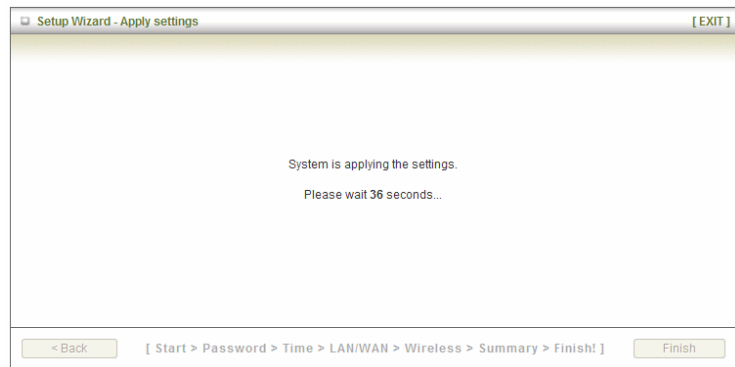
[WAN Setting]	
WAN Type	Dynamic IP Address
Host Name	-
WAN's MAC Address	-
[Wireless Setting]	
Wireless	Enable
SSID	default
Channel	11
Authentication	Auto (Open/Shared)
Encryption	None

Do you want to proceed the network testing?

< Back [Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!] Apply Settings

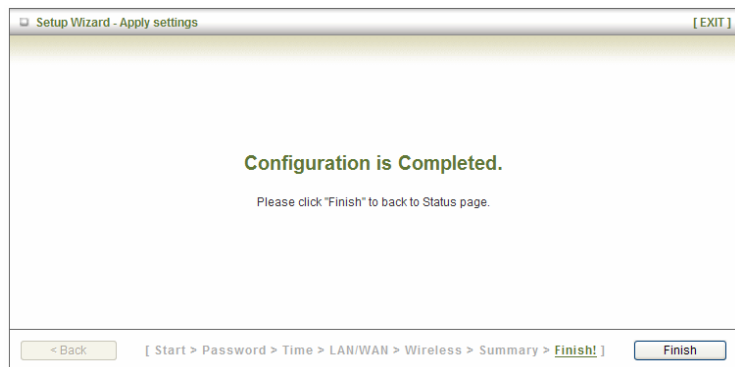
Step 7

System is applying the setting.



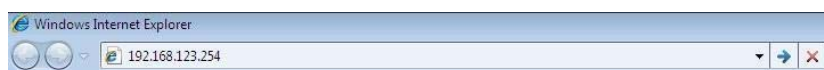
Step 8

Click finish to complete it.



Chapter 3 Making Configuration

Whenever you want to configure your network or this device, you can access the Configuration Menu by opening the web-browser and typing in the IP Address of the device. The default IP Address is: 192.168.123.254.



Enter the default username and password "admin" in the System Password and then click 'login' button.



SSID : default
FW Version: R0.07

Username :
Password :
Login
(default: admin)

Network diagram showing connections to xDSL/Cable, WiFi, Client:0, and Client:1.

Item	WAN Status	Sidenote
Remaining Lease Time	-	
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0, 0.0.0.0	

Afterwards, you can go Wizard, Basic Network, Advanced Network, Application or System respectively on left hand side of web page.



3.1 Basic Network

Status page.

IPv4 System Status [HELP]		
Item	WAN Status	Sidenote
Remaining Lease Time	-	Renew
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0, 0.0.0.0	

IPv6 System Status		
Item	WAN Status	Sidenote
WAN Link-Local Address		
Global IPv6 Address	/64	
LAN IPv6 Link-Local Address		
Link Status		

Wireless Modem Information		
Item	Status	Sidenote
Card Info	HSPA USB MODEM	
Link Status	Disconnected.	
Signal Strength	N/A	
Network Name		

Wireless Status		
Item	WLAN Status	Sidenote
Wireless mode	Enable	(B/G/N Mixed)
SSID	default	
Channel	11	
Security	Auto	(None)

VoIP Status		
Item	Status	Sidenote
VoIP	Unregistered	

Statistics Information		
Statistics of WAN	Inbound	Outbound
Octets	0	492
Unicast packets	0	6
Multicast packets	0	0

Device Time: Thu, 01 Jan 2009 00:30:27 +0000

Note : You can see all the status of this RG on 'Status' page.

3.1.1 LAN & WAN Setup

You can enter Basic Network, LAN(WiFi) & WAN for LAN and Internet setting as below.

3.1.1.1 Network Setup

3.1.1.1.1 IPv4

1. **LAN IP Address:** The local IP address of this device. The computer on your network must use the LAN IP address of this device as their Default Gateway. You

can change it if necessary.

2. **Subnet Mask:** Input your Subnet mask. (All devices in the network must have the same subnet mask.) The default subnet mask is 255.255.255.0

3.1.1.1.2 IPv6

The screenshot shows a network configuration page for IPv6. At the top, there are tabs for 'Network Setup', 'IPv6', and 'Wireless'. The main content is titled 'IPv6 Setting' and includes a '[HELP]' link. The settings are organized into several sections:

Item	Setting
▶ IPv6	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
▶ IPv6 Connection	Static IPv6
WAN IPv6 Address Settings	
▶ IPv6 Address	<input type="text"/>
▶ Subnet Prefix Length	<input type="text"/>
▶ Default Gateway	<input type="text"/>
▶ Primary DNS Address	<input type="text"/>
▶ Secondary DNS Address	<input type="text"/>
LAN IPv6 Address Settings	
▶ LAN IPv6 Address	<input type="text"/> /64
▶ LAN IPv6 Link-Local Address	<input type="text"/>
Address Autoconfiguration Settings	
▶ Autoconfiguration	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
▶ Autoconfiguration Type	Stateless
▶ Router Advertisement Lifetime	200 Seconds

At the bottom of the form, there are 'Save' and 'Undo' buttons.

1. **IPv6 setting:** Disable or enable the IPv6 settings.
2. **IPv6 Connection:** you may select the connection of Static IPv6/ DHCPv6/ PPPoE/ PPPoA / 6to4/IP 6 in IPv4 tunnel.
3. **DNS Setting:** you may select to obtain DNS server address automatically or use following DNS address.
4. **IPv6 address setting:** you may add IPv6 address Primary DNS address and secondary DNS address.
5. **LAN IPv6 address setting:** LAN IPv6 address and LAN IPv6 Link-Local address.
6. **Address auto configuration setting:** Disable or enable this auto configuration setting. You may set stateless or stateful (Dynamic IPv6), and also check if need to send Router advertisement messages periodically.

IPv6 Setting [HELP]	
Item	Setting
IPv6	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IPv6 Connection	6 to 4
6 to 4 Settings	
6 to 4 Address	
Primary DNS Address	
Secondary DNS Address	
LAN IPv6 Address Settings	
LAN IPv6 Address	
LAN IPv6 Link-Local Address	
Address Autoconfiguration Settings	
Autoconfiguration	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Autoconfiguration Type	Stateless
Router Advertisement Lifetime	200 Seconds

Save Undo

- WAN IPv6 address setting for 6to4:** you may obtain IPv6 DNS automatically or set DNS address manually for Primary DNS address and secondary DNS address.
- LAN IPv6 address setting:** LAN IPv6 address and LAN IPv6 Link-Local address.
- Address auto configuration setting:** Disable or enable this auto configuration setting. You may set stateless or stateful (Dynamic IPv6), and also check if need to send Router advertisement messages periodically.

IPv6 Setting [HELP]	
Item	Setting
IPv6	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IPv6 Connection	IPv6 in IPv4 Tunnel
IPv6 in IPv4 Tunnel Settings	
Remote IPv4 Address	88.193.34.0
Local IPv4 Address	88.193.34.0
Local IPv6 Address	
Primary DNS Address	
Secondary DNS Address	
LAN IPv6 Address Settings	
LAN IPv6 Address	
LAN IPv6 Link-Local Address	
Address Autoconfiguration Settings	
Autoconfiguration	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Autoconfiguration Type	Stateless
Router Advertisement Lifetime	200 Seconds

Save Undo

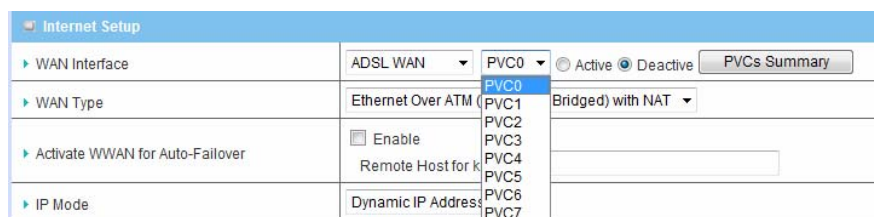
1. **WAN IPv6 address setting for IPv6 in IPv4 Tunnel:** you may add remote / local IPv4 address and local IPv6 address, then set DNS address manually for Primary DNS address and secondary DNS address.
2. **LAN IPv6 address setting:** LAN IPv6 address and LAN IPv6 Link-Local address.
3. **Address auto configuration setting:** Disable or enable this auto configuration setting. You may set stateless or stateful (Dynamic IPv6), and also check if need to send Router advertisement messages periodically.

3.1.1.2 Internet Setup

1. **WAN Interface:** You may select the following WAN type for your internet connection

ADSL WAN Type: WAN connection type of your ISP. You can click WAN Type to choose a correct one from the following options and select PVC0~7 :

- Ethernet Over ATM(RFC1483 Bridged) with NAT
- IP over ATM(RFC 1483 Routed)
- PPP over Ethernet
- PPP over ATM



Multiple-PVC Summary table can list PVC0~7 for PVCs' WAN type you selected.

Note : PVC0 = as main ADSL WAN

Service Information Summary

#	Active	VPI	VCI	ENCAP	Mux	IP Address	Status
PVC0	yes	8	35	PPPoE	LLC		N/A
PVC1	yes	0	100	Bridge Mode	VCMux	Dynamic	N/A
PVC2	No						N/A
PVC3	No						N/A
PVC4	No						N/A
PVC5	No						N/A
PVC6	No						N/A
PVC7	No						N/A

A. Ethernet Over ATM(RFC1483 Bridged) with NAT

▶ WAN Type	Ethernet Over ATM (RFC 1483 Bridged) with NAT ▼
▶ Activate WWAN for Auto-Failover	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
▶ IP Mode	Dynamic IP Address ▼
▶ Host Name	<input type="text"/> (optional)
▶ ISP registered MAC Address	<input type="text"/> <input type="button" value="Clone"/>
▶ Connection Control	Auto Reconnect (always-on) ▼
▶ NAT disable	<input checked="" type="checkbox"/> Enable
▶ Bridge Mode	<input checked="" type="checkbox"/> Enable
▶ Data Encapsulation	VCMux ▼
▶ VPI Number	0 <input type="text"/> (range: 0~255)
▶ VCI Number	100 <input type="text"/> (range: 1~65535)
▶ Schedule type	UBR ▼
▶ Multicast	Auto ▼
▶ IGMP Snooping	<input type="checkbox"/> Enable
▶ VLAN TAG	<input type="checkbox"/> Enable <input type="text" value="1"/> (range: 1~4094)
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

1. **Activate WWAN for Auto-failover** : Once you enable this function, you have to input WWAN information for 3G Auto-Backups (see as WWAN 3G portion).
Host Name : ISP host name
2. **IP mode**: select Dynamic IP address or Static IP address
3. **Host Name**: input your host name if you have one.
4. ISP registered MAC Address if you have one.
5. **Connection Control** : you can choose Connect-on-demand, Auto

Reconnect(always-on) and Manually.

6. **Maximum idle time** : 600 seconds
7. **NATdisable** : If you enable this option, it will act with a non-NAT function.
8. **Bridge mode** : If you enable this option, it will act with a bridge mode for ADSL function.
9. **Data Encapsulation:** Vc-MUX and LLC, these two options depend on your ISP setting.
10. **VPI and VCI, Schedule Type:** these values depend on your ISP setting.
11. **Schedule type** : UBR / CBR / VBR / GFR, depend on your ISP setting.
12. **Multicast** : you may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
13. **IGMP Snooping** : enable or disable IGMP snooping function.
14. **VLAN TAG** : you may input the value of VLAN Tag by your ISP setting.
(Range : 1~4094)

B. PPPoE

▶ WAN Type	PPP over Ethernet ▾
▶ Activate WWAN for Auto-Failover	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
▶ IPv6 Dualstack	<input type="checkbox"/> Enable
▶ PPPoE Account	<input type="text"/>
▶ PPPoE Password	<input type="text"/>
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ Connection Control	Auto Reconnect (always-on) ▾
▶ PPPoE Service Name	<input type="text"/> (optional)
▶ Assigned IP Address	<input type="text"/> (optional)
▶ MTU	0 (0 is auto)
▶ NAT disable	<input type="checkbox"/> Enable
▶ Bridge Mode	<input type="checkbox"/> Enable
▶ Data Encapsulation	LLC ▾
▶ VPI Number	8 (range: 0~255)
▶ VCI Number	35 (range: 1~65535)
▶ Schedule type	UBR ▾
▶ Multicast	Auto ▾
▶ IGMP Snooping	<input type="checkbox"/> Enable
▶ VLAN TAG	<input type="checkbox"/> Enable 1 (range: 1~4094)

1. **Activate WWAN for Auto-failover** : Once you enable this function, you have to input WWAN information for 3G Auto-Backups (see as WWAN 3G portion).
Host Name : ISP host name
2. **IPv6 Dual-stack** : You can enable / disable the function of IPv4/IPv6 stack.
3. **PPPoE Account and Password** : The account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it blank.
4. **Primary DNS/ Secondary DNS** : input the Primary/Secondary DNS if necessary.
5. **Connection Control** : you can choose Connect-on-demand, Auto Reconnect(always-on) and Manually.
6. **PPPoE Service name and assigned IP address** : input the value if necessary.
7. **MTU** : put all information here.

8. **NATdisable** : If you enable this option, it will act with a non-NAT function.
9. **Bridge mode** : If you enable this option, it will act with a bridge mode for ADSL function.
10. **Data Encapsulation:** Vc-MUX and LLC, these two options depend on your ISP setting.
11. **VPI and VCI, Schedule Type:** these values depend on your ISP setting.
12. **Schedule type** : UBR / CBR / VBR / GFR, depend on your ISP setting.
13. **Multicast** : you may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
14. **IGMP Snooping** : enable or disable IGMP snooping function.
15. **VLAN TAG** : you may input the value of VLAN Tag by your ISP setting.
(Range : 1~4094)

C. PPPoA

▶ WAN Type	PPP over ATM ▼
▶ Activate WWAN for Auto-Failover	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
▶ IPv6 Dualstack	<input type="checkbox"/> Enable
▶ PPPoA Account	<input type="text"/>
▶ PPPoA Password	<input type="text"/>
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ Connection Control	Auto Reconnect (always-on) ▼
▶ Service Name	<input type="text"/> (optional)
▶ Assigned IP Address	<input type="text"/> (optional)
▶ MTU	0 (0 is auto)
▶ NAT disable	<input type="checkbox"/> Confirm
▶ Bridge Mode	<input type="checkbox"/> Enable
▶ Data Encapsulation	VCmux ▼
▶ VPI Number	0 (range: 0~255)
▶ VCI Number	100 (range: 1~65535)
▶ Schedule type	UBR ▼
▶ Multicast	Auto ▼
▶ IGMP Snooping	<input type="checkbox"/> Enable
▶ VLAN TAG	<input type="checkbox"/> Enable <input type="text" value="1"/> (range: 1~4094)

1. **Activate WWAN for Auto-failover** : Once you enable this function, you have to input WWAN information for 3G Auto-Backups (see as WWAN 3G portion).
Host Name : ISP host name
2. **IPv6 Dual-stack** : You can enable / disable the function of IPv4/IPv6 stack.
3. **PPPoE Account and Password** : The account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it blank.
4. **Primary DNS/ Secondary DNS** : input the Primary/Secondary DNS if necessary.
5. **Connection Control** : you can choose Connect-on-demand, Auto Reconnect(always-on) and Manually.
6. **PPPoE Service name and assigned IP address** : input the value if necessary.
7. **MTU** : put all information here.

8. **NATdisable** : If you enable this option, it will act with a non-NAT function.
9. **Bridge mode** : If you enable this option, it will act with a bridge mode for ADSL function.
10. **Data Encapsulation:** Vc-MUX and LLC, these two options depend on your ISP setting.
11. **VPI and VCI, Schedule Type:** these values depend on your ISP setting.
12. **Schedule type** : UBR / CBR / VBR / GFR, depend on your ISP setting.
13. **Multicast** : you may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
14. **IGMP Snooping** : enable or disable IGMP snooping function.
15. **VLAN TAG** : you may input the value of VLAN Tag by your ISP setting.
(Range : 1~4094)

E. Wireless WAN - 3G

(USB 3G support only for CDD561-U03 model)

▶ WAN Interface	Wireless WAN ▾
▶ Dial-Up Profile	<input checked="" type="radio"/> Auto-Detection <input type="radio"/> Manual
▶ PIN Code	<input type="text"/> (optional)
▶ Connection Control	Auto Reconnect (always-on) ▾
▶ Allowed Connection Time	<input checked="" type="radio"/> Always <input type="radio"/> By Schedule
▶ MTU	0 <input type="text"/> (0 is auto)
▶ Keep Alive	<input checked="" type="radio"/> Disable <input type="radio"/> LCP Echo Request ▶ Interval <input type="text" value="10"/> seconds ▶ Max Failure Time <input type="text" value="3"/> times <input type="radio"/> Ping Remote Host ▶ Host IP <input type="text"/> ▶ Interval <input type="text" value="60"/> seconds
▶ Multicast	Auto ▾
▶ IGMP Snooping	<input type="checkbox"/> Enable

1. **Auto-Detection and Manually** : If you select auto-detection, then system will check the information automatically.
2. **Pin Code**: Enter the Pin Code for your SIM card(Optional)
3. **Connection Control**: select your connection control
4. **Allow connection time** : you can select always or by schedule for connection method. If you choose schedule rule, you can add a new schedule for this connection.
5. **MTU and Keep alive** : you can diagnose your connection by it.
6. **IGMP Snooping** : enable or disable IGMP snooping function.
7. **VLAN TAG** : you may input the value of VLAN Tag by your ISP setting.
(Range : 1~4094)

Ethernet WAN

A. Dynamic IP Address

▶ WAN Interface	Ethernet WAN ▾
▶ WAN Type	Dynamic IP Address ▾ Dynamic IP Address Static IP Address PPP over Ethernet PPTP L2TP
▶ Activate WWAN for Auto-Failover	<input type="checkbox"/> <small>alive:</small> <input type="text"/>
▶ Host Name	<input type="text"/> (optional)
▶ ISP registered MAC Address	<input type="text"/> <input type="button" value="Clone"/>
▶ Connection Control	Auto Reconnect (always-on) ▾
▶ NAT disable	<input type="checkbox"/> Enable
▶ Multicast	Auto ▾
▶ IGMP Snooping	<input type="checkbox"/> Enable
▶ VLAN TAG	<input checked="" type="checkbox"/> Enable <input type="text" value="3"/> (range: 1~4094)
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

1. **Activate WWAN for Auto-Failover:** With this function enabled, when the Ethernet WAN connection is broken, the device will automatically activate the WWAN connection and keep you connected to internet with the alternative WWAN broadband service. Meanwhile, if the device detected that the Ethernet WAN connection is recovered, your broadband connection will be switched to use the Ethernet WAN service.
2. **Host Name:** Optional, required by some ISPs, for example, @Home.
3. **ISP registered MAC Address:** Enter MAC address of your ISP. (Optional)
4. **Connection Control:** Connect-on-demand is the device will link up with ISP when the clients send outgoing packets. Auto Reconnect (Always-on) is the device will link with ISP until the connection is established. Manually mode is the device will not make the link until someone clicks the connect-button in the Status-page.
5. **NATdisable :** If you enable this option, it will act with a non-NAT function.
6. **Multicast :** you may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.

7. **IGMP Snooping** : enable or disable IGMP snooping function.
8. **VLAN TAG** : you may input the value of VLAN Tag by your ISP setting.
(Range : 1~4094)

B. Static IP Address

▶ WAN Interface	Ethernet WAN ▾
▶ WAN Type	Static IP Address ▾
▶ Activate WWAN for Auto-Failover	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
▶ WAN IP Address	<input type="text"/>
▶ WAN Subnet Mask	<input type="text"/>
▶ WAN Gateway	<input type="text"/>
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ NAT disable	<input checked="" type="checkbox"/> Enable
▶ Multicast	Auto ▾
▶ IGMP Snooping	<input checked="" type="checkbox"/> Enable
▶ VLAN TAG	<input checked="" type="checkbox"/> Enable 3 (range: 1~4094)

1. **Activate WWAN for Auto-failover** : Once you enable this function, you have to input WWAN information for 3G Auto-Backups (see as WWAN 3G portion).
Host Name : ISP host name
2. **WAN assigned IP address/ Subne mask/ Gateway IP.**
3. **Primary DNS/ Secondary DNS** : input the Primary/Secondary DNS if necessary.
4. **NAT** : If you enable this option, it will act with a NAT function.
5. **NATdisable** : If you enable this option, it will act with a non-NAT function.
6. **Multicast** : you may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
7. **IGMP Snooping** : enable or disable IGMP snooping function.

8. **VLAN TAG** : you may input the value of VLAN Tag by your ISP setting.
(Range : 1~4094)

C. PPP over Ethernet

▶ WAN Interface	Ethernet WAN ▾
▶ WAN Type	PPP over Ethernet ▾
▶ Activate WWAN for Auto-Failover	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
▶ IPv6 Dualstack	<input type="checkbox"/> Enable
▶ PPPoE Account	<input type="text"/>
▶ PPPoE Password	<input type="text"/>
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ Connection Control	Auto Reconnect (always-on) ▾
▶ PPPoE Service Name	<input type="text"/> (optional)
▶ Assigned IP Address	<input type="text"/> (optional)
▶ MTU	0 (0 is auto)
▶ NAT disable	<input type="checkbox"/> Enable
▶ Multicast	Auto ▾
▶ IGMP Snooping	<input type="checkbox"/> Enable
▶ VLAN TAG	<input checked="" type="checkbox"/> Enable 3 (range: 1~4094)

1. **Activate WWAN for Auto-failover** : Once you enable this function, you have to input WWAN information for 3G Auto-Backups (see as WWAN 3G portion).
Host Name : ISP host name
2. **IPv6 Dual-stack** : You can enable / disable the function of IPv4/IPv6 stack.
3. **PPPoE Account and Password** : The account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it blank.
4. **Connection Control** : you can choose Connect-on-demand, Auto Reconnect(always-on) and Manually.
5. **Service name and assigned IP address.**

6. **Primary DNS/ Secondary DNS** : input the Primary/Secondary DNS if necessary.
7. **MTU** : Most ISP offers MTU value to users. The default MTU value is 0 (auto)
8. **NATdisable** : If you enable this option, it will act with a non-NAT function.
9. **Multicast** : you may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
10. **IGMP Snooping** : enable or disable IGMP snooping function.
11. **VLAN TAG** : you may input the value of VLAN Tag by your ISP setting.
(Range : 1~4094)

D. PPTP

▶ WAN Interface	Ethernet WAN ▼
▶ WAN Type	PPTP ▼
▶ Activate WWAN for Auto-Failover	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
▶ IP Mode	Dynamic IP Address ▼
▶ Server IP Address/Name	<input type="text"/>
▶ PPTP Account	<input type="text"/>
▶ PPTP Password	<input type="text"/>
▶ Connection ID	<input type="text"/> (optional)
▶ Connection Control	Auto Reconnect (always-on) ▼
▶ MTU	0 (0 is auto)
▶ MPPE	<input type="checkbox"/>
▶ Multicast	Auto ▼
▶ IGMP Snooping	<input type="checkbox"/> Enable
▶ VLAN TAG	<input checked="" type="checkbox"/> Enable 3 (range: 1~4094)
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

1. **Activate WWAN for Auto-Failover**: With this function enabled, when the Ethernet WAN connection is broken, the device will automatically activate the WWAN connection and keep you connected to internet with the alternative WWAN broadband service. Meanwhile, if the device detected that the Ethernet WAN connection is

recovered, your broadband connection will be switched to use the Ethernet WAN service

2. **IP Mode:** Please check the IP mode your ISP assigned, and select “Static IP Address” or “Dynamic IP Address”.
3. **Server IP** and **Server IP Address/Name:** The IP address of the PPTP server and designated Gateway provided by your ISP.
4. **PPTP Account** and **Password:** The account and password your ISP assigned to you. If you don't want to change the password, keep it blank.
5. **Connection ID:** Optional. Input the connection ID if your ISP requires it.
6. **Connection Control:** Connect-on-demand is the device will link up with ISP when the clients send outgoing packets. Auto Reconnect (Always-on) is the device will link with ISP until the connection is established. Manually mode is the device will not make the link until someone clicks the connect-button in the Status-page.
7. **Maximum Transmission Unit (MTU):** Most ISP offers MTU value to users. The default MTU value is 0 (auto).
8. **MPPE (Microsoft Point-to-Point Encryption):** enable or disable this function.
9. **Multicast :** you may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
10. **IGMP Snooping :** enable or disable IGMP snooping function.
11. **VLAN TAG :** you may input the value of VLAN Tag by your ISP setting. (Range : 1~4094)

E. L2TP

Internet Setup [HELP]	
▶ WAN Interface	Ethernet WAN ▾
▶ WAN Type	L2TP ▾
▶ Activate WWAN for Auto-Failover	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
▶ IP Mode	Dynamic IP Address ▾
▶ IP Address	<input type="text"/>
▶ Subnet Mask	<input type="text"/>
▶ WAN Gateway IP	<input type="text"/>
▶ Server IP Address/Name	<input type="text"/>
▶ L2TP Account	<input type="text"/>
▶ L2TP Password	<input type="text"/>
▶ Maximum Idle Time	600 seconds
▶ Connection Control	Connect-on-Demand ▾
▶ MTU	0 (0 is auto)
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

1. **Activate WWAN for Auto-Failover:** With this function enabled, when the Ethernet WAN connection is broken, the device will automatically activate the WWAN connection and keep you connected to internet with the alternative WWAN broadband service. Meanwhile, if the device detected that the Ethernet WAN connection is recovered, your broadband connection will be switched to use the Ethernet WAN service
2. **IP Mode:** Please check the IP mode your ISP assigned, and select “Static IP Address” or “Dynamic IP Address”.
3. **My IP Address and My Subnet Mask:** The private IP address and subnet mask your ISP assigned to you.
4. **Gateway IP and Server IP Address/Name:** The IP address of the L2TP server and designated Gateway provided by your ISP.
5. **L2TP Account and Password:** The account and password your ISP assigned to you.

If you don't want to change the password, keep it blank.

6. **Maximum Idle Time:** The time of no activity to disconnect your L2TP session. Set it to zero or enable "Auto-reconnect" to disable this feature. If Auto-reconnect is enabled, this device will connect with ISP automatically, after system is restarted or connection is dropped.
7. **Connection Control:** Connect-on-demand is the device will link up with ISP when the clients send outgoing packets. Auto Reconnect (Always-on) is the device will link with ISP until the connection is established. Manually mode is the device will not make the link until someone clicks the connect-button in the Status-page.
8. **Maximum Transmission Unit (MTU):** Most ISP offers MTU value to users. The default MTU value is 0 (auto).

3.1.1.2 Wireless Settings

Wireless Setting [HELP]	
Item	Setting
Wireless Module	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network ID(SSID)	default
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	6
Wireless Mode	B/G/N mixed
Authentication	Auto
Encryption	WEP
<input checked="" type="radio"/> WEP Key 1	HEX 1234567890
<input type="radio"/> WEP Key 2	HEX 1234567890
<input type="radio"/> WEP Key 3	HEX 1234567890
<input type="radio"/> WEP Key 4	HEX 1234567890
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="WDS Setting..."/> <input type="button" value="WPS Setup..."/> <input type="button" value="Wireless Client List..."/>	

Wireless settings allow you to set the wireless configuration items.

1. **Wireless Module:** You can enable or disable wireless function.
2. **Network ID (SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is “default”)
3. **SSID Broadcast:** The router will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, the wireless clients can not find the device from beacons.
4. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is as the following: channel 6 for North America; channel 7 for European (ETSI); channel 7 for Japan.

5. **Wireless Mode:** Choose “B/G mixed”, “B only”, “G only”, “N only”, “G/N mixed” or “B/G/N mixed”. The factory default setting is “B/G/N mixed”.
6. **Authentication mode:** You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.

- **Open**

Open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration.

- **Shared**

Shared key authentication relies on the fact that both stations taking part in the authentication process have the same "shared" key or passphrase. The shared key is manually set on both the client station and the AP/router. Three types of shared key authentication are available today for home or small office WLAN environments.

- **Auto**

The AP will Select the Open or Shared by the client's request automatically.

- **WPA-PSK**

Select Encryption and Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits.

If you select ASCII, the length of pre-share key is from 8 to 63.

Fill in the key, Ex 12345678

- **WPA**

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server IP address or the 802.1X server's domain-name.

Select Encryption and RADIUS Shared Key.

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits.

If you select ASCII, the length of pre-share key is from 8 to 63.

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

- **WPA2-PSK**

WPA2-PSK user AES and TKIP for Same the encryption, the others are same as the WPA2-PSK.

- **WPA-PSK/WPA2-PSK**

Another encryption options for WPA-PSK-TKIP and WPA2-PSK-AES, the others are same as the WPA-PSK.

- **WPA/WPA2**

Another encryption options for WPA-TKIP and WPA2-AES, the others are same the WPA.

Press “**WDS Setting**” and It allows PC to get connected to wireless network within the area.

WDS Setting [HELP]	
Item	Setting
▶ Wireless Bridging	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Remote AP MAC 1	<input type="text"/>
▶ Remote AP MAC 2	<input type="text"/>
▶ Remote AP MAC 3	<input type="text"/>
▶ Remote AP MAC 4	<input type="text"/>
▶ Encryption type	WEP ▼
▶ Encryption key	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Back"/>	

1. **Wireless Bridging:** You could enable this function by selecting “Enable”.
2. **Remote AP MAC 1~Remote AP MAC 2:** Enter the wireless MAC into the blank.
3. **Encryption type:** Select the appropriate category. Once you set up that type of encryption, second LAN PC must enter the same encryption type as the first one.
4. **Encryption key:** Set up encryption key based on the rule of encryption type. Once you set up encryption, second LAN PC must enter the same encryption type as the first one.

Press “**WPS Setup**”, you can configure and enable the easy setup feature WPS (Wi-Fi Protected Setup) for your wireless network.

Wi-Fi Protected Setup	
Item	Setting
▶ WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ AP PIN	22192677 <input type="button" value="Generate New PIN"/>
▶ Config Mode	Registrar ▼
▶ Config Status	CONFIGURED <input type="button" value="Release"/>
▶ Config Method	Push Button ▼
▶ WPS status	NOUSED
<input type="button" value="Save"/> <input type="button" value="Trigger"/> <input type="button" value="Cancel"/>	

1. **WPS:** You can enable this function by selecting “Enable”. WPS offers a safe and easy way to allow the wireless clients connected to your wireless network.
2. **AP PIN:** You can press Generate New Pin to get an AP PIN.
3. **Config Mode:** Select your config Mode from “Registrar” or “Enrollee”.
4. **Config Status:** It shows the status of your configuration.
5. **Config Method:** You can select the Config Method here from “Pin Code” or “Push Button”.
6. **WPS status:** According to your setting, the status will show “Start Process” or “No used”.

Press “**Wireless Clients List**” and the list of wireless clients will be shown consequently.

Wireless Clients List	
ID	MAC Address
<input type="button" value="Back"/> <input type="button" value="Refresh"/>	

3.1.2 Client Server Proxy

3.1.2.1 DHCP Server

DHCP Server [HELP]	
Item	Setting
▶ DHCP Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
▶ IP Pool Starting Address	<input type="text" value="100"/>
▶ IP Pool Ending Address	<input type="text" value="200"/>
▶ Lease Time	<input type="text" value="86400"/> Seconds
▶ Domain Name	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="More>>"/> <input type="button" value="Clients List..."/> <input type="button" value="Fixed Mapping..."/>	

1. **DHCP Server:** Choose either **Disable** or **Enable**. If you enable the DHCP Server function, the following settings will be effective.
2. **IP Pool Starting/Ending Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool.
3. **Lease Time:** DHCP lease time to the DHCP client.
4. **Domain Name:** Optional, this information will be passed to the clients.

Press “**More>>**” and you can find more settings.

5. **Primary DNS/Secondary DNS:** Optional. This feature allows you to assign a DNS Servers
6. **Primary WINS/Secondary WINS:** Optional. This feature allows you to assign a WINS Servers
7. **Gateway:** Optional. Gateway Address would be the IP address of an alternate Gateway. This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.

Press “**Clients List**” and the list of DHCP clients will be shown consequently.

DHCP Clients List					
IP Address	Host Name	MAC Address	Type	Lease Time	Select
192.168.123.100	joseph	00-0B-6A-F4-40-D6	Wired	23:59:34	<input type="checkbox"/>
<input type="button" value="Delete"/> <input type="button" value="Back"/> <input type="button" value="Refresh"/> <input type="button" value="Fixed Mapping"/>					

Press “**Fixed Mapping**” and the DHCP Server will reserve the special IP for designated MAC address.

ID	MAC Address	IP Address	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

3.1.2.2 Dynamic DNS

To host your server on a changing IP address, you have to use dynamic domain name service (DDNS). Therefore, anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

Before you enable **Dynamic DNS**, you need to register an account on one of these Dynamic DNS servers that we list in **Provider** field.

Item	Setting
▶ DDNS	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
▶ Provider	DynDNS.org(Dynamic) ▼
▶ Host Name	<input type="text"/>
▶ Username / E-mail	<input type="text"/>
▶ Password / Key	<input type="text"/>

1. **DDNS:** Select enable if you would like to trigger this function.

2. **Provider:** The DDNS provider supports service for you to bind your IP(even private IP) with a certain Domain name. You could choose your favorite provider.
3. **Host Name:** Register a domain name to the DDNS provider. The fully domain name is concatenated with hostname(you specify) and a suffix(DDNS provider specifies).
4. **Username/E-mail:** Input username or E-mail based on the DDNS provider you select.
5. **Password/Key:** Input password or key based on the DDNS provider you select.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.3 NAT

3.1.3.1 Virtual Server

This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

A virtual server is defined as a **Service Port**, and all requests to this port will be redirected to the computer specified by the **Server IP**. **Virtual Server** can work with **Scheduling Rules**, and give user more flexibility on Access control. For the details, please refer to **Scheduling Rule**.

ID	Service Ports	Server IP	Enable	Use Rule#
1			<input type="checkbox"/>	(0) Always
2			<input type="checkbox"/>	(0) Always
3			<input type="checkbox"/>	(0) Always
4			<input type="checkbox"/>	(0) Always
5			<input type="checkbox"/>	(0) Always
6			<input type="checkbox"/>	(0) Always
7			<input type="checkbox"/>	(0) Always
8			<input type="checkbox"/>	(0) Always
9			<input type="checkbox"/>	(0) Always

For example, if you have an FTP server (port 21) at 192.168.123.1, a Web server (port 80) at 192.168.123.2, and a VPN server at 192.168.123.6, then you need to specify the following virtual server mapping table:

Service Port	Server IP	Enable
21	192.168.123.1	V
80	192.168.123.2	V
1723	192.168.123.6	V

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.3.2 Special AP

Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. **The Special Applications** feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the DMZ host instead.

ID	Trigger	Incoming Ports	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

This device provides some predefined settings. Select your application and click “Copy to” to add the predefined setting to your list.

1. **Trigger:** The outbound port number issued by the application.
2. **Incoming Ports:** When the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

Afterwards, Click on “Save” to store your settings or click “Undo” to give up the changes.

Miscellaneous

Miscellaneous Items		[HELP]
Item	Setting	Enable
▶ IP Address of DMZ Host	<input type="text"/>	<input type="checkbox"/>
▶ UPnP setting		<input checked="" type="checkbox"/>

1. IP Address of DMZ Host

DMZ (Demilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

2. UPnP Setting

The device supports the UPnP function. If the OS of your client computer supports this function, and you enabled it, like Windows XP, you can see the following icon when the client computer gets IP from the device.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the **changes**.

3.1.4 Routing

3.1.4.1 Routing Table

If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other. The routing table allows you to determine which physical interface addresses are utilized for outgoing IP data grams.

Routing Table [HELP]					
Item		Setting			
▶ Dynamic Routing		<input checked="" type="radio"/> Disable <input type="radio"/> RIPv1 <input type="radio"/> RIPv2			
▶ Static Routing		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>					

1. **Dynamic Routing:** Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnets in your network. Otherwise, please select RIPv1 if you need this protocol.
2. **Static Routing:** For static routing, you can specify up to 8 routing rules. You can enter the **destination IP address**, **subnet mask**, **gateway**, and **hop** for each routing rule, and then enable or disable the rule by checking or un-checking the Enable checkbox. Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

3.1.4 Change Password

Change Password	
Item	Setting
▶ Old Password	<input type="text"/>
▶ New Password	<input type="text"/>
▶ Reconfirm	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

You can change the System Password here. We **strongly** recommend you to change the system password for security reason. Click on “Save” to store your settings or click “Undo” to give up the changes.

3.2. Advance Network

3.2.1. Firewall

3.2.1.1. Packet Filters

Packet Filter includes both outbound filter and inbound filter. And they have same way to setting. It enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies:

1. Allow all to pass except those match the specified rules.
2. Deny all to pass except those match the specified rules.

ID	Source IP	Destination IP : Ports	Enable	Use rule#
1	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
2	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
3	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
4	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
5	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
6	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
7	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>
8	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always <input type="button" value="v"/>

You can specify 8 rules for each direction: inbound or outbound. For each rule, you can define the following:

- Source IP address

- Source port
- Destination IP address
- Destination port
- Protocol: TCP or UDP or both.
- Use Rule#

For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.

For source or destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999, No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. Packet Filter can work with **Scheduling Rules**, and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule**.

Each rule can be enabled or disabled individually.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

3.2.1.2. Domain Filters

Item		Setting	
Domain Filter		<input type="checkbox"/> Enable	
Log DNS Query		<input type="checkbox"/> Enable	
Privilege IP Addresses Range		From <input type="text"/> To <input type="text"/>	
ID	Domain Suffix	Action	Enable
1	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
10	* (all others)	<input type="checkbox"/> Drop <input type="checkbox"/> Log	-

Domain Filter prevents users under this device from accessing specific URLs.

1. **Domain Filter:** Check if you want to enable Domain Filter.
2. **Log DNS Query:** Check if you want to log the action when someone accesses the specific URLs.
3. **Privilege IP Address Range:** Setting a group of hosts and privilege these hosts to access network without restriction.
4. **Domain Suffix:** A suffix of URL can be restricted, for example, ".com", "xxx.com".
5. **Action:** When someone is accessing the URL met the domain-suffix, what kind of action you want.
Check "Drop" to block the access. Check "Log" to log these access.
6. **Enable:** Check to enable each rule.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

3.2.1.3. URL Blocking

URL Blocking will block LAN computers to connect with pre-define Websites. The major difference between "Domain filter" and "URL Blocking" is Domain filter requires user to

input suffix (like .com or .org, etc), while URL Blocking requires user to input a keyword only. In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a keyword.

URL Blocking [HELP]		
Item	Setting	
▶ URL Blocking	<input type="checkbox"/> Enable	
ID	URL	Enable
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>		

1. **URL Blocking:** Check if you want to enable URL Blocking.
2. **URL:** If any part of the Website's URL matches the pre-defined word, the connection will be blocked.

For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".
3. **Enable:** Check to enable each rule.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.2.1.4. MAC Control

MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.

MAC Address Control [HELP]				
Item	Setting			
▶ MAC Address Control	<input type="checkbox"/> Enable			
<input type="checkbox"/> Connection control	Wireless and wired clients with C checked can connect to this device; and <input type="button" value="allow"/> unspecified MAC addresses to connect.			
<input type="checkbox"/> Association control	Wireless clients with A checked can associate to the wireless LAN; and <input type="button" value="allow"/> unspecified MAC addresses to associate.			
DHCP clients <input type="button" value="-- select one --"/> <input type="button" value="Copy to"/> ID <input type="button" value="--"/>				
ID	MAC Address	IP Address	C	A
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value=" << Previous"/> <input type="button" value=" Next >>"/> <input type="button" value=" Save"/> <input type="button" value=" Undo"/>				

1. **MAC Address Control:** Check "Enable" to enable the "MAC Address Control". All of the settings in this page will take effect only when "Enable" is checked.
2. **Connection control:** Check "Connection control" to enable the controlling of which wired and wireless clients can connect with this device. If a client is denied to connect with this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect with this device.
3. **Association control:** Check "Association control" to enable the controlling of

which wireless client can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

3.2.1.5. Miscellaneous

Miscellaneous Items		[HELP]
Item	Setting	Enable
▶ Administrator Time-out	<input type="text" value="300"/> seconds (0 to disable)	
▶ Remote Administrator Host: Port	<input type="text"/> / <input type="text"/> : <input type="text"/>	<input type="checkbox"/>
▶ Discard PING from WAN side		<input type="checkbox"/>
▶ DoS Attack Detection		<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>		

1. **Administrator Time-out:** The time of no activity to logout automatically, you may set it to zero to disable this feature.
2. **Remote Administrator Host/Port**
 In general, only Internet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect with this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses for example, "10.1.2.0/24".
 NOTE: When Remote Administration is enabled, the web server port will be shifted to 80. You can change web server port to other port, too.
3. **Discard PING from WAN side:** When this feature is enabled, any host on the WAN

cannot ping this product.

4. **DoS Attack Detection:** When this feature is enabled, the router will detect and log the DoS attack coming from the Internet. Currently, the router can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack etc.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.2.2. QoS

3.2.2.1. QoS

Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

3.2.2.1.1. Smart QoS

Item	Setting
▶ Cross-layer QoS	Disable ▾
▶ QoS Mode	Smart-QoS ▾
▶ Bandwidth of Upstream	2000 kbyte
▶ Bandwidth of Downstream	4000 kbyte
▶ Flexible Bandwidth Management	Enable ▾

1. **Cross-layer QoS** : you can select enable/disable the QoS control
2. **QoS Mode** : you can select Smart-QoS or User defined QoS rule for your own QoS control
3. **Bandwidth of upstream / bandwidth of Downstream** : you can input the value of maximize of upstream and downstream bandwidth from your ISP
4. **Enable Flexible Bandwidth management** : If you enable this management, system will share the bandwidth of those selected applications to other applications if user do not run those selected application, for example, If you select Game/ VoIP/ Video 3 applications for higher priority in your system, then the system will automatically reserve 10% of bandwidth to other application, and share the rest of bandwidth $(100-10)/3=30\%$ each to Game/VoIP/Video, so if user do not play a game, then the system will flexible share the 30% of bandwidth to other application.

Item	Select
▶ Game	<input checked="" type="checkbox"/>
▶ Chat	<input type="checkbox"/>
▶ VoIP	<input checked="" type="checkbox"/>
▶ P2P	<input type="checkbox"/>
▶ Video	<input checked="" type="checkbox"/>
▶ Web	<input type="checkbox"/>

Example for Smart-QoS with FBM enable : Mr. Wang selects Game/ VoIP/ Video 3 applications for higher priority in his system, the system will automatically reserve 10% of minimum rate of bandwidth to other application, and share the rest minimum rate of bandwidth $(100-10)/3=30\%$ each to Game/VoIP/Video. If Mr. Wang's son plays on-line game in the morning, the total bandwidth will all reserve to his son. By the evening, when Mr. Wang back home and wants to watch IPTV, then he will get the same priority with his son, and share the bandwidth.

5. **Disable Flexible Bandwidth Management :** If you disable this management, system will allow you to input percentage of bandwidth manually.

Item	Select	Setting
▶ Game	<input checked="" type="checkbox"/>	50 %
▶ Chat	<input type="checkbox"/>	0 %
▶ VoIP	<input checked="" type="checkbox"/>	30 %
▶ P2P	<input type="checkbox"/>	0 %
▶ Video	<input type="checkbox"/>	0 %
▶ Web	<input type="checkbox"/>	0 %

3.2.2.1.2. User defined QoS rule

Item	Setting
▶ Cross-layer QoS	Enable ▼
▶ QoS Mode	User define QoS rule ▼
▶ Bandwidth of Upstream	2000 kbyte
▶ Bandwidth of Downstream	5000 kbyte
▶ Flexible Bandwidth Management	Enable ▼

1. Cross-layer QoS : you can enable/disable this QoS system.
2. **QoS Mode** : you can select User defined QoS rule for your own QoS control
3. **Bandwidth of upstream / bandwidth of Downstream** : you can input the value of maximize of upstream and downstream bandwidth from your ISP
4. **Advance setting** : you can press the button of 'Add New Rule' to create a new QoS rule.

▣ Advanced Setting

QoS Rules Table
<input type="button" value="Add New Rule..."/>
<input type="button" value="Restart"/> <input type="button" value="Reset"/>

5. **Create a QoS Rule** : you can enable the rule, and select QoS class type as below.

▣ QoS Rule Setting - Rule ID 1

Item	Setting
▶ Rule	<input checked="" type="checkbox"/> Enable
▶ Class	IP ▼
▶ Class Info - IP	<input type="text"/> ~ <input type="text"/>
▶ Function	PRI ▼
▶ Function data - Priority	<input type="text"/>
▶ Direction	In ▼
▶ Schedule	(0) Always ▼

Class : You can create your own QoS rule by different classes as below.

Class	Description

IP	IP address base
N	TCP port
UDPPORT	UDP port
MAC	MAC base
DSCP	DSCP base

Function : you can set your own function value to enable your QoS rule as below.

Function	Description	Data
PRI	Priority	1~6
MAXR	Maximum bandwidth Rate	KBps/MBps
MINR	Minimum bandwidth Rate	KBps/MBps
SESSION	Connection session	number
DROP	Drop packet	None
LOG	Log event	None
ALERT	Alert event	None

Direction : you can select inbond/ outbond for your direction.

Direction	
IN	inbond
OUT	outbond
BOTH	inbond & outbond

6. **DSCP setting** : you can set your own DSCP value here.

DiffServ Code Point : you can select code value.

Service Type : you can select their service type.

Function : PRI

Function data- Priority : 1~6

QoS Rule Setting - Rule ID 1	
Item	Setting
▶ Rule	<input checked="" type="checkbox"/> Enable
▶ Class	DSCP ▾
▶ DiffServ CodePoint	IP Precedence 2(CS2) ▾
▶ Service Type	SIP(UDP:5060) ▾
▶ Function	PRI ▾
▶ Function data - Priority	1
▶ Direction	In ▾
▶ Schedule	(0) Always ▾
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

DSCP marking : you can add your inbound / outbound packets a DCSP marking, please see one example as below.

Item	Setting
Rule	<input checked="" type="checkbox"/> Enable
Class	DSCP ▾
DiffServ CodePoint	IP Precedence 2(CS2) ▾
Service Type	SIP(UDP:5060) ▾
Function	MARKING ▾
Function data - none	
Direction	Both ▾
Schedule	(0) Always ▾
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

Ex. Please mark CS3 when an packet in/ out via UDP port 5060.

Once you saved the QoS rule, system will show you the rule as below, you can add another new rule accordingly.

Advanced Setting	
QoS Rules Table	
<input checked="" type="checkbox"/> 1.	<input checked="" type="checkbox"/> DSCP : CS2 Set PRI Priority : 1 (In) (Always)
AND	<input checked="" type="checkbox"/> UDPPORT : 5060
<input type="button" value="Add New Rule..."/>	
<input type="button" value="Restart"/> <input type="button" value="Reset"/>	
Saved!	

System will show you all your QoS rule as below



Note 1. : You can move up or down the priority of all rules by pointing the ‘↑’ or ‘↓’ if you want to change the priority.

Note 2. : You can unmark any rule if you do not want it enable now.



3.2.3. VLAN

The VLAN function allows you to divide local network into different “virtual LAN”. In some cases, ISP may need router to support “VLAN tag” for certain kinds of services (e.g. IPTV) to work properly.

There are four LAN ports with this router, so you can have up to 4 VLAN if required. Those four LAN ports belong to one VLAN by default. If you want to divide them into different VLAN, you just need to assign different “VID” for them. If ISP requests a “VLAN Tag” with your outgoing data, please remember to check the checkbox of “Tx TAG”.

LAN VLAN Settings				
Ethernet	WAN/LAN	VID	Tx TAG	
Port 1	LAN	1	<input type="checkbox"/>	
Port 2	LAN	1	<input type="checkbox"/>	
Port 3	LAN	20	<input checked="" type="checkbox"/>	
Port 4	LAN	1	<input type="checkbox"/>	
VLAN ID on LAN	LAN/Wireless LAN(Interface)	Tag	Type	Internet or ISP map WAN(VLAN ID)
1	Port1, Port2, Port4	No	NAT	0
20	Port3	Yes	NAT	0

If you want to mapping WAN ID, you can enter WAN VLAN setting, and change router type to Bridge and add WAN Map VLAN ID to your value.

VLAN Settings	
Item	Setting
▶ VID	20
▶ Routing Type	Bridge
▶ WAN Map VLAN ID	0 (0 is untag)

3.2.4. Management

3.2.4.1. SNMP

In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

SNMP Setting [HELP]	
Item	Setting
▶ Enable SNMP	<input type="checkbox"/> Local <input type="checkbox"/> Remote
▶ Get Community	<input type="text"/>
▶ Set Community	<input type="text"/>
▶ IP 1	<input type="text"/>
▶ IP 2	<input type="text"/>
▶ IP 3	<input type="text"/>
▶ IP 4	<input type="text"/>
▶ SNMP Version	<input checked="" type="radio"/> V1 <input type="radio"/> V2c
▶ WAN Access IP Address	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

1. **Enable SNMP:** You must check “Local”, “Remote” or both to enable SNMP function. If “Local” is checked, this device will respond request from LAN. If “Remote” is checked, this device will respond request from WAN.
2. **Get Community:** The community of GetRequest is that this device will respond.
3. **Set Community:** The community of SetRequest is that this device will accept.
4. **IP 1, IP 2, IP 3, IP 4:** Enter the IP addresses of your SNMP Management PCs. User has to configure where this device should send SNMP Trap message.
5. **SNMP Version:** Select proper SNMP Version that your SNMP Management software supports.
6. **WAN Access IP Address:** If you want to limit the remote SNMP access to specific computer, please enter the PC’s IP address. The default value is 0.0.0.0, and it means that any Internet connected computer can get some information of the device with SNMP protocol.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.2.4.2. TR-069

TR-069 Setting	
Item	Setting
▶ TR-069	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
ACS Setting	
▶ ACS URL	<input type="text"/>
▶ ACS UserName	<input type="text"/>
▶ ACS Password	<input type="text"/>
CPE Setting	
▶ ConnectionRequest Port	<input type="text" value="8099"/>
▶ ConnectionRequest UserName	<input type="text"/>
▶ ConnectionRequest Password	<input type="text"/>
Inform Setting	
▶ Inform	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
▶ Interval	<input type="text" value="900"/> seconds
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

1. **TR-069:** Disable or enable the TR-069 settings.
2. **ACS setting:** you may add ACS URL/ Username/ Password.
3. **CPE setting:** you may add CPE connection request port/ username /password.
4. **Inform setting:** you may enable/disable the interval of informing CPE.
5. **Interval :** you may input seconds for every interval.

Note: TR-069 is a customized feature for ISP, please contact with us once you get any problem to configure.

3.3. Application

3.3.1. NAS (This section is only for CDD561-U03 model)

3.3.1.1. Disk Utility

1. Format

This utility would format the certain partition.

Please be noted! This action will clear all your data in this partition. You will not be able to recover it any more.

Disk Distribution			
▶ Disk Total Capacity = 7628 MB			
Partition	Free(MB)	Used(MB)	Total(MB)
1 [FAT32]	841	6786	7628
*Warning! Formatting will erase all data on this partition.			
<input type="button" value="Format"/> <input type="button" value="Check"/>			

2. Check

This utility could help you check the partition, find the lost files, try to fix some problems.

3.3.1.2. File Sharing

Basic Setting	
Item	Setting
▶ Computer Name	<input type="text" value="NAS"/>
▶ WorkGroup	<input type="text" value="WORKGROUP"/>
▶ Server Comment	<input type="text" value="samba server"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="FTP Service Configuration"/>	

These settings are for Samba Server (Windows Network Neighbors).

1. Computer Name

The name that is showed on the windows network neighbors search result.

2. WorkGroup

This name MUST be the same as your computer, or you could not search this device via windows.

3. Server Comment

Just a comment for recognize.

3.3.1.3. FTP Service

FTP Setting	
Item	Setting
▶ FTP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ FTP Port	<input type="text" value="21"/>
▶ FTP Max Connection per IP	<input type="text" value="2"/> ▼
▶ FTP MAX Clients	<input type="text" value="5"/> ▼
▶ Client Support UTF8	<input type="radio"/> Yes <input checked="" type="radio"/> No
▶ Codepage	<input type="text" value="Arabic(CP864)"/> ▼
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

These settings are for FTP service.

1. FTP Port:

The default port is 21, but sometimes you might want to hide your FTP service by changing it. We have the ability to receive the request on non-standard FTP port, but please be noted, some NAT router could not support non-standard FTP port, that means some of your clients might have to use passive mode to get file.

2. Client Support UTF8:

This option is used when your FTP client could support UTF8. Usually, the default value "No" is okay for most clients.

3. Codepage:

Please set correct value to suit your language.

3.3.1.4. Access Control

User Access Configuration	
Item	Setting
▶ Security Level	<input checked="" type="radio"/> Guest mode <input type="radio"/> Authorization mode
<input type="button" value="Save"/> <input type="button" value="User Configuration"/>	

The default setting is “Guest mode”, all clients could access as anonymous users.

If you want to control the permission, change to “Authorization mode” and save it, then go to “User Configuration”.

3.3.1.5. User Configuration

User Access Configuration			
Item		Setting	
▶ User Name		<input type="text"/>	(Max. 20 users)
▶ Password		<input type="text"/>	
ID	Username	Password	Select
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Cancel"/> <input type="button" value="Back"/>			

In this page, you can manage the user account.

Key in the user name and password then press “Add” could let you add a new user.

If you want to delete an account, select it and click “Delete” button.

3.3.1.6. iTunes Server

iTunes Server Configuration	
Item	Setting
▶ Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Service Name	<input type="text"/>
▶ Service Port	<input type="text" value="3689"/>
▶ Access Password	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

This function could enable the built-in iTunes Server to support iTunes which is a media player released by Apple.

1. Server Name:

The name of this server, it will be shown on the iTunes.

2. Service Port:

The TCP port for WEB management interface, for example, if the default value is 3689, then your iTunes server URL will be http://This_Device_IP:3689

3. Access Password:

The password for iTunes Server WEB management interface.

3.3.1.7. Download Assistant

3.3.1.7.1. FTP

If you want to download something from a FTP site regularly but you don't want to spend time on remembering doing this, this FTP download assistant could help you.

Download Assistant - FTP	
Item	Setting
▶ Download Type	<input checked="" type="radio"/> FTP <input type="radio"/> HTTP <input type="radio"/> BT
▶ Job Name	<input type="text"/>
▶ URL	<input type="text"/> Port <input type="text" value="21"/>
▶ Save To	<input type="text" value="/C/Downloads/FTP"/>
▶ Login method	<input checked="" type="radio"/> Anonymous <input type="radio"/> Account
▶ Username	<input type="text"/>
▶ Password	<input type="text"/>
▶ Start Time	<input type="radio"/> Schedule <input checked="" type="radio"/> At Once
Time	<input type="text" value="2010"/> / <input type="text" value="Jun"/> / <input type="text" value="29"/> - <input type="text" value="16"/> : <input type="text" value="56"/>
<p><i>*When you use the download service of FTP, HTTP, or BT, please check if these files you downloaded are legal or not.</i></p>	
<input type="button" value="E-mail Alert Configuration"/> <input type="button" value="Save"/> <input type="button" value="Undo"/>	

1. Job Name:

It's for you to remember the job easily, and the device would use this name to info you when the job is done.

2. URL:

The URL for the file you want to download.

You have to use this format:

IP/path/file, you don't have to add protocol part such like "ftp://".

3. Save To:

The destination path on USB disk that you want to save files.

Default value is /C/Download/FTP

4. Login method:

Anonymous, you can access this site without any authentication

Account, you have to enter the username and password to login.

5. Start Time:

Schedule: this device will start FTP download on the time that you specified. The schedule job that is saved could be check on Status page by selecting "View Scheduled Download Status".

At Once: the FTP download would be started immediately.

3.3.1.8. HTTP

Download Assistant - HTTP	
Item	Setting
▶ Download Type	<input type="radio"/> FTP <input checked="" type="radio"/> HTTP <input type="radio"/> BT
▶ Job Name	<input type="text"/>
▶ URL	<input type="text"/>
▶ Save To	<input type="text" value="/C/Downloads/HTTP"/>
▶ Start Time	<input type="radio"/> Schedule <input checked="" type="radio"/> At Once
	Time <input type="text" value="2010"/> / <input type="text" value="Jun"/> / <input type="text" value="29"/> - <input type="text" value="16"/> : <input type="text" value="56"/>
<i>*When you use the download service of FTP, HTTP, or BT, please check if these files you downloaded are legal or not.</i>	
<input type="button" value="E-mail Alert Configuration"/> <input type="button" value="Save"/> <input type="button" value="Undo"/>	

1. Job Name:

It's for you to remember the job easily, and the device would use this name to info you when the job is done.

2. URL:

The URL for the file you want to download.

You have to use this format:

IP/path/file, you don't have to add protocol part such like "http://".

3. Save To:

The destination path on USB disk that you want to save files.

Default value is /C/Download/HTTP

4. Start Time:

Schedule: this device will start FTP download on the time that you specified. The schedule job that is saved could be check on Status page by selecting "View Scheduled Download Status".

At Once: the FTP download would be started immediately.

3.3.2. How to access data on the NAS?

3.3.2.1. Windows User

3.3.2.1.1. By network place

Then start your “file manager”, type the IP with “\\” on the beginning, as follow picture shown. Then press enter.

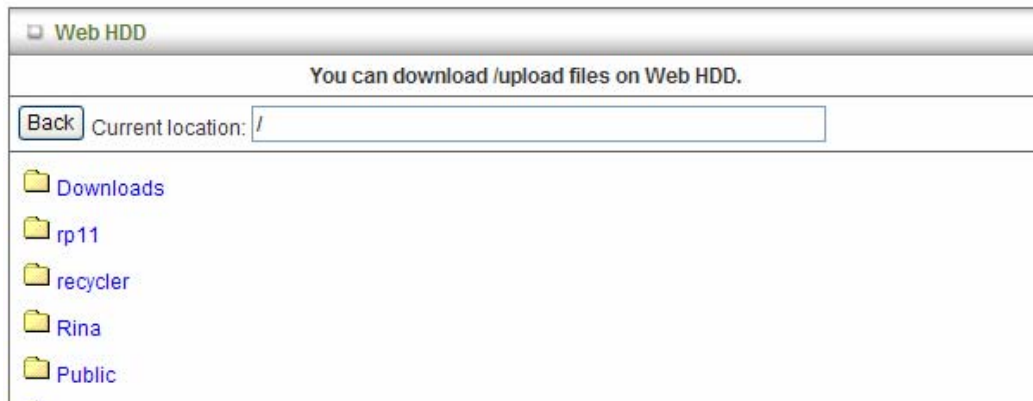


You could find a folder named “Storage”. It is what you are looking for.



3.3.2.1.2. By Web HDD

This Web HDD can allow you to enter HDD by web UI, and also can allow you to let ‘guest’ to enter the ‘public’ area only.



3.3.2.2. Unix User

We do not provide NFS support, so the only way for UNIX to get files is FTP.

Use your FTP client to connect the FTP server.

3.4. System

3.4.1. Scheduling

You can set the schedule time to decide which service will be turned on or off.

Schedule Rule		[HELP]
Item	Setting	
▶ Schedule	<input type="checkbox"/> Enable	
Rule#	Rule Name	Action
1		<input type="button" value="New Add"/>
2		<input type="button" value="New Add"/>
3		<input type="button" value="New Add"/>
4		<input type="button" value="New Add"/>
5		<input type="button" value="New Add"/>
6		<input type="button" value="New Add"/>
7		<input type="button" value="New Add"/>
8		<input type="button" value="New Add"/>
9		<input type="button" value="New Add"/>
10		<input type="button" value="New Add"/>
<input type="button" value=" << Previous"/> <input type="button" value=" Next >>"/> <input type="button" value=" Save"/> <input type="button" value=" Add New Rule..."/>		

1. **Schedule:** Check to enable the schedule rule settings.
2. **Add New Rule:** To create a schedule rule, click the “New Add” button. You can edit the **Name of Rule, Policy**, and set the schedule time (**Week day, Start Time**, and **End Time**). The following example configures “wake-up time” everyday from 06:00 to 07:00.

Edit Schedule Rule				[HELP]
Item	Setting			
▶ Name of Rule 1	<input type="text" value="wake-up time"/>			
▶ Policy	<input type="button" value="Inactivate"/> except the selected days and hours below.			
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)	
1	<input type="button" value="Every Day"/>	<input type="text" value="06:00"/>	<input type="text" value="07:00"/>	
2	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>	
3	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>	
4	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>	
5	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>	
6	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>	
7	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>	
8	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>	
<input type="button" value=" Save"/> <input type="button" value=" Undo"/> <input type="button" value=" Back"/>				

Afterwards, click “save” to store your settings or click “Undo” to give up the changes.

3.4.2. System Tools

3.4.2.1. System Log

System Log		[HELP]
Item	Setting	Enable
▶ IP address for syslogd	<input type="text"/>	<input type="checkbox"/>
▶ Setting of Email alert		<input type="checkbox"/>
• SMTP Server : port	<input type="text"/> : <input type="text"/>	
• SMTP Username	<input type="text"/>	
• SMTP Password	<input type="text"/>	
• E-mail addresses	<input type="text"/>	
• E-mail subject	<input type="text"/>	

This page supports two methods to export system logs to specific destination by means of syslog (UDP) and SMTP(TCP). The items you have to setup include:

1. **IP Address for Syslog:** Host IP of destination where syslog will be sent to. Check **Enable** to enable this function.
2. **Setting of Email alert:** Check if you want to enable Email alert (send syslog via email).
3. **SMTP Server: Port:** Input the SMTP server IP and port, which are connected with ':'. If you do not specify port number, the default value is 25.
For example, "mail.your_url.com" or "192.168.1.100:26".
4. **SMTP Username:** Enter the Username offered by your ISP.
5. **SMTP Password:** Enter the User name offered by your ISP.
6. **E-mail Addresses:** The recipients are the ones who will receive these logs. You can

assign more than 1 recipient, using ';' or ',' to separate these email addresses.

7. **E-mail Subject:** The subject of email alert is optional.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.4.2.2. System Time

System Time [HELP]	
Item	Setting
▶ Time Zone	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
▶ Auto-Synchronization	<input checked="" type="checkbox"/> Enable Time Server (RFC-868): Auto
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Sync with Time Server"/> <input type="button" value="Sync with my PC (undefined December 21, 2009 09:29:06)"/>	

1. **Time Zone:** Select a time zone where this device locates.
2. **Auto-Synchronization:** Check the “Enable” checkbox to enable this function. Besides, you can select a NTP time server to consult UTC time.
3. **Sync with Time Server:** Click on the button if you want to set Date and Time by NTP Protocol .
4. **Sync with my PC:** Click on the button if you want to set Date and Time using PC’s Date and Time.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.4.2.3. System Info

System Information	
Item	Setting
WAN Type	3G
Display time	Mon, 21 Dec 2009 09:52:30 +0800
System Log	
Time	Log
Dec 21 08:31:59	kernel: klogd started: BusyBox v1.3.2 (2009-12-16 11:05:05 CST)
Dec 21 08:32:04	udhcpd[816]: udhcpd (v0.9.9-pre) started
Dec 21 08:32:04	udhcpd[816]: SIOCGIFINDEX failed!: No such device
Dec 21 08:32:07	syslog: Failure parsing line 11 of /etc/udhcpd.conf
Dec 21 08:32:07	udhcpd[1417]: udhcpd (v0.9.9-pre) started
Dec 21 08:32:07	udhcpd[1417]: Unable to open /var/run/udhcpd.leases for reading
Dec 21 08:32:08	init: Starting pid 1453, console /dev/ttyS1: '/bin/bash'
Dec 21 08:32:09	oomander: STOP WANTYPE 3G
Dec 21 08:32:29	udhcpd[1419]: sending OFFER of 192.168.123.100
Dec 21 08:32:29	udhcpd[1419]: sending ACK to 192.168.123.100
Dec 21 08:37:43	udhcpd[1419]: Received a SIGUSR1
Dec 21 08:53:15	udhcpd[1419]: sending OFFER of 192.168.123.101
Dec 21 08:59:44	rtalrt: fail to read pid file
Dec 21 09:20:01	udhcpd[1419]: sending OFFER of 192.168.123.101
Dec 21 09:20:05	udhcpd[1419]: sending OFFER of 192.168.123.101

Page: 1/2 (Log Number: 29)

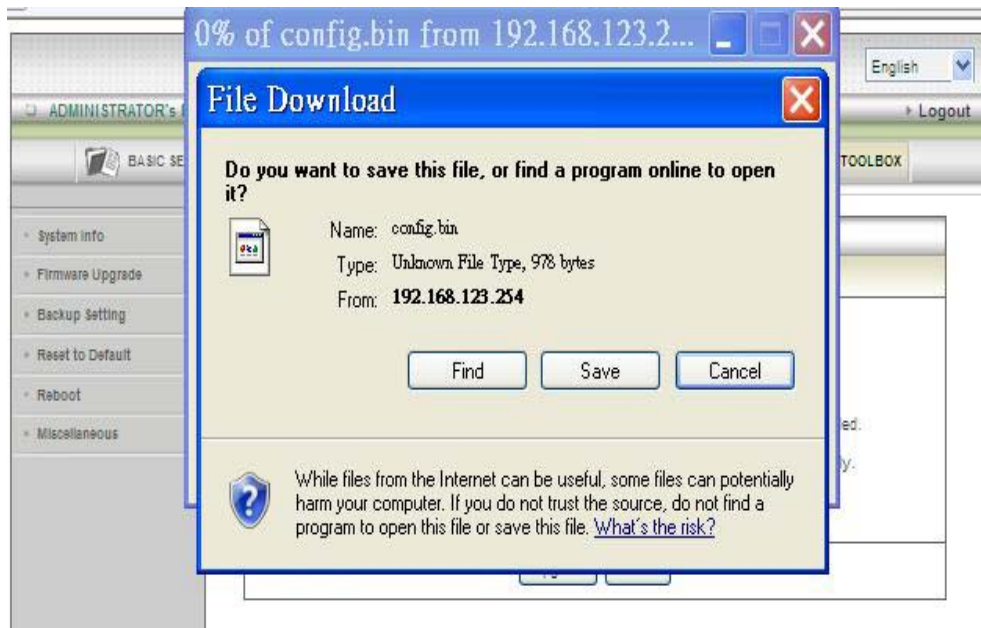
You can view the System Information and System log, and download/clear the System log, in this page.

3.4.2.4. Firmware Upgrade

You can upgrade firmware by clicking “Upgrade” button.

Firmware Upgrade	
Firmware Filename	
<input type="text"/>	<input type="button" value="Browse..."/>
Current firmware version is R1.01b1 .	
<p>Note! Do not interrupt the process or power off the unit when it is being upgraded.</p> <p>When the process is done successfully, the unit will be restarted automatically.</p>	
<input type="checkbox"/> Accept unofficial firmware.	
<input type="button" value="Upgrade"/>	<input type="button" value="Cancel"/>

3.4.2.5. Backup Setting



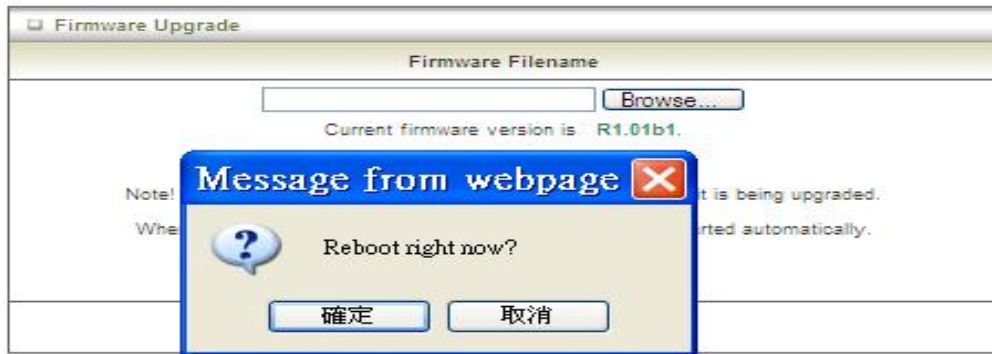
You can backup your settings by clicking the “**Backup Setting**” function item and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you saved.

3.4.2.6. Reset to Default



You can also reset this device to factory default settings by clicking the **Reset to default** function item.

3.4.2.7. Reboot



You can also reboot this device by clicking the **Reboot** function item.

3.4.2.8. Miscellaneous

Miscellaneous Items [HELP]	
Item	Setting
▶ MAC Address for Wake-on-LAN	<input type="text"/> <input type="button" value="Wake up"/>
▶ Domain Name or IP address for Ping Test	<input type="text"/> <input type="button" value="Ping"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

1. **MAC Address for Wake-on-LAN:** It enables you to power up a networked device remotely. If you would like to trigger this function, you have to know the MAC address of this device. For instance if the MAC address is 00-11-22-33-44-55, enter it into the blank of MAC Address for Wake-on-LAN. Afterwards, click "Wake up" button which makes the router to send the wake-up frame to the target device immediately.
2. **Domain Name or IP address for Ping Test:** Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

4 . Troubleshooting

This Chapter provides solutions to problems for the installation and operation of the WiFi Broadband Router. You can refer to the following if you are having problems.

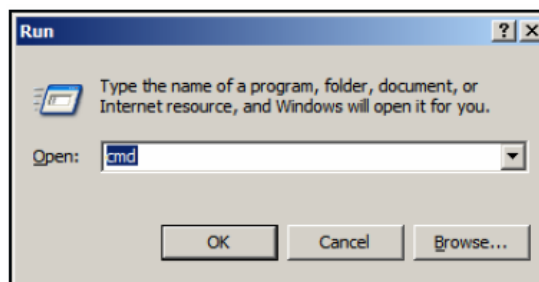
1 Why can't I configure the router even the cable is plugged and the LED is lit?

Do a **Ping test** to make sure that the WiFi Broadband Router is responding.

Note: It is recommended that you use an

Go to **Start > Run**.

1. Type **cmd**.



2. Press **OK**.
3. Type **ipconfig** to get the IP of default gateway.
4. Type "**ping 192.168.123.254**". Assure that you ping the correct IP Address assigned to the WiFi Broadband Router. It will show four replies if you ping

correctly.

```
Pinging 192.168.123.254 with 32 bytes of data:  
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64  
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64  
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64  
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64
```

Ensure that your Ethernet Adapter is working, and that all network drivers are installed properly. Network adapter names will vary depending on your specific adapter. The installation steps listed below are applicable for all network adapters.

1. Go to **Start > Right click on “My Computer” > Properties**.
2. **Select the Hardware Tab**.
3. Click **Device Manager**.
4. Double-click on **“Network Adapters”**.
5. Right-click on **Wireless Card bus Adapter** or **your specific network adapter**.
6. Select **Properties** to ensure that all drivers are installed properly.
7. Look under **Device Status** to see if the device is working properly.
8. Click **“OK”**.

2 What can I do if my Ethernet connection does not work properly?

- A. Make sure the RJ45 cable connects with the router.
- B. Ensure that the setting on your Network Interface Card adapter is “Enabled”.
- C. If settings are correct, ensure that you are not using a crossover Ethernet cable, not all Network Interface Cards are MDI/MDIX compatible, and use a patch cable is recommended.
- D. If the connection still doesn’t work properly, then you can reset it to default.

3 Something wrong with the wireless connection?

A. Can't setup a wireless connection?

- I. Ensure that the SSID and the encryption settings are exactly the same to the Clients.
- II. Move the WiFi Broadband Router and the wireless client into the same room, and then test the wireless connection.
- III. Disable all security settings such as **WEP**, and **MAC Address Control**.
- IV. Turn off the WiFi Broadband Router and the client, then restart it and then turn on the client again.
- V. Ensure that the LEDs are indicating normally. If not, make sure that the power and Ethernet cables are firmly connected.
- VI. Ensure that the IP Address, subnet mask, gateway and DNS settings are correctly entered for the network.
- VII. If you are using other wireless device, home security systems or ceiling fans, lights in your home, your wireless connection may degrade dramatically. Keep your product away from electrical devices that generate RF noise such as microwaves, monitors, electric motors...

B. What can I do if my wireless client can not access the Internet?

- I. Out of range: Put the router closer to your client.
- II. Wrong SSID or Encryption Key: Check the SSID or Encryption setting.
- III. Connect with wrong AP: Ensure that the client is connected with the correct Access Point.
 - i. **Right-click** on the **Local Area Connection icon** in the taskbar.
 - ii. Select **View Available Wireless Networks in Wireless Configure**. Ensure you have selected the correct available network.

- iii. Reset the WiFi Broadband Router to default setting

C. Why does my wireless connection keep dropping?

- I. Antenna Orientation.
 - i. Try different antenna orientations for the WiFi Broadband Router.
 - ii. Try to keep the antenna at least 6 inches away from the wall or other objects.
- II. Try changing the channel on the WiFi Broadband Router, and your Access Point and Wireless adapter to a different channel to avoid interference.
- III. Keep your product away from electrical devices that generate RF noise, like microwaves, monitors, electric motors, etc.

4 What to do if I forgot my encryption key?

1. Go back to advanced setting to set up your Encryption key again.
2. Reset the WiFi Broadband Router to default setting

5 How to reset to default?

1. Ensure the WiFi Broadband Router is powered on
2. Find the **Reset** button on the right side
3. Press the **Reset** button for 8 seconds and then release.
4. After the WiFi Broadband Router reboots, it has back to the factory **default** settings.

Appendix A. Spec Summary Table

Device Interface		CDD531AM-U03
ADSL2 /2+ Standard Module	ADSL2+ connector, 1 x RJ-11 port ITU 992.1 (G.dmt) Annex A, ITU 992.2 (G.lite), ITU 992.3 ADSL2 (G.dmt.bis), ITU 992.5 ADSL2+	•
Wireless WAN	USB 2.0 for external HSPA modem(only for CDD531AM-U03)	1
Ethernet WAN	1 xRJ45 port LAN/WAN configurable	1
Ethernet LAN	3 xRJ-45 port, 10/100Mbps, auto-MDI/MDIX	3
USB Sharing	USB 2.0 for file sharing, same as 3G USB port (only for CDD531AM-U03)	1
Antenna	1.8 dBi Fixed antenna	1
Reset / WPS / Wireless On/Off Button	3-in-1 Reset / WPS / Wireless On/Off Button	1
LED Indication	Status(USB)/ADSL/ LAN1 ~ LAN4/ WiFi	•
Power Jack	DC Power Jack, powered via external DC 5V/2A switching power adapter (CDD530AM-003 for DC5V/1.2A)	1
Wireless LAN (WiFi)		
Standard	IEEE 802.11b/g/n (1x1) compliance	•
SSID	SSID broadcast or in stealth mode	•
Channel	Auto-selection, manually	•
Security	WEP, WPA, WPA-PSK, WPA2, WPA2-PSK	•
WPS	WPS (Wi-Fi Protected Setup)	•
WMM	WMM (Wi-Fi Multimedia)	•
Functionality		
ADSL WAN	PPPoE / PPPoA / IPoA / Static IP / Dynamic IP/Bridge up to 8 PVCs supported	•
WAN Connection	Auto-reconnect, dial-on-demand,	•

	manually	
Connection scheme	Fail-over Backup	•
Ethernet WAN	ADSL as primary, LAN Port 1 configures to WAN for WAN connection when ADSL line is not working	•
IPv6 support	Support IPv4/IPv6 dual stack protocol	•
One-to-Many NAT	Virtual server, special application, DMZ, IPTV IGMP V1 V2 Pass through	•
NAT Session	Support NAT session	•
SPI Firewall	IP/Service filter, URL blocking, MAC control	•
DoS Protection	DoS (Deny of Service) detection and protection	•
Routing Protocol	Static route, dynamic route (RIP v1/v2)	•
IPTV features	Support IPTV IGMPv1/v2/v3 snooping and filtering, VLAN tagged/ Untagged frames	•
QoS	Support QoS mechanism for prioritizing the various type of traffics, TOS/DSCP to 802.1p mapping (DiffServ)	•
Storage/File Sharing	FAT16/FAT32, EXT2, NTFS (Read only) Samba server, FTP server	•
Media server	UPnP AV media server, iTunes server	•
Scheduling Download management	FTP HTTP	•
Management	SNMP, UPnP IGD, syslog	•
Remote Management	TR069 (support ACS 2-wire)	•
Administration	Web-based UI, remote login, backup/restore setting	•
Environment & Certification		
Package Content	CDD531AM-U03, Power adapter, Quick Installation Guide, CD	•

Package Information	Device dimension (mm)	150x112x20
	Package dimension (246x210x62mm) SP/MP/ZP	●
	Package dimension (214x146x69mm) PP	○
	Package dimension (290x234x100mm) AP	○
Package weight	Package weight (g)	TBD
Operation Temp.	Temp.: 0~40°C, Humidity 10%~90% non-condensing	●
EMI Certification	CE/FCC compliance	●
RoHS	RoHS compliance	●

*Specifications are subject to change without prior notice.

Appendix B. Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please refer to the GNU General Public License below to check the detailed terms of this license.

The following parts of this product are subject to the GNU GPL, and those software packages are copyright by their respective authors.

Linux Kernel	GPLv2	Linux-2.6.21
busybox	GPLv2	busybox_1.3.2
bridge-utils	GPLv2	bridge-utils 1.1
udhcp server	GPLv2	udhcp-0.9.9
udhcp client		
fdisk	GPLv2	util-linux 2.12q
mke2fs, e2fsck	GPLv2	e2fsprogs v1.40.2
samba	GNUv2	samba 3.0.20
wireless tools	GPLv2	wireless tools
vsftpd	GPLv2	vsftpd-2.0.3
Transmission	MIT	Transmission-1.74
mt-daapd	GNUv2	mt-daapd-0.2.4
dnrd	GNUv2	DNRD-2.17
libcurl		cURL-7.19.6
OpenSSL	BSD	openssl-1.0.0b3
ntfs-3g	GNUv2	ntfs-3g-2009.4.4
Zebra	GNUv2	zebra-0.95a
snmpd		CMU snmp-4.1.2
pptp	GNUv2	pptp-1.7.1
pppoe	GPLv2	pppoe-3.8
pppd	BSD	ppp-2.4
l2tpd	GPLv2	l2tp-0.4
iptables	GNUv2	iptables-1.4.2
tc	GNUv2	iproute2-2.6.11
wget	GNU	wget-1.7.1

Availability of source code

Please visit our web site or contact us to obtain more information.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the

term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange;

- or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the

rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS