



LevelOne



WGR-6012

300Mbps *N_Max* Wireless Gigabit Router

User Manual

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.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

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

The specification is subject to change without notice.

Table of Contents

Chapter 1 Introduction	4
1.1 Packing List	4
1.2 Spec Summary Table	4
1.3 Hardware.....	5
1.4 LED Indicators.....	5
1.5 Procedure for Hardware Installation	6
Chapter 2 Getting Start	10
2.1 Select Language	10
2.2 Setup mode	11
2.3 Advanced mode Setup.....	11
2.4 Quick Wizard Install mode Setup	12
2.5 Wireless Setting.....	12
2.6 Auto Detect WAN Service.	13
2.7. Manual select WAN Service	13
2.8 Summary of the settings and Next to “Reboot”	13
2.9 Apply the Settings or Modify.	14
2.10 Test the Internet connection.	14
2.11 Setup Completed.....	15
Chapter 3 Making Configuration	16
3.1 Login to Configure from Wizard.....	17
3.2 System Status	21
3.3 Advanced	21
3.3.1 Basic Setting	21
3.3.1.1 Primary Setup – WAN Type, Virtual Computers	23
3.3.2 Forwarding Rules	36
3.3.3 Security Settings.....	39
3.3.4 Advanced Settings	53
3.3.5 Toolbox.....	61
Appendices and Index	64
802.1x Setting	64
1. Equipment Details.....	64
2. DUT Configuration:	65
3. DUT and Windows 2000 Radius Server Setup.....	65
4. Windows 2000 RADIUS server Authentication testing:	67
WPA Settings	70
FAQ and Troubleshooting	79

Chapter 1 Introduction

Congratulations on your purchase of this outstanding Wireless Broadband Router. This product is specifically designed for Small Office and Home Office needs. It provides a complete SOHO solution for Internet surfing, and is easy to configure and operate even for non-technical users. 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 Packing List

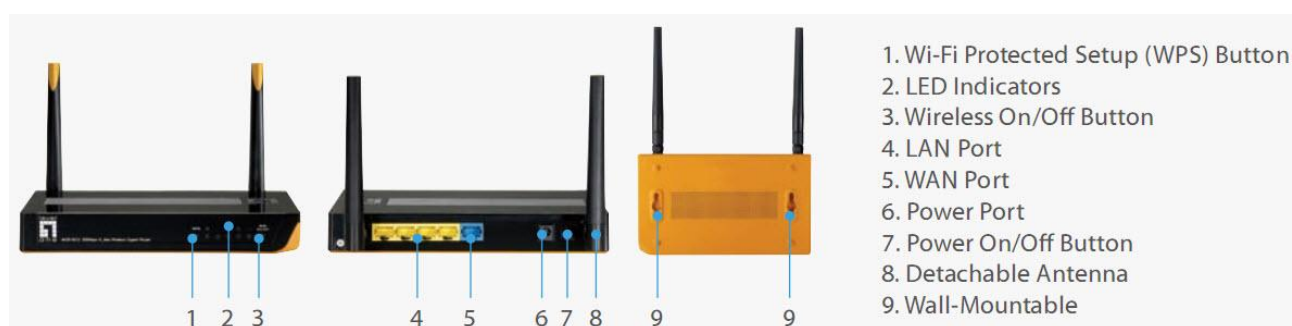
- WGR-6012 x1
- RJ-45 Ethernet LAN Cable x1
- Antenna x 2
- Power Adapter x1
- Quick Installation Guide x1
- CD Manual x1

1.2 Spec Summary Table

Device Interface		
Ethernet WAN	RJ-45 port, 10/100/1000Mbps, auto-MDI/MDIX	1
Ethernet LAN	RJ-45 port, 10/100/1000Mbps, auto-MDI/MDIX	4
Antenna	2 dBi detachable antenna	2
WPS Button	For WPS connection	1
Wireless Enable/disable	To enable or disable Wireless Radio	1
LED Indication	Power/Status / WAN / LAN1 ~ LAN4/ Wi-Fi	●
Power Jack	DC Power Jack, powered via external DC 12V/1A switching power adapter	1
Wireless LAN (Wi-Fi)		
Standard	IEEE 802.11b/g/n 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		

Ethernet WAN	PPPoE, DHCP client, Static IP, PPTP, L2TP	●
WAN Connection	Auto-reconnect, dial-on-demand, manually	●
One-to-Many NAT	Virtual server, special application, DMZ, Super DMZ (IP Passthrough)	●
NAT Session	Support NAT session	20000
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)	●
Management	SNMP, UPnP IGD, syslog, DDNS	●
Administration	Web-based UI, remote login, backup/restore setting	●
Performance	NAT up to 700Mbps and Wireless up to 150Mbps	
Environment & Certification		
Package Information	Package dimension (mm)	
	Package weight (g)	
Operation Temp.	Temp.: 0~40°C, Humidity 10%~90% non-condensing	●
Storage Temp.	Temp.: -10~70°C, Humidity: 0~95% non-condensing	●
EMI Certification	CE/FCC compliance	●
RoHS	RoHS compliance	●

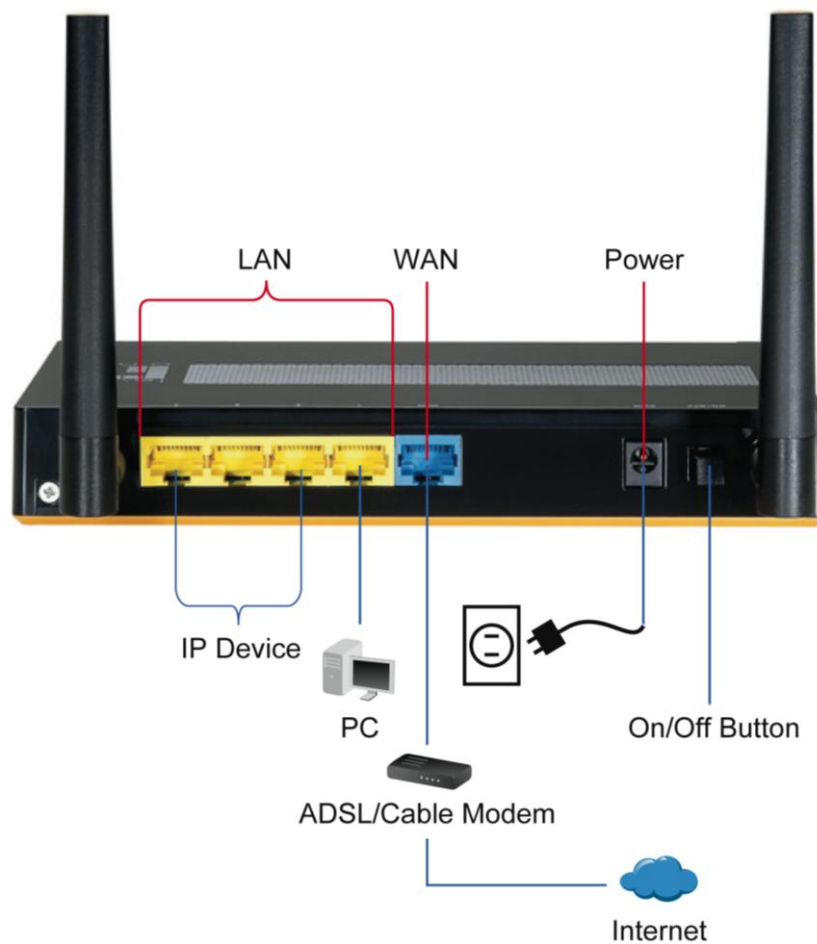
1.3 Hardware



1.4 LED Indicators

	LED status	Description
Status	Green in flash	Device status is working.
WAN LED	Green	RJ-45 cable is plugged
	Green in flash	Data access
LAN LED	Green	RJ-45 cable is plugged
	Green in flash	Data access
Wi-Fi LED	Green	WLAN is on
	Green in flash	Data access
	Green in fast flash	Device is in WPS PBC mode
	Green in dark	Wi-Fi Radio is disabled

1.5 Procedure for Hardware Installation





Step 1. Attach the antenna.

- 1.1. Remove the antenna from its plastic wrapper.
- 1.2. Screw the antenna in a clockwise direction to the back panel of the unit.
- 1.3. Once secured, position the antenna upward at its connecting joint. This will ensure optimal reception.



1. Turn off the Power Switch first.



Step 2 Insert the Ethernet cable into LAN Port:

Insert the Ethernet patch cable into LAN port on the back panel of Router, and an available Ethernet port on the network adapter in the computer you will use to configure the unit.



Step 3 Insert the Ethernet patch cable into Wired WAN port:

Insert the Ethernet patch cable form DSL Modem into Wired WAN port on the back panel of Router.



Step 4. Power on Router:

4.1. Connect the power adapter to the receptor on the back panel of your Router and Push Power switch

Step 5. Complete the setup.

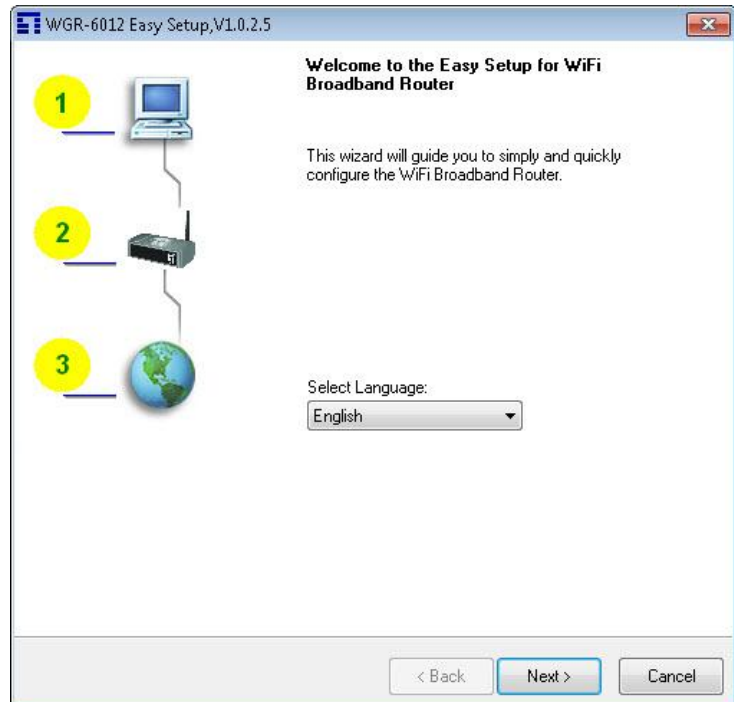
5.1. When complete, the Status LED will flash.

Chapter 2 Getting Start

Insert the CD into CD reader on your PC. The program, AutoRun, will be executed automatically. And then you can click the Easy setup Icon for this utility.

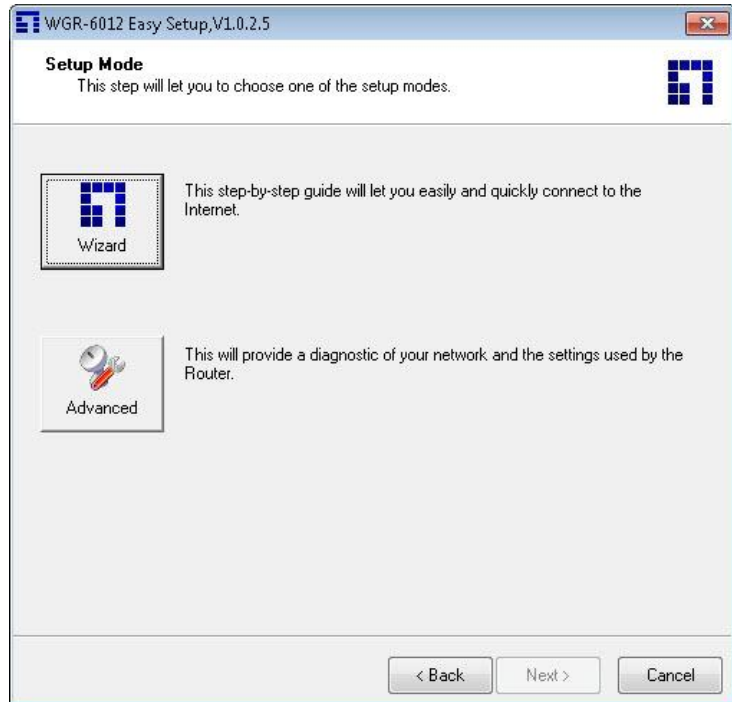
Configure the settings by the following steps.

2.1 Select Language then click “Next”
for continues.



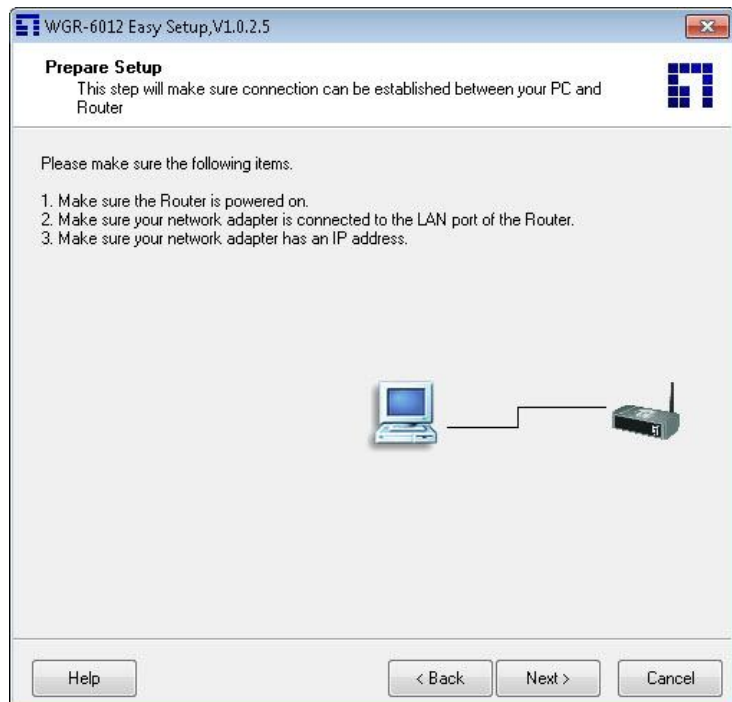
2.2 Setup mode

You can select Wizard mode to run the setup step-by-step or run advanced mode to diagnose the network settings of the router.



2.3 Advanced mode Setup.

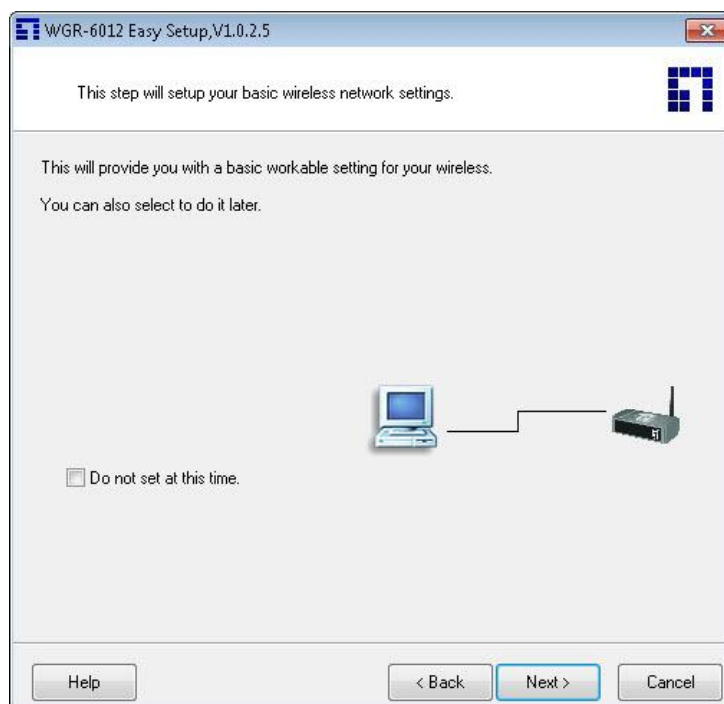
Check the PC, Router or Internet icons for the Status of PC, Router or Internet.



2.4 Quick Wizard Install mode Setup

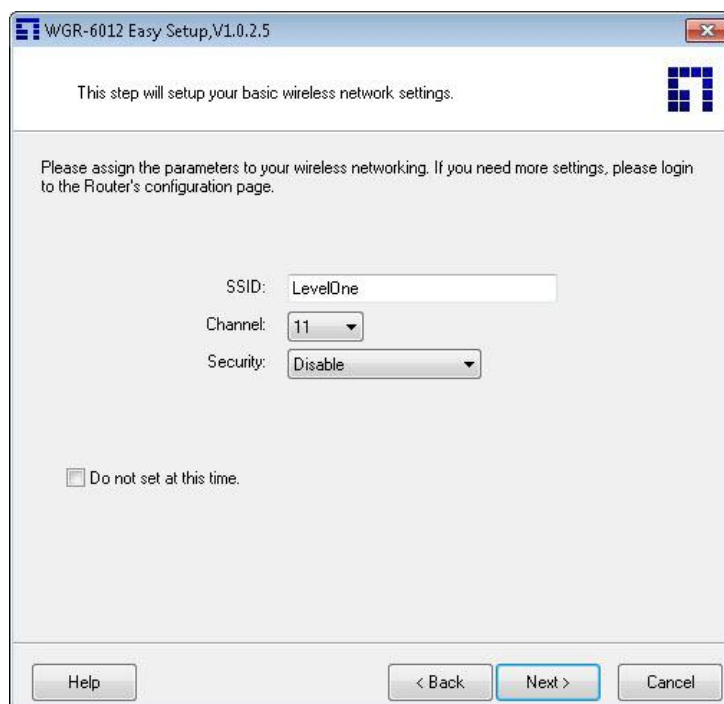
1. Make sure the router is powered on.
2. Make sure your network adapter is connected to the LAN port of the router
3. Make sure your network adapter has an IP address.

Click “Next” for continues



2.5 Wireless Setting.

Key in the SSID, Channel and Security options, and then click “Next” for continues.



2.6 Auto Detect WAN Service.

Click “Next” for continue.

Click the button, “Let me select WAN service by myself”, to disable this function.

Note: The Item supports to detect the Dynamic and PPPoE WAN Services only



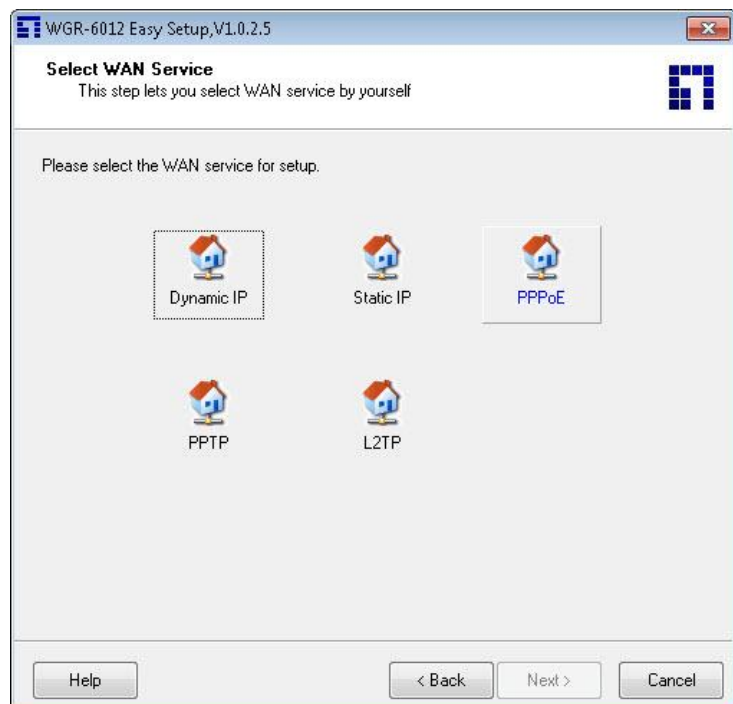
Example, the Dynamic WAN type is tested.

2.7. Manual select WAN Service

In the manual mode, Click the any icons for continues.

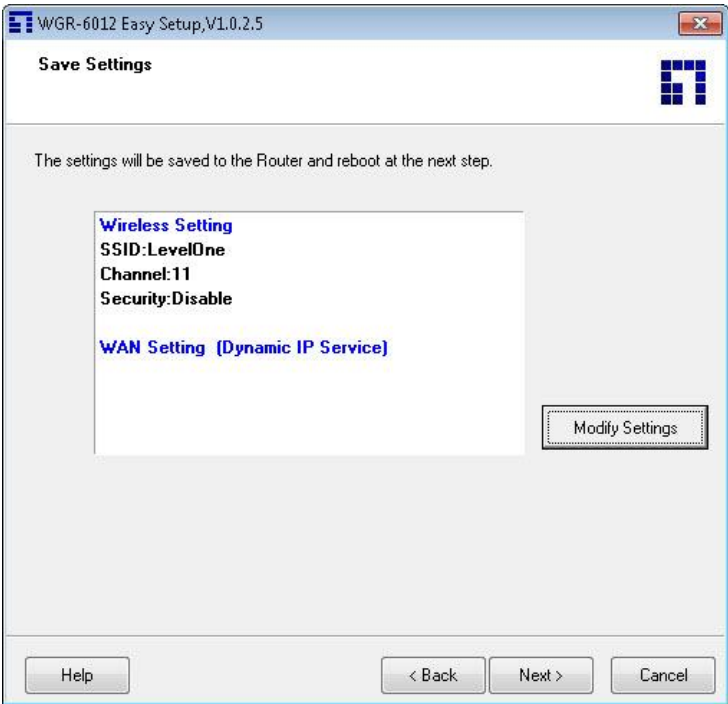
2.8 Summary of the settings and Next to “Reboot”

Click “Next” for continue.



2.9 Apply the Settings or Modify.

Click “Next” for continue.



2.10 Test the Internet connection.

Test WAN Networking service. Click “Next” for continue.

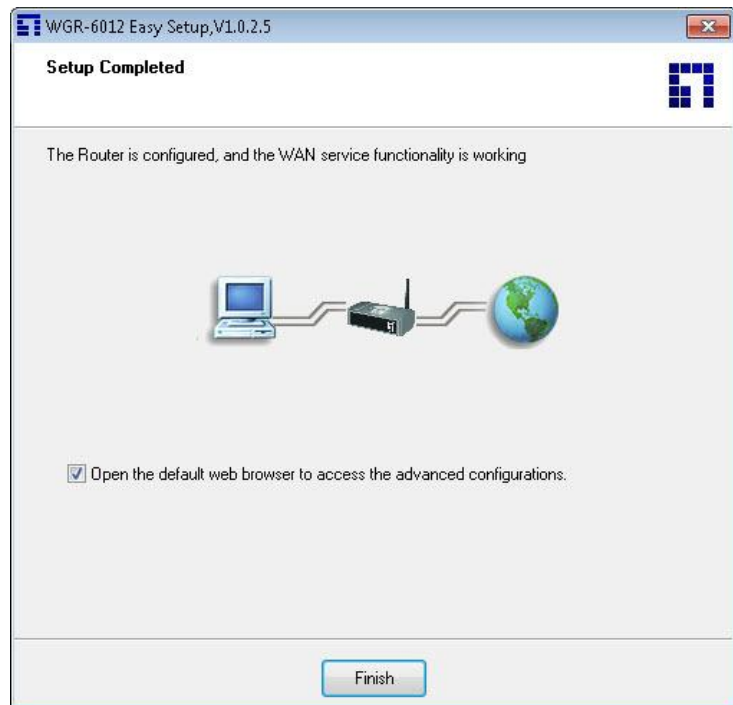
You can ignore the by select the “Ignore Test”.



2.11 Setup Completed.

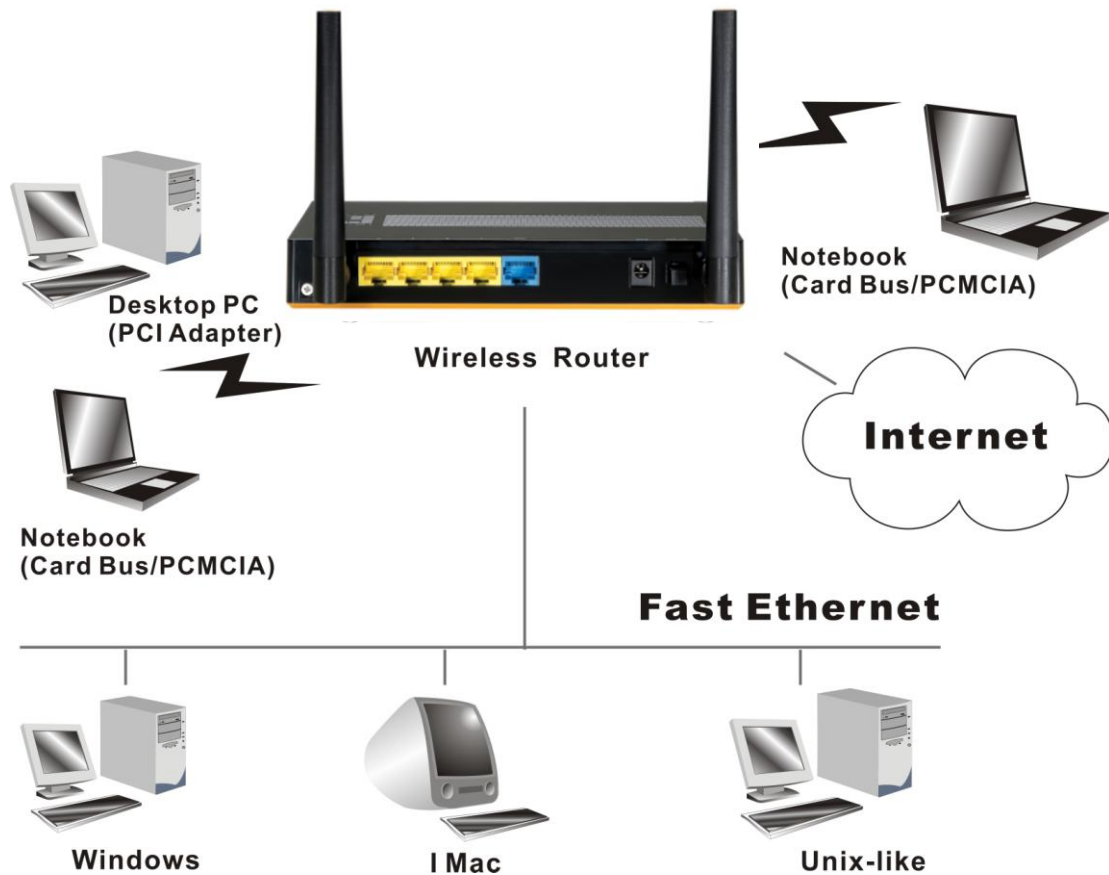
The EzSetup is finish, you can open the default web browser to configure advanced settings of the Router.

Click “Finish” to complete the installation.



Chapter 3 Making Configuration

This product provides Web based configuration scheme, that is, configuring by your Web browser, such as Mozilla Firefox or Internet Explorer. This approach can be adopted in any MS Windows, Macintosh or UNIX based platforms.



3.1 Login to Configure from Wizard

Type in the IP Address

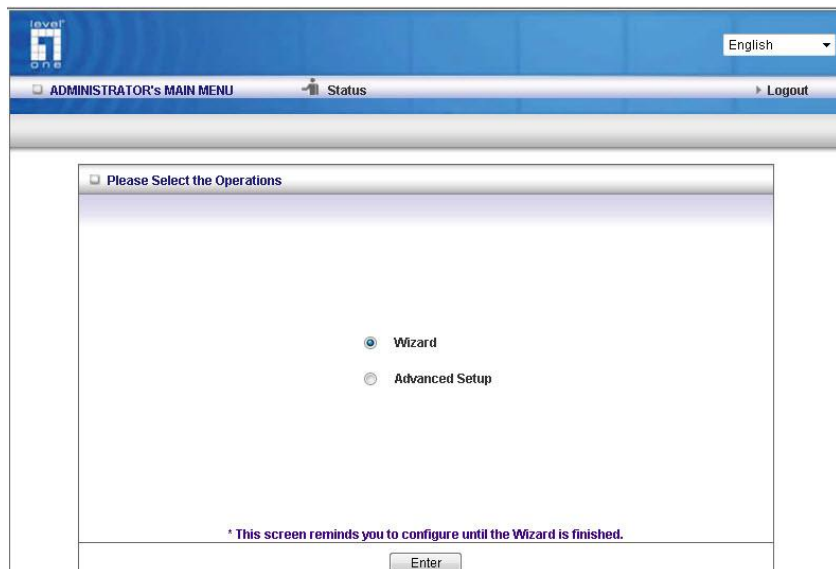
(<http://192.168.1.1/>)



Type password, the default is
"admin" and click 'login' button.



Press "Wizard" for basic
settings with simple way.



Press "Next" to start wizard.



Step 1:
Set up your system password.

Setup Wizard - Setup Login Password

[EXIT]

Old Password

New Password

Reconfirm

< Back

[Start > Password > WAN > Wireless > Summary > Finish!]

Next >

Step 2:
Select Wan Type.

Auto Detecting or
Setup Manually.

Setup Wizard - WAN Type Setup

[EXIT]

☒ Auto Detecting WAN Type

☐ Setup WAN Type Manually

< Back

[Start > Password > WAN > Wireless > Summary > Finish!]

Next >

Setup Wizard - Select WAN Type

[EXIT]

☐ ISP assigns you a static IP address. (Static IP Address)

☒ Obtain an IP address from ISP automatically. (Dynamic IP Address)

☐ Dynamic IP Address with Road Runner Session Management. (e.g. Telstra BigPond)

☐ Some ISPs require the use of PPPoE to connect to their services. (PPP over Ethernet)

☐ Some ISPs require the use of PPTP to connect to their services. (PPTP)

☐ Some ISPs require the use of L2TP to connect to their services. (L2TP)

< Back

[Start > Password > WAN > Wireless > Summary > Finish!]

Next >

Step 3:
Setup the LAN IP and WAN
Type.

Setup Wizard - WAN Settings - Dynamic IP Address

[EXIT]

▶ LAN IP Address

192.168.1.1

▶ Account

▶ Password

▶ Login Server

(optional)

< Back

[Start > Password > WAN > Wireless > Summary > Finish!]

Next >

Example:

Step 4:
Please fill in PPPoE service
information which is provided by
your ISP.

Setup Wizard - WAN Settings - PPP over Ethernet

[EXIT]

▶ LAN IP Address

192.168.1.1

▶ Account

▶ Password

▶ Primary DNS

0.0.0.0

▶ Secondary DNS

0.0.0.0

▶ PPPoE Service Name

(optional)

▶ Assigned IP Address

0.0.0.0

(optional)

< Back

[Start > Password > WAN > Wireless > Summary > Finish!]

Next >

Step 5:
Set up your Wireless.

Setup Wizard - Wireless settings

[EXIT]

▶ Wireless function

☒ Enable ☐ Disable

▶ Network ID(SSID)

LevelOne

▶ Channel

11

< Back

[Start > Password > WAN > Wireless > Summary > Finish!]

Next >

Set up your Authentication and Encryption.

Setup Wizard - Wireless Security

[EXIT]

Security

WEP

Key 1

Key 2

Key 3

Key 4

WEP

64 bits

128 bits

1234567890

< Back

[Start > Password > WAN > **Wireless** > Summary > Finish!]

Next >

Step 6:
Then click Apply Setting.
And then the device will reboot.

Setup Wizard - Summary

[EXIT]

Please confirm the information below.

[WAN Setting]

WAN Type

Account

Password

Service Name

Assigned IP Address

PPPoE

123

1234

-

0.0.0.0

[Wireless Setting]

Wireless

SSID

Channel

Security

Enable

LevelOne

11

64-bit WEP Enabled

☒ Do you want to proceed the network testing?

< Back

[Start > Password > WAN > Wireless > **Summary** > Finish!]

Apply Settings

Step 7:
Click Finish to complete it.

Setup Wizard

[EXIT]

Configuration is Completed.

Please click "Finish" to back to Status page.

Or you can click "Configure Again" to setup the wizard again.

Configure Again

[Start > Password > WAN > Wireless > Summary > **Finish!**]

Finish

3.2 System Status



The screenshot shows the LevelOne Administrator's Main Menu. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The 'Status' section is active, displaying a table for 'System Status' with columns for 'Item', 'WAN Status', and 'Sidenote'. The table lists various network parameters and their current values.

Item	WAN Status	Sidenote
IP Address	0.0.0.0	PPPoE
Subnet Mask	255.255.255.255	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0	
Connection Time	-	
MAC Address	00-50-18-21-D4-34	

Below the table, there is a section for 'Wireless Status'.

This option provides the function for observing this product's working status:

WAN Port Status.


If the WAN port is assigned a dynamic IP, there may appear a **"Renew"** or **"Release"** button on the Side note column. You can click this button to renew or release IP manually.

Statistics of WAN: enables you to monitor inbound and outbound packets

3.3 Advanced

3.3.1 Basic Setting


Please Select "Advanced Setup" to Setup





English


ADMINISTRATOR's MAIN MENU


StatusWizardAdvancedLogout

BASIC SETTING

FORWARDING RULES

SECURITY SETTING

ADVANCED SETTING

TOOLBOX

Primary Setup

DHCP Server

Wireless

Change Password

Basic Setting

- Primary Setup**
 - Configure LAN IP, and select WAN type.
- DHCP Server**
 - The settings include Host IP, Subnet Mask, Gateway, DNS, and WINS configurations.
- Wireless**
 - Wireless settings allow you to configure the wireless configuration items.
- Change Password**
 - Allow you to change system password.

3.3.1.1 Primary Setup – WAN Type, Virtual Computers

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

Primary Setup [Help]

Item	Setting
▶ LAN IP Address	192.168.1.1
▶ WAN Type	Dynamic IP Address Change...
▶ Host Name	WGR-6012 (optional)
▶ WAN's MAC Address	00-50-18-21-D4-34 Clone MAC
▶ Renew IP Forever	<input type="checkbox"/> Enable (Auto-reconnect)
▶ IGMP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

[Save](#) [Undo](#) [Virtual Computers...](#)

Press “Change”

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

Choose WAN Type

Type	Usage
<input type="radio"/> Static IP Address	ISP assigns you a static IP address.
<input checked="" type="radio"/> Dynamic IP Address	Obtain an IP address from ISP automatically.
<input type="radio"/> Dynamic IP Address with Road Runner Session Management (e.g. Telstra BigPond)	
<input type="radio"/> PPP over Ethernet	Some ISPs require the use of PPPoE to connect to their services.
<input type="radio"/> PPTP	Some ISPs require the use of PPTP to connect to their services.
<input type="radio"/> L2TP	Some ISPs require the use of L2TP to connect to their services.

[Save](#) [Cancel](#)

This option is primary to enable this product to work properly. The setting items and the web appearance depend on the WAN type. Choose correct WAN type before you start.

1. **LAN IP Address:** the local IP address of this device. The computers on your network must use the LAN IP address of your product as their Default Gateway. You can change it if necessary.

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Primary Setup
- DHCP Server
- Wireless

Primary Setup [Help]

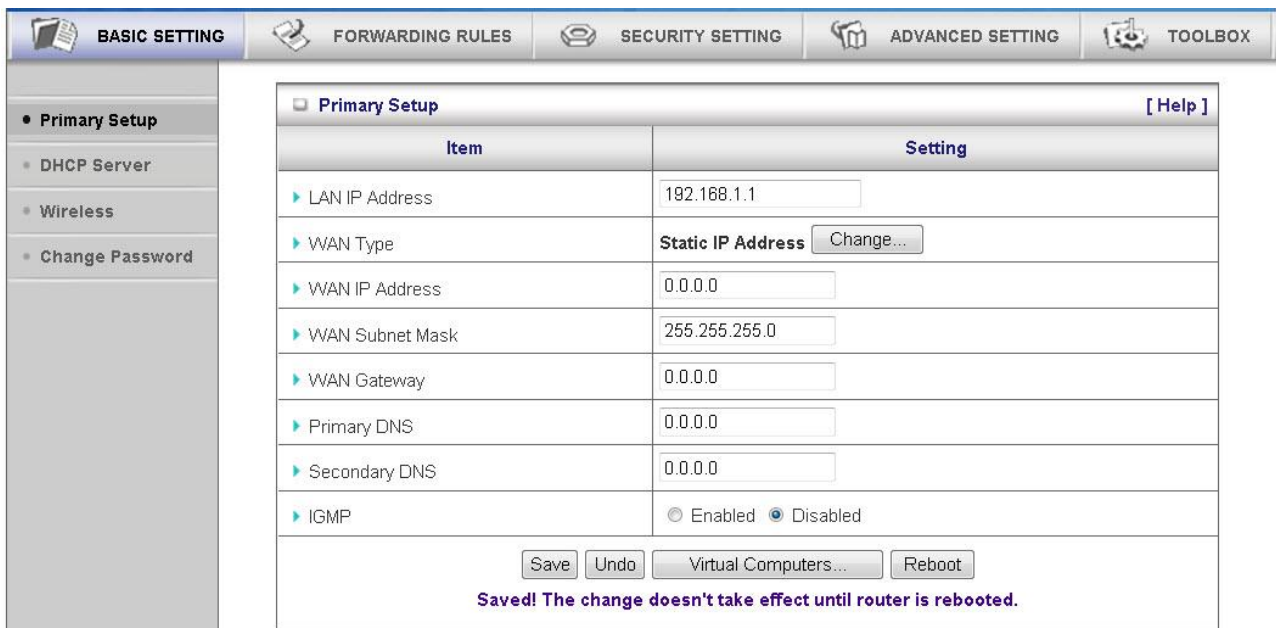
Item	Setting
▶ LAN IP Address	192.168.1.1

2. **WAN Type:** WAN connection type of your ISP. You can click **Change** button to choose a correct one from the following four options:

- A. Static IP Address: ISP assigns you a static IP address.
- B. Dynamic IP Address: Obtain an IP address from ISP automatically.
- C. PPP over Ethernet: Some ISPs require the use of PPPoE to connect to their services.
- D. PPTP: Some ISPs require the use of PPTP to connect to their services.
- F. L2TP: Some ISPs require the use of L2TP to connect to their services

Static IP Address: ISP assigns you a static IP address:

WAN IP Address, Subnet Mask, Gateway, Primary and Secondary DNS: enter the proper setting provided by your ISP.



Primary Setup [Help]	
Item	Setting
▶ LAN IP Address	192.168.1.1
▶ WAN Type	Static IP Address Change...
▶ WAN IP Address	0.0.0.0
▶ WAN Subnet Mask	255.255.255.0
▶ WAN Gateway	0.0.0.0
▶ Primary DNS	0.0.0.0
▶ Secondary DNS	0.0.0.0
▶ IGMP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

[Save](#)
[Undo](#)
[Virtual Computers...](#)
[Reboot](#)

Saved! The change doesn't take effect until router is rebooted.

Dynamic IP Address: Obtain an IP address from ISP automatically.

Host Name: optional. Required by some ISPs, for example, @Home.

Renew IP Forever: this feature enables this product to renew your IP address automatically when the lease time is expiring-- even when the system is idle.

BASIC SETTING	FORWARDING RULES	SECURITY SETTING	ADVANCED SETTING	TOOLBOX														
<ul style="list-style-type: none"> Primary Setup DHCP Server Wireless Change Password 	<div>Primary Setup [Help]</div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>▶ LAN IP Address</td> <td>192.168.1.1</td> </tr> <tr> <td>▶ WAN Type</td> <td>Dynamic IP Address Change...</td> </tr> <tr> <td>▶ Host Name</td> <td>WGR-6012 (optional)</td> </tr> <tr> <td>▶ WAN's MAC Address</td> <td>00-50-18-21-D4-34 Clone MAC</td> </tr> <tr> <td>▶ Renew IP Forever</td> <td><input type="checkbox"/> Enable (Auto-reconnect)</td> </tr> <tr> <td>▶ IGMP</td> <td><input type="radio"/> Enabled <input checked="" type="radio"/> Disabled</td> </tr> </tbody> </table> <div> Save Undo Virtual Computers... Reboot </div> <p>Saved! The change doesn't take effect until router is rebooted.</p>				Item	Setting	▶ LAN IP Address	192.168.1.1	▶ WAN Type	Dynamic IP Address Change...	▶ Host Name	WGR-6012 (optional)	▶ WAN's MAC Address	00-50-18-21-D4-34 Clone MAC	▶ Renew IP Forever	<input type="checkbox"/> Enable (Auto-reconnect)	▶ IGMP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Item	Setting																	
▶ LAN IP Address	192.168.1.1																	
▶ WAN Type	Dynamic IP Address Change...																	
▶ Host Name	WGR-6012 (optional)																	
▶ WAN's MAC Address	00-50-18-21-D4-34 Clone MAC																	
▶ Renew IP Forever	<input type="checkbox"/> Enable (Auto-reconnect)																	
▶ IGMP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled																	

PPP over Ethernet: Some ISPs require the use of PPPoE to connect to their services.

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 empty.

PPPoE Service Name: optional. Input the service name if your ISP requires it. Otherwise, leave it blank.

Maximum Idle Time: the amount of time of inactivity before disconnecting your PPPoE session. Set it to zero or enable Auto-reconnect to disable this feature.

Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The most common MTU value is 1492.

Connection Control: There are 3 modes to select:

Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

Auto-Reconnect(Always-on):The device will link with ISP until the connection is established.

Manually :The device will not make the link until someone clicks the connect-button in the Status-page.

<ul style="list-style-type: none"> Primary Setup DHCP Server Wireless Change Password 	<div> <div>Primary Setup</div> <div>[Help]</div> </div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>▶ LAN IP Address</td> <td>192.168.1.1</td> </tr> <tr> <td>▶ WAN Type</td> <td>PPP over Ethernet Change...</td> </tr> <tr> <td>▶ PPPoE Account</td> <td></td> </tr> <tr> <td>▶ PPPoE Password</td> <td></td> </tr> <tr> <td>▶ Primary DNS</td> <td>0.0.0.0</td> </tr> <tr> <td>▶ Secondary DNS</td> <td>0.0.0.0</td> </tr> <tr> <td>▶ Maximum Idle Time</td> <td>300 seconds</td> </tr> <tr> <td>▶ Authentication method</td> <td>Auto</td> </tr> <tr> <td>▶ Connection Control</td> <td>Connect-on-demand</td> </tr> <tr> <td>▶ PPPoE Service Name</td> <td>(optional)</td> </tr> <tr> <td>▶ Assigned IP Address</td> <td>0.0.0.0 (optional)</td> </tr> <tr> <td>▶ MTU</td> <td>1492</td> </tr> </tbody> </table>	Item	Setting	▶ LAN IP Address	192.168.1.1	▶ WAN Type	PPP over Ethernet Change...	▶ PPPoE Account		▶ PPPoE Password		▶ Primary DNS	0.0.0.0	▶ Secondary DNS	0.0.0.0	▶ Maximum Idle Time	300 seconds	▶ Authentication method	Auto	▶ Connection Control	Connect-on-demand	▶ PPPoE Service Name	(optional)	▶ Assigned IP Address	0.0.0.0 (optional)	▶ MTU	1492
Item	Setting																										
▶ LAN IP Address	192.168.1.1																										
▶ WAN Type	PPP over Ethernet Change...																										
▶ PPPoE Account																											
▶ PPPoE Password																											
▶ Primary DNS	0.0.0.0																										
▶ Secondary DNS	0.0.0.0																										
▶ Maximum Idle Time	300 seconds																										
▶ Authentication method	Auto																										
▶ Connection Control	Connect-on-demand																										
▶ PPPoE Service Name	(optional)																										
▶ Assigned IP Address	0.0.0.0 (optional)																										
▶ MTU	1492																										

PPTP: Some ISPs require the use of PPTP to connect to their services

First, please check your ISP assigned and Select Static IP Address or Dynamic IP Address.

1. My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned to you.
2. Server IP Address: the IP address of the PPTP server.
3. PPTP Account and Password: the account and password your ISP assigned to you. If you don't want to change the password, keep it empty.
3. Connection ID: optional. Input the connection ID if your ISP requires it.
4. Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will connect to ISP automatically, after system is restarted or connection is dropped.

Connection Control: There are 3 modes to select:

Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

Auto-Reconnect (Always-on): The device will link with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

<ul style="list-style-type: none"> Primary Setup DHCP Server Wireless Change Password 	<div> Primary Setup [Help] </div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>▶ LAN IP Address</td> <td>192.168.1.1</td> </tr> <tr> <td>▶ WAN Type</td> <td>PPTP Change...</td> </tr> <tr> <td>▶ IP Mode</td> <td>Static IP Address ▼</td> </tr> <tr> <td>▶ My IP Address</td> <td>0.0.0.0</td> </tr> <tr> <td>▶ My Subnet Mask</td> <td>255.255.255.0</td> </tr> <tr> <td>▶ Gateway IP</td> <td>0.0.0.0</td> </tr> <tr> <td>▶ Server IP Address/Name</td> <td></td> </tr> <tr> <td>▶ PPTP Account</td> <td>123</td> </tr> <tr> <td>▶ PPTP Password</td> <td></td> </tr> <tr> <td>▶ Connection ID</td> <td>(optional)</td> </tr> <tr> <td>▶ Maximum Idle Time</td> <td>300 seconds</td> </tr> <tr> <td>▶ Connection Control</td> <td>Connect-on-demand ▼</td> </tr> </tbody> </table>	Item	Setting	▶ LAN IP Address	192.168.1.1	▶ WAN Type	PPTP Change...	▶ IP Mode	Static IP Address ▼	▶ My IP Address	0.0.0.0	▶ My Subnet Mask	255.255.255.0	▶ Gateway IP	0.0.0.0	▶ Server IP Address/Name		▶ PPTP Account	123	▶ PPTP Password		▶ Connection ID	(optional)	▶ Maximum Idle Time	300 seconds	▶ Connection Control	Connect-on-demand ▼
Item	Setting																										
▶ LAN IP Address	192.168.1.1																										
▶ WAN Type	PPTP Change...																										
▶ IP Mode	Static IP Address ▼																										
▶ My IP Address	0.0.0.0																										
▶ My Subnet Mask	255.255.255.0																										
▶ Gateway IP	0.0.0.0																										
▶ Server IP Address/Name																											
▶ PPTP Account	123																										
▶ PPTP Password																											
▶ Connection ID	(optional)																										
▶ Maximum Idle Time	300 seconds																										
▶ Connection Control	Connect-on-demand ▼																										

L2TP: Some ISPs require the use of L2TP to connect to their services

First, please check your ISP assigned and Select Static IP Address or Dynamic IP Address.

For example: Use Static

1. My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned to you.
2. Server IP Address: the IP address of the PPTP server.
3. PPTP Account and Password: the account and password your ISP assigned to you. If you don't want to change the password, keep it empty.
3. Connection ID: optional. Input the connection ID if your ISP requires it.
4. Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will connect to ISP automatically, after system is restarted or connection is dropped.

Connection Control: There are 3 modes to select:

Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

Auto-Reconnect (Always-on): The device will link with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

<ul style="list-style-type: none"> Primary Setup DHCP Server Wireless Change Password 	<div> <div>Primary Setup</div> <div>[Help]</div> </div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>▶ LAN IP Address</td> <td>192.168.1.1</td> </tr> <tr> <td>▶ WAN Type</td> <td>L2TP <input type="button" value="Change..."/></td> </tr> <tr> <td>▶ IP Mode</td> <td>Static IP Address</td> </tr> <tr> <td>▶ IP Address</td> <td>0.0.0.0</td> </tr> <tr> <td>▶ Subnet Mask</td> <td>255.255.255.0</td> </tr> <tr> <td>▶ WAN Gateway IP</td> <td>0.0.0.0</td> </tr> <tr> <td>▶ Server IP Address/Name</td> <td></td> </tr> <tr> <td>▶ L2TP Account</td> <td>123</td> </tr> <tr> <td>▶ L2TP Password</td> <td></td> </tr> <tr> <td>▶ Maximum Idle Time</td> <td>300 seconds</td> </tr> <tr> <td>▶ Connection Control</td> <td>Connect-on-demand</td> </tr> <tr> <td>▶ MTU</td> <td>1460</td> </tr> </tbody> </table>	Item	Setting	▶ LAN IP Address	192.168.1.1	▶ WAN Type	L2TP <input type="button" value="Change..."/>	▶ IP Mode	Static IP Address	▶ IP Address	0.0.0.0	▶ Subnet Mask	255.255.255.0	▶ WAN Gateway IP	0.0.0.0	▶ Server IP Address/Name		▶ L2TP Account	123	▶ L2TP Password		▶ Maximum Idle Time	300 seconds	▶ Connection Control	Connect-on-demand	▶ MTU	1460
Item	Setting																										
▶ LAN IP Address	192.168.1.1																										
▶ WAN Type	L2TP <input type="button" value="Change..."/>																										
▶ IP Mode	Static IP Address																										
▶ IP Address	0.0.0.0																										
▶ Subnet Mask	255.255.255.0																										
▶ WAN Gateway IP	0.0.0.0																										
▶ Server IP Address/Name																											
▶ L2TP Account	123																										
▶ L2TP Password																											
▶ Maximum Idle Time	300 seconds																										
▶ Connection Control	Connect-on-demand																										
▶ MTU	1460																										

Virtual Computers (Only for Static and dynamic IP address WAN type)

<div> <div>BASIC SETTING</div> <div>FORWARDING RULES</div> <div>SECURITY SETTING</div> <div>ADVANCED SETTING</div> <div>TOOLBOX</div> </div> <ul style="list-style-type: none"> Primary Setup DHCP Server Wireless Change Password 	<div> <div>Virtual Computers</div> <div>[Help]</div> </div> <div> DHCP clients --- Select one --- <input type="button" value="Copy to"/> ID -- </div> <table border="1"> <thead> <tr> <th>ID</th> <th>Global IP</th> <th>Local IP</th> <th>Enable</th> </tr> </thead> <tbody> <tr> <td>1</td> <td></td> <td>192.168.1.</td> <td><input type="checkbox"/></td> </tr> <tr> <td>2</td> <td></td> <td>192.168.1.</td> <td><input type="checkbox"/></td> </tr> <tr> <td>3</td> <td></td> <td>192.168.1.</td> <td><input type="checkbox"/></td> </tr> <tr> <td>4</td> <td></td> <td>192.168.1.</td> <td><input type="checkbox"/></td> </tr> <tr> <td>5</td> <td></td> <td>192.168.1.</td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <div> <input type="button" value="Save"/> <input type="button" value="Undo"/> </div>	ID	Global IP	Local IP	Enable	1		192.168.1.	<input type="checkbox"/>	2		192.168.1.	<input type="checkbox"/>	3		192.168.1.	<input type="checkbox"/>	4		192.168.1.	<input type="checkbox"/>	5		192.168.1.	<input type="checkbox"/>
ID	Global IP	Local IP	Enable																						
1		192.168.1.	<input type="checkbox"/>																						
2		192.168.1.	<input type="checkbox"/>																						
3		192.168.1.	<input type="checkbox"/>																						
4		192.168.1.	<input type="checkbox"/>																						
5		192.168.1.	<input type="checkbox"/>																						

Virtual Computer enables you to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple global IP address and local IP address.

- Global IP: Enter the global IP address assigned by your ISP.
- Local IP: Enter the local IP address of your LAN PC corresponding to the global IP address.
- Enable: Check this item to enable the Virtual Computer feature.

3.3.1.2 DHCP Server

Item	Setting
DHCP Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Lease Time	0 Minutes
IP Pool Starting Address	50
IP Pool Ending Address	200
Domain Name	
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Primary WINS	0.0.0.0
Secondary WINS	0.0.0.0
Gateway	0.0.0.0 (optional)

Save Undo Clients List... Fixed Mapping...

Press “More>>”

1. **DHCP Server:** Choose “Disable” or “Enable.”
2. **Lease time:** This is the length of time that the client may use the IP address it has been Assigned by DHCP server.
3. **IP pool starting Address/ IP pool starting 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 and ending address of the IP address pool.
4. **Domain Name:** Optional, this information will be passed to the client.
5. **Primary DNS/Secondary DNS:** This feature allows you to assign DNS Servers
6. **Primary WINS/Secondary WINS:** This feature allows you to assign WINS Servers
7. **Gateway:** The 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.

8. **DHCP Client List:**

IP Address	Host Name	MAC Address	Select
192.168.1.65	AaronLee	00-1F-C6-20-46-1B	<input type="checkbox"/>

Wake up Delete Back Refresh

3.3.1.3 Wireless

• Primary Setup	Wireless Setting [Help]
• DHCP Server	
• Wireless	
• Change Password	

Item	Setting
▶ Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Network ID(SSID)	<input type="text" value="LevelOne"/>
▶ Wireless Mode	<input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only
▶ SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Channel	<input type="text" value="11"/>
▶ WDS	<input type="button" value="Enter..."/>
▶ WPS	<input type="button" value="Enter..."/>
▶ Security	<input type="text" value="WEP"/>
▶ WEP	<input checked="" type="radio"/> 64 bits <input type="radio"/> 128 bits
▶ Key 1	<input checked="" type="radio"/> <input type="text" value="1234567890"/>
▶ Key 2	<input type="radio"/> <input type="text"/>

Wireless settings allow you to set the wireless configuration items.

Wireless : The user can enable or disable wireless function.

Network ID (SSID): Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. (The factory setting is “default”)

SSID Broadcast: The router will Broadcast beacons that have some information, including ssid so that The wireless clients can know how many AP devices by scanning function in the network. Therefore, This function is disabled; the wireless clients can not find the device from beacons.

Channel: The radio channel number. The permissible channels depend on the Regulatory Domain.

WPS (Wi-Fi Protection Setup)

WPS is Wi-Fi Protection Setup which is similar to WCN-NET and offers safe and easy way in Wireless Connection.

BASIC SETTING	FORWARDING RULES	SECURITY SETTING	ADVANCED SETTING	TOOLBOX												
<ul style="list-style-type: none"> Primary Setup DHCP Server Wireless Change Password 	<div>Wi-Fi Protected Setup</div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>▶ WPS</td> <td><input checked="" type="radio"/> Enable <input type="radio"/> Disable</td> </tr> <tr> <td>▶ Setup</td> <td> <input type="radio"/> Current AP PIN <input type="radio"/> Configure Wireless Station </td> </tr> <tr> <td>▶ WPS state</td> <td>Idle</td> </tr> <tr> <td>▶ WPS status</td> <td>Configured <input type="button" value="Release"/></td> </tr> <tr> <td colspan="2"> <input type="button" value="Save"/> <input type="button" value="Trigger"/> <input type="button" value="Back"/> </td> </tr> </tbody> </table>				Item	Setting	▶ WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	▶ Setup	<input type="radio"/> Current AP PIN <input type="radio"/> Configure Wireless Station	▶ WPS state	Idle	▶ WPS status	Configured <input type="button" value="Release"/>	<input type="button" value="Save"/> <input type="button" value="Trigger"/> <input type="button" value="Back"/>	
Item	Setting															
▶ WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable															
▶ Setup	<input type="radio"/> Current AP PIN <input type="radio"/> Configure Wireless Station															
▶ WPS state	Idle															
▶ WPS status	Configured <input type="button" value="Release"/>															
<input type="button" value="Save"/> <input type="button" value="Trigger"/> <input type="button" value="Back"/>																

WDS (Wireless Distribution System)

WDS operation as defined by the IEEE802.11 standard has been made available. Using WDS it is possible to wirelessly connect Access Points, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.

BASIC SETTING	FORWARDING RULES	SECURITY SETTING	ADVANCED SETTING	TOOLBOX																	
<ul style="list-style-type: none"> Primary Setup DHCP Server Wireless Change Password 	<div>WDS Setting [Help]</div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>▶ AP Mode:</td> <td>AP Only</td> </tr> <tr> <td>▶ Remote AP MAC</td> <td> <div>MAC 1 <input type="text"/></div> <div>MAC 2 <input type="text"/></div> <div>MAC 3 <input type="text"/></div> <div>MAC 4 <input type="text"/></div> </td> </tr> <tr> <td colspan="2"> <div>Scanned AP's MAC --- Select one --- <input type="button" value="Copy to"/></div> <div>Remote AP MAC -- --</div> </td> </tr> <tr> <td>SSID</td> <td>Channel</td> <td>MAC Address</td> </tr> <tr> <td>QC-6020</td> <td>1</td> <td>00-50-18-5D-0A-20</td> </tr> <tr> <td>WBR-6022TSD</td> <td>1</td> <td>00-11-6B-50-EC-A0</td> </tr> </tbody> </table>				Item	Setting	▶ AP Mode:	AP Only	▶ Remote AP MAC	<div>MAC 1 <input type="text"/></div> <div>MAC 2 <input type="text"/></div> <div>MAC 3 <input type="text"/></div> <div>MAC 4 <input type="text"/></div>	<div>Scanned AP's MAC --- Select one --- <input type="button" value="Copy to"/></div> <div>Remote AP MAC -- --</div>		SSID	Channel	MAC Address	QC-6020	1	00-50-18-5D-0A-20	WBR-6022TSD	1	00-11-6B-50-EC-A0
Item	Setting																				
▶ AP Mode:	AP Only																				
▶ Remote AP MAC	<div>MAC 1 <input type="text"/></div> <div>MAC 2 <input type="text"/></div> <div>MAC 3 <input type="text"/></div> <div>MAC 4 <input type="text"/></div>																				
<div>Scanned AP's MAC --- Select one --- <input type="button" value="Copy to"/></div> <div>Remote AP MAC -- --</div>																					
SSID	Channel	MAC Address																			
QC-6020	1	00-50-18-5D-0A-20																			
WBR-6022TSD	1	00-11-6B-50-EC-A0																			

Hybrid Mode

It means the device can support WDS and AP Mode simultaneously.

BASIC SETTING	FORWARDING RULES	SECURITY SETTING	ADVANCED SETTING	TOOLBOX										
<ul style="list-style-type: none"> Primary Setup DHCP Server Wireless Change Password 	<div>Wi-Fi Protected Setup</div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>▶ WPS</td> <td><input checked="" type="radio"/> Enable <input type="radio"/> Disable</td> </tr> <tr> <td>▶ Setup</td> <td> <input type="radio"/> Current AP PIN <input type="radio"/> Configure Wireless Station </td> </tr> <tr> <td>▶ WPS state</td> <td>Idle</td> </tr> <tr> <td>▶ WPS status</td> <td>Configured <input type="button" value="Release"/></td> </tr> </tbody> </table> <div> <input type="button" value="Save"/> <input type="button" value="Trigger"/> <input type="button" value="Back"/> </div>				Item	Setting	▶ WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	▶ Setup	<input type="radio"/> Current AP PIN <input type="radio"/> Configure Wireless Station	▶ WPS state	Idle	▶ WPS status	Configured <input type="button" value="Release"/>
Item	Setting													
▶ WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable													
▶ Setup	<input type="radio"/> Current AP PIN <input type="radio"/> Configure Wireless Station													
▶ WPS state	Idle													
▶ WPS status	Configured <input type="button" value="Release"/>													

Security: Select the data privacy algorithm you want. Enabling the security can protect your data while it is transferred from one station to another.

There are several security types to use:

WEP:

When you enable the 128 or 64 bit WEP key security, please select one WEP key to be used and input 26 or 10 hexadecimal (0, 1, 2...8, 9, A, B...F) digits.

802.1X

Check Box was used to switch the function of the 802.1X. When the 802.1X 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.

RADIUS Shared Key

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

<ul style="list-style-type: none"> Primary Setup DHCP Server Wireless Change Password 	<div> <div>Wireless Setting</div> <div>[Help]</div> </div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>Wireless</td> <td><input checked="" type="radio"/> Enable <input type="radio"/> Disable</td> </tr> <tr> <td>Network ID(SSID)</td> <td>LevelOne</td> </tr> <tr> <td>Wireless Mode</td> <td><input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only</td> </tr> <tr> <td>SSID Broadcast</td> <td><input checked="" type="radio"/> Enable <input type="radio"/> Disable</td> </tr> <tr> <td>WMM</td> <td><input type="radio"/> Enable <input checked="" type="radio"/> Disable</td> </tr> <tr> <td>Channel</td> <td>11</td> </tr> <tr> <td>WDS</td> <td>Enter...</td> </tr> <tr> <td>WPS</td> <td>Enter...</td> </tr> <tr> <td>Security</td> <td>WEP</td> </tr> <tr> <td>WEP</td> <td><input checked="" type="radio"/> 64 bits <input type="radio"/> 128 bits</td> </tr> <tr> <td>Key 1</td> <td><input checked="" type="radio"/> 1234567890</td> </tr> <tr> <td>Key 2</td> <td><input type="radio"/> </td> </tr> </tbody> </table>	Item	Setting	Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Network ID(SSID)	LevelOne	Wireless Mode	<input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only	SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Channel	11	WDS	Enter...	WPS	Enter...	Security	WEP	WEP	<input checked="" type="radio"/> 64 bits <input type="radio"/> 128 bits	Key 1	<input checked="" type="radio"/> 1234567890	Key 2	<input type="radio"/>
Item	Setting																										
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable																										
Network ID(SSID)	LevelOne																										
Wireless Mode	<input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only																										
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable																										
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable																										
Channel	11																										
WDS	Enter...																										
WPS	Enter...																										
Security	WEP																										
WEP	<input checked="" type="radio"/> 64 bits <input type="radio"/> 128 bits																										
Key 1	<input checked="" type="radio"/> 1234567890																										
Key 2	<input type="radio"/>																										

WPA-PSK

1. 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 ASCII, the length of pre-share key is from 8 to 63.

2. Fill in the key, Ex 12345678

<ul style="list-style-type: none"> Primary Setup DHCP Server Wireless Change Password 	<div> <div>Wireless Setting</div> <div>[Help]</div> </div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>Wireless</td> <td><input checked="" type="radio"/> Enable <input type="radio"/> Disable</td> </tr> <tr> <td>Network ID(SSID)</td> <td>LevelOne</td> </tr> <tr> <td>Wireless Mode</td> <td><input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only</td> </tr> <tr> <td>SSID Broadcast</td> <td><input checked="" type="radio"/> Enable <input type="radio"/> Disable</td> </tr> <tr> <td>WMM</td> <td><input type="radio"/> Enable <input checked="" type="radio"/> Disable</td> </tr> <tr> <td>Channel</td> <td>11</td> </tr> <tr> <td>WDS</td> <td>Enter...</td> </tr> <tr> <td>WPS</td> <td>Enter...</td> </tr> <tr> <td>Security</td> <td>WPA-PSK</td> </tr> <tr> <td>Encryption</td> <td><input checked="" type="radio"/> TKIP <input type="radio"/> AES</td> </tr> <tr> <td>Preshare Key Mode</td> <td>ASCII</td> </tr> <tr> <td>Preshare Key</td> <td></td> </tr> </tbody> </table>	Item	Setting	Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Network ID(SSID)	LevelOne	Wireless Mode	<input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only	SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Channel	11	WDS	Enter...	WPS	Enter...	Security	WPA-PSK	Encryption	<input checked="" type="radio"/> TKIP <input type="radio"/> AES	Preshare Key Mode	ASCII	Preshare Key	
Item	Setting																										
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable																										
Network ID(SSID)	LevelOne																										
Wireless Mode	<input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only																										
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable																										
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable																										
Channel	11																										
WDS	Enter...																										
WPS	Enter...																										
Security	WPA-PSK																										
Encryption	<input checked="" type="radio"/> TKIP <input type="radio"/> AES																										
Preshare Key Mode	ASCII																										
Preshare Key																											

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 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(AES)

1. Select 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 ASCII, the length of Pre-share key is from 8 to 63.

2. Fill in the key, Ex 12345678

WPA2(AES)

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 RADIUS Shared Key

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

If 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.

WPA-PSK /WPA2-PSK

The router will detect automatically which Security type the client uses to encrypt.

1. Select 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 ASCII, the length of Pre-share key is from 8 to 63.

2. Fill in the key, Ex 12345678

<ul style="list-style-type: none"> • Primary Setup • DHCP Server • Wireless • Change Password 	<div> <div> <div>Wireless Setting</div> <div>[Help]</div> </div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>Wireless</td> <td><input checked="" type="radio"/> Enable <input type="radio"/> Disable</td> </tr> <tr> <td>Network ID(SSID)</td> <td>LevelOne</td> </tr> <tr> <td>Wireless Mode</td> <td><input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only</td> </tr> <tr> <td>SSID Broadcast</td> <td><input checked="" type="radio"/> Enable <input type="radio"/> Disable</td> </tr> <tr> <td>WMM</td> <td><input type="radio"/> Enable <input checked="" type="radio"/> Disable</td> </tr> <tr> <td>Channel</td> <td>11</td> </tr> <tr> <td>WDS</td> <td>Enter...</td> </tr> <tr> <td>WPS</td> <td>Enter...</td> </tr> <tr> <td>Security</td> <td>WPA-PSK / WPA2-PSK</td> </tr> <tr> <td>Encryption</td> <td>TKIP + AES</td> </tr> <tr> <td>Preshare Key Mode</td> <td>ASCII</td> </tr> <tr> <td>Preshare Key</td> <td></td> </tr> </tbody> </table> </div>	Item	Setting	Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Network ID(SSID)	LevelOne	Wireless Mode	<input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only	SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Channel	11	WDS	Enter...	WPS	Enter...	Security	WPA-PSK / WPA2-PSK	Encryption	TKIP + AES	Preshare Key Mode	ASCII	Preshare Key	
Item	Setting																										
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable																										
Network ID(SSID)	LevelOne																										
Wireless Mode	<input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only																										
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable																										
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable																										
Channel	11																										
WDS	Enter...																										
WPS	Enter...																										
Security	WPA-PSK / WPA2-PSK																										
Encryption	TKIP + AES																										
Preshare Key Mode	ASCII																										
Preshare Key																											

WPA/WPA2

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

The router will detect automatically which Security type(WPA-PSK version 1 or 2) the client uses to encrypt.

IP address or the 802.1X server's domain-name.

Select RADIUS Shared Key

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

If 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.

Wireless Client List

<ul style="list-style-type: none"> • Primary Setup • DHCP Server • Wireless • Change Password 	<div> <div> <div>Wireless Client List</div> </div> <table border="1"> <thead> <tr> <th>Connected Time</th> <th>MAC Address</th> </tr> </thead> <tbody> <tr> <td>Tue Jan 26 09:39:58 2010</td> <td>00-1C-BF-00-C6-37</td> </tr> </tbody> </table> <div> <div>Back</div> <div>Refresh</div> </div> </div>	Connected Time	MAC Address	Tue Jan 26 09:39:58 2010	00-1C-BF-00-C6-37
Connected Time	MAC Address				
Tue Jan 26 09:39:58 2010	00-1C-BF-00-C6-37				

3.3.1.4 Change Password

Item	Setting
Old Password	<input type="text"/>
New Password	<input type="text"/>
Reconfirm	<input type="text"/>

You can change Password here. We **strongly** recommend you to change the system password for security reason.

3.3.2 Forwarding Rules

Forwarding Rules

- **Virtual Server**
 - Allows others to access WWW, FTP, and other services on your LAN.
- **Special Application**
 - This configuration allows some applications to connect, and work with the NAT router.
- **Miscellaneous**
 - IP Address of DMZ Host: Allows a computer to be exposed to unrestricted 2-way communication. Note that, this feature should be used only when needed.
 - Non-standard FTP port: You have to configure this item if you want to access an FTP server whose port number is not 21 (when Client uses active mode).
 - UPnP Setting: If you enable UPnP function, the router will work with UPnP devices/software.

3.3.2.1 Virtual Server

ID	Server IP	Public Port	Private Port	Protocol	Enable	Schedule Rule#
1	192.168.1.123		21	Both	<input checked="" type="checkbox"/>	0
2	192.168.1.7		25	Both	<input checked="" type="checkbox"/>	0
3	192.168.1.20		110	Both	<input checked="" type="checkbox"/>	0
4	192.168.1.			Both	<input type="checkbox"/>	0
5	192.168.1.			Both	<input type="checkbox"/>	0
6	192.168.1.			Both	<input type="checkbox"/>	0
7	192.168.1.			Both	<input type="checkbox"/>	0

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 Detail, please refer to **Scheduling Rule**.

3.3.2.2 Special AP

ID	Trigger	Incoming Ports	Enable
1	7175	51200-51201,51210	<input checked="" type="checkbox"/>
2	47624	2300-2400,28800-29000	<input checked="" type="checkbox"/>
3			<input type="checkbox"/>
4			<input type="checkbox"/>
5			<input type="checkbox"/>
6			<input type="checkbox"/>
7			<input type="checkbox"/>
8			<input type="checkbox"/>

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.

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.

This product provides some predefined settings Select your application and click **Copy to** to add the predefined setting to your list.

Note! At any given time, only one PC can use each Special Application tunnel.

3.3.2.3 Miscellaneous Items

Item	Setting	Enable
▶ IP Address of DMZ Host	192.168.1. <input type="text"/>	<input type="checkbox"/>
▶ Non-standard FTP port	<input type="text"/>	
▶ UPnP setting		<input checked="" type="checkbox"/>
▶ Xbox Support		<input checked="" type="checkbox"/>

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.

NOTE: This feature should be used only when needed.

Non-standard FTP port

You have to configure this item if you want to access an FTP server whose port number is not 21. This setting will be lost after rebooting.

Xbox Support

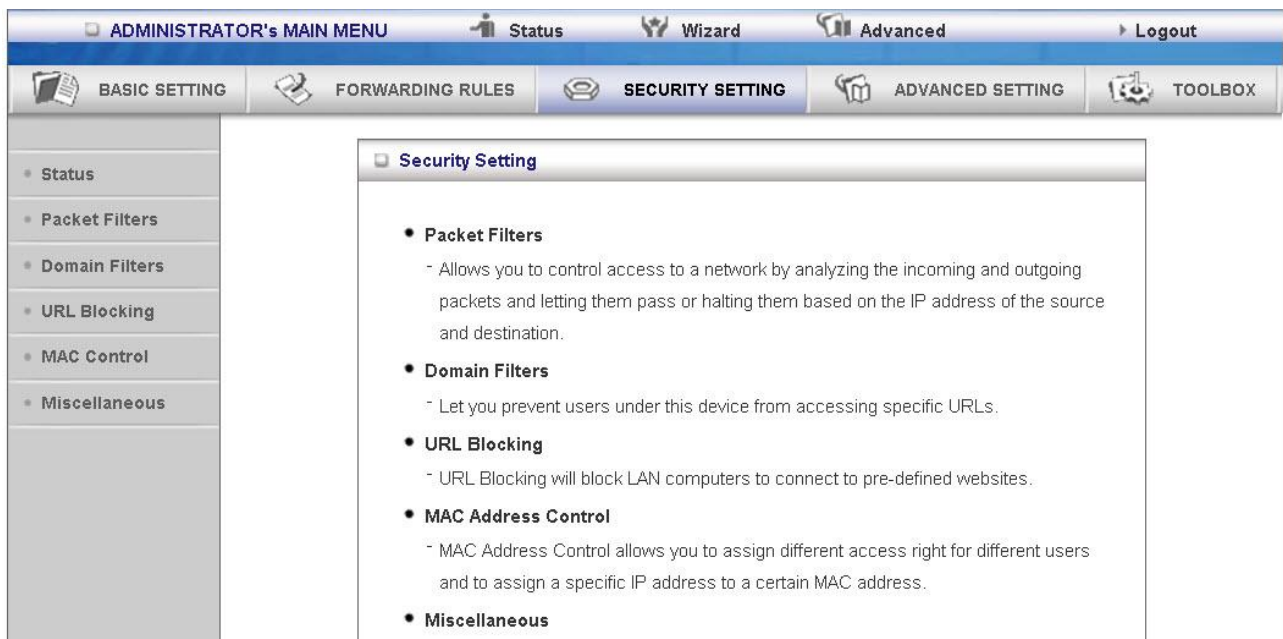
The Xbox is a video game console produced by Microsoft Corporation. Please enable this function when you play games.

UPnP Setting

The device also supports this function. If the OS supports this function enable it, like Windows XP. When the user get IP from Device and will see icon as below:



3.3.3 Security Settings



3.3.3.1 Packet Filters

ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#
1			<input type="checkbox"/>	0
2			<input type="checkbox"/>	0
3			<input type="checkbox"/>	0
4			<input type="checkbox"/>	0
5			<input type="checkbox"/>	0
6			<input type="checkbox"/>	0
7			<input type="checkbox"/>	0

Packet Filter 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

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

- Source IP address
- Source port address
- Destination IP address
- Destination port address
- 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.

Inbound Filter:

To enable **Inbound Packet Filter** click the check box next to **Enable** in the **Inbound Packet Filter** field.

Suppose you have SMTP Server (25), POP Server (110), Web Server (80), FTP Server (21), and News Server (119) defined in Virtual Server or DMZ Host.

Example 1:

ADMINISTRATOR'S MAIN MENU Status Wizard Advanced Logout

BASIC SETTING **FORWARDING RULES** **SECURITY SETTING** ADVANCED SETTING TOOLBOX

• Status
• Packet Filters
• Domain Filters
• URL Blocking
• MAC Control
• Miscellaneous

Outbound Packet Filter [Help]

Item	Setting
Outbound Filter	<input checked="" type="checkbox"/> Enable
<input type="radio"/> Allow all to pass except those match the following rules. <input checked="" type="radio"/> Deny all to pass except those match the following rules.	
Schedule rule (00)Always Copy to ID --	

ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#
1	1.2.3.100-1.2.3.149 :	: 25-100	<input checked="" type="checkbox"/>	0
2	1.2.3.10-1.2.3.20 :	:	<input checked="" type="checkbox"/>	0
3	:	:	<input type="checkbox"/>	0
4	:	:	<input type="checkbox"/>	0
5	:	:	<input type="checkbox"/>	0
6	:	:	<input type="checkbox"/>	0
7	:	:	<input type="checkbox"/>	0
8	:	:	<input type="checkbox"/>	0

Save Undo Inbound Filter... MAC Level...

(1.2.3.100-1.2.3.149) Remote hosts are allow to send mail (port 25), and browse the Internet (port 80)

(1.2.3.10-1.2.3.20) Remote hosts can do everything (block nothing)

Others are all blocked.

Example 2:

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES **SECURITY SETTING** ADVANCED SETTING TOOLBOX

• Status
• Packet Filters
• Domain Filters
• URL Blocking
• MAC Control
• Miscellaneous

Outbound Packet Filter [Help]

Item	Setting
▶ Outbound Filter	<input checked="" type="checkbox"/> Enable
<input checked="" type="radio"/> Allow all to pass except those match the following rules. <input type="radio"/> Deny all to pass except those match the following rules.	
Schedule rule (00)Always Copy to ID -- ▼	

ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#
1	1.2.3.100-1.2.3.199 : <input type="text"/>	<input type="text"/> : 21	<input checked="" type="checkbox"/>	0 <input type="text"/>
2	1.2.3.100-1.2.3.199 : <input type="text"/>	<input type="text"/> : 199	<input checked="" type="checkbox"/>	0 <input type="text"/>
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>

Save Undo Inbound Filter... MAC Level...

(1.2.3.100-1.2.3.119) Remote hosts can do everything except read net news (port 119) and transfer files via FTP (port 21) behind Router Server.

Others are all allowed.

After **Inbound Packet Filter** setting is configured, click the **save** button.

Outbound Filter:

To enable **Outbound Packet Filter** click the check box next to **Enable** in the **Outbound Packet Filter** field.

Example 1:

Router LAN IP is 192.168.1.1

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING **FORWARDING RULES** **SECURITY SETTING** **ADVANCED SETTING** **TOOLBOX**

Outbound Packet Filter [Help]

Item **Setting**

▶ Outbound Filter ☒ Enable

☐ Allow all to pass except those match the following rules.
☒ Deny all to pass except those match the following rules.

Schedule rule (00)Always Copy to ID --

ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#
1	100-192.168.1.149 :	: 21-100	<input checked="" type="checkbox"/>	0
2	2.10-192.168.1.20 :	:	<input checked="" type="checkbox"/>	0
3	:	:	<input type="checkbox"/>	0
4	:	:	<input type="checkbox"/>	0
5	:	:	<input type="checkbox"/>	0
6	:	:	<input type="checkbox"/>	0
7	:	:	<input type="checkbox"/>	0
8	:	:	<input type="checkbox"/>	0

Save Undo Inbound Filter... MAC Level...

(192.168.1.100-192.168.1.149) Located hosts are only allowed to send mail (port 25), receive mail (port 110), and browse Internet (port 80); port 53 (DNS) is necessary to resolve the domain name.

(192.168.1.10-192.168.1.20) Located hosts can do everything (block nothing)

Others are all blocked.

Example 2:

Router LAN IP is 192.168.1.1

The screenshot shows the 'Outbound Packet Filter' configuration page. The interface has a top navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary navigation bar with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING' (selected), 'ADVANCED SETTING', and 'TOOLBOX'. On the left is a sidebar menu with 'Status', 'Packet Filters', 'Domain Filters', 'URL Blocking', 'MAC Control', and 'Miscellaneous'. The main content area is titled 'Outbound Packet Filter' with a '[Help]' link. It contains a table with two columns: 'Item' and 'Setting'. The 'Item' column has a sub-header 'Outbound Filter'. The 'Setting' column has a checkbox for 'Enable' which is checked. Below this, there are two radio buttons: 'Allow all to pass except those match the following rules.' (selected) and 'Deny all to pass except those match the following rules.'. There is a 'Schedule rule' dropdown set to '(00)Always' and a 'Copy to' button. Below this is a table with 5 columns: 'ID', 'Source IP : Ports', 'Destination IP : Ports', 'Enable', and 'Schedule Rule#'. The table has 8 rows. Row 1: ID 1, Source IP: 100-192.168.1.100, Destination IP: 21, Enable checked, Schedule Rule# 0. Row 2: ID 2, Source IP: 2.10-192.168.1.119, Destination IP: 119, Enable checked, Schedule Rule# 0. Rows 3-8: Empty source and destination IP fields, Enable unchecked, Schedule Rule# 0. At the bottom are buttons for 'Save', 'Undo', 'Inbound Filter...', and 'MAC Level...'.

ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#
1	100-192.168.1.100	21	<input checked="" type="checkbox"/>	0
2	2.10-192.168.1.119	119	<input checked="" type="checkbox"/>	0
3			<input type="checkbox"/>	0
4			<input type="checkbox"/>	0
5			<input type="checkbox"/>	0
6			<input type="checkbox"/>	0
7			<input type="checkbox"/>	0
8			<input type="checkbox"/>	0

(192.168.1.100 and 192.168.1.119) Located Hosts can do everything except read net news (port 119) and transfer files via FTP (port 21)

Others are allowed

After **Outbound Packet Filter** setting is configured, click the **save** button.

3.3.3.2 Domain filters

The screenshot shows a web-based configuration interface for a network device. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING' (which is active), 'ADVANCED SETTING', and 'TOOLBOX'. On the left side, there is a sidebar menu with options: 'Status', 'Packet Filters', 'Domain Filters' (selected), 'URL Blocking', 'MAC Control', and 'Miscellaneous'. The main content area is titled 'Domain Filter' with a '[Help]' link. It contains several settings: 'Domain Filter' (checked), 'Log DNS Query' (unchecked), and 'Privilege IP Addresses Range' (From 0 To 17). Below these is a table with 4 columns: 'ID', 'Domain Suffix', 'Action', and 'Enable'. The table has 10 rows. The first row is pre-filled with 'www.xyz.com' and has 'Drop' and 'Log' checkboxes, with 'Enable' checked. The remaining 9 rows have empty 'Domain Suffix' fields and 'Drop' and 'Log' checkboxes, with 'Enable' unchecked.

Domain Filter [Help]			
Item		Setting	
Domain Filter		<input checked="" type="checkbox"/> Enable	
Log DNS Query		<input type="checkbox"/> Enable	
Privilege IP Addresses Range		From 0 To 17	
ID	Domain Suffix	Action	Enable
1	www.xyz.com	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input checked="" type="checkbox"/>
2		<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
3		<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
4		<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
5		<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
6		<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
7		<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
8		<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
9		<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
10		<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>

Domain Filter

Let you prevent users under this device from accessing specific URLs.

Domain Filter Enable

Check if you want to enable Domain Filter.

Log DNS Query

Check if you want to log the action when someone accesses the specific URLs.

Privilege IP Addresses Range

Setting a group of hosts and privilege these hosts to access network without restriction.

Domain Suffix

A suffix of URL to be restricted. For example, ".com", "xxx.com".

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.

Enable

Check to enable each rule.

Example:

ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout

BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX

- Status
- Packet Filters
- Domain Filters
- URL Blocking
- MAC Control
- Miscellaneous

Domain Filter
[Help]

Item	Setting
Domain Filter	<input checked="" type="checkbox"/> Enable
Log DNS Query	<input checked="" type="checkbox"/> Enable
Privilege IP Addresses Range	From <input type="text" value="100"/> To <input type="text" value="199"/>

ID	Domain Suffix	Action	Enable
1	<input type="text" value="www.msn.com"/>	<input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
2	<input type="text" value="www.sina.com"/>	<input type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
3	<input type="text" value="www.baidu.com"/>	<input checked="" type="checkbox"/> Drop <input type="checkbox"/> Log	<input checked="" 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	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>

In this example:

1. URL include "www.msn.com" will be blocked, and the action will be record in log-file.
2. URL include "www.sina.com" will not be blocked, but the action will be record in log-file.
3. URL include "www.baidu.com" will be blocked, but the action will not be record in log-file.
4. IP address x.x.x.1~x.x.x.99 can access Internet without restriction.

3.3.3.3 URL Blocking

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"/>

URL Blocking will block LAN computers to connect to pre-defined Websites.

The major difference between “Domain filter” and “URL Blocking” is Domain filter require user to input suffix (like .com or .org, etc), while URL Blocking require 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 Enable

Checked if you want to enable URL Blocking.

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".

Enable

Checked to enable each rule.

ADMINISTRATOR'S MAIN MENU
Status
Wizard
Advanced
Logout

BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX

- Status
- Packet Filters
- Domain Filters
- URL Blocking
- MAC Control
- Miscellaneous

URL Blocking [Help]

Item	Setting
URL Blocking	<input checked="" type="checkbox"/> Enable
ID	URL
1	msn
2	sina
3	
4	
5	
6	
7	
8	
9	
10	

In this example:

1. URL include “msn” will be blocked, and the action will be record in log-file.
2. URL include “sina” will be blocked, but the action will be record in log-file

3.3.3.4 Internet Access Control

The device provides "Administrator MAC Control" for specific MAC to access the device or Internet without restriction. It also provides 3 features to access Internet: MAC Control by host, Group MAC Control and Interface Access Control depend as user-defined time Schedule.

1. MAC control

The screenshot shows the 'MAC Address Control' configuration page. The interface has a top navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary bar with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING' (selected), 'ADVANCED SETTING', and 'TOOLBOX'. A left sidebar lists navigation options: 'Status', 'Packet Filters', 'Domain Filters', 'URL Blocking', 'MAC Control' (selected), and 'Miscellaneous'. The main content area is titled 'MAC Address Control' with a '[Help]' link. It contains several settings: 'MAC Address Control' (checked 'Enable'), 'Connection control' (checked, with a dropdown set to 'allow'), and 'Association control' (checked, with a dropdown set to 'deny'). A note states: 'Note: Association control has no effect on wired clients.' Below these are 'DHCP clients' (a dropdown menu) and a 'Copy to ID' button. At the bottom is a table with 5 columns: 'ID', 'MAC Address', 'IP Address', 'C', and 'A'. The table has 4 rows of data, each with a unique ID and a 192.168.1.x IP address. Each row has checkboxes for 'C' and 'A'. At the very bottom are buttons for '<< Previous', 'Next >>', 'Save', and 'Undo'.

ID	MAC Address	IP Address	C	A
1		192.168.1.	<input type="checkbox"/>	<input type="checkbox"/>
2		192.168.1.	<input type="checkbox"/>	<input type="checkbox"/>
3		192.168.1.	<input type="checkbox"/>	<input type="checkbox"/>
4		192.168.1.	<input type="checkbox"/>	<input type="checkbox"/>

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 Check "Enable" to enable the "MAC Address Control". All of the settings in this page will take effect only when "Enable" is checked.

Connection control Check "Connection control" to enable the controlling of which wired and wireless clients can connect to this device. If a client is denied to connect to 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 to this device.

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.

Control table

ID	MAC Address	IP Address	C	A
1	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

"Control table" is the table at the bottom of the "MAC Address Control" page. Each row of this table indicates the MAC address and the expected IP address mapping of a client. There are four columns in this table:

MAC Address	MAC address indicates a specific client.
IP Address	Expected IP address of the corresponding client. Keep it empty if you don't care its IP address.
C	When " Connection control " is checked, check " C " will allow the corresponding client to connect to this device.
A	When " Association control " is checked, check " A " will allow the corresponding client to associate to the wireless LAN.

In this page, we provide the following Combobox and button to help you to input the MAC address.

DHCP clients

ID

You can select a specific client in the "DHCP clients" Combobox, and then click on the "Copy to" button to copy the MAC address of the client you select to the ID selected in the "ID" Combobox.

Previous page and Next Page To make this setup page simple and clear, we have divided the "Control table" into several pages. You can use these buttons to navigate to different pages.

Example:

BASIC SETTING **FORWARDING RULES** **SECURITY SETTING** **ADVANCED SETTING** **TOOLBOX**

• Status
• Packet Filters
• Domain Filters
• URL Blocking
• MAC Control
• Miscellaneous

MAC Address Control [Help]

Item	Setting
MAC Address Control	<input type="checkbox"/> Enable
<input checked="" type="checkbox"/> Connection control	Wireless and wired clients with C checked can connect to this device; and allow unspecified MAC addresses to connect.
<input checked="" type="checkbox"/> Association control	Wireless clients with A checked can associate to the wireless LAN; and deny unspecified MAC addresses to associate. Note: Association control has no effect on wired clients.

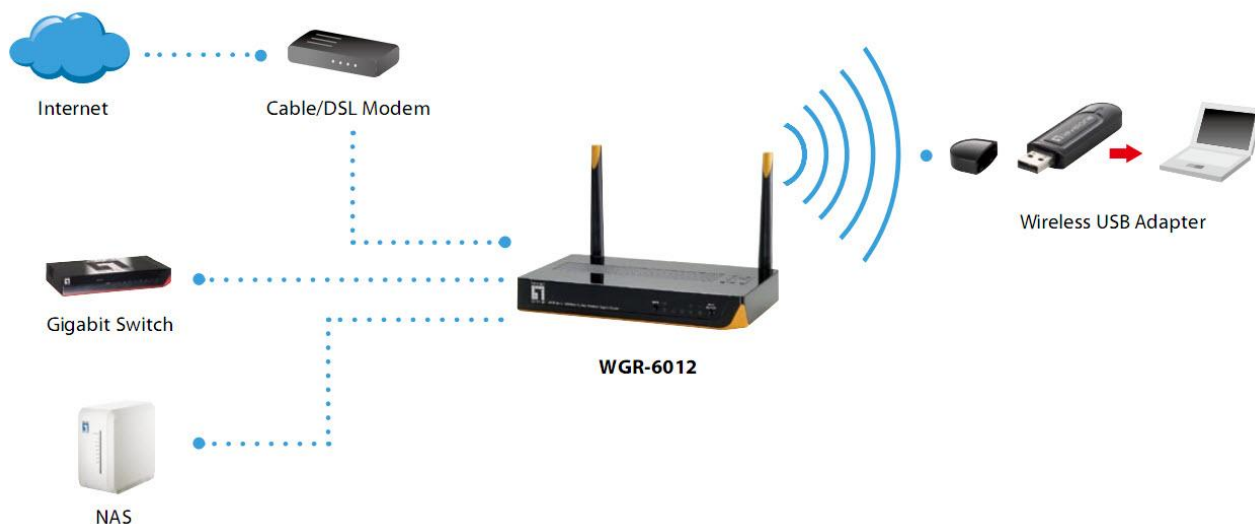
DHCP clients ID

ID	MAC Address	IP Address	C	A
1	00-12-34-56-78-90	192.168.1.100	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	00-12-34-56-78-92	192.168.1.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	00-09-76-54-32-10	192.168.1.101	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4		192.168.1.	<input type="checkbox"/>	<input type="checkbox"/>

In this scenario, there are three clients listed in the Control Table. Clients 1 and 2 are wireless, and client 3 is wired.

- 1.The "MAC Address Control" function is enabled.
- 2."Connection control" is enabled, and all of the wired and wireless clients not listed in the "Control table" are "allowed" to connect to this device.
- 3."Association control" is enabled, and all of the wireless clients not listed in the "Control table" are "denied" to associate to the wireless LAN.
- 4.Clients 1 and 3 have fixed IP addresses either from the DHCP server of this device or manually assigned:
ID 1 - "00-12-34-56-78-90" --> 192.168.1.100
ID 3 - "00-09-76-54-32-10" --> 192.168.1.101
Client 2 will obtain its IP address from the IP Address pool specified in the "DHCP Server" page or can use a manually assigned static IP address.
If, for example, client 3 tries to use an IP address different from the address listed in the Control table (192.168.1.101), it will be denied to connect to this device.
- 5.Clients 2 and 3 and other wired clients with a MAC address unspecified in the Control table are all allowed to connect to this device. But client 1 is denied to connect to this device.
- 6.Clients 1 and 2 are allowed to associate to the wireless LAN, but a wireless client with a MAC address not specified in the Control table is denied to associate to the wireless LAN. Client 3 is a wired client and so is

not affected by Association control.



3.3.3.5 Miscellaneous Items

ADMINISTRATOR's MAIN MENU																				
Status	Wizard	Advanced																		
Logout																				
BASIC SETTING	FORWARDING RULES	SECURITY SETTING																		
ADVANCED SETTING																				
TOOLBOX																				
<ul style="list-style-type: none"> Status Packet Filters Domain Filters URL Blocking MAC Control Miscellaneous 	<div>Miscellaneous Items [Help]</div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> <th>Enable</th> </tr> </thead> <tbody> <tr> <td>▶ Remote Administrator Host / Port</td> <td>0.0.0.0 / 8080</td> <td><input type="checkbox"/></td> </tr> <tr> <td>▶ Administrator Time-out</td> <td>600 seconds (0 to disable)</td> <td></td> </tr> <tr> <td>▶ Discard PING from WAN side</td> <td></td> <td><input type="checkbox"/></td> </tr> <tr> <td>▶ SPI mode</td> <td></td> <td><input type="checkbox"/></td> </tr> <tr> <td>▶ DoS Attack Detection</td> <td></td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <div> <input type="button" value="Save"/> <input type="button" value="Undo"/> </div>		Item	Setting	Enable	▶ Remote Administrator Host / Port	0.0.0.0 / 8080	<input type="checkbox"/>	▶ Administrator Time-out	600 seconds (0 to disable)		▶ Discard PING from WAN side		<input type="checkbox"/>	▶ SPI mode		<input type="checkbox"/>	▶ DoS Attack Detection		<input type="checkbox"/>
Item	Setting	Enable																		
▶ Remote Administrator Host / Port	0.0.0.0 / 8080	<input type="checkbox"/>																		
▶ Administrator Time-out	600 seconds (0 to disable)																			
▶ Discard PING from WAN side		<input type="checkbox"/>																		
▶ SPI mode		<input type="checkbox"/>																		
▶ DoS Attack Detection		<input type="checkbox"/>																		

Remote Administrator Host/Port

In general, only Intranet 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 to 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 88. You can change

web server port to other port, too.

Administrator Time-out

The time of no activity to logout automatically. Set it to zero to disable this feature.

Discard PING from WAN side

When this feature is enabled, any host on the WAN cannot ping this product.

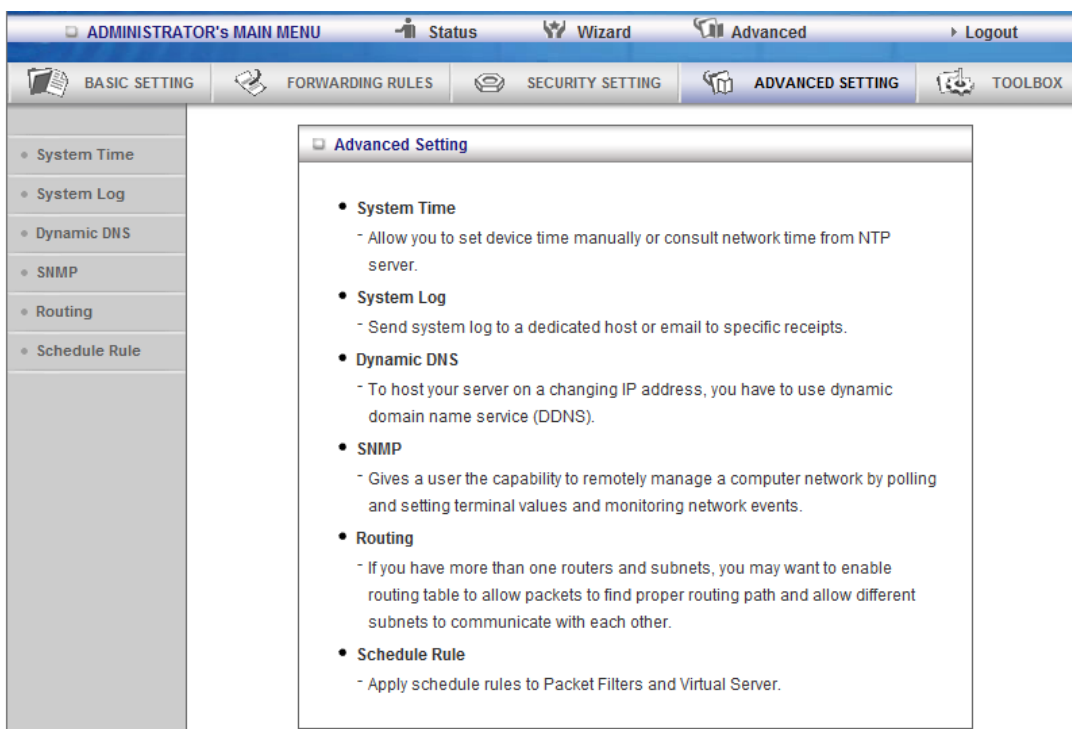
SPI Mode

When this feature is enabled, the router will record the packet information pass through the router like IP address, port address, ACK, SEQ number and so on. And the router will check every incoming packet to detect if this packet is valid.

DoS Attack Detection

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

3.3.4 Advanced Settings



3.3.4.1 System Time

BASIC SETTING		FORWARDING RULES		SECURITY SETTING		ADVANCED SETTING		TOOLBOX																																			
<ul style="list-style-type: none"> System Time System Log Dynamic DNS SNMP Routing Schedule Rule 																																											
<div> <div>System Time</div> <div>[HELP]</div> </div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>System Time</td> <td>2010年1月26日 下午 01:31:56</td> </tr> <tr> <td> <input checked="" type="radio"/> Get Date and Time by NTP Protocol <div>Sync Now!</div> </td> <td></td> </tr> <tr> <td>Time Server</td> <td>time.nist.gov</td> </tr> <tr> <td>Time Zone</td> <td>(GMT+08:00) Beijing, Hong Kong, Singapore, Taipei</td> </tr> <tr> <td colspan="2"> <input type="radio"/> Set Date and Time using PC's Date and Time <div>PC Date and Time: 2010年1月26日 下午 01:31:55</div> </td> </tr> <tr> <td colspan="2"> <input type="radio"/> Set Date and Time manually <div> <table border="1"> <tr> <td>Date</td> <td>Year: 2009</td> <td>Month: Jun</td> <td>Day: 01</td> </tr> <tr> <td>Time</td> <td>Hour: 0 (0-23)</td> <td>Minute: 0 (0-59)</td> <td>Second: 0 (0-59)</td> </tr> </table> </div> </td> </tr> <tr> <td>Daylight Saving</td> <td> <input type="radio"/> Enable <input checked="" type="radio"/> Disable <div> <table border="1"> <tr> <td>Start</td> <td>Month: Jan</td> <td>Day: 01</td> <td>Hour: 00</td> </tr> <tr> <td>End</td> <td>Month: Jan</td> <td>Day: 01</td> <td>Hour: 00</td> </tr> </table> </div> </td> </tr> <tr> <td colspan="2"> <div>Save</div> <div>Undo</div> </td> </tr> </tbody> </table>										Item	Setting	System Time	2010年1月26日 下午 01:31:56	<input checked="" type="radio"/> Get Date and Time by NTP Protocol <div>Sync Now!</div>		Time Server	time.nist.gov	Time Zone	(GMT+08:00) Beijing, Hong Kong, Singapore, Taipei	<input type="radio"/> Set Date and Time using PC's Date and Time <div>PC Date and Time: 2010年1月26日 下午 01:31:55</div>		<input type="radio"/> Set Date and Time manually <div> <table border="1"> <tr> <td>Date</td> <td>Year: 2009</td> <td>Month: Jun</td> <td>Day: 01</td> </tr> <tr> <td>Time</td> <td>Hour: 0 (0-23)</td> <td>Minute: 0 (0-59)</td> <td>Second: 0 (0-59)</td> </tr> </table> </div>		Date	Year: 2009	Month: Jun	Day: 01	Time	Hour: 0 (0-23)	Minute: 0 (0-59)	Second: 0 (0-59)	Daylight Saving	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <div> <table border="1"> <tr> <td>Start</td> <td>Month: Jan</td> <td>Day: 01</td> <td>Hour: 00</td> </tr> <tr> <td>End</td> <td>Month: Jan</td> <td>Day: 01</td> <td>Hour: 00</td> </tr> </table> </div>	Start	Month: Jan	Day: 01	Hour: 00	End	Month: Jan	Day: 01	Hour: 00	<div>Save</div> <div>Undo</div>	
Item	Setting																																										
System Time	2010年1月26日 下午 01:31:56																																										
<input checked="" type="radio"/> Get Date and Time by NTP Protocol <div>Sync Now!</div>																																											
Time Server	time.nist.gov																																										
Time Zone	(GMT+08:00) Beijing, Hong Kong, Singapore, Taipei																																										
<input type="radio"/> Set Date and Time using PC's Date and Time <div>PC Date and Time: 2010年1月26日 下午 01:31:55</div>																																											
<input type="radio"/> Set Date and Time manually <div> <table border="1"> <tr> <td>Date</td> <td>Year: 2009</td> <td>Month: Jun</td> <td>Day: 01</td> </tr> <tr> <td>Time</td> <td>Hour: 0 (0-23)</td> <td>Minute: 0 (0-59)</td> <td>Second: 0 (0-59)</td> </tr> </table> </div>		Date	Year: 2009	Month: Jun	Day: 01	Time	Hour: 0 (0-23)	Minute: 0 (0-59)	Second: 0 (0-59)																																		
Date	Year: 2009	Month: Jun	Day: 01																																								
Time	Hour: 0 (0-23)	Minute: 0 (0-59)	Second: 0 (0-59)																																								
Daylight Saving	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <div> <table border="1"> <tr> <td>Start</td> <td>Month: Jan</td> <td>Day: 01</td> <td>Hour: 00</td> </tr> <tr> <td>End</td> <td>Month: Jan</td> <td>Day: 01</td> <td>Hour: 00</td> </tr> </table> </div>	Start	Month: Jan	Day: 01	Hour: 00	End	Month: Jan	Day: 01	Hour: 00																																		
Start	Month: Jan	Day: 01	Hour: 00																																								
End	Month: Jan	Day: 01	Hour: 00																																								
<div>Save</div> <div>Undo</div>																																											

Get Date and Time by NTP Protocol

Selected if you want to Get Date and Time by NTP Protocol.

Time Server

Select a NTP time server to consult UTC time

Time Zone

Select a time zone where this device locates.

Set Date and Time manually

Selected if you want to Set Date and Time manually.

Set Date and Time manually

Selected if you want to Set Date and Time manually.

Function of Buttons

Sync Now: Synchronize system time with network time server

Daylight Saving: Set up where the location is.

3.3.4.2 System Log

Item	Setting	Enable
IP Address for Syslog	192.168.1.	<input checked="" type="checkbox"/>
IP Address of Outgoing Mail Server	Send Mail Now	<input checked="" type="checkbox"/>
SMTP Server IP/Port		
E-mail address		
E-mail Subject		
User name		
Password		
Log Type	<input checked="" type="checkbox"/> System Activity <input checked="" type="checkbox"/> Debug Information <input checked="" type="checkbox"/> Attacks <input checked="" type="checkbox"/> Dropped Packets <input checked="" type="checkbox"/> Notice	

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

IP Address for Syslog

Host IP of destination where syslogs will be sent to.

Check **Enable** to enable this function.

E-mail Alert Enable

Check if you want to enable Email alert (send syslog via email).

SMTP Server IP and Port

Input the SMTP server IP and port, which are concerted 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".

Send E-mail alert to

The recipients who will receive these logs. You can assign more than 1 recipient, using ';' or ',' to separate these email addresses.

3.3.4.3 DDNS Service

The screenshot shows a web interface for configuring DDNS. At the top is a navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary bar with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. On the left is a sidebar menu with 'System Time', 'System Log', 'Dynamic DNS', 'SNMP', 'Routing', and 'Schedule Rule'. The main content area is titled 'Dynamic DNS' with a '[Help]' link. It contains a table with two columns: 'Item' and 'Setting'. The table has five rows: 'DDNS' with radio buttons for 'Disable' (selected) and 'Enable'; 'Provider' with a dropdown menu showing 'DynDNS.org(Dynamic)' and a 'Provider website' button; 'Host Name' with a text input field; 'Username / E-mail' with a text input field; and 'Password / Key' with a text input field. At the bottom of the table are 'Save' and 'Undo' buttons.

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

To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).

So that 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.

To enable **Dynamic DNS** click the check box next to **Enable** in the **DDNS** field.

Next you can enter the appropriate information about your Dynamic DNS Server.

You have to define:

Provider

Host Name

Username/E-mail

Password/Key

You will get this information when you register an account on a Dynamic DNS server.

3.3.4.4 SNMP

The screenshot shows a web interface for configuring SNMP. At the top is a navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary bar with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING' (which is highlighted), and 'TOOLBOX'. On the left is a sidebar menu with 'System Time', 'System Log', 'Dynamic DNS', 'SNMP' (highlighted), 'Routing', and 'Schedule Rule'. The main content area is titled 'SNMP Setting' with a '[Help]' link. It contains a table with two columns: 'Item' and 'Setting'. The table has the following rows: 'Enable SNMP' with checkboxes for 'Local' (checked) and 'Remote'; 'Get Community' with a text box containing 'public'; 'Set Community' with a text box containing 'private'; 'IP 1', 'IP 2', 'IP 3', and 'IP 4', each with an empty text box; and 'SNMP Version' with radio buttons for 'V1' and 'V2c' (selected). At the bottom of the table are 'Save' and 'Undo' buttons.

Item	Setting
▶ Enable SNMP	<input checked="" type="checkbox"/> Local <input type="checkbox"/> Remote
▶ Get Community	<input type="text" value="public"/>
▶ Set Community	<input type="text" value="private"/>
▶ IP 1	<input type="text"/>
▶ IP 2	<input type="text"/>
▶ IP 3	<input type="text"/>
▶ IP 4	<input type="text"/>
▶ SNMP Version	<input type="radio"/> V1 <input checked="" type="radio"/> V2c

Save Undo

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.

Enable SNMP

You must check Local, Remote or both to enable SNMP function. If Local is checked, this device will response request from LAN. If Remote is checked, this device will response request from WAN.

Get Community

Setting the community of GetRequest your device will response.

Set Community

Setting the community of SetRequest your device will accept.

IP 1, IP 2, IP 3, IP 4

Input your SNMP Management PC's IP here. User has to configure to where this device should send SNMP Trap message.

SNMP Version

Please select proper SNMP Version that your SNMP Management software supports.

3.3.4.5 Routing

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"/>

Save Undo

Routing Tables allow you to determine which physical interface address to use for outgoing IP data grams. 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.

Routing Table settings are settings used to setup the functions of static.

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 subnet in your network.

Otherwise, please select RIPv1 if you need this protocol.

Static Routing: For static routing, you can specify up to 8 routing rules. You can enter the destination IP address, subnet mask, gateway, hop for each routing rule, and then enable or disable the rule by checking or un-checking the Enable checkbox.

3.3.4.6 Schedule Rule

The screenshot shows the 'ADMINISTRATOR's MAIN MENU' with tabs for BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING, and TOOLBOX. The left sidebar lists various system settings, with 'Schedule Rule' selected. The main content area is titled 'Schedule Rule' and includes a '[Help]' link. It features a table with two columns: 'Item' and 'Setting'. Under the 'Item' column, there is a 'Schedule' section with an 'Enable' checkbox. Below this, there is a table with three columns: 'Rule#', 'Rule Name', and 'Action'. At the bottom of the main content area, there are 'Save' and 'Add New Rule...' buttons.

Schedule Rule		[Help]
Item	Setting	
▶ Schedule	<input type="checkbox"/> Enable	
Rule#	Rule Name	Action
<div>Save Add New Rule...</div>		

You can set the schedule time to decide which service will be turned on or off. Select the “enable” item.

Press “Add New Rule”

You can write a rule name and set which day and what time to schedule from “Start Time” to “End Time”. The following example configure “ftp time” as everyday 14:10 to 16:20

The screenshot shows the 'ADMINISTRATOR's MAIN MENU' with tabs for BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING, and TOOLBOX. The left sidebar lists various system settings, with 'Schedule Rule' selected. The main content area is titled 'Schedule Rule Setting' and includes a '[Help]' link. It features a table with two columns: 'Item' and 'Setting'. Under the 'Item' column, there is a 'Name of Rule 1' field and a 'System Time' field. Below this, there is a table with three columns: 'Week Day', 'Start Time (hh:mm)', and 'End Time (hh:mm)'. At the bottom of the main content area, there are 'Save', 'Undo', and 'Back' buttons.

Schedule Rule Setting			[Help]
Item	Setting		
▶ Name of Rule 1	<input type="text"/>		
▶ System Time	2008年11月1日 上午 01:07:30		
Week Day	Start Time (hh:mm)	End Time (hh:mm)	
Sunday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	
Monday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	
Tuesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	
Wednesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	
Thursday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	
Friday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	
Saturday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	
Every Day	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	
<div>Save Undo Back</div>			

Schedule Enable

Selected if you want to Enable the Scheduler.

Edit

To edit the schedule rule.

Delete

To delete the schedule rule, and the rule# of the rules behind the deleted one will decrease one automatically.
Schedule Rule can be apply to Virtual server and Packet Filter, for example:

Example1: **Virtual Server** – Apply Rule#1 (ftp time: everyday 14:20 to 16:30)

The screenshot shows the 'Virtual Server' configuration page. The left sidebar has a tree view with 'Virtual Server' selected. The main area has a title bar 'Virtual Server' with a '[Help]' link. Below the title bar, there are dropdowns for 'Well known services' (set to '-- select one --') and 'Schedule rule' (set to '(00)Always'). There is a 'Copy to' button and an 'ID' dropdown. Below these is a table with 7 columns: ID, Server IP, Public Port, Private Port, Protocol, Enable, and Schedule Rule#. The table contains 10 rows. Row 1 has ID 1, Server IP 192.168.1.1, Public Port, Private Port 21, Protocol Both, Enable checked, and Schedule Rule# 1. Rows 2-10 have IDs 2-10, Server IP 192.168.1., Public Port, Private Port, Protocol Both, Enable checked, and Schedule Rule# 0. At the bottom of the table are buttons for 'Next >>', 'Save', and 'Undo'.

ID	Server IP	Public Port	Private Port	Protocol	Enable	Schedule Rule#
1	192.168.1.1		21	Both	<input checked="" type="checkbox"/>	1
2	192.168.1.			Both	<input checked="" type="checkbox"/>	0
3	192.168.1.			Both	<input checked="" type="checkbox"/>	0
4	192.168.1.			Both	<input checked="" type="checkbox"/>	0
5	192.168.1.			Both	<input checked="" type="checkbox"/>	0
6	192.168.1.			Both	<input checked="" type="checkbox"/>	0
7	192.168.1.			Both	<input checked="" type="checkbox"/>	0
8	192.168.1.			Both	<input checked="" type="checkbox"/>	0
9	192.168.1.			Both	<input checked="" type="checkbox"/>	0
10	192.168.1.			Both	<input checked="" type="checkbox"/>	0

Example2: **Packet Filter** – Apply Rule#1 (ftp time: everyday 14:20 to 16:30).

The screenshot shows the 'Outbound Packet Filter' configuration page. The left sidebar has a tree view with 'Status' selected. The main area has a title bar 'Outbound Packet Filter' with a '[Help]' link. Below the title bar, there is a table with 2 columns: Item and Setting. The first row has Item 'Outbound Filter' and Setting 'Enable' with a checked checkbox. Below this, there are two radio buttons: 'Allow all to pass except those match the following rules.' (selected) and 'Deny all to pass except those match the following rules.'. Below the radio buttons is a dropdown for 'Schedule rule' (set to '(00)Always') and a 'Copy to' button. Below these is a table with 5 columns: ID, Source IP : Ports, Destination IP : Ports, Enable, and Schedule Rule#. The table contains 8 rows. Row 1 has ID 1, Source IP : Ports, Destination IP : Ports, Enable checked, and Schedule Rule# 1. Rows 2-8 have IDs 2-8, Source IP : Ports, Destination IP : Ports, Enable unchecked, and Schedule Rule# 0. At the bottom of the table are buttons for 'Save', 'Undo', 'Inbound Filter...', and 'MAC Level...'.

ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#
1			<input checked="" type="checkbox"/>	1
2			<input type="checkbox"/>	0
3			<input type="checkbox"/>	0
4			<input type="checkbox"/>	0
5			<input type="checkbox"/>	0
6			<input type="checkbox"/>	0
7			<input type="checkbox"/>	0
8			<input type="checkbox"/>	0

3.3.5 Toolbox

The screenshot shows the 'ADMINISTRATOR's MAIN MENU' with tabs for Status, Wizard, Advanced, and Logout. Below these are tabs for BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING, and TOOLBOX. The TOOLBOX tab is selected, displaying a list of tools: View Log, Firmware Upgrade, Backup Setting, Reset to Default, Reboot, and Miscellaneous. Each tool has a brief description of its function.

- **View Log**
 - View the system logs.
- **Firmware Upgrade**
 - Prompt the administrator for a file and upgrade it to this device.
- **Backup Setting**
 - Save the settings of this device to a file.
- **Reset to Default**
 - Reset the settings of this device to the default values.
- **Reboot**
 - Reboot this device.
- **Miscellaneous**
 - MAC Address for Wake-on-LAN: Let you to power up another network device remotely.
 - 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.

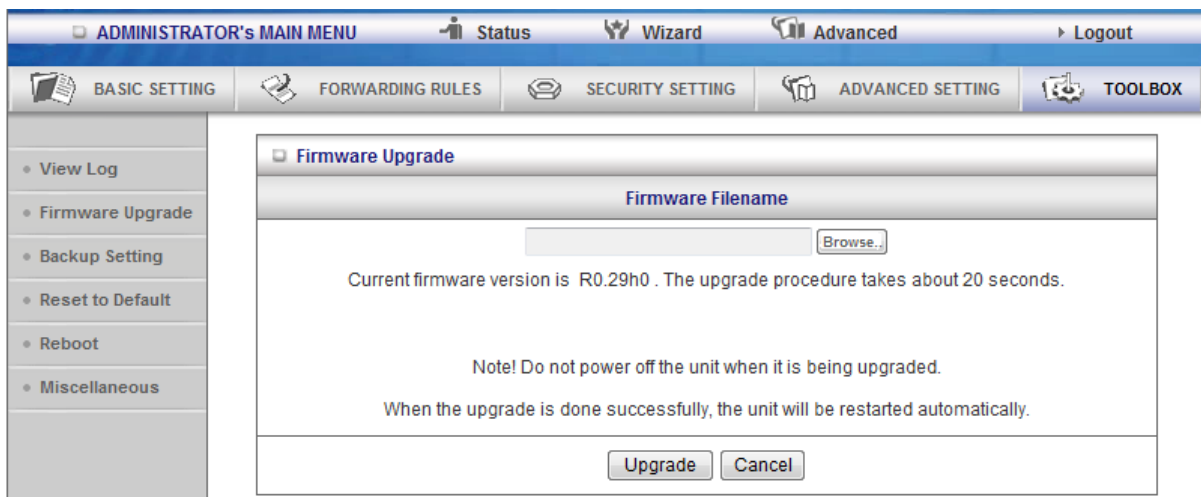
3.3.5.1 View Log

The screenshot shows the 'ADMINISTRATOR's MAIN MENU' with the same tabs as the previous image. The TOOLBOX tab is selected, and the 'System Log' option is chosen. The log is displayed in a table with two columns: Item and Info. The log shows several entries of blocked access attempts from specific WLAN addresses.

Item	Info
WAN Type:	Dynamic IP Address (R0.29h0)
Display time	Sat Nov 01 01:13:52 2008
Time	Log
2008年11月1日 上午 01:13:26	Blocked access attempt from WLAN 00-1F-D4-00-5B-51
2008年11月1日 上午 01:13:26	Blocked access attempt from WLAN 00-1F-D4-00-5B-51
2008年11月1日 上午 01:13:26	Blocked access attempt from WLAN 06-1F-D4-00-5B-51
2008年11月1日 上午 01:13:26	Blocked access attempt from WLAN 00-1F-D4-00-5B-51
2008年11月1日 上午 01:13:26	Blocked access attempt from WLAN 06-1F-D4-00-5B-51

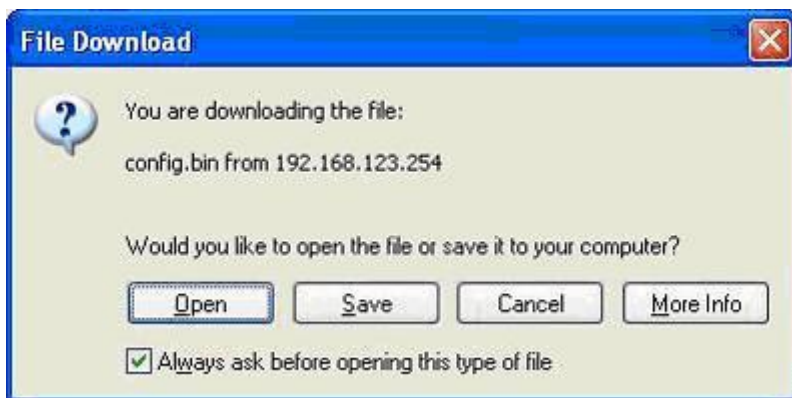
You can View system log by clicking the **View Log** button

3.3.5.2 Firmware Upgrade



You can upgrade firmware by clicking **Firmware Upgrade** button.

3.3.5.3 Backup Setting



You can backup your settings by clicking the **Backup Setting** button 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.

3.3.5.4 Reset to default



You can also reset this product to factory default by clicking the **Reset to default** button.

3.3.5.5 Reboot



You can also reboot this product by clicking the **Reboot** button.

3.3.5.6 Miscellaneous Items

A screenshot of a web interface for configuring a device. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary navigation bar with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. On the left side, there is a sidebar menu with options: 'View Log', 'Firmware Upgrade', 'Backup Setting', 'Reset to Default', 'Reboot', and 'Miscellaneous'. The main content area is titled 'Miscellaneous Items' and contains a table with two columns: 'Item' and 'Setting'. The table has two rows: one for 'MAC Address for Wake-on-LAN' with a 'Wake up' button, and one for 'Domain Name or IP address for Ping Test' with a 'Ping' button. At the bottom of the table are 'Save' and 'Undo' buttons. A '[Help]' link is visible in the top right corner of the table area.

MAC Address for Wake-on-LAN

Wake-on-LAN is a technology that enables you to power up a networked device remotely. In order to enjoy this feature, the target device must be Wake-on-LAN enabled and you have to know the MAC address of this device, say 00-11-22-33-44-55. Clicking "Wake up" button will make the router to send the wake-up frame to the target device immediately.

Domain Name or IP Address for Test

Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

Appendices and Index

802.1x Setting

1. Equipment Details

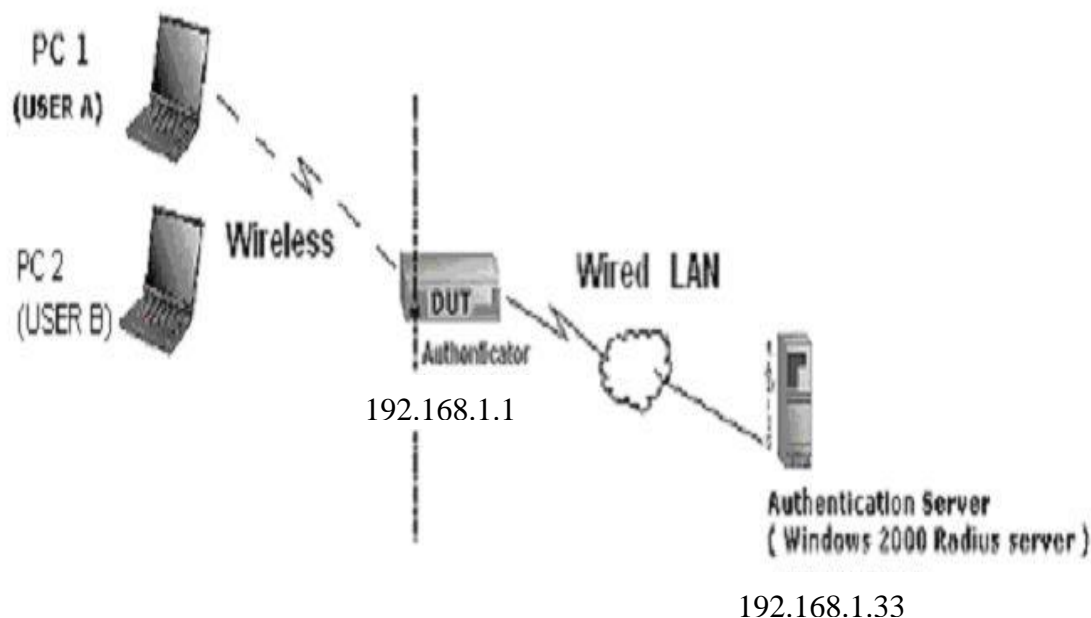


Figure 1: Testing Environment (Use Windows 2000 Radius Server)

PC1:

Microsoft Windows XP Professional without Service Pack 1.

Wireless Cardbus:3.0.3.0

Driver version:

PC2:

Microsoft Windows XP Professional with Service Pack 1a or latter.

Wireless Cardbus:1.0.1.0

Driver version: 1.7.29.0 (Driver date: 10.20.2001)

Authentication Server: Windows 2000 RADIUS server with Service Pack 3 and HotFix Q313664.

Note. Windows 2000 RADIUS server only supports PEAP after upgrade to service pack 3 and HotFix Q313664 (You can get more information from

<http://support.microsoft.com/default.aspx?scid=kb;en-us;313664>)

2. DUT Configuration:

- 1.Enable DHCP server.
- 2.WAN setting: static IP address.
- 3.LAN IP address: 192.168.1.1/24.
- 4.Set RADIUS server IP.
- 5.Set RADIUS server shared key.
- 6.Configure WEP key and 802.1X setting.

The following test will use the inbuilt 802.1X authentication method such as ,EAP_TLS, PEAP_CHAPv2(Windows XP with SP1 only), and PEAP_TLS(Windows XP with SP1 only) using the Smart Card or other Certificate of the Windows XP Professional.

3. DUT and Windows 2000 Radius Server Setup

3-1-1. Setup Windows 2000 RADIUS Server

We have to change authentication method to MD5_Challenge or using smart card or other certificate on RADIUS server according to the test condition.

3-1-2. Setup DUT

- 1.Enable the 802.1X (check the “Enable checkbox”).
- 2.Enter the RADIUS server IP.
- 3.Enter the shared key. (The key shared by the RADIUS server and DUT).
- 4.We will change 802.1X encryption key length to fit the variable test condition.

3-1-3. Setup Network adapter on PC

- 1.Choose the IEEE802.1X as the authentication method. (Fig 2)

Note.

Figure 2 is a setting picture of Windows XP without service pack 1. If users upgrade to service pack 1, then they can't see MD5-Challenge from EAP type list any more, but they will get a new Protected EAP (PEAP) option.

- 2.Choose MD5-Challenge or Smart Card or other Certificate as the EAP type.

- 3.If choosing use smart card or the certificate as the EAP type, we select to

use a certificate on this computer. (Fig 3)

4. We will change EAP type to fit the variable test condition.

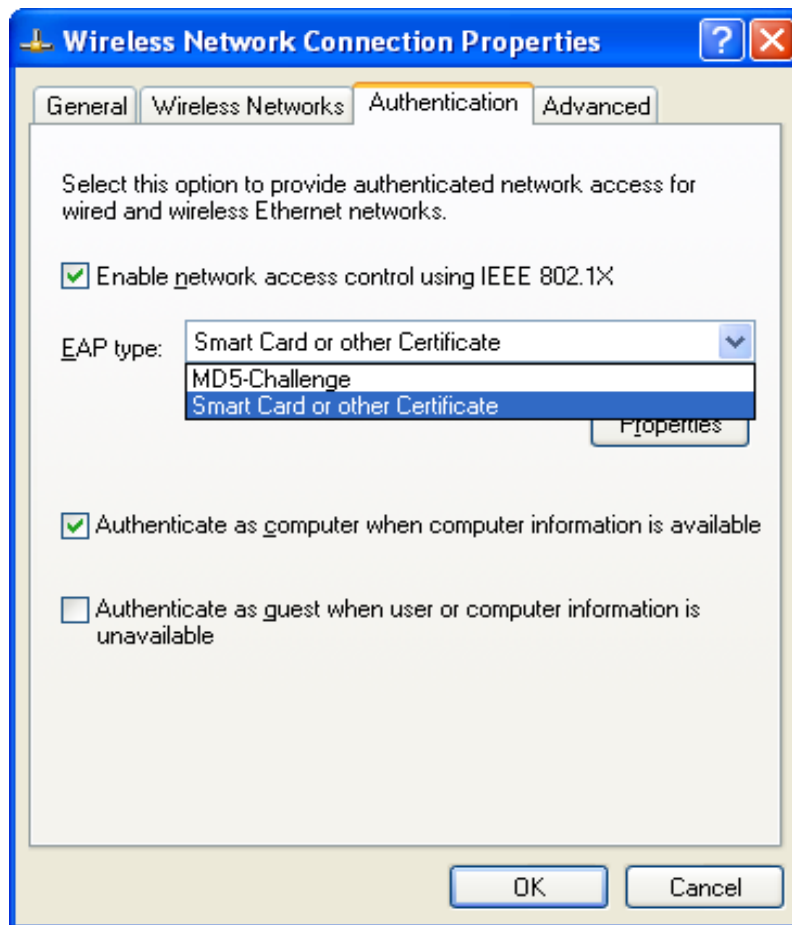


Figure 2: Enable IEEE 802.1X access control

Figure 3: Smart card or certificate properties

4. Windows 2000 RADIUS server Authentication testing:

4.1 DUT authenticate PC1 using certificate. (PC2 follows the same test procedures.)

1. Download and install the certificate on PC1. (Fig 4)
2. PC1 choose the SSID of DUT as the Access Point.
3. Set authentication type of wireless client and RADIUS server both to EAP_TLS.
4. Disable the wireless connection and enable again.
5. The DUT will send the user's certificate to the RADIUS server, and then send the message of authentication result to PC1. (Fig 5)
6. Windows XP will prompt that the authentication process is success or fail and end the authentication procedure. (Fig 6)
7. Terminate the test steps when PC1 get dynamic IP and PING remote host successfully.

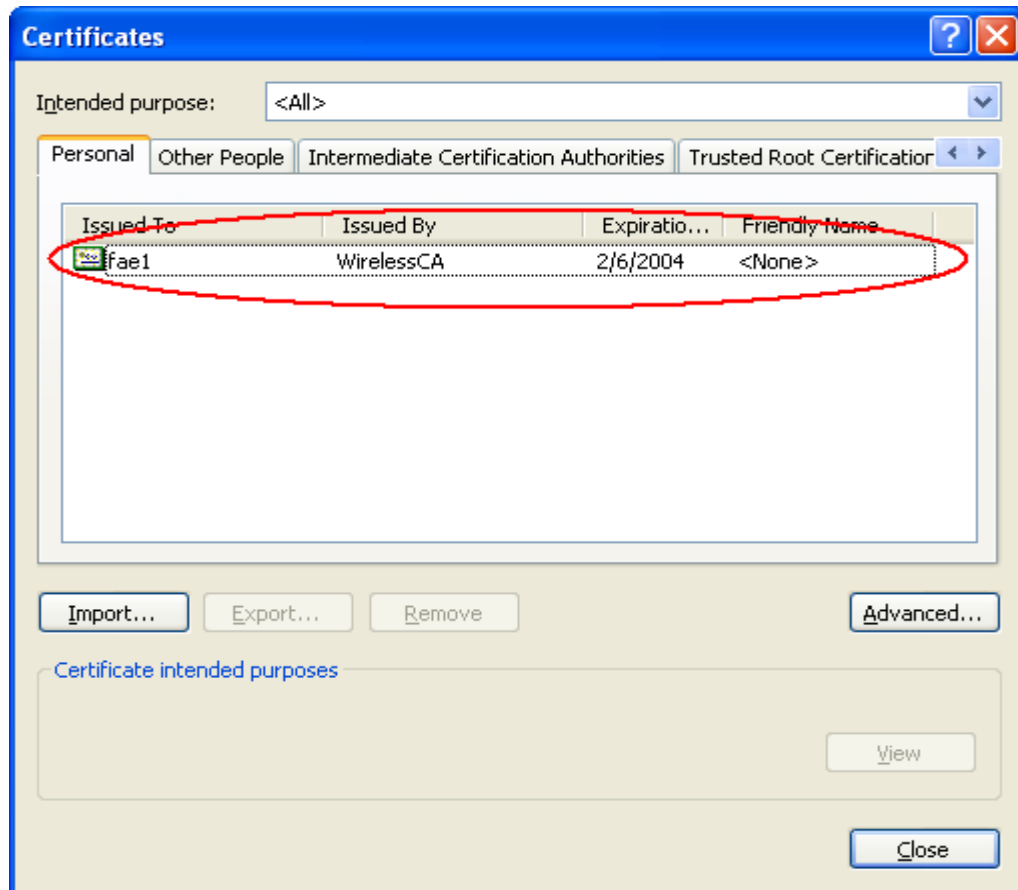


Figure 4: Certificate information on PC1

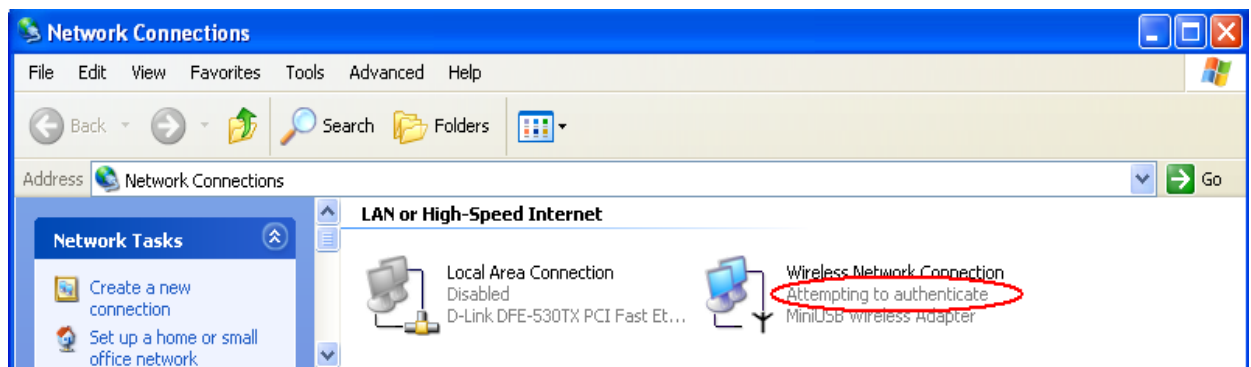


Figure 5: Authenticating

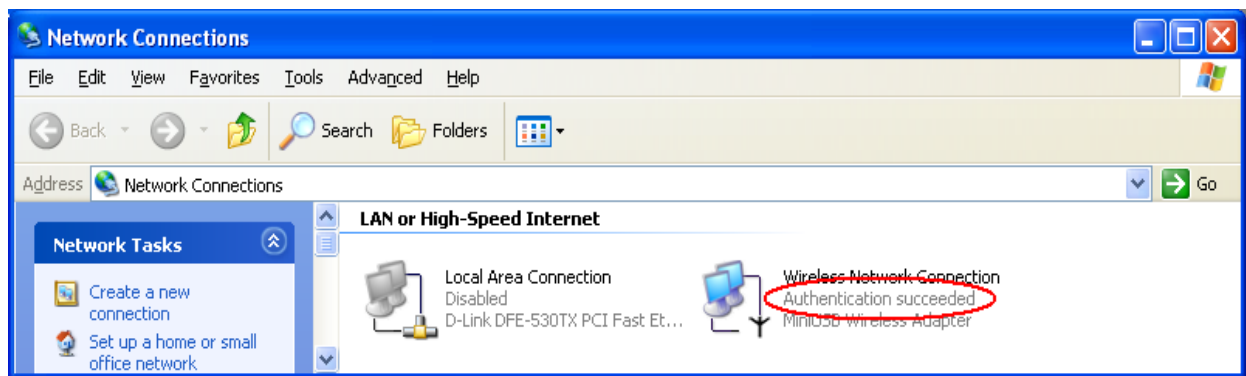


Figure 6: Authentication success

4.2DUT authenticate PC2 using PEAP-TLS.

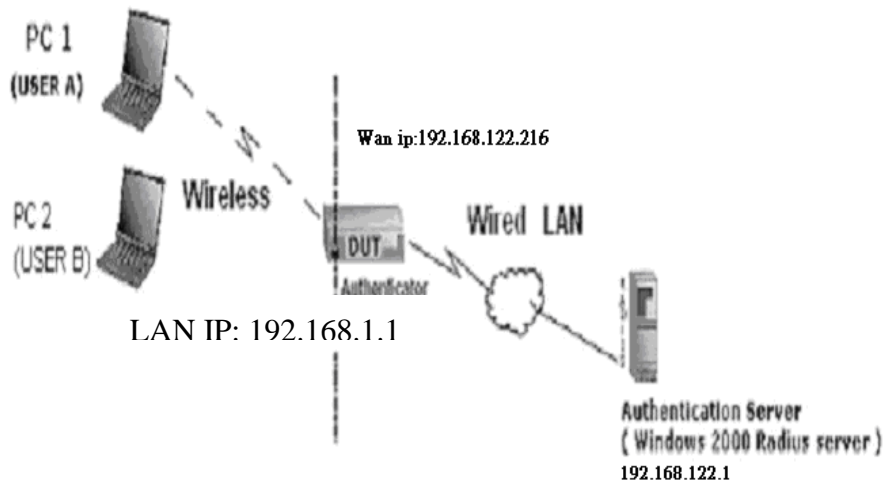
1. PC2 choose the SSID of DUT as the Access Point.
2. Set authentication type of wireless client and RADIUS server both to PEAP_TLS.
3. Disable the wireless connection and enable again.
- 4.The DUT will send the user's certificate to the RADIUS server, and then send the message of authentication result to PC2.
5. Windows XP will prompt that the authentication process is success or fail and end the authentication procedure.
6. Terminate the test steps when PC2 get dynamic IP and PING remote host successfully.

**Support Type: The router supports the types of 802.1x Authentication:
PEAP-CHAPv2 and PEAP-TLS.**

Note.

- 1.PC1 is on Windows XP platform without Service Pack 1.
- 2.PC2 is on Windows XP platform with Service Pack 1a.
- 3.PEAP is supported on Windows XP with Service Pack 1 only.
- 4.Windows XP with Service Pack 1 allows 802.1x authentication only when data encryption function is enable.

WPA Settings



Wireless Router: LAN IP: 192.168.1.1

WAN IP: 192.168.122.216

Radius Server: 192.168.122.1

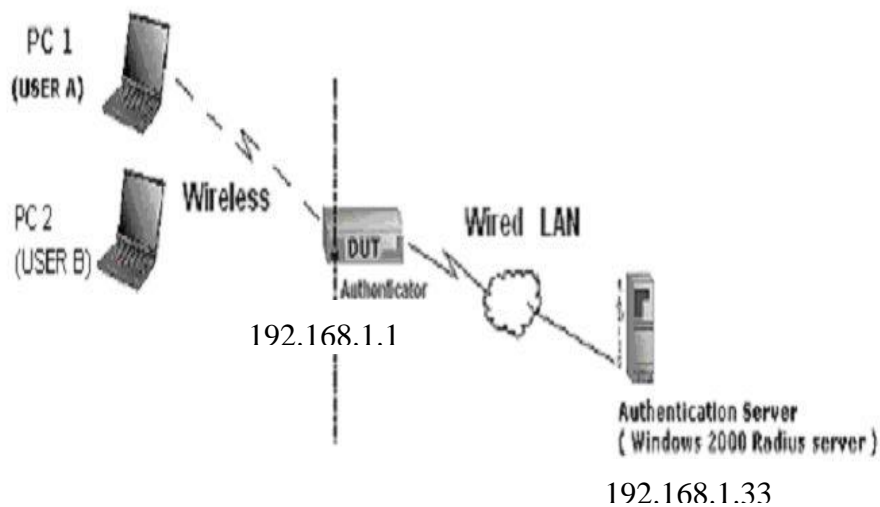
UserA : XP Wireless Card:Ti-11g

Tool: Odyssey Client Manager

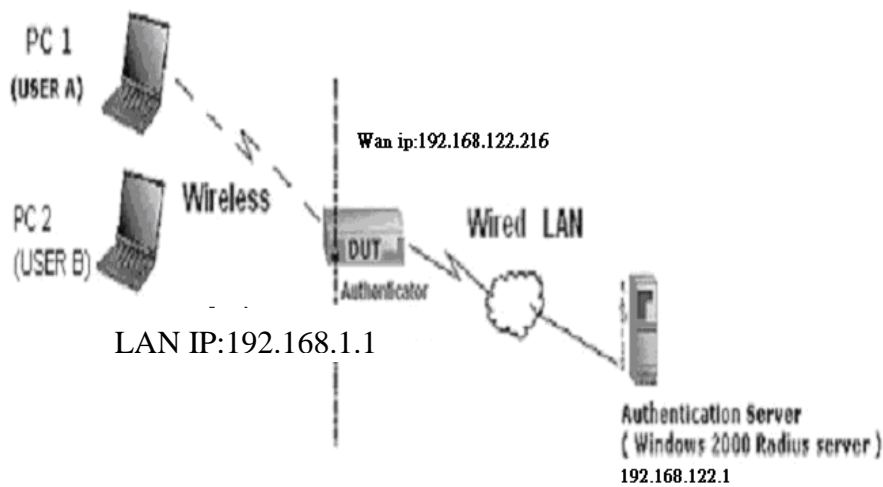
Refer to: www.funk.com

Download: http://www.funk.com/News&Events/ody_c_wpa_preview_pn.asp

Or Another Configuration:



For this function, we need the server to authenticate. This function is like 802.1x.



The above is our environment:

Method 1:

1. The UserA or UserB have to get certificate from Radius, first.

<http://192.168.122.1/certsrv>

account : fae1

passwd : fae1



2. Then, Install this certificate and finish.

3. Go to the Web manager of Wireless Router to configure, like below:

Network ID(SSID)	123kk
Channel	8
Security	WPA

802.1X Settings

RADIUS Server IP	192.168.122.1
RADIUS port	1812
RADIUS Shared Key	costra

4. Go to Odyssey Client Manager, choose “Profiles” and Setup Profile name as “1”

Add Profile

Profile name: 1

User Info | Authentication | ITLS Settings | PEAP Settings

Login name: fae1

Password

- ☒ Permit login using password
- ☐ use Windows password
- ☐ prompt for password
- ☒ use the following password:

fae1

☒ Unmask

Certificate

- ☒ Permit login using my certificate:

fae1

View ... Browse ...

OK Cancel

Login name and password are fae1 and fae1.

Remember that you get certificate from Radius in Step1.

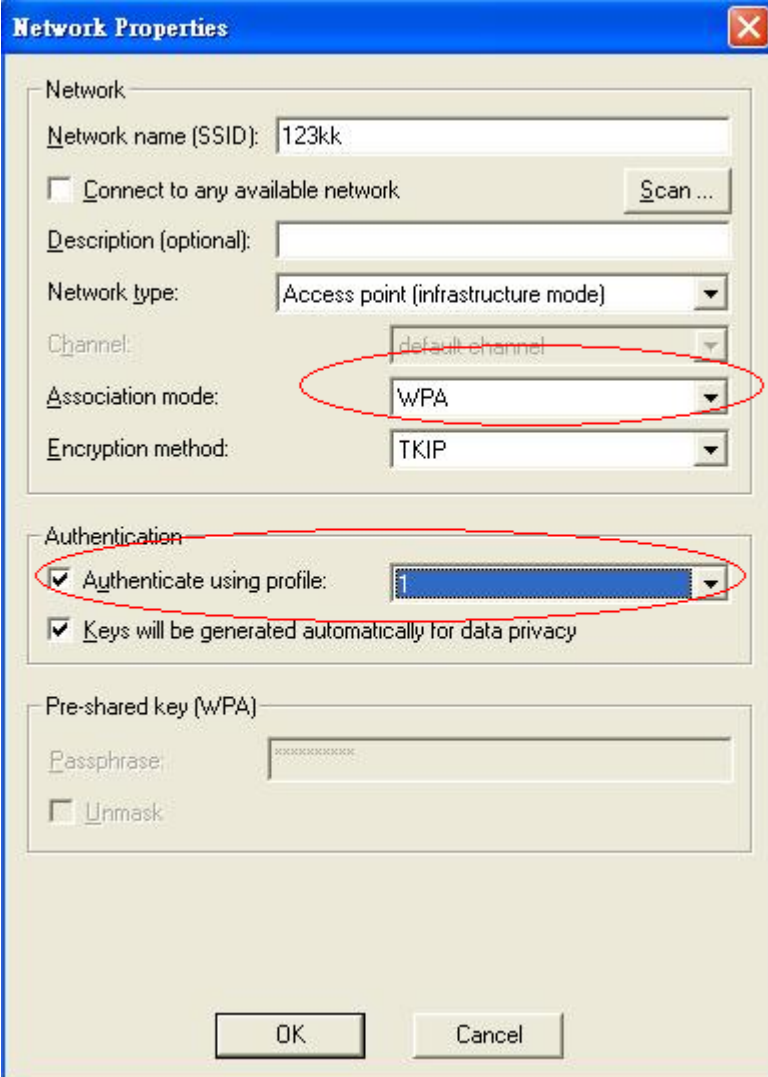
5. Then Choose “certificate” like above.



6. Then go to Authentication and first Remove EAP/ TLS and Add EAP/TLS again.



7. Go "Network" and Select "1" and ok



The image shows a "Network Properties" dialog box with a blue title bar and a close button. It contains three main sections: "Network", "Authentication", and "Pre-shared key (WPA)".

Network section:

- Network name (SSID): 123kk
- ☐ Connect to any available network (with a "Scan ..." button)
- Description (optional):
- Network type: Access point (infrastructure mode)
- Channel: default channel
- Association mode: WPA (circled in red)
- Encryption method: TKIP

Authentication section:

- ☒ Authenticate using profile: 1 (circled in red)
- ☒ Keys will be generated automatically for data privacy

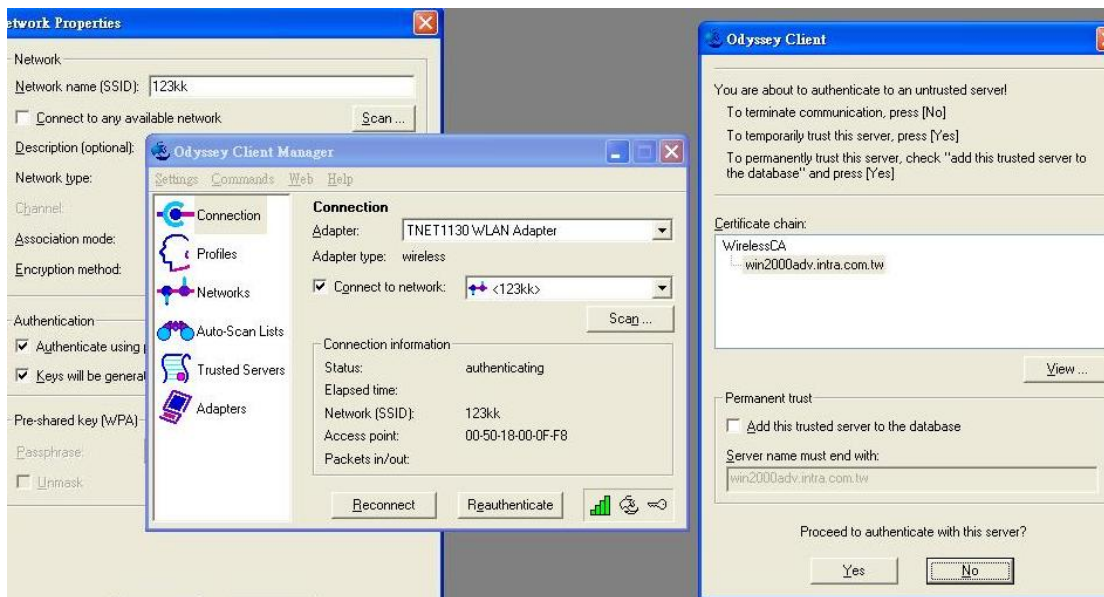
Pre-shared key (WPA) section:

- Passphrase: (masked with dots)
- ☐ Unmask

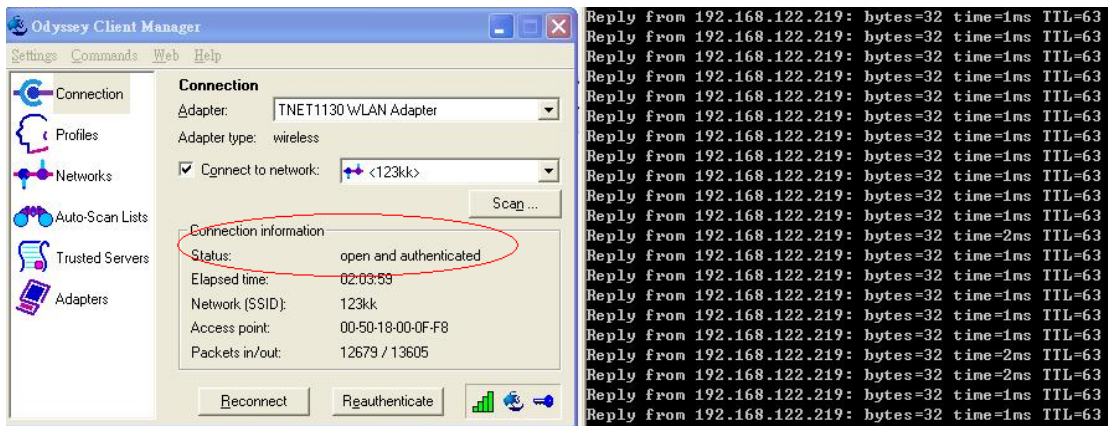
At the bottom are "OK" and "Cancel" buttons.

8. Back to Connection and Select "123kk.

If **successfully**, the wireless client has to authenticate with Radius Server, like below:



9.Result:



Method 2:

1. The UserA or UserB have to get certificate from Radius,first.

<http://192.168.122.1/certsrv>

account:fae1

passwd:fae1



2. Then Install this certificate and finish.

3. Setting on the router and client:

Router:

Network ID(SSID)	<input type="text" value="123kk"/>
Channel	<input type="text" value="8"/>
Security	<input type="text" value="WPA"/>

802.1X Settings

RADIUS Server IP	<input type="text" value="192.168.122.1"/>
RADIUS port	<input type="text" value="1812"/>
RADIUS Shared Key	<input type="text" value="costra"/>

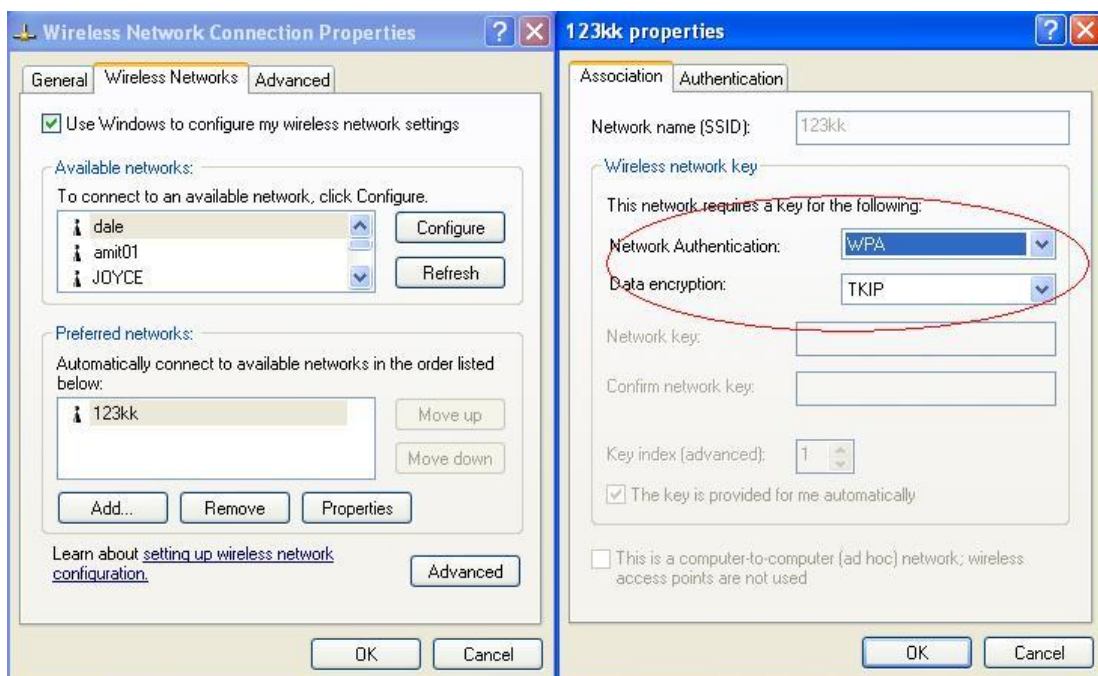
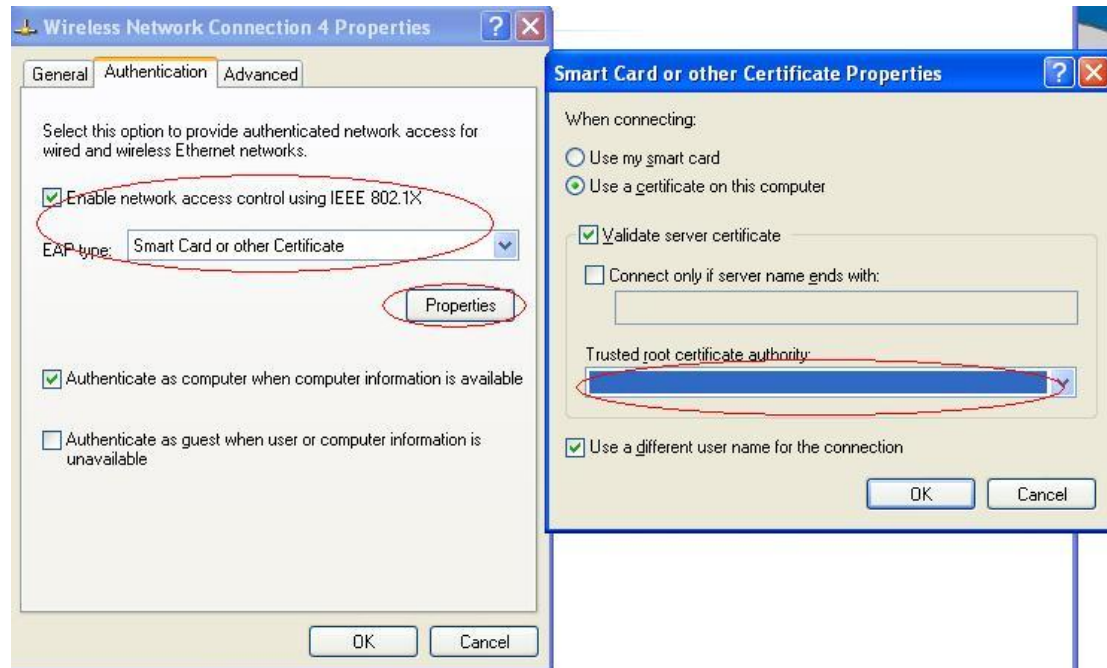
Client:

Go to “Network Connection” and select wireless adapter.

Choose “View available Wireless Networks” like below:

Advanced→ choose “123kk”

Select “WirelessCA and Enable” in Trusted root certificate authority:



Then, if the wireless client wants to associate, it has to request to authenticate.

FAQ and Troubleshooting

What can I do when I have some trouble at the first time?

1. Why can I not configure the router even if the cable is plugged in the ports of Router and the led is also light?

A: First, make sure that which port is plugged. If the cable is in the Wan port, please change to plug in LAN port 1 or LAN port 4:



Then, please check if the Pc gets IP address from Router. Use command mode as below:

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 192.168.1.115
    IP Address. . . . . : 255.255.255.0
    Subnet Mask . . . . . : 
    Default Gateway . . . . . : 192.168.1.1
```

If yes, please execute Browser, like Mozilla and key 192.168.1.1 in address.

If not, please ipconfig /release, then ipconfig /renew.

```
C:\>ipconfig /release

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 

C:\>ipconfig /renew

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 192.168.1.115
    IP Address. . . . . : 255.255.255.0
    Subnet Mask . . . . . : 
    Default Gateway . . . . . : 192.168.1.1
```

Whatever I setup, the pc can not get ip. Please check Status Led and refer to the Q2:

2. Why can I not connect the router even if the cable is plugged in LAN port and the led is

light?

A: First, please check Status Led. If the device is normal, the led will blink per second.

If not, please check How blinking Status led shows.

There are many abnormal symptoms as below:

Status Led is bright or dark in work: The system hanged up .Suggest powering off and on the router. But this symptom often occurs, please reset to default or upgrade latest FW to try again.

Status led flashes irregularly: Maybe the root cause is Flash ROM and please press reset Button to reset to default or try to use Recovery mode.(Refer to Q3 and Q4)

Status flashes very fast while powering on: Maybe the router is the recovery mode and please refer to Q4.

3.How to reset to factory default?

A: Press Wireless on /off and WPS button simultaneously about 5 sec

Status will start flashing about 5 times, remove the finger. The RESTORE process is completed.

4.Why can I not connect Internet even though the cables are plugged in Wan port and LAN port and the LEDs are blink. In addition, Status led is also normal and I can configure web management?

A: Make sure that the network cable from DSL or Cable modem is plugged in WAN port of Router and that the network cable from LAN port of router is plugged in Ethernet adapter. Then, please check which wan type you use. If you are not sure, please call the ISP. Then please go to this page to input the information ISP is assigned.

Choose WAN Type	
Type	Usage
<input type="radio"/> Static IP Address	ISP assigns you a static IP address.
<input checked="" type="radio"/> Dynamic IP Address	Obtain an IP address from ISP automatically.
<input type="radio"/> Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond)	
<input type="radio"/> PPP over Ethernet	Some ISPs require the use of PPPoE to connect to their services.
<input type="radio"/> PPTP	Some ISPs require the use of PPTP to connect to their services.
<input type="radio"/> L2TP	Some ISPs require the use of L2TP to connect to their services.
<div>Save Cancel</div>	

5. When I use Static IP Address to roam Internet, I can access or ping global IP 202.93.91.218, But I can not access the site that inputs domain name, for example <http://espn.com> ?

A: Please check the DNS configuration of Static IP Address. Please refer to the information of ISP and assign one or two in DNS item.

How do I connect router by using wireless?

1. How to start to use wireless?

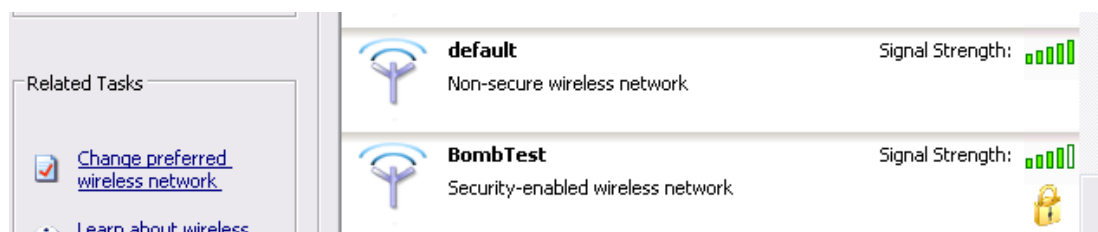
A: First, make sure that you already installed wireless client device in your computer. Then check the Configuration of wireless router. The default is as below:

Wireless Setting [Help]	
Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network ID(SSID)	LevelOne
Wireless Mode	<input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Channel	Auto
WDS	Enter...
WPS	Enter...
Security	None

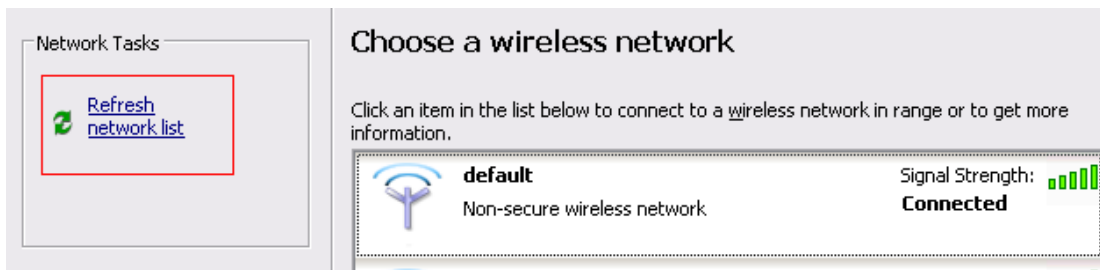
About wireless client, you will see wireless icon:



Then click and will see the AP list that wireless client can be accessed:



If the client can not access your wireless router, please refresh network list again. However, I still can not find the device which SSID is "default", please refer to Q3.



Choose the one that you will want to connect and Connect:



If successfully, the computer will show



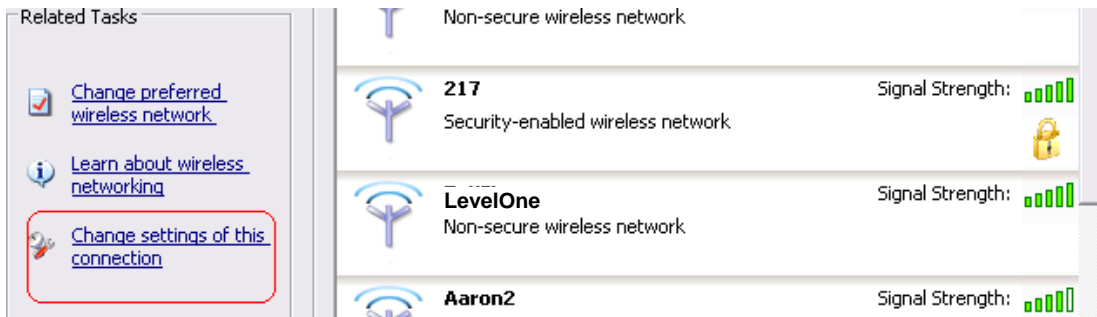
and get IP from router:

```
Ethernet adapter Wireless Network Connection 5:

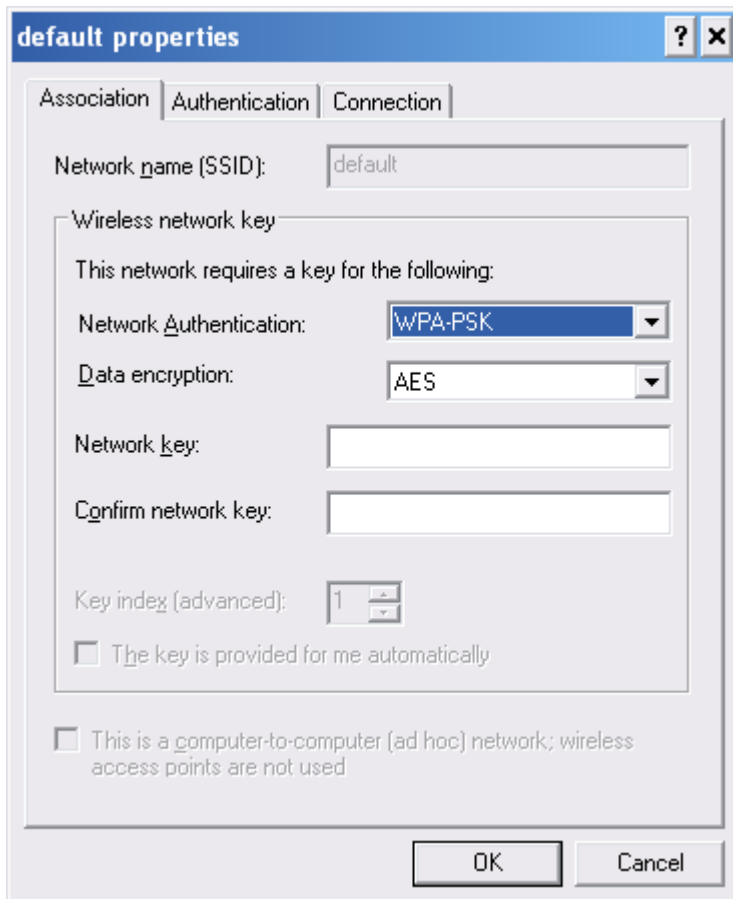
Connection-specific DNS Suffix  . : 
IP Address. . . . . : 192.168.1.115
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

2. When I use AES encryption of WPA-PSK to connect even if I input the correct pre-share key?

A: First, you must check if the driver of wireless client supports AES encryption. Please refer to the below:



If SSID is default and click “Properties” to check if the driver of wireless client supports AES encryption.



3. When I use wireless to connect the router, but I find the signal is very low even if I am close to the router?

A: Please check if the wireless client is normal, first. If yes, please send the unit to the seller and verify what the problem is.