# WIC168AM User's 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	hapter 1 Introduction				
Functions and Features					
Packin	Packing List5				
Chapter 2	Hardware Installation	6			
2.1 Pai	nel Layout	6			
2.2 Pro	cedure for Hardware Installation	8			
Chapter 3	Network Settings and Software Installation	9			
3.1 Ma	ke Correct Network Settings of Your Computer	9			
Chapter 4	Configuring Wireless Broadband Router	10			
4.1 Sta	rt-up and Log in	11			
4.2 Sta	tus	12			
4.3 Wi	zard	13			
4.4 Ba	sic Setting	14			
4.5 For	warding Rules	29			
4.6 Sec	curity Settings	33			
4.7 Ad	vanced Settings	47			
4.8 Too	olbox	58			
Appendix A	TCP/IP Configuration for Windows 95/98	63			
Appendix B	802.1x Setting	68			
Appendix C	WPA-PSK and WPA	74			
Appendix D WDS Setting					
Appendix E	Appendix E FAQ and Troubleshooting				
What can I do when I have some trouble at the first time? 91					
How d	How do I connect router by using wireless?				

## **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.

#### **Functions and Features**

#### **Router Basic functions**

• Auto-sensing Ethernet Switch

Equipped with a 4-port auto-sensing Ethernet switch.

• WAN type supported

The router supports some WAN types, Static, Dynamic, PPPoE, PPTP, L2TP, Dynamic IP with Road Runner.

#### • Firewall

All unwanted packets from outside intruders are blocked to protect your Intranet.

#### • DHCP server supported

All of the networked computers can retrieve TCP/IP settings automatically from this product.

#### Web-based configuring

Configurable through any networked computer's web browser using Netscape or Internet Explorer.

#### • Virtual Server supported

Enable you to expose WWW, FTP and other services on your LAN to be accessible to Internet users.

#### • User-Definable Application Sensing Tunnel

User can define the attributes to support the special applications requiring multiple connections, like Internet gaming, video conferencing, Internet telephony and so on, then this product can sense the application type and open multi-port tunnel for it.

#### • DMZ Host supported

Lets a networked computer be fully exposed to the Internet; this function is used when special application sensing tunnel feature is insufficient to allow an application to function correctly.

#### • Statistics of WAN Supported

Enables you to monitor inbound and outbound packets

#### Wireless functions

#### • High speed for wireless LAN connection

Up to 54Mbps data rate by incorporating Orthogonal Frequency Division Multiplexing (OFDM).

#### • Roaming

Provides seamless roaming within the IEEE 802.11b (11M) and IEEE 802.11g (54M) WLAN infrastructure.

#### • IEEE 802.11b compatible (11M)

Allowing inter-operation among multiple vendors.

• IEEE 802.11g compatible (54M)

Allowing inter-operation among multiple vendors.

#### • Auto fallback

54M, 48M, 36M, 24M, 18M, 12M, 6M data rate with auto fallback in 802.11g mode.

11M, 5.5M, 2M, 1M data rate with auto fallback in 802.11b mode.

#### **Security functions**

#### • Packet filter supported

**Packet Filter** allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.

#### • Domain Filter Supported

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

• URL Blocking Supported

URL Blocking can block hundreds of websites connection by simply a keyword.

• VPN Pass-through

The router also supports VPN pass-through.

• 802.1X supported

When the 802.1X function is enabled, the Wireless user must authenticate to this router first to use the Network service.

### • Support WPA-PSK and WPA version 1 and 2

When the WPA function is enabled, the Wireless user must authenticate to this router first to use the Network service

#### • SPI Mode Supported

When SPI Mode is enabled, the router will check every incoming packet to detect if this

packet is valid.

#### • DoS Attack Detection Supported

When this feature is enabled, the router will detect and log the DoS attack comes from the Internet.

### **Advanced functions**

#### • System time Supported

Allow you to synchronize system time with network time server.

• E-mail Alert Supported

The router can send its info by mail.

• Dynamic dns Supported

At present, the router has 3 ddns.dyndns, TZO.com and dhs.org.

#### • SNMP Supported

The router supports basic SNMP function.

#### • Routing Table Supported

Now, the router supports static routing.

#### • Schedule Rule supported

Customers can control some functions, like virtual server and packet filters when to access or when to block.

## **Other functions**

• UPNP (Universal Plug and Play)Supported

The router also supports this function. The applications: X-box, Msn Messenger.

#### **Packing List**

- Wireless broadband router unit
- Installation CD-ROM
- Power adapter
- CAT-5 UTP Fast Ethernet cable

## Chapter 2 Hardware Installation

## 2.1 Panel Layout

2.1.1. Front Panel

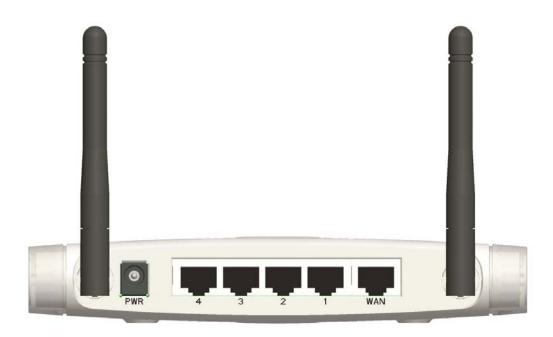


Figure 2-1 Front Panel

## LED: Ports:

Port	Description
PWR	Power inlet
WAN	the port where you will connect your cable (or DSL) modem or Ethernet router.
Port 1-4	the ports where you will connect networked computers and other devices.

#### 2.1.2. Rear Panel

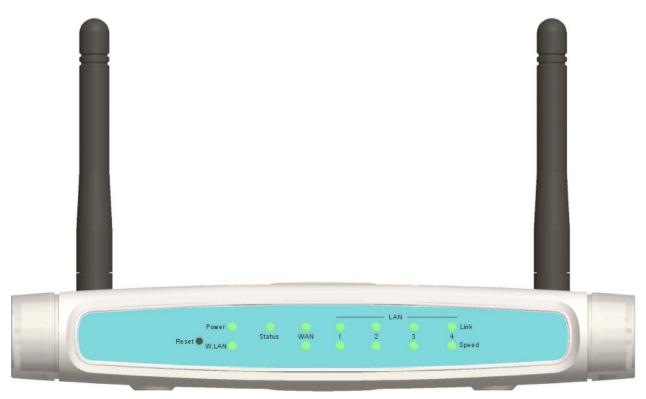


Figure 2-2 Rear Panel

## LED:

LED	Function	Color	Status	Description
Power	Power indication	Green	On	Power is being applied to this product.
Status	System status	Green	Blinking	Status is flashed once per second to indicate system is alive.
WAN	WAN port activity	Green	On	The WAN port is linked.
			Blinking	The WAN port is sending or receiving data.
WLAN	Wireless activity	Green	Blinking	Sending or receiving data via wireless
Link. 1~4	Link status	Green	On	An active station is connected to the corresponding LAN port.
Speed			Blinking	The corresponding LAN port is sending or receiving data.
10/100	Data Rate	Green	On	Data is transmitting in 100Mbps on the corresponding LAN port.
Reset				To reset system settings to factory defaults

#### **2.2 Procedure for Hardware Installation**

#### 2. Decide where to place your Wireless Broadband Router

You can place your Wireless Broadband Router on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your Wireless Broadband Router in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to power and network connection.

#### 2. Setup LAN connection

- **a.** Wired LAN connection: connects an Ethernet cable from your computer's Ethernet port to one of the LAN ports of this product.
- **b.** Wireless LAN connection: locate this product at a proper position to gain the best transmit performance.

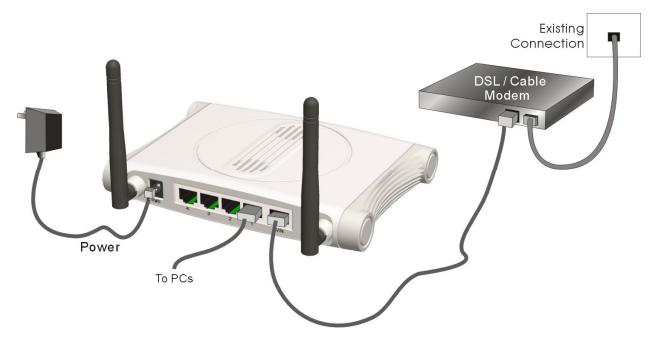


Figure 2-3 Setup of LAN and WAN connections for this product.

#### 3. Setup WAN connection

Prepare an Ethernet cable for connecting this product to your cable/xDSL modem or Ethernet backbone. Figure 2-3 illustrates the WAN connection.

#### 4. Power on

Connecting the power cord to power inlet and turning the power switch on, this product will automatically enter the self-test phase. When it is in the self-test phase, the indicators M1 will be lighted ON for about 10 seconds, and then M1 will be flashed 3 times to indicate that the self-test operation has finished. Finally, the M1 will be continuously flashed once per second to indicate that this product is in normal operation.

## Chapter 3 Network Settings and Software Installation

To use this product correctly, you have to properly configure the network settings of your computers and install the attached setup program into your MS Windows platform (Windows 95/98/NT/2000).

### 3.1 Make Correct Network Settings of Your Computer

The default IP address of this product is 192.168.123.254, and the default subnet mask is 255.255.255.0. These addresses can be changed on your need, but the default values are used in this manual. If the TCP/IP environment of your computer has not yet been configured, you can refer to **Appendix A** to configure it. For example,

- 1. configure IP as 192.168.123.1, subnet mask as 255.255.255.0 and gateway as 192.168.123.254, or more easier,
- 2. configure your computers to load TCP/IP setting automatically, that is, via DHCP server of this product.

After installing the TCP/IP communication protocol, you can use the **ping** command to check if your computer has successfully connected to this product. The following example shows the ping procedure for Windows 95 platforms. First, execute the **ping** command

#### ping 192.168.123.254

If the following messages appear:

Pinging 192.168.123.254 with 32 bytes of data:

#### Reply from 192.168.123.254: bytes=32 time=2ms TTL=64

a communication link between your computer and this product has been successfully established. Otherwise, if you get the following messages,

#### Pinging 192.168.123.254 with 32 bytes of data:

#### **Request timed out.**

There must be something wrong in your installation procedure. You have to check the following items in sequence:

1. Is the Ethernet cable correctly connected between this product and your computer?

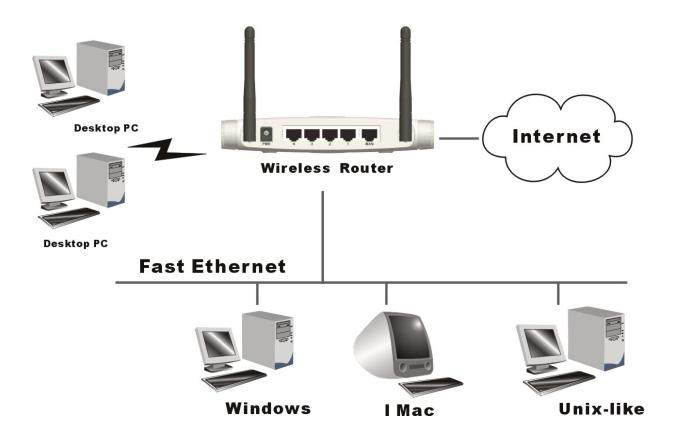
**Tip**: The LAN LED of this product and the link LED of network card on your computer must be lighted.

2. Is the TCP/IP environment of your computers properly configured?

**Tip**: If the IP address of this product is 192.168.123.254, the IP address of your computer must be 192.168.123.X and default gateway must be 192.168.123.254.

## Chapter 4 Configuring Wireless Broadband Router

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



## 4.1 Start-up and Log in

inistrator's Main Menu	System Status			
	Item	WAN Status	Sidenote	
	Remaining Lease Time	00:00:00	Renew	
	IP Address	0.0.0.0		
<u>s</u>	Subnet Mask	0.0.0.0		
	Gateway	0.0.0.0	Unreachable	
	Domain Name Server	0.0.0.0		
	Statistics of WAN	Inbound	Outbound	
	Octets	0	336	
	Unicast Packets	0	0	
	Non-unicast Packets	0	8	

Activate your browser, and **disable the proxy** or **add the IP address of this product into the exceptions**. Then, type this product's IP address in the Location (for Netscape) or Address (for IE) field and press ENTER. For example: http://192.168.123.254.

After the connection is established, you will see the web user interface of this product. There are two appearances of web user interface: for general users and for system administrator.

To log in as an administrator, enter the system password (the factory setting is "admin") in the **System Password** field and click on the **Log in** button. If the password is correct, the web appearance will be changed into administrator configure mode. As listed in its main menu, there are several options for system administration.

## 4.2 Status

Administrator's Main Menu	System Status			
Status	Item	WAN Status	Sidenote	
Wizard	Remaining Lease Time	00:00:00	Renew	
+ Basic Setting	IP Address	0.0.0.0		
+ Forwarding Rules	Subnet Mask	0.0.0.0		
Security Setting	Gateway	0.0.0.0	Unreachable	
Advanced Setting	Domain Name Server	0.0.0.0		
- <u>Toolbox</u>	Circle Calle ST	<b>T</b> , ,	0.4 1	
	Statistics of WAN	Inbound	Outbound	
Log out	Octets	0	336	
	Unicast Packets	0	0	
	Non-unicast Packets	0	8	
	View Log Clients List Device Time: Wed Sep 01 00:01:31	Help Refresh 2004		

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

A. WAN Port Status.

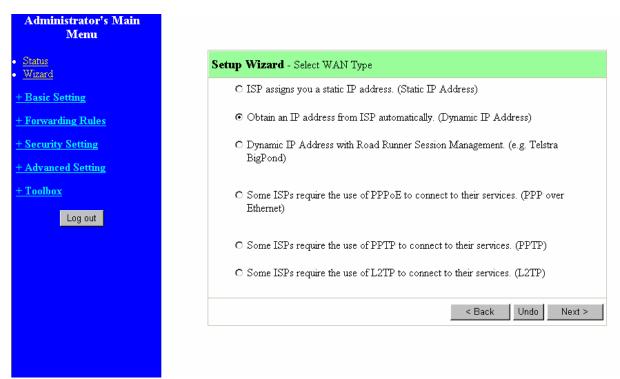
If the WAN port is assigned a dynamic IP, there may appear a "**Renew**" or "**Release**" button on the Sidenote column. You can click this button to renew or release IP manually.

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

## 4.3 Wizard



Setup Wizard will guide you through a basic configuration procedure step by step.Press "Next >"



Setup Wizard - Select WAN Type: For detail settings, please refer to 4.4.1 primary setup.

## 4.4 Basic Setting

	Basic Setting
1	
Setting	<ul> <li>Primary Setup         <ul> <li>Configure LAN IP, and select WAN type.</li> </ul> </li> </ul>
ling Rules	DHCP Server
7 Setting	- The settings include Host IP, Subnet Mask, Gateway, DNS, and WINS configurations.
d Setting	• Wireless
	- Wireless settings allow you to configure the wireless configuration items.
	Change Password
.og out	- Allow you to change system password.

## 4.4.1 Primary Setup – WAN Type, Virtual Computers

Administrator's Main Menu		Primary Setup
<u>Status</u>	Item	Setting
<u>Wizard</u>	▶ LAN IP Address	192.168.123.254
Basic Setting	▶ WAN Type	Dynamic IP Address Change
Primary Setup	▶ Host Name	(optional)
DHCP Server Wireless	▶ WAN's MAC Address	00-50-29-22-3A-AC Restore MAC
Change Password	▶ Renew IP Forever	□ Enable (Auto-reconnect)
Forwarding Rules	Save Undo Virtual Computers	Help
Security Setting		
Advanced Setting		
<u>Toolbox</u>		
Log out		

#### Press "Change"

Administrator's Main Menu	Choose WAN Type			
• <u>Status</u>		Туре	Usage	
• <u>Wizard</u>	0	Static IP Address	ISP assigns you a static IP address.	
- Basic Setting	o	Dynamic IP Address	Obtain an IP address from ISP automatically.	
<ul> <li>Primary Setup</li> </ul>	0	Dynamic IP Address with Road Runner	Session Management (e.g. Telstra BigPond)	
<ul> <li><u>DHCP Server</u></li> <li>Change Password</li> </ul>	0	PPP over Ethernet	Some ISPs require the use of PPPoE to connect to their services.	
+ Forwarding Rules	0	PPTP	Some ISPs require the use of PPTP to connect to their services.	
+ Security Setting	0	L2TP	Some ISPs require the use of L2TP to connect to their services.	
<u>+ Advanced Setting</u> <u>+ Toolbox</u>	Save	Cancel		
Log out				

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.
- 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. Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond)
  - D. PPP over Ethernet: Some ISPs require the use of PPPoE to connect to their services.
  - E. 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

#### 4.4.1.1 Static IP Address

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

#### 4.4.1.2 Dynamic IP Address

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

2. 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.

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

- 1. LAN IP Address is the IP address of this product. It must be the default gateway of your computers.
- 2. WAN Type is Dynamic IP Address. If the WAN type is not correct, change it!
- 3. Host Name: optional. Required by some ISPs, e.g. @Home.
- 4. Renew IP Forever: this feature enable this product renew IP address automatically when the lease time is being expired even the system is in idle state.

#### 4.4.1.4 PPP over Ethernet

- 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.
- 4. **Maximum Transmission Unit (MTU)**: Most ISP offers MTU value to users. The most common MTU value is 1492.
- 5. 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 upw with ISP until the connection is established.

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

#### 4.4.1.5 PPTP

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

- 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.
- 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.
- 5. 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 upw with ISP until the connection is established.

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

Administrator's Main Menu		Primary Setup
	Item	Setting
Status	▶ LAN IP Address	192.168.123.254
Wizard	▶ WAN Type	PPTPChange
Basic Setting	▶ IP Mode	Static IP Address
• <u>Primary Setup</u>	▶ My IP Address	Dynamic IP Address Static IP Address
• <u>DHCP Server</u>	▶ My Subnet Mask	255.255.255.0
<ul> <li><u>Wireless</u></li> <li>Change Password</li> </ul>	▶ Gateway IP	0.0.0.0
	▶ Server IP Address/Name	
• Forwarding Rules	▶ PPTP Account	
Security Setting	▶ PPTP Password	
Advanced Setting	Connection ID	(optional)
	Maximum Idle Time	600 seconds
Toolbox Log out	Connection Control	Connect-on-demand
	▶ MTU	1460
	Save Undo Help Reboot	

#### 4.4.1.6 L2TP

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.
- 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.

6. 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 upw with ISP until the connection is established.

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

Staus-page.

Administrator's Main Menu		Primary Setup
• <u>Status</u>	Item	Setting
• <u>Wizard</u>	LAN IP Address	192.168.122.237
- Basic Setting	▶ WAN Type	L2TP Change
Primary Setup	▶ IP Mode	Static IP Address
<ul> <li><u>DHCP Server</u></li> <li>Change Password</li> </ul>	▶ IP Address	10.0.0.100
	Subnet Mask	255.255.255.0
+ Forwarding Rules	▶ WAN Gateway IP	10.0.0.1
+ Security Setting	▶ Server IP Address/Name	
+ Advanced Setting	L2TP Account	
<u>+ Toolbox</u>	▶ L2TP Password	
	Maximum Idle Time	600 seconds
Log out	Connection Control	Connect-on-demand
	Save Undo Help Reboot Saved! The change doesn't take effective unt	il rebooting!

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

Administrator's Main Menu		Virtua	l Computers	
• <u>Status</u>	ID	Global IP	Local IP	Enable
• <u>Wizard</u>	1		192.168.123.	
- Basic Setting	2		192.168.123.	
<ul> <li><u>Primary Setup</u></li> <li><u>DHCP Server</u></li> </ul>	3		192.168.123.	
• <u>Wireless</u>	4		192.168.123.	
<u>Change Password</u>	5		192.168.123.	
+ Forwarding Rules + Security Setting + Advanced Setting + Toolbox Log out	Save Und	o Help		

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.

## 4.4.2 DHCP Server

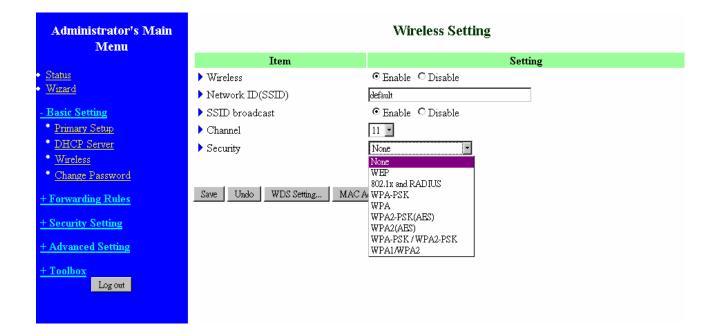
Administrator's Main Menu		DHCP Server
<u>Status</u>	Item	Setting
<u>Wizard</u>	DHCP Server	O Disable 💿 Enable
- Basic Setting	▶ IP Pool Starting Address	100
<ul> <li>Primary Setup</li> </ul>	▶ IP Pool Ending Address	199
<ul> <li><u>DHCP Server</u></li> <li>Wireless</li> </ul>	▶ Domain Name	
Change Password	<ul> <li>Primary DNS</li> </ul>	0.0.0.0
+ Forwarding Rules	Secondary DNS	0.0.0.0
	Primary WINS	0.0.0.0
<u>+ Security Setting</u>	Secondary WINS	0.0.0.0
<u>+ Advanced Setting</u>	▶ Gateway	0.0.0.0 (optional)
<u>+ Toolbox</u> Log out	Save Undo Clients List	Fixed Mapping Help

#### Press "More>>"

The settings of a TCP/IP environment include host IP, Subnet Mask, Gateway, and DNS configurations. It is not easy to manually configure all the computers and devices in your network. Fortunately, DHCP Server provides a rather simple approach to handle all these settings. This product supports the function of DHCP server. If you enable this product's DHCP server and configure your computers as "automatic IP allocation" mode, then when your computer is powered on, it will automatically load the proper TCP/IP settings from this product. The settings of DHCP server include the following items:

- 1. **DHCP Server**: Choose "Disable" or "Enable."
- 2. **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.
- 3. **Domain Name**: Optional, this information will be passed to the client.
- 4. **Primary DNS/Secondary DNS**: This feature allows you to assign DNS Servers
- 5. Primary WINS/Secondary WINS: This feature allows you to assign WINS Servers
- 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.

## 4.4.3 Wireless Setting, 802.1X setting and WDS



Wireless settings allow you to set the wireless configuration items.

Wireless : The user can enable or disalbe 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. The factory setting is as follow: channel 6 for North America; channel 7 for European (ETSI); channel 7 for Japan.

**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.

Administrator's Main Menu	Wireless Setting			
	Item	Setting		
• <u>Status</u>	▶ Wireless	⊙ Enable ⊂ Disable		
• <u>Wizard</u>	▶ Network ID(SSID)	default		
- Basic Setting	▶ SSID broadcast	⊙ Enable ○ Disable		
<ul> <li><u>Primary Setup</u></li> </ul>	▶ Channel	11 💌		
• <u>DHCP Server</u>	Security	802.1x and RADIUS		
• <u>Wireless</u>				
<u>Change Password</u> <u>+ Forwarding Rules</u>	Encryption Key Length	© 64 bits € 128 bits		
+ Security Setting	RADIUS Server IP	192.168.123.33		
<u>+ security setting</u>	RADIUS port	1812		
+ Advanced Setting	RADIUS Shared Key			
+ Toolbox Log out	Save Undo WDS Setting MAC A	Address Control Help		

#### 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

Administrator's Main Menu	Wireless Setting			
	Item	Setting		
Status	Wireless	⊙ Enable ⊂ Disable		
• <u>Wizard</u>	▶ Network ID(SSID)	default		
- Basic Setting	▶ SSID broadcast	⊙ Enable ⊂ Disable		
<ul> <li>Primary Setup</li> </ul>	Channel	11 -		
<ul> <li><u>DHCP Server</u></li> </ul>	Security	WPA-PSK -		
• Wireless				
<u>Change Password</u>	Encryption	© TKIP CAES		
+ Forwarding Rules	▶ Preshare Key Mode	ASCII 🔽		
+ Security Setting	▶ Preshare Key			
+ Advanced Setting	Save Undo WDS Setting MAC	Address Control Help		
+ Toolbox Log out				

### 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.

Administrator's Main Menu	Wireless Setting			
	Item	Setting		
<u>Status</u>	Wireless	$\odot$ Enable $\odot$ Disable		
• <u>Wizard</u>	▶ Network ID(SSID)	default		
- Basic Setting	▶ SSID broadcast	© Enable O Disable		
<ul> <li>Primary Setup</li> </ul>	▶ Channel	11 •		
<ul> <li><u>DHCP Server</u></li> <li>Wireless</li> </ul>	Security	WPA		
<u>Change Password</u>	• Encryption	© TKIP CAES		
<u>+ Forwarding Rules</u>	▶ RADIUS Server IP	192.168.123.33		
+ Security Setting	RADIUS port	1812		
+ Advanced Setting	▶ RADIUS Shared Key	1234		
<u>+ Toolbox</u>	Save Undo WDS Setting MAC	Address Control Help		

### 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

Administrator's Main Menu		Wireless Setting	
Status	Item	Setting	
Wizard	▶ Wireless	• Enable C Disable	
- Basic Setting	▶ Network ID(SSID)	default	
Primary Setup	▶ SSID broadcast	• Enable C Disable	
• <u>DHCP Server</u>	▶ Channel	11 💌	
• <u>Wireless</u>	Security	WPA2-PSK(AES)	
<ul> <li><u>Change Password</u></li> </ul>		22 - 22/27	
+ Forwarding Rules	Preshare Key Mode	ASCII 💌	
+ Security Setting	▶ Preshare Key		
+ Advanced Setting	Save Undo WDS Setting M	AC Address Control Help	
+ Toolbox Log out			

### 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.

Administrator's Main Menu		Wireless Setting	
<u>Status</u>	Item	Setting	
• <u>Wizard</u>	▶ Wireless	⊙ Enable ○ Disable	
- Basic Setting	▶ Network ID(SSID)	default	
Primary Setup	▶ SSID broadcast	⊙ Enable ○ Disable	
• <u>DHCP Server</u>	▶ Channel	11 💌	
<u>Wireless</u> <u>Change Password</u>	> Security	WPA2(AES)	
+ Forwarding Rules	▶ RADIUS Server IP	0.0.0.0	
<u>+ Security Setting</u> + Advanced Setting	<ul> <li>RADIUS port</li> <li>RADIUS Shared Key</li> </ul>	1812	
+ Toolbox Log out	Save Undo WDS Setting	MAC Address Control Help	

### WPA-PSK /WPA2-PSK

The router will detect automatically which Security type(Wpa-psk version 1 or 2) 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

Administrator's Main Menu	Wireless Setting			
• <u>Status</u>	Item	Setting		
• <u>Wizard</u>	▶ Wireless	⊙ Enable C Disable		
- Basic Setting	▶ Network ID(SSID)	default		
Primary Setup	▶ SSID broadcast	⊙ Enable O Disable		
• <u>DHCP Server</u>	▶ Channel	11 -		
<u>Wireless</u> <u>Change Password</u>	Security	WPA-PSK/WPA2-PSK		
+ Forwarding Rules	▶ Preshare Key Mode	ASCII 💌		
+ Security Setting	▶ Preshare Key			
+ Advanced Setting	Save Undo WDS Setting MAC	C Address Control Help		
+ Toolbox Log out				

#### 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.

Administrator's Main Menu	Wireless Setting			
• <u>Status</u>	Item	Setting		
• <u>Wizard</u>	Wireless	⊙ Enable ⊂ Disable		
- Basic Setting	▶ Network ID(SSID)	default		
Primary Setup	▶ SSID broadcast	€ Enable C Disable		
• <u>DHCP Server</u>	Channel	11 -		
• <u>Wireless</u>	Security	WPA1/WPA2		
<ul> <li><u>Change Password</u></li> </ul>	i.			
+ Forwarding Rules	▶ RADIUS Server IP	0.0.0		
+ Security Setting	RADIUS port	1812		
	RADIUS Shared Key			
<u>+ Advanced Setting</u>				
+ Toolbox	Save Undo WDS Setting	MAC Address Control Help		
Logout				

#### 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.

## 4.4.4 Change Password

Administrator's Main Menu	Change Password			
• <u>Status</u>	Item		Setting	
• <u>Wizard</u>	Old Password		-	
- Basic Setting	New Password			
<ul> <li><u>Primary Setup</u></li> <li><u>DHCP Server</u></li> </ul>	Reconfirm			
<u>Wireless</u> <u>Change Password</u>	Save Undo			
+ Forwarding Rules				
<u>+ Security Setting</u>				
+ Advanced Setting				
<u>+ Toolbox</u>				
Log out				

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

## **4.5 Forwarding Rules**

Forwarding Rules
A 17 - 16
• 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
<ul> <li>IP Address of DMZ Host: Atlows a computer to be exposed to unrestricted 2-wa communication. Note that, this feature should be used only when needed.</li> </ul>
- 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).

## 4.5.1 Virtual Server

Administrator's Main Menu			Virtual Server		
<u>Status</u>	ID	Service Ports	Server IP	Enable	Use Rule
• <u>Wizard</u>	1		192.168.123.		0
<u>+ Basic Setting</u>	2		192.168.123.		0
- Forwarding Rules	3		192.168.123.		0
Virtual Server	4		192.168.123.		0
<u>Special AP</u>	5		192.168.123.		0
• <u>Miscellaneous</u>	6		192.168.123.		0
<u>+ Security Setting</u>	7		192.168.123.		0
<u>+ Advanced Setting</u>	8		192.168.123.		0
<u>+ Toolbox</u>	9		192.168.123.		0
Log out	10		192.168.123.		0
	11		192.168.123.		0
	12		192.168.123.		0
	13		192.168.123.		0
	14		192.168.123.		0
	15		192.168.123.		0

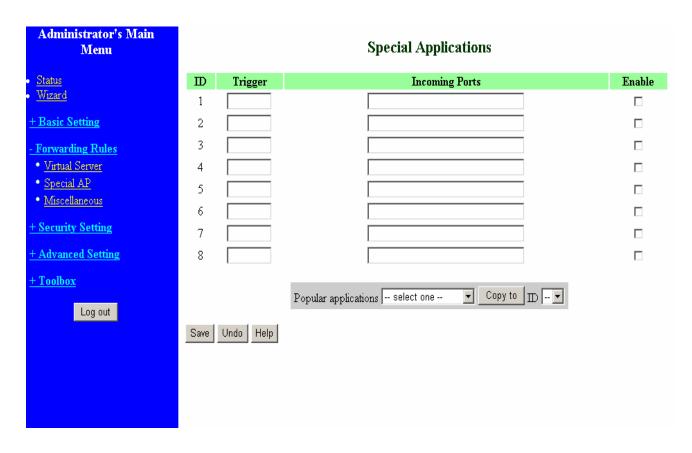
This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

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**.

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

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

## 4.5.2 Special AP



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

- 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.

## 4.5.3 Miscellaneous Items

Administrator's Main Menu	Miscellaneous Items				
	Item	Setting	Enable		
Status	▶ IP Address of DMZ Host	192.168.122.			
Wizard	▶ Non-standard FTP port	0			
+ Basic Setting	▶ UPnP setting				
- Forwarding Rules • <u>Virtual Server</u>	Save Undo Help				
<ul> <li>Special AP</li> </ul>					
• <u>Miscellaneous</u>					
+ Security Setting					
+ Advanced Setting					
+ Toolbox Log out					

#### **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.

## **UpnP Setting**

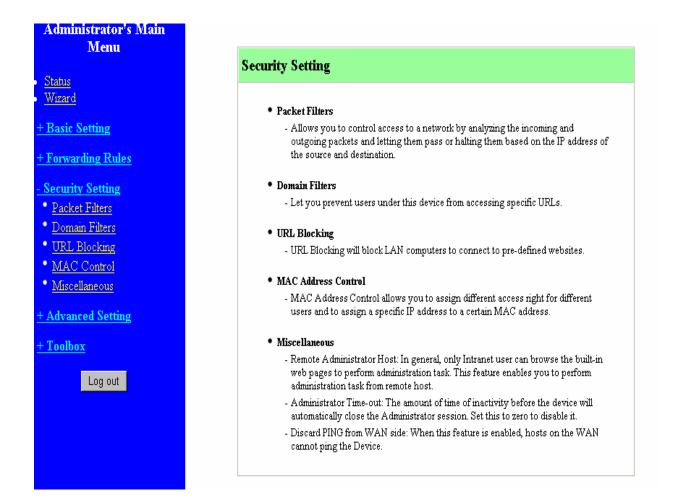
The device also supports this function. If the OS supports this function enable it, like Windows

Xp.When the user get ip from Device and will see icon as below:





## 4.6 Security Settings



## 4.6.1 Packet Filter

Administrator's Main Menu	Outbound Packet Filter								
		Item			Setting				
Status	🕨 Outba	▶ Outbound Filter			🗆 Enable				
<u>Wizard</u>		$\odot$ Allow all to pass except those match the following rules.							
+ Basic Setting	<sup>O</sup> Deny all to pass except those match the following rules.								
+ Forwarding Rules	D	Source IP :	Ports	Desti	nation IP : Ports	Enable	Use Rule#		
- Security Setting	1		:		:		0		
Packet Filters	2		:		:		0		
• Domain Filters	3		:		:		0		
URL Blocking	4				:		0		
• <u>MAC Control</u>	5						0		
• <u>Miscellaneous</u>	6						0		
+ Advanced Setting	7						0		
+ Toolbox	8				·				
Log out	Ů			I		-	•		
			Schedule rule	(00)Always 💌	Copy to ID 💌				

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	Outbound Packet Filter							
<u>Status</u>		Item			Setting			
<u>Wizard</u>	▶ Outbound Filter				🗹 Enable			
+ Basic Setting	C Allow all to pass except those match the following rules.							
+ Forwarding Rules		© Deny all to pass ex	xcept those mate	h the follow	wing rules.			
- Security Setting	ID	Source IP :	Ports	De	stination IP : Ports	Enable	Use Rule#	
<ul> <li>Packet Filters</li> </ul>	1	1.2.3.100-1.2.3.149	:		: 25-100		0	
<ul> <li><u>Domain Filters</u></li> </ul>	2	1.2.3.10-1.2.3.20	:		:	•	0	
• URL Blocking	3		:		:		0	
<u>MAC Control</u> <u>Miscellaneous</u>	4				:		0	
	5						0	
+ Advanced Setting	6	·					0	
<u>+ Toolbox</u>	7							
	8	[						
Log out	0				:		μ	
			ŗ					
			Schedule rule	(UU)Always	▼ Copy to ID ▼			
	Save	Undo Inbound Fi	ilter MA	C Level	Help			

(1.2.3.100-1.2.3.149) They are allow to send mail (port 25), receive mail (port 110), and browse the Internet (port 80)

(1.2.3.10-1.2.3.20) They can do everything (block nothing)

Others are all blocked.

#### Example 2:

+ Basic Setting + Forwarding Rules - Security Setting Deceter Filters Domain Filters URL Blocking MAC Control Miscellaneous Deceter Setting 4	Item			Outbound Packet Filter						
+ Basic Setting + Forwarding Rules - Security Setting ID • Packet Filters 1 • Domain Filters 2 • URL Blocking 3 • MAC Control 4			Sett	Setting						
+ Forwarding Rules - Security Setting ID • Packet Filters 1 • Domain Filters 2 • URL Blocking 3 • MAC Control 4	utbound Filter	🗹 Enable								
Security Setting     ID       • Packet Filters     1       • Domain Filters     2       • URL Blocking     3       • MAC Control     4	C Allow all to pass except those match the following rules.									
Packet Filters     1     Domain Filters     2     URL Blocking     3     MAC Control     Miscellaneous	© Deny all to pass except those match the following rules.									
Domain Filters 2     URL Blocking 3     MAC Control 4	Source IP : Ports	Des	stination IP : Ports	Enable	Use Rule#					
• URL Blocking 3 • MAC Control • Miscellaneous 4	1.2.3.100-1.2.3.119		: 21	V	0					
<u>MAC Control</u> <u>Miscellaneous</u>	1.2.3.100-1.2.3.119		: 119	V	0					
• Miscellaneous 4	:		:		0					
			:		0					
+ Advanced Setting			:		0					
6	:		:		0					
+ Toolbox 7	:		:		0					
Log out 8	:		:		0					
Save	Schedule rule	(00)Always] C Level	▼ Copy to ID ▼							

(1.2.3.100-1.2.3.119) They can do everything except read net news (port 119) and transfer files via FTP (port 21)

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.

# **Outbound Packet Filter**

	Item		Setting			
Out	bound Filter		🗹 Enable			
	• Allow all to pass except th O Deny all to pass except th	-				
ID	Source IP : Port	s D	estination IP : Ports	Enable	Use Rule#	
1	192.168.123.149 :		: 25-110		0	
2	192.168.123.20 :		:		0	
3	:		:		0	
4	:		:		0	
5	:		:		0	
6	:		:		0	
7	:		:		0	
8	:		:		0	
		chedule rule (00)Always				
Save	Undo Inbound Filter	MAC Level He	lp			

(192.168.123.100-192.168.123.149) They are 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.

(192.168.123.10-192.168.123.20) They can do everything (block nothing)

Others are all blocked.

## Example 2:

# **Outbound Packet Filter**

Item	Setting
Outbound Filter	🗹 Enable

• Allow all to pass except those match the following rules.

 $\mathbb C$  Deny all to pass except those match the following rules.

ID	Source IP : Ports	Destination IP : Ports	Enable	Use Rule#
1	192.168.123.100 :	: 25		0
2	192.168.123.119 :	: 119		0
3	:			0
4	:			0
5	:			0
6	:			0
7	:			0
8	:			0
		e rule (00)Always 💌 Copy to ID 💌		
Save	Undo Inbound Filter M	AC Level Help		

(192.168.123.100-192.168.123.119) They 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.

## 4.6.2 Domain Filter

Administrator's Main Menu	Domain Filter					
• <u>Status</u>		Item		Setting		
• <u>Wizard</u>	▶ Doma	in Filter	🗹 Enable			
+ Basic Setting	🕨 Log D	NS Query	🗹 Enable			
+ Forwarding Rules	Privile	ge IP Addresses Range	From 1 To 20			
- Security Setting	ID	Domain Suffix		Action	Enable	
• <u>Packet Filters</u>	1	www.msn.com		□Drop □Log		
Domain Filters	2			□Drop □Log		
<ul> <li><u>URL Blocking</u></li> <li>MAC Control</li> </ul>	3			🗆 Drop 🗖 Log		
• Miscellaneous	4			□Drop □Log		
+ Advanced Setting	5			□Drop □Log		
+ Toolbox	6			🗆 Drop 🗖 Log		
	7			□Drop □Log		
Log out	8			□Drop □Log		
	9			□Drop □Log		
	10	* (all others)		□Drop □Log	-	
	Save	Undo Help				

#### **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.

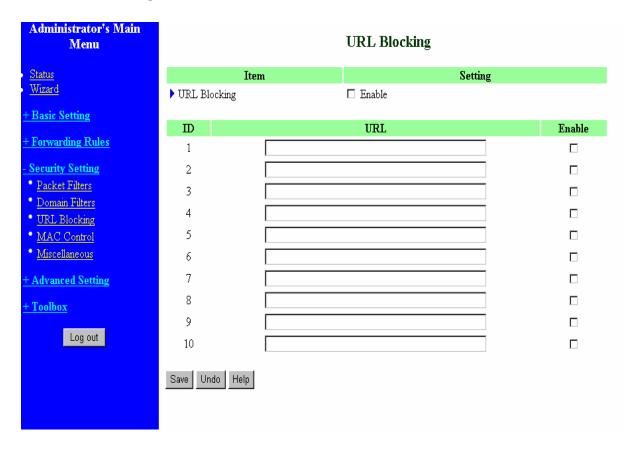
#### Example:

Administrator's Main Menu	Domain Filter					
<u>Status</u>		Item		Setting		
• <u>Wizard</u>	▶ Doma	in Filter	🗹 Enable			
+ Basic Setting	🕨 Log D	NS Query	🗹 Enable			
<u>+ Forwarding Rules</u>	Privile,	ge IP Addresses Range	From 1 To 20			
- Security Setting	ID	Domain Suffix		Action	Enable	
Packet Filters	1	www.msn.com		🗹 Drop 🔽 Log		
• Domain Filters	2	www.sina.com		🗖 Drop 🗹 Log		
<u>URL Blocking</u> <u>MAC Control</u>	3	www.google.com		🗹 Drop 🗖 Log		
• Miscellaneous	4			□Drop □Log		
+ Advanced Setting	5			□Drop □Log		
+ Toolbox	6			□Drop □Log		
<u> </u>	7			□Drop □Log		
Log out	8			□Drop □Log		
	9			🗆 Drop 🗖 Log		
	10	* (all others)		□Drop □Log	-	
	Save	Jndo Help				

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.google.com" will be blocked, but the action will not be record in log-file.
- 4. IP address X.X.X.1~ X.X.X.20 can access network without restriction.

## 4.6.3 URL Blocking



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			URL Blocking	5	
Status		Item		Setting	
Wizard	VRL Bloc	king	🗹 Enable		
<u>+ Basic Setting</u>	TD		1001		T 11
+ Forwarding Rules	ID 1		URL		Enable
	1	msn			
- Security Setting	2	sina			
Packet Filters	3	cnnsi			
<ul> <li><u>Domain Filters</u></li> <li><u>URL Blocking</u></li> </ul>	4	espn			
<u>MAC Control</u>	5				
• <u>Miscellaneous</u>	6				
+ Advanced Setting	7				
<u>+ Toolbox</u>	8				
	9				
Log out	10				
	Save Undo	Help			

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. URL include "cnnsi" will not be blocked, but the action will be record in log-file.

4. URL include "espn" will be blocked, but the action will be record in log-file

#### 4.6.4 MAC Address Control

Administrator's Main Menu	MAC Address Control					
Status		Item		Setting		
<u>Wizard</u>	MA	C Address Control	🗆 Enable			
+ Basic Setting	□Ca	onnection control	Wireless and wired clie	nts with ${f C}$ checked can connect to this de	vice; and	
+ Forwarding Rules			allow 🔽 unspecified M	AC addresses to connect.		
- Security Setting Packet Filters	□ As	sociation control	Wireless clients with A unspecified MAC addre	checked can associate to the wireless LA esses to associate.	N; and de	eny 💌
• <u>Domain Filters</u>	ID	MAC	Address	IP Address	С	Α
URL Blocking	1			192.168.123.		
<ul> <li><u>MAC Control</u></li> <li>Miscellaneous</li> </ul>	2			192.168.123.		
	3			192.168.123.		
+ Advanced Setting	4			192.168.123.		
<u>+ Toolbox</u>		-				
Log out			DHCP clients selec	t one 💌 Copy to 🔟 💌		
	<< Previous Next >> Save Undo Help					

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.

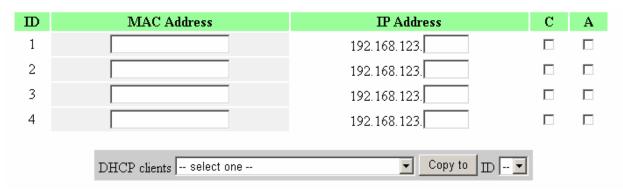
MAC Address Control Check "Enable" to enable the "MAC Address Control". All of the settings in this page will take effect only when "Enable" is checked.

**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**



"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.			
<b>IP Address</b>	Expected IP address of the corresponding			
	client. Keep it empty if you don't care its IP			
	address.			
С	When "Connection control" is checked,			
	check "C" will allow the corresponding client			
	to connect to this device.			
Α	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.

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:**

	Item		Setting		
MA	C Address Control	💌 Enable			
✓ Connection control		Wireless and wired clients with C checked can connect to this device; and allow 🔽 unspecified MAC addresses to connect.			
🗹 As:	sociation control		A checked can associate to the wireless L MAC addresses to associate.	AN; and	
_					
ID	MAC	Address	IP Address	С	Α
<b>ID</b> 1	MAC 00-12-34-5		IP Address 192.168.123.100	C	A
<b>ID</b> 1 2		6-78-90		-	
1	00-12-34-5	i6-78-90 i6-78-92	192.168.123.100		•

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" --> 192.168.123.100

ID 3 - "00-98-76-54-32-10" --> 192.168.123.101

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 (192.168.123.101), 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.

#### 4.6.5 Miscellaneous Items



#### **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.

# 4.7 Advanced Settings

Advanced Setting  • System Time  - Allow you to set device time manually or consult network time from NTP server.  • System Log
- Allow you to set device time manually or consult network time from NTP server.
- Allow you to set device time manually or consult network time from NTP server.
System Log
- Send system log to a dedicated host or email to specific receipts.
• Dynamic DNS
<ul> <li>To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).</li> </ul>
• SNMP
<ul> <li>Gives a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.</li> </ul>
• Routing
<ul> <li>If you have more than one routers and subnets, you may want to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.</li> </ul>
Schedule Rule
<ul> <li>Schedule Rule - Apply schedule rules to Packet Filters and Virtual Server.</li> </ul>

# 4.7.1 System Time

Administrator's Main Menu		Syst	em Time	
<u>Status</u>	Item		Setting	
• <u>Wizard</u>	▶ ○ Get Date and Time	by NTP Protocol 📃 S	ync Now !	
+ Basic Setting	Time Server	time.nist.gov 💌	]	
+ Forwarding Rules	Time Zone	(GMT-08:00) Pacific Ti	me (US & Canada)	•
+ Security Setting	▶ ○ Set Date and Time	using PC's Date and Tir	ne	
- Advanced Setting	PC Date and Time:	2004年10月15日下午0	7:27:10	
<ul> <li><u>System Time</u></li> </ul>				
<ul> <li>System Log</li> </ul>	🕨 💿 Set Date and Time	manually		
• <u>Dynamic DNS</u>	Date	Year: 2004 💌	Month: Sep 💌	Day: 1 💽
• <u>SNMP</u>	Time	Hour: 0 (0-23)	Minute: 0 (0-59)	Second:0 (0-59)
<ul> <li><u>Routing</u></li> <li>Schedule Rule</li> </ul>				
Schedule Kule	Daylight Saving	O Enable 💿 Disab	le	
<u>+ Toolbox</u>	Start	Month : Jan 💌	Day : 1 💽	Hour: 0 💌
Log out	End	Month : Jan 💌	Day : 1 💌	Hour: 0 💌
	Save Undo Help			

#### 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.

# 4.7.2 System Log

Administrator's Main Menu	s	ystem Log	
<u>Status</u>	Item	Setting	Enable
• <u>Wizard</u>	▶ IP Address for Syslogd	192.168.123.	
+ Basic Setting	▶ IP Address of Outgoing Mail Server		
+ Forwarding Rules	• Log or Alert Recipient		
<u>+ Security Setting</u>	View Log Save Undo Help		
- Advanced Setting			
<ul> <li><u>System Time</u></li> </ul>			
System Log			
Dynamic DNS			
• <u>SNMP</u> • Deuting			
<ul> <li><u>Routing</u></li> <li><u>Schedule Rule</u></li> </ul>			
<u>+ Toolbox</u>			
Log out			

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 concated 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.

# 4.7.3 Dynamic DNS

Administrator's Main Menu		Dynamic DNS
<u>Status</u>	Item	Setting
<u>Wizard</u>	DDNS	C Disable 💿 Enable
+ Basic Setting	▶ Provider	DynDNS.org(Dynamic)
+ Forwarding Rules	▶ Host Name	kink. dyndns. org
	▶ Username / E-mail	12345
<u>+ Security Setting</u>	▶ Password / Key	****
<ul> <li><u>Advanced Setting</u></li> <li><u>System Time</u></li> <li><u>System Log</u></li> <li><u>Dynamic DNS</u></li> <li><u>SNMP</u></li> <li><u>Routing</u></li> <li><u>Schedule Rule</u></li> <li><u>Log out</u></li> </ul>	Save Undo Help	

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.

#### **Example:**

Administrator's Main Menu		Dynamic DNS
<u>Status</u>	Item	Setting
Wizard	▶ DDNS	O Disable 💿 Enable
+ Basic Setting	▶ Provider	DynDNS.org(Dynamic) 💌
+ Forwarding Rules	▶ Host Name	kink.dyndns.org
	▶ Username / E-mail	12345
+ Security Setting	▶ Password / Key	*****
- Advanced Setting		
• <u>System Time</u>	Save Undo Help	
• <u>System Log</u> • <u>Dynamic DNS</u>		
SNMP		
Routing		
Schedule Rule		
+ Toolbox		
Log out		

After Dynamic DNS setting is configured, click the save button.

## 4.7.4 SNMP Setting

Administrator's Main Menu	SNMP Setting			
	Item		Setting	
Status	▶ Enable SNMP	🗹 Local 🗖 Remote		
• <u>Wizard</u>	▶ Get Community	public		
+ Basic Setting	▶ Set Community	private		
<u>+ Forwarding Rules</u>	▶ WAN Access IP Address	0.0.0.0		
+ Security Setting	Save Undo Help			
- Advanced Setting				

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 either Local or 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.

#### WAN Access IP Address

IF the user wants to limit to specific the ip address to access, please input in the item. The default 0.0.0.0 and means every ip of Internet can get some information of device with snmp protocol.

## 4.7.5 Routing

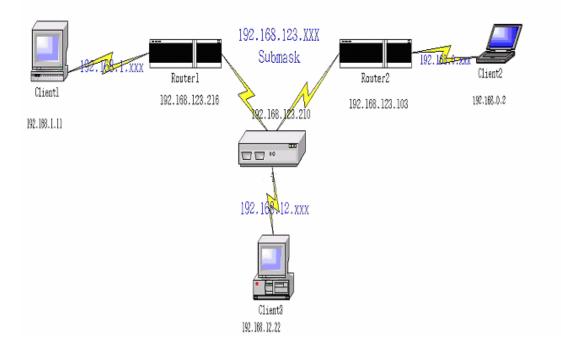
Administrator's Main Menu			Routing <b>T</b>	able		
Status	ID	Destination	Subnet Mask	Gateway	Hop	Enable
Wizard	1					
+ Basic Setting	2					
+ Forwarding Rules	3					
+ Security Setting	4					
- Advanced Setting	5					
System Time	6					
• System Log	7					
• <u>Dynamic DNS</u>	8					
• <u>SNMP</u>						
<ul> <li><u>Routing</u></li> <li><u>Schedule Rule</u></li> </ul>	Save	Undo Help				
<u>+ Toolbox</u>						

**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.

**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 unchecking the Enable checkbox.

#### **Example:**



Configuration on NAT Router

Destination	SubnetMask	Gateway	Нор	Enabled
192.168.1.0	255.255.255.0	192.168.123.216	1	V
192.168.0.0	255.255.255.0	192.168.123.103	1	V

So if, for example, the client3 wanted to send an IP data gram to 192.168.0.2, it would use the above table to determine that it had to go via 192.168.123.103 (a gateway),

And if it sends Packets to 192.168.1.11 will go via 192.168.123.216

Each rule can be enabled or disabled individually.

After **routing table** setting is configured, click the **save** button.

# 4.7.6 Schedule Rule

Administrator's Main Menu		Schedule Rule		
• <u>Status</u>	Item		Setting	
• <u>Wizard</u>	▶ Schedule	🔽 Enable		
+Basic Setting	Rule#	Rule Name		Action
<u>+ Forwarding Rules</u> <u>+ Security Setting</u>	Save Add New Rule	Help		
- Advanced Setting  • System Time				
• <u>System Log</u> • <u>Dynamic DNS</u>				
• <u>SNMP</u> • <u>Routing</u> • <u>Schedule Rule</u>				
+ Toolbox				
Log out				

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

Administrator's Main Menu	Schedule Rule Setting			
• <u>Status</u>	Item		Setting	
• <u>Wizard</u>	▶ Name of Rule 1	ftp time		
<u>+ Basic Setting</u>				
+ Forwarding Rules	Week Day	Start Time (hh:mm)	End Time (hh:mm)	
	Sunday			
<u>+ Security Setting</u>	Monday			
- Advanced Setting	Tuesday			
• <u>System Time</u>	Wednesday	:	:	
• <u>System Log</u> • Dynamic DNS	Thursday		:	
• <u>SNMP</u>	Friday			
• <u>Routing</u>	Saturday			
• <u>Schedule Rule</u>	Every Day	14 : 10	16 : 20	
+ Toolbox Log out	Save Undo Help Back			

#### After configure Rule $1 \rightarrow$

Administrator's Main Menu		Schedule R	Cule		
• <u>Status</u>	Item		Setting		
• <u>Wizard</u>	▶ Schedule	🗖 Enable			
<u>+ Basic Setting</u>	D-1-#	D-l- N			- <b>4</b>
<u>+ Forwarding Rules</u>	Rule# 1	Rule Name ftp time		Edit	ction Delete
<u>+ Security Setting</u>					
- Advanced Setting	Save Add New Rule	Help			
• <u>System Time</u>					
• <u>System Log</u> • <u>Dynamic DNS</u>					
• <u>SNMP</u>					
• Routing					
Schedule Rule					
<u>+ Toolbox</u>					
Log out					

#### **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:

Administrator's Main Menu			Virtual Server		
• <u>Status</u>	D	Service Ports	Server IP	Enable	Use Rule#
• <u>Wizard</u>	1	21	192.168.122.33		1
<u>+ Basic Setting</u>	2		192.168.122.		0
- Forwarding Rules	3		192.168.122.		0
• <u>Virtual Server</u>	4		192.168.122.		0
• <u>Special AP</u>	5		192.168.122.		0
• <u>Miscellaneous</u>	6		192.168.122.		0
<u>+ Security Setting</u>	7		192.168.122.		0
<u>+ Advanced Setting</u>	8		192.168.122.		0
<u>+ Toolbox</u>	9		192.168.122.		0
Los out	10		192.168.122.		0
Log out	11		192.168.122.		0
	12		192.168.122.		0
	13		192.168.122.		0
	14		192.168.122.		0
	15		192.168.122.		0

## Example1: Virtual Server – Apply Rule#1 (ftp time: everyday 14:10 to 16:20)

Example2: Packet Filter – Apply Rule#1 (ftp time: everyday 14:10 to 16:20).

Administrator's Main Menu	Outbound Packet Filter					
Status		Item		Set	ting	
<u>Wizard</u>	Outbound	Filter		🗹 Enable		
+ Basic Setting		ow all to pass except those m		-		
+ Forwarding Rules	ΟDe	ny all to pass except those ma	atch the follo	wing rules.		
- Security Setting	ID	Source IP : Ports	De	estination IP : Ports	Enable	Use Rule#
• Packet Filters	1	:		: 20-21	V	1
<ul> <li><u>Domain Filters</u></li> </ul>	2	:		:		0
URL Blocking	3	:		:		0
<u>MAC Control</u> <u>Miscellaneous</u>	4	:		:		0
+ Advanced Setting	5	:		:		0
	6			:		0
<u>+ Toolbox</u>	7	:		:		0
Log out	8			:		0
	Save Undo	Schedule rul	s (00)Always	Copy to ID V		

## 4.8 Toolbox

Administrator's Main Menu • Status • Wizard + Basic Setting + Forwarding Rules + Security Setting + Advanced Setting • Toolbox • View Log • Firmware Upgrade • Backup Setting • Reset to Default • Reboot • Miscellaneous

Log out

## Toolbox

# 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 secific IP to test whether it is alive.

## 4.8.1 System Log

Administrator's Main Menu	System Log
Status	WANT The series TD Address (D1 0414-TTC)
• <u>Wizard</u>	WAN Type: Dynamic IP Address (R1.9414vTIG) Display time: Wed Oct 01 00:10:04 2003
+ Basic Setting	
	2003年10月1日 上午 12:01:30 DOD:TCP trigger from 192.168.123.125:2288 to 207.46.104.20:186
+ Forwarding Rules	2003年10月1日 上午 12:01:30 DHCP:discover()
+ Security Setting	2003年10月1日 上午 12:01:34 DHCP:discover()
· security setting	2003年10月1日 上午 12:01:35 Admin from 192.168.123.125 login successfully 2003年10月1日 上午 12:01:42 DHCP:discover()
+ Advanced Setting	2003年10月1日 上午 12:01:58 DHCP:discover()
	2003年10月1日 上午 12:02:47 DOD:triggered internally
<u>- Toolbox</u>	2003年10月1日 上午 12:02:47 DHCP:discover()
• <u>View Log</u>	2003年10月1日 上午 12:02:51 DHCP:discover()
<ul> <li>Firmware Upgrade</li> </ul>	2003年10月1日 上午 12:02:59 DHCP:discover()
<ul> <li><u>Backup Setting</u></li> </ul>	2003年10月1日 上午 12:03:15 DHCP:discover() 2003年10月1日 上午 12:03:48 DOD:triggered internally
<ul> <li><u>Reset to Default</u></li> </ul>	2003年10月1日 上午 12:03:48 DOD:01:01ggered Internally 2003年10月1日 上午 12:03:48 DHCP:discover()
• <u>Reboot</u>	2003年10月1日 上午 12:03:52 DHCP:discover()
• <u>Miscellaneous</u>	2003年10月1日 上午 12:04:00 DHCP:discover()
	2003年10月1日 上午 12:04:16 DHCP:discover()
Log out	
	Back Refresh Download Clear

You can View system log by clicking the View Log button

#### 4.8.2 Firmware Upgrade

Administrator's Main Menu	Firmware Upgrade		
• <u>Status</u>	Firmware Filename		
• <u>Wizard</u>			
<u>+ Basic Setting</u>	瀏覽		
<u>+ Forwarding Rules</u>	Current firmware version is R1.94l4vTIG. The upgrade procedure takes about 20 seconds. Note! Do not power off the unit when it is being upgraded. When the upgrade is done successfully, the unit will be restarted automatically.		
+ Security Setting	ale and when h is being appraced. When are apprace is done successionly, are and win be researced automaticany.		
<u>+ Advanced Setting</u>	Upgrade Cancel		
<u>- Toolbox</u>			
• <u>View Log</u>			
• Firmware Upgrade			
<u>Backup Setting</u>			
<ul> <li><u>Reset to Default</u></li> <li><u>Reboot</u></li> </ul>			
<ul> <li>Miscellaneous</li> </ul>			
Log out			

You can upgrade firmware by clicking Firmware Upgrade button.

## 4.8.3 Backup Setting

File Dov	wnload 🛛 🛛 🕅
?	You are downloading the file: config.bin from 192.168.123.254 Would you like to open the file or save it to your computer? Open       Save       Cancel       More Info         Image: Always ask before opening this type of file

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.

#### 4.8.4 Reset to default



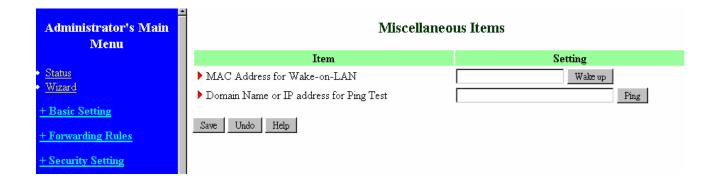
You can also reset this product to factory default by clicking the **Reset to default** button.

#### 4.8.5 Reboot

Microso	ft Internet Explorer 🔯
2	Reboot right now?
	OK Cancel

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

#### 4.8.6 Miscellaneous Items



#### 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 secific IP to test whether it is alive.

# Appendix A TCP/IP Configuration for Windows 95/98

This section introduces you how to install TCP/IP protocol into your personal computer. And suppose you have been successfully installed one network card on your personal computer. If not, please refer to your network card manual. Moreover, the Section B.2 tells you how to set TCP/IP values for working with this NAT Router correctly.

#### A.1 Install TCP/IP Protocol into Your PC

- 1. Click Start button and choose Settings, then click Control Panel.
- 2. Double click Network icon and select Configuration tab in the Network window.
- 3. Click Add button to add network component into your PC.
- 4. Double click **Protocol** to add TCP/IP protocol.

Select Network Component Type	
Click the type of network component you want to install:	
📃 Client	<u>A</u> dd
Adapter	
Y Protocol	Cancel
Service	
Protocol is a 'language' a computer uses. Computers must use the same protocol to communicate.	

5. Select **Microsoft** item in the manufactures list. And choose **TCP/IP** in the Network Protocols. Click **OK** button to return to Network window.

	otocol that you want to install, then click OK. If you have or this device, click Have Disk.
Manufacturers: Banyan IBM Microsoft Novell	Network Protocols: Fast Infrared Protocol IPX/SPX-compatible Protocol Microsoft 32-bit DLC Microsoft DLC NetBEUI TCP/IP
	<u>H</u> ave Disk OK Cancel

6. The TCP/IP protocol shall be listed in the Network window. Click **OK** to complete the install procedure and restart your PC to enable the TCP/IP protocol.

## A.2 Set TCP/IP Protocol for Working with NAT Router

- 1. Click **Start** button and choose **Settings**, then click **Control Panel**.
- 2. Double click **Network** icon. Select the TCP/IP line that has been associated to your network card in the **Configuration** tab of the Network window.

Network ? 🗙
Configuration Identification Access Control
The following <u>n</u> etwork components are installed:
PCI Fast Ethernet DEC 21140 Based Adapter
NetBEUI -> Dial-Up Adapter     NetBEUI -> PCI Fast Ethernet DEC 21140 Based Adapter
TCP/IP -> Dial-Up Adapter
TCP/IP -> PCI Fast Ethernet DEC 21140 Based Adapter
📮 File and printer sharing for Microsoft Networks 📃 📃
Add R <u>e</u> move P <u>r</u> operties
Primary Network Logon:
Client for Microsoft Networks
<u>F</u> ile and Print Sharing
Description TCP/IP is the protocol you use to connect to the Internet and wide-area networks.
OK Cancel

- 3. Click **Properties** button to set the TCP/IP protocol for this NAT Router.
- 4. Now, you have two setting methods:

a. Select **Obtain an IP address automatically** in the IP Address tab.

TCP/IP Properties		? ×
Bindings DNS Configuration	Advanced Gateway WINS Confi	NetBIOS iguration IP Address
If your network doe	be automatically assigne is not automatically assign iistrator for an address, an	n IP addresses, ask
Obtain an IP	address automatically	
-O <u>S</u> pecify an IP	address:	
[P Address:		
S <u>u</u> bnet Mask	k:	
	OK	Cancel

b. Don't input any value in the Gateway tab.

TCP/IP Properties		? ×
Bindings DNS Configuration	Advanced Gateway WINS Confi	NetBIOS iguration IP Address
	n the Installed Gateway li: in the list will be the order d.	
New gateway:	. <u>A</u> dd	
_ Installed gatewa	ys: <u>H</u> emo	ve
	OK	Cancel

c. Choose **Disable DNS** in the DNS Configuration tab.

TCP/IP Properties			? ×
Bindings A DNS Configuration Gatewa	dvanced v Í WINS Confi		tBIOS
Disable DNS	,	guidaon	
Enable DNS	D <u>o</u> main:		_
DNS Server Search Orde			_
		<u>A</u> dd emove	
Domain Suffix Search Dro			—
		A <u>d</u> d e <u>m</u> ove	
	ОК		Cancel

- B. Configure IP manually
  - a. Select Specify an IP address in the IP Address tab. The default IP address of this product is 192.168.123.254. So please use 192.168.123.xxx (xxx is between 1 and 253) for IP Address field and 255.255.255.0 for Subnet Mask field.

<b>TCP/IP Properties</b>		? ×
Bindings DNS Configuration	Advanced Gateway WINS Confi	NetBIOS guration IP Address
If your network do	be automatically assigned as not automatically assign nistrator for an address, an	n IP addresses, ask
O <u>O</u> btain an IP <b>-⊙</b> Specify an IP	address automatically address:	
IP Address:	192.168.123	.115
S <u>u</u> bnet Mas	k: <b>255.255.255</b>	. 0
	OK	Cancel

In the Gateway tab, add the IP address of this product (default IP is 192.168.123.254)
 in the New gateway field and click Add button.

<b>TCP/IP</b> Properties				?	×
Bindings DNS Configuration		anced     WINS Confi		NetBIOS	
The first gateway i The address order machines are used	r in the list wi				
<u>N</u> ew gateway: 192.168.1		Add			
- Installed gatewa		Hemov	/8		
		ОК		Cancel	

c. In the DNS Configuration tab, add the DNS values which are provided by the ISP into DNS Server Search Order field and click **Add** button.

TCP/IP Properties
Bindings         Advanced         NetBIOS           DNS Configuration         Gateway         WINS Configuration         IP Address
<ul> <li>○ Djsable DNS</li> <li>○ Enable DNS</li> </ul>
Host: MyComputer Domain:
DNS Server Search Order           168.95.192.1
168.95.1.1 <u>Eemove</u>
Domain Suffix Search Order
Add
Remove
OK Cancel

# Appendix B 802.1x Setting

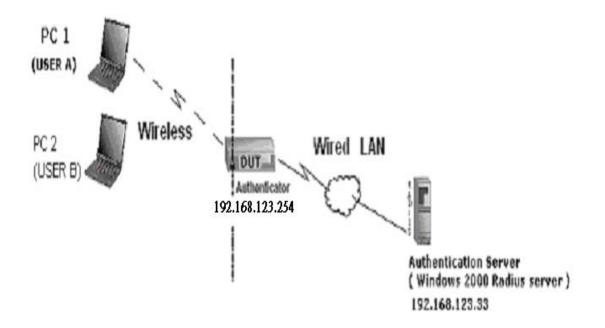


Figure 1: Testing Environment (Use Windows 2000 Radius Server)

#### **1 Equipment Details**

#### PC1:

Microsoft Windows XP Professional without Service Pack 1.

AMIT 531C Wireless Cardbus: 3.0.3.0

Driver version:

#### PC2:

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

AMIT 561C 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:**

Enable DHCP server.
 WAN setting: static IP address.
 LAN IP address: 192.168.123.254/24.
 Set RADIUS server IP.
 Set RADIUS server shared key.
 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.

🕹 Wireless	Network Con	nection Prop	erties	? 🗙
General W	ïreless Networks	Authentication	Advanced	_
wired and w	option to provide wireless Ethernet r <u>n</u> etwork access o	networks.		or
<u>E</u> AP type:	Smart Card or o MD5-Challenge Smart Card or o		Fiobe	rues
	ticate as <u>c</u> ompute ticate as guest wh able			
		0	K C	Cancel

Figure 2: Enable IEEE 802.1X access control

#### Figure 3: Smart card or certificate properties

#### 4. Windows 2000 RADIUS server Authentication testing:

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

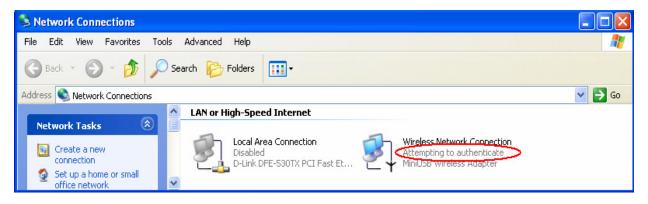
- 1. Download and install the certificate on PC1. (Fig 4)
- 2. PC1 choose the SSID of DUT as the Access Point.
- 3. Set authentication type of wireless client and RADIUS server both to

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)
- Windows XP will prompt that the authentication process is success or fail and end the authentication procedure. (Fig 6)
- Terminate the test steps when PC1 get dynamic IP and PING remote host successfully.

tificate ended p		<all></all>				
ersonal	Other Pe	ople 🛛 Inte	ermediate Certificati	on Authorities	Trusted Root	Certificatior 🤜
Issued			Issued By	Expirati	o Friendly	Nome
🔛 faet	1		WirelessCA	2/6/2004	4 <none></none>	
Import	····	xport	<u>R</u> emove			Advanced

Figure 4: Certificate information on PC1



**Figure 5: Authenticating** 

S Network Connections		
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> o	ools Adva <u>n</u> ced <u>H</u> elp	<b>1</b>
🕞 Back + 🕑 + 🏂 🖌	Search 🍺 Folders	
Address 🔇 Network Connections		💌 🔁 Go
Network Tasks	LAN or High-Speed Internet	
<ul> <li>Create a new connection</li> <li>Set up a home or small office network</li> </ul>	Local Area Connection Disabled D-Link DFE-530TX PCI Fast Et	

**Figure 6: Authentication success** 

**4.2**DUT 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.

 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.

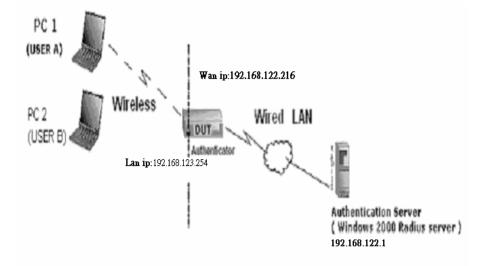
1.PC1 is on Windows XP platform without Service Pack 1.

2.PC2 is on Windows XP platform with Service Pack 1a.

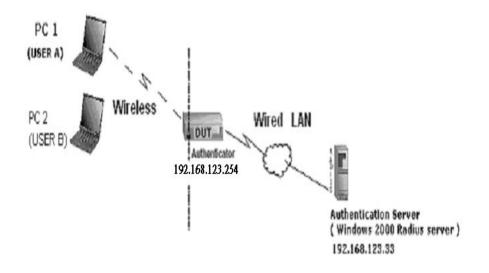
3.PEAP is supported on Windows XP with Service Pack 1 only.

4. Windows XP with Service Pack 1 allows 802.1x authentication only when data encryption function is enable.

# Appendix C WPA-PSK and WPA



Wireless Router: LAN IP: 192.168.123.254 WAN IP: 192.168.122.216 Radius Server: 192.168.122.1 UserA : XP Wireless Card:Ti-11g Tool: Odyssey Client Manager Refer to: <u>www.funk.com</u> Download: <u>http://www.funk.com/News&Events/ody\_c\_wpa\_preview\_pn.asp</u> Or Another Configuration:



## WPA-PSK

In fact, it is not necessary for this function to authenticate by Radius Server, the client and wireless Router authenticate by themselves.

#### Method1:

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

Network ID(SSID)	123kk	
Channel	8	
Security	VVPA-PSK	
Key Mode	ASCI 💽	
Preshare Key	12345678	

2. Go to Odyssey Client Manager, first choose "Network"

Before doing that, you should verify if the software can show the wireless card. Open "Adapters"

と Odyssey Client Ma	mager	
<u>S</u> ettings <u>C</u> ommands <u>J</u>	<u>N</u> eb <u>H</u> elp	
	<b>Networks</b> The following <u>n</u> etworks are configured:	
Profiles	<[any]>	<u>A</u> dd
+++Networks	<123kk>	<u>R</u> emove
Auto-Scan Lists		Properties
Trusted Servers		
Adapters		

3. Add and edit some settings:

	123kk	>
Connect to any av	ailable network	<u>S</u> can
Description (optional):		
Network <u>t</u> ype:	Access point (infrastructure mo	ode) 🚽
C <u>h</u> annel	default channel	
Association mode:	WPA	
Encyption method:	TKIP	1.
	profile:	,
Authenticate using     Keys will be genera  Pre-shared Key (WPA)	S. Arrenteering and the second s	
☐ Keys will be generated	S. Arrenteering and the second s	, , >
□ Keys will be genera Pre-shared Key (WPA)	ated automatically for data privac	, , ,
□ Keys will be genera Pre-shared Key (WPA) Possphrase:	ated automatically for data privac	, , ,

#### 4. Back to Connection:

Then Select "Connect to network" You will see:

av C:\WINDOWS\System32\cmd.exe - ping 192.168.0.248 -t	👌 Odyssey Client M	anager	
C:WINDOWS/System32/cmd.exe - ping 192.168.0.248 -t     Media State	Settings Commands <sup>1</sup>	Web Help Connection	130 WLAN Adapter

Method2:

1. First, patch windows XP and have to install "Service package 1"

Patch:

http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=5039ef4a-61e0-4c44 -94f0-c25c9de0ace9

- 2. Then reboot.
- 3. Setting on the router and client:

#### Router:

Network ID(SSID)	123kk	
Channel	8 💌	
Security	WPA-PSK 💌	
Key Mode	ASCI 💉	
Preshare Key	12345678	

# Client:

Go to "Network Connection" and select wireless adapter.

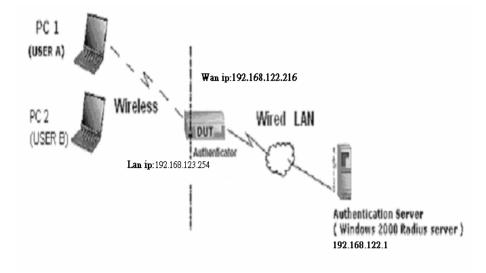
Choose "View available Wireless Networks" like below:

Advanced  $\rightarrow$  choose "123kk"

Wireless Network Connection Properties 🛛 🔹 🔀	123kk properties
General Wireless Networks Advanced	Association Authentication
Use Windows to configure my wireless network settings Available networks:	Network name (SSID): 123kk
To connect to an available network, click Configure.	This network requires a key for the following:
k amit01	Network Authentication: WPA-PSK
JOYCE Refresh	Qata encryption: TKIP
Preferred networks: Automatically connect to available networks in the order listed	Network key:
below: 123kk Move up	Confirm network key:
Move down	Key index (advanced):
Add Remove Properties	The key is provided for me automatically
Learn about <u>setting up wireless network</u> configuration. Advanced	This is a computer-to-computer (ad hoc) network; wireless access points are not used
OK Cancel	OK Cancel

#### WPA:

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

Connect to 192	2.168.122.1 🛛 🛛 🔀
	GR
Connecting to 19	2.168.122.1
<u>U</u> ser name:	
Password:	
	Remember my password
-	OK Cancel

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	
802.1X Settings	
	192.168.122.1
802.1X Settings RADIUS Server IP RADIUS port	192.168.122.1 1812

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

Profile	e name:	1		
Use	r Info Aut <u>h</u> e	nticatio	on <u>  I</u> TLS Setting	s   <u>P</u> EAP Settings
Log	gin name: 🏼 🗍	ae1		
FF	assword			
Г	Permit logi	n using	password	
1000	use <u>W</u> indo			
10.725	prompt for use the fol			
	ae1			
F	✓ U <u>n</u> mask			
	Certificate			
100		o uning	my <u>c</u> ertificate:	
100	ae1	rusing	my <u>c</u> entricate.	
1			Minu	Province
			<u>V</u> iew	Browse

Login name and passwd are fae1 and fae1.

Remember that you get certificate from Radius in Step1.

# 5. Then Choose "certificate" like above.

Select Certificate			? 🛛
Personal Certificates			
Issued To	Issued By		<u>Е</u>
fae1	WirelessCA		2
<			>
			⊻iew
<u>.</u>	 	-	
	[	確定	

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

n ITLS Settings PEAP Settin
*
<u>A</u> dd
<u>R</u> emov

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

<u>N</u> etwork name (SSII	D): 123kk		
Connect to any	available netw	vork	<u>S</u> can
Description (optiona	I):		1.5
Network <u>t</u> ype:	Access p	point (infrastructure mo	ode) 💌
C <u>h</u> annel:		default channel	
Association mode:	$\leq$	WPA	÷
Encryption method:		TKIP	
· Keys will be gen		atically for data privacy	r
	A)		
Pre-shared key (WP Bassphrase 「Unmask	1		
<u>P</u> assphrase:	1		

8. Back to Connection and Select "123kk.

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

etwork Properties			110	Od yssey Client
Network				🕹 Odyssey Client
Network name (SSID):	123kk			You are about to authenticate to an untrusted server!
Connect to any avai	ilable network	<u>S</u> can		To terminate communication, press [No]
Description (optional):	🖲 Odyssey Client Ma	nager		To temporarily trust this server, press [Yes] To permanently trust this server, check "add this trusted server to
Network type:	Settings Commands W	leb <u>H</u> elp		the database" and press [Yes]
Channel:		Connection Adapter: TNET1130 WLAN Adapter		<u>C</u> ertificate chain:
Association mode:	Profiles	Adapter type: wireless		WirelessCA win2000adv.intra.com.tw
Authentication	Auto-Scan Lists	Connection information	Scan	
✓ Keys will be general	Trusted Servers	Status: authenticating Elapsed time:		
Pre-shared key (WPA)	Adapters	Network (SSID): 123kk Access point: 00-50-18-00-0F-F8	i i	Add this trusted server to the database
Passphrase:		Packets in/out:		Server name must end with:
Linmask		Beconnect Reauthenticate	षिङ्ञ	win2000adv.intra.com.tw       Proceed to authenticate with this server?       Yes

## 9.Result:

👶 Odyssey Client Ma	nager				192.168.122.219:			
Settings Commands W	eb <u>H</u> elp				192.168.122.219: 192.168.122.219:	-		
Comments W Connection Profiles Networks Auto-Scan Lists	Connection	30 WLAN Adapter	• Scan	Reply from Reply from Reply from Reply from Reply from Reply from Reply from Reply from Reply from Reply from	192.168.122.219: 192.168.122.219: 192.168.122.219: 192.168.122.219: 192.168.122.219: 192.168.122.219: 192.168.122.219: 192.168.122.219: 192.168.122.219: 192.168.122.219: 192.168.122.219:	bytes = 32 bytes = 32	time=1ns time=1ns time=1ns time=1ns time=1ns time=1ns time=1ns time=2ns time=1ns	TTL=63 TTL=63 TTL=63 TTL=63 TTL=63 TTL=63 TTL=63 TTL=63 TTL=63 TTL=63
Adapters	Network (SSID): Access point: Packets in/out: <u>R</u> econnect	123kk 00-50-18-00-0F-F8 12679 / 13605 Reauthenticate	[ € <b>⊸</b>	Reply from Reply from Reply from Reply from Reply from	192.168.122.219: 192.168.122.219: 192.168.122.219: 192.168.122.219: 192.168.122.219: 192.168.122.219: 192.168.122.219: 192.168.122.219:	bytes=32 bytes=32 bytes=32 bytes=32 bytes=32	time=1ms time=1ms time=2ms time=2ms time=1ms	TTL=63 TTL=63 TTL=63 TTL=63 TTL=63

#### Method 2:

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

http://192.168.122.1/certsrv

account:fae1

passwd:fae1

Connect to 19	2.168.122.1	? 🛛
		S.
Connecting to 19	2.168.122.1	
User name:	<b>2</b>	× 10
Password:		
	Remember my pass	word
	ОК	Cancel

- 2. Then Install this certificate and finish.
- 3. Setting on the router and client:

Router:

Network ID(SSID)	123kk	
Channel	8 💌	
Security		

# 802.1X Settings

RADIUS Server IP

RADIUS port

RADIUS Shared Key

192.168.122.1	
1812	
costra	

## Client:

Go to "Network Connection" and select wireless adapter.

Choose "View available Wireless Networks" like below:

Advanced  $\rightarrow$  choose "123kk"

Select "WirelessCA and Enable" in Trusted root certificate authority:

General Authentication Advanced	Smart Card or other Certificate Properties
Select this option to provide authenticated network access for wired and wireless Ethernet networks. Enable network access control using IEEE 802.1X EXP-type: Smart Card or other Certificate Properties Authenticate as computer when computer information is available Authenticate as guest when user or computer information is unavailable	When connecting: Use my smart card Use a certificate on this computer Validate server certificate Connect only if server name ends with: Trusted root certificate authority: Vuse a different user name for the connection OK Cancel
OK Cancel	

🖢 Wireless Network Connection Properties 💦 🛛 🛛	123kk properties
General Wireless Networks Advanced	Association Authentication
Use Windows to configure my wireless network settings Available networks: To connect to an available network, click Configure.	Network name (SSID): 123kk Wireless network key This network requires a key for the following:
L dale Configure L amit01 L JDYCE	Network Authentication: WPA
Preferred networks: Automatically connect to available networks in the order listed below: 123kk Move up	Network key:
Add Remove Properties Learn about setting up wireless network	Key index (advanced): 1
Configuration. Advanced	access points are not used OK Cancel

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

# **Appendix D WDS Setting**

#### How to setup and work:

First, check the Wlan-mac address of AP1, AP2 and AP3. Please goto command mode and use

"Arp –а ".

If you can not find the information of Mac, please make the cable to plug in lan-port of ap and ping the lan ip address then arp -a. There are some information in the screen. For example:

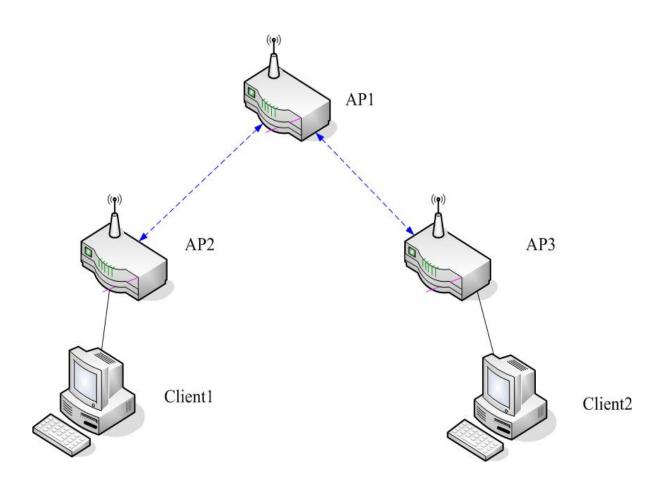
```
C:\>ping 192.168.122.217
Pinging 192.168.122.217 with 32 bytes of data:
Reply from 192.168.122.217: bytes=32 time<10ms TTL=64
Ping statistics for 192.168.122.217:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = Oms, Maximum = Oms, Average = Oms
Control-C
°C
C:∖>arp -a
Interface: 192.168.122.14 on Interface 0x1000003
  Internet Address
                        Physical Address
                                               Туре
 192.168.122.3
                        00-50-fc-3f-cc-ed
                                               dynamic
  192.168.122.217
                        00-50-18-00-0f-d9
                                               dynamic
```

AP 1:	AP2:	AP3:
IP:192.168.123.254	IP:192.168.123.253	IP:192.168.123.252
Mac:00-50-18-00-0f-fe	Mac:00-50-18-00-0f-fd	Mac:00-50-18-00-0f-fc
SSID:Default	SSID:Default	SSID:Default
Channel:11	Channel:11	Channel:11

Dhcp Server:Enable

Blue Line:Wireless

Black Line:Wire



If the Settings are ok, the client1 and client2 can get ip from dhcp server of AP1. Then Client1 and Client2 can get information each other.

AP1 Setting:

 $AP1 \leftrightarrow AP2$ (Remote Mac: 00-50-18-00-0f-fd)

 $AP1 \leftrightarrow AP3$ (Remote Mac: 00-50-18-00-0f-fc)

Administrator's Main Menu		WDS Setting
<u>Status</u>	Item	Setting
Wizard	<ul> <li>Wireless Bridging</li> </ul>	C Disable 💿 Enable
- Basic Setting	Remote AP MAC	00-50-18-00-0f-fd
<ul> <li>Primary Setup</li> </ul>		00-50-18-00-0f-fc
• <u>DHCP Server</u>		
• <u>Wireless</u> • <u>Change Password</u>		
	Save Undo Help	
+ Forwarding Rules		
+ Security Setting		
+ Advanced Setting		
<u>+ Toolbox</u>		
Log out		

AP2 Setting:

# AP2 ← → AP1(Remote Mac: 00-50-18-00-0f-fe)

Administrator's Main Menu		WDS Setting
• <u>Status</u>	Item	Setting
• <u>Wizard</u>	<ul> <li>Wireless Bridging</li> </ul>	C Disable 💿 Enable
- Basic Setting	▶ Remote AP MAC	00-50-18-00-0f-fe
<ul> <li><u>Primary Setup</u></li> </ul>		
• <u>DHCP Server</u>		
• <u>Wireless</u>		
<ul> <li><u>Change Password</u></li> </ul>	Save Undo Help	
+ Forwarding Rules		
+ Security Setting		
+ Advanced Setting		
<u>+ Toolbox</u>		
Log out		

AP3 Setting

AP3 ← → AP1(Remote Mac: 00-50-18-00-0f-fe)

Administrator's Main Menu		WDS Setting
• <u>Status</u>	Item	Setting
• <u>Wizard</u>	<ul> <li>Wireless Bridging</li> </ul>	C Disable 💿 Enable
- Basic Setting	▶ Remote AP MAC	00-50-18-00-0f-fe
<ul> <li>Primary Setup</li> </ul>		
• <u>DHCP Server</u>		
• <u>Wireless</u> • <u>Change Password</u>		
	Save Undo Help	
+ Forwarding Rules		
+ Security Setting		
+ Advanced Setting		
<u>+ Toolbox</u>		
Log out		

# Appendix E 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:



If yes, please execute Browser, like Mozilla and key 192.168.123.254 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.....
Subnet Mask....
Default Gateway....
                                                          0.0.0.0
0.0.0.0
C:∖>ipconfig ∕renew
Windows IP Configuration
Ethernet adapter Local Area Connection:
          Connection-specific DNS Suffix
          IP Address. . .
Subnet Mask . .
Default Gateway
                                                                 .168
                                                                        123
                                                                              115
                                                             25
                                                                        255
                                                                             Й
                                                                             254
```

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

	listory <u>G</u> roups <u>O</u> ptions <u>T</u> ools Ta <u>b</u> s Help	Links	
🗋 • 🔘 • 🔘 • 🚺	ù 🖻 🏠 🔎 📩 🚱 🖉	🎍 🛃 🛛 🖬 • 🎹 •	
dress 🛃 http://192.168.12	3.254/		- 🔁 - 🛛
Wireless Broadband N			
	Multi-Functional Wireless Bro	oadband NAT Router (R1.97e8b	-R61)
ser's Main Menu		System Status	
<u>'tatus</u>			
System Password (default: <b>admin</b> )	Item	WAN Status	Sidenote
	Remaining Lease Time	00:00:00	
	IP Address	0.0.0.0	
	Subnet Mask	0.0.0.0	
Log in	Gateway	0.0.0.0	Unreachable
	Domain Name Server	0.0.0.0	
	1		
	Statistics of WAN	Inbound	Outbound
	Octets	0	1312
	Unicast Packets	0	0

# 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: There are 2 methods to reset to default.

1. Restore with RESET button

First, turn off the router and press the RESET button in. And then, power on the router and push the RESET button down until the M1 and or M2 LED (or Status LED) start flashing, then remove the finger. If LED flashes about 8 times, the RESTORE process is completed. However, if LED flashes 2 times, repeat.

#### 2. Restore directly when the router power on

First, push the RESET button about 5 seconds (Status will start flashing about 5 times), remove the finger. The RESTORE process is completed.

#### 4. How to do recovery mode when the router is abnormal?

A: Allocate a Static IP Address on your computer as below:

Step1:First, press the reset button and power on the router until Status blinks very ffast.

Step2:Find the Inter Protocol(TCP/IP) Properties from My Network Places and check Properties of Local Area Network Connection. And click the "General" icon and assign one IP address which can be from 192.168.123.1 to 192.168.123.253. Here we use the 192.168.123.88 as the IP address. The Subnet mask must be 255.255.255.0, and the Default gateway must be 192.168.123.254. Then click "OK" button to complete TCP/IP setup.

🔵 <u>O</u> btain an IP address au	utomatically
-----------------------------------	--------------

Use the following IP address: —	
<u>I</u> P address:	192 . 168 . 123 . 88
S <u>u</u> bnet mask:	255 . 255 . 255 . 0
<u>D</u> efault gateway:	192 . 168 . 123 . 254

**Step2:** Open the command mode and input "**cmd**" then check if the router replies to ping 192.168.123.254

Run				? 🔀
	Type the name of Internet resource			
Open:	cmd			~
	ОК	Cancel	Browse	

C:\>ping 1	92.168.123.254			
Pinging 19	2.168.123.254 wit}	n 32 bytes (	of data:	
Reply from Reply from	192.168.123.254: 192.168.123.254:	bytes=32 t butes=32 t	ime<1ms ime<1ms	TTL=64 TTL=64
	192.168.123.254:			

Step3:Please use the exe-file of fw and click as below:

Select one device. Or you can input IP ma	nually :
192.168.123.254 crash	<ul> <li>Refresh</li> </ul>
Upgrade	Exit

Then click" Upgrade" if necessary, please input password "admin". Then reset to default and refer to Q1 How to connect Router.

However, if those methods can not make the router normal, please send the unit to the seller to check, thanks.

# 5.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.

Administrator's Main Menu		Choo	se WAN Type
• <u>Status</u>		Туре	Usage
• <u>Wizard</u>	0	Static IP Address	ISP assigns you a static IP address.
- Basic Setting	$\odot$	Dynamic IP Address	Obtain an IP address from ISP automatically.
Primary Setup	0	Dynamic IP Address with Road Ru	nner Session Management (e.g. Telstra BigPond)
<ul> <li><u>DHCP Server</u></li> <li>Wireless</li> </ul>	0	PPP over Ethernet	Some ISPs require the use of PPPoE to connect to their services.
• Change Password	0	PPTP	Some ISPs require the use of PPTP to connect to their services.
+ Forwarding Rules + Security Setting	0	L2TP	Some ISPs require the use of L2TP to connect to their services.

# 6.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.

Administrator's  Main Menu		Primary Setup
	Item	Setting
<u>Status</u> Wizard	LAN IP Address	192.168.122.217
Dente October	🕨 WAN Type	Static IP Address Change
- Basic Setting • Primary Setup	▶ WAN IP Address	
• DHCP Server	▶ WAN Subnet Mask	255.255.255.240
• Wireless	▶ WAN Gateway	-
• <u>Change Password</u>	Primary DNS	168.95.1.1
+ Forwarding Rules	Secondary DNS	168.95.192.1

# 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:

🎇 Crazy Browser - [Wireles	ss Broadband NAT Router Web-	Console]	- 0	×
Eile Edit View Favorites Hist	tory <u>G</u> roups <u>O</u> ptions <u>T</u> ools Ta <u>b</u> s	Help		
] 🗋 •   🚱 • 🕥 - 💌	🔁 🏠 🔎 📩 🥴 🖉	3 실 🛃 🖃 • 🎹 •		
Address 🙆 http://192.168.123.3	254/		- 🔁 - 🛛	×
Wireless Broadband N D:1	\ccostra\myhit.htm			
	Multi-Functional Wireless	Broadband NAT Router (R1.97e8b-R	61)	
Administrator's  Main Menu		Wireless Setting		
• <u>Status</u>	Item	Setting		
• <u>Wizard</u>	▶ Wireless			
- Basic Setting	▶ Network ID(SSID)	default		
• Primary Setup	▶ SSID broadcast	• Enable • Disable		
• DHCP Server	▶ Channel	11 💌		
<ul> <li>Wireless</li> <li>Change Password</li> </ul>	Security	None		
+ Forwarding Rules + Security Setting + Advanced Setting	Save Undo WDS Set	ting MAC Address Control	Help	
e	8	% Tab Counts:2 😪 👁 🛛	🧿 Internet 🛛 🖌 🕅	11.

About wireless client, you will see wireless icon:

« <del>y</del> B

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 fine the device which ssid is "default", please refer to Q3.

Network Tasks	Choose a wireless network	
Refresh network list	Click an item in the list below to connect to a <u>w</u> ireless information.	network in range or to get more
	default Non-secure wireless network	Signal Strength: <b>BBB</b> Connected

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

Related Tasks	Image: strength interview of the strength interview o
Change preferred wireless network Wireles	This is network is configured for open access. Information sent over this s Network Connection
Learn about wirele <u>networking</u> <u>Change settings of</u> <u>connection</u>	"default" does not require a network key. Information sent over this network is not encrypted and may be visible to others. If you are sure you want to connect to this network, click Connect. Otherwise, click Cancel.
	Connect Cancel

If successfully, the computer will show



and get ip from router:



# 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.

default properties	×
Association Authentication Connection	
Network name (SSID): default	
Wireless network key	
This network requires a key for the following:	
Network Authentication:	
Data encryption:	
Network key:	
Confirm network key:	
Key inde <u>x</u> (advanced): 1 👘	
The key is provided for me automatically	
This is a <u>c</u> omputer-to-computer (ad hoc) network; wireless access points are not used	
OK Cancel	

# **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.

Attention :

1.Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

2. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter. A minimum separation distance of 20 cm between the antenna and from all persons must be maintained to satisfy the RF exposure requirements.