



# ***802.11n Wireless Gigabit Broadband Router***

**WNRT-632**

**User's Manual**

## Copyright

Copyright © 2010 PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

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

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

## FCC Caution:

To assure continued compliance, (example-use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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

## **Federal Communication Commission (FCC) Radiation Exposure Statement**

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

## **CE mark Warning**

This is a class B device, in a domestic environment; this product may cause radio interference, in which case the user may be required to take adequate measures.

## **Energy Saving Note of the Device**

This power required device does not support Stand by mode operation.

For energy saving, please remove the DC-plug or push the hardware Power Switch to OFF position to disconnect the device from the power circuit.

Without remove the DC-plug or switch off the device, the device will still consuming power from the power circuit. In the view of Saving the Energy and reduce the unnecessary power consuming, it is strongly suggested to switch off or remove the DC-plug for the device if this device is not intended to be active.

## **R&TTE Compliance Statement**

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

## **Safety**

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

## **WEEE regulation**



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

## **Revision**

User's Manual for PLANET 802.11n Wireless Gigabit Broadband Router

Model: WNRT-632

Rev: 1.0 (Sep. 2010)

## Table of Contents

Chapter 1	Introduction .....	7
1.1	Packing Contents .....	7
1.2	Spec Summary Table .....	8
1.3	Hardware Configuration .....	9
1.4	LED indicators.....	11
1.5	Procedure for Hardware Installation.....	12
Chapter 2	Making Configuration .....	14
2.1	Login to Configure from Wizard .....	15
2.2	System Status .....	19
2.3	Advanced .....	20
2.3.1	Basic Setting .....	20
2.3.1.1	Primary Setup – WAN Type, Virtual Computers.....	21
2.3.1.2	DHCP Server .....	25
2.3.1.3	Wireless .....	26
2.3.1.4	Change Password.....	31
2.3.2	Forwarding Rules .....	32
2.3.2.1	Virtual Server .....	32
2.3.2.2	Special AP .....	33
2.3.2.3	Miscellaneous Items .....	34
2.3.3	Security Settings.....	35
2.3.3.1	Packet Filters .....	36
2.3.3.2	Domain filters .....	41
2.3.3.3	URL Blocking .....	43
2.3.3.4	Internet Access Control.....	45
2.3.3.5	Miscellaneous Items .....	52
2.3.4	Advanced Settings.....	53
2.3.4.1	System Time .....	54
2.3.4.2	System Log .....	55
2.3.4.3	DDNS Service.....	56
2.3.4.4	SNMP .....	57
2.3.4.5	Routing.....	58
2.3.4.6	Schedule Rule .....	60
2.3.4.7	QoS Rule .....	61
2.3.5	Toolbox.....	62
2.3.5.1	View Log .....	62
2.3.5.2	Firmware Upgrade .....	63

2.3.5.3 Backup Setting .....	63
2.3.5.4 Reset to default .....	64
2.3.5.5 Reboot .....	64
2.3.5.6 Miscellaneous Items .....	65
Appendices and Index .....	66
802.1x Setting .....	66
WPA Settings .....	72
FAQ and Troubleshooting .....	81
What can I do when I have some trouble at the first time?.....	81
How do I connect router by using wireless? .....	84

# Chapter 1 Introduction

Thank you for purchasing WNRT-632. This manual guides you on how to install and properly use the WNRT-632 in order to take full advantage of its features.

## 1.1 Packing Contents

Make sure that you have the following items:

- WNRT-632 x 1
- Power Adapter x 1
- Ethernet Cable x 1
- CD x 1 (Quick Installation Guide and User's Manual)
- Quick Installation Guide x 1

**Note:** If any of the above items are missing, please contact your supplier for support.

## 1.2 Spec Summary Table

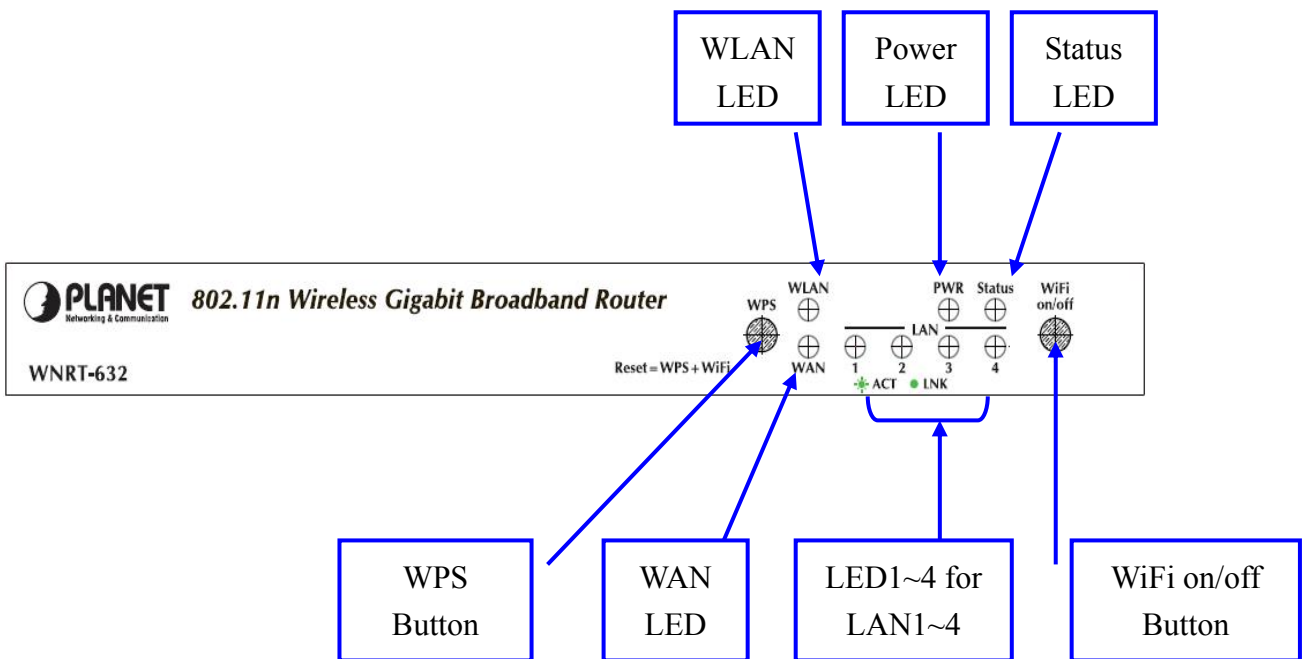
Device Interface		WNRT-632
Ethernet WAN	RJ-45 port, 10/100/1000Mbps, auto-MDI/MDIX	1
Ethernet LAN	RJ-45 port, 10/100/1000Mbps, auto-MDI/MDIX	4
Antenna	3dBi detachable antenna	2
WPS Button	For WPS connection	1
Wireless Enable/disable	To enable or disable Wireless Radio	1
LED Indication	Power/Status / WAN / LAN1 ~ LAN4/ Wi-Fi	•
Power Jack	DC Power Jack, powered via external DC 12V/1A switching power adapter	1
Wireless LAN (WiFi)		
Standard	IEEE 802.11b/g/n compliance	•
SSID	SSID broadcast or in stealth mode	•
Channel	Auto-selection, manually	•
Security	WEP, WPA, WPA-PSK, WPA2, WPA2-PSK	•
WPS	WPS (Wi-Fi Protected Setup)	•
WMM	WMM (Wi-Fi Multimedia)	•
Functionality		
Ethernet WAN	PPPoE, DHCP client, Static IP, PPTP, L2TP	•
WAN Connection	Auto-reconnect, dial-on-demand, manually	•
One-to-Many NAT	Virtual server, special application, DMZ, Super DMZ (IP Pass through)	•
NAT Session	Support NAT session	20000
SPI Firewall	IP/Service filter, URL blocking, MAC control	•
DoS Protection	DoS (Deny of Service) detection and protection	•
Routing Protocol	Static route, dynamic route (RIP v1/v2)	•
Management	SNMP, UPnP IGD, syslog, DDNS	•
Administration	Web-based UI, remote login, backup/restore setting	•
Performance	NAT up to 700Mbps and Wireless up to 150Mbps	



Environment & Certification		
Package Information	Package dimension (W x D x H) (mm)	245 x 207 x 60
	Package weight (gross weight) (g)	674
Operation Temp.	Temp.: 0~40°C, Humidity 10%~90% non-condensing	•
Storage Temp.	Temp.: -10~70°C, Humidity: 0~95% non-condensing	•
EMI Certification	CE/FCC compliance	•
RoHS	RoHS compliance	•

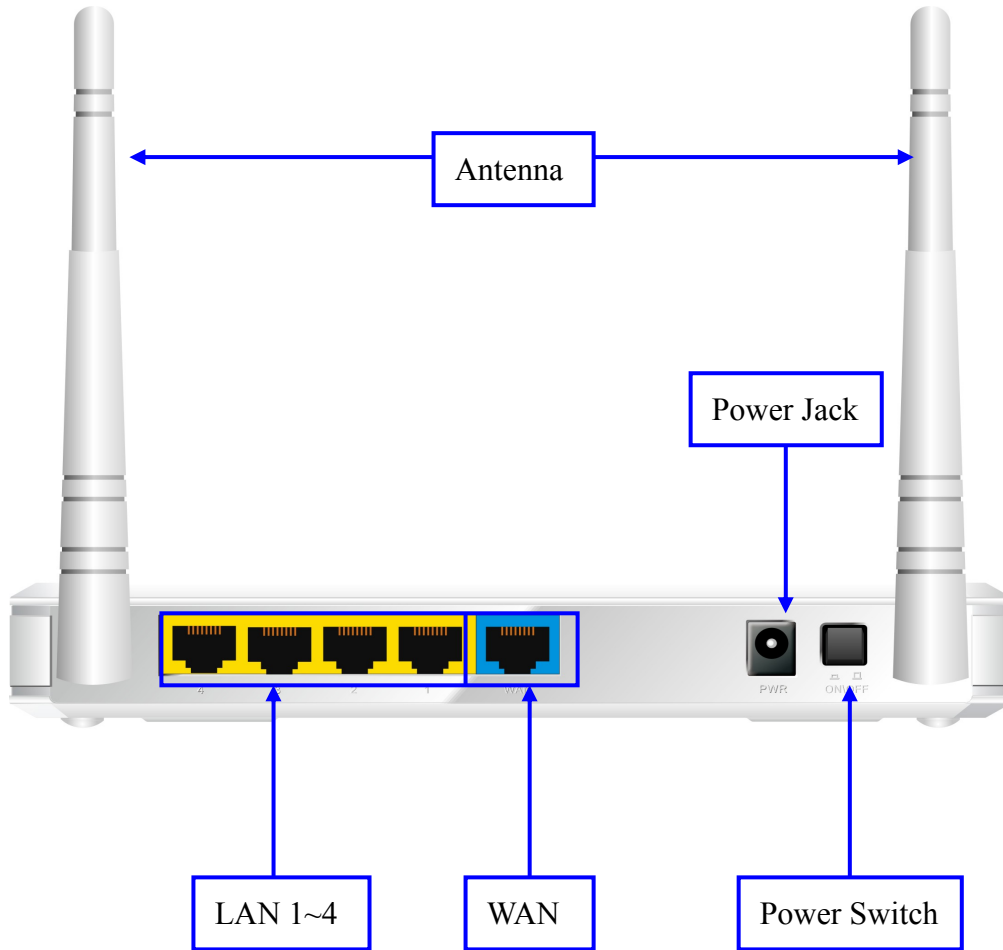
### 1.3 Hardware Configuration

Figure 2-1 Front Panel



**Note:** Reset = Press Wi-Fi on/off and WPS buttons simultaneously about 5 sec.

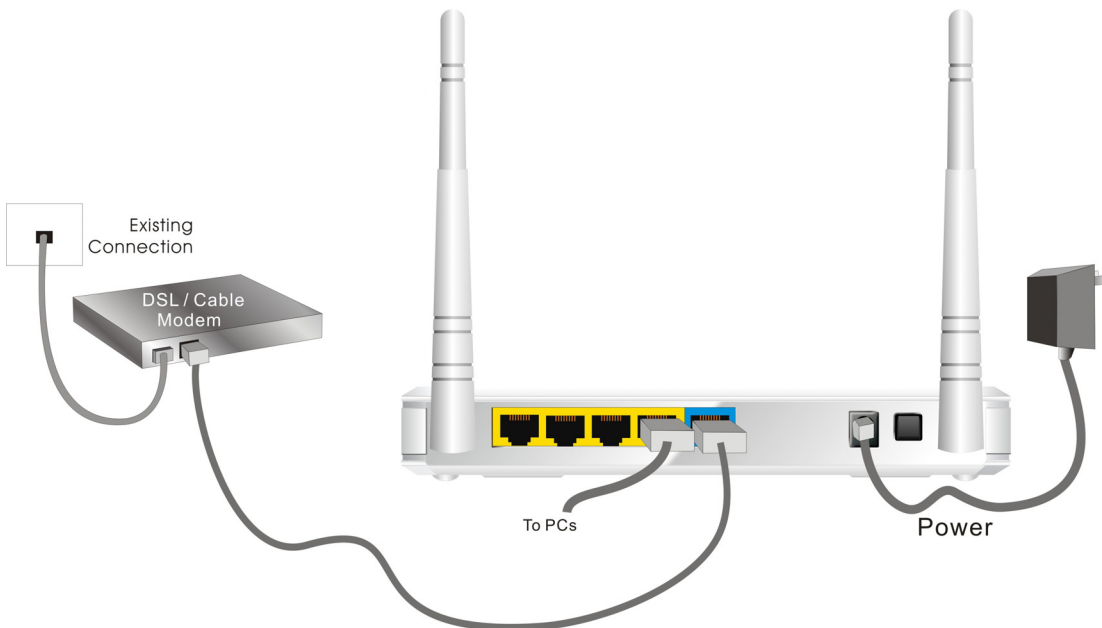
Figure 2-2 Rear Panel



## 1.4 LED indicators

	LED status	Description
Status	Green in flash	Device status is working.
WAN LED	Green	RJ45 cable is plugged
	Green in flash	Data access
LAN LED	Green	RJ45 cable is plugged
	Green in flash	Data access
WiFi LED	Green	WLAN is on
	Green in flash	Data access
	Green in fast flash	Device is in WPS PBC mode
	Green in dark	Wi-Fi Radio is disabled

## 1.5 Procedure for Hardware Installation



### Step 1. Attach the antenna.

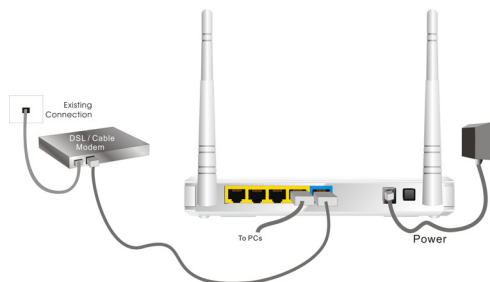
- 1.1. Remove the antenna from its plastic wrapper.
- 1.2. Screw the antenna in a clockwise direction to the back panel of the unit.
- 1.3. Once secured, position the antenna upward at its connecting joint. This will ensure optimal reception.



1. Turn off the Power Switch first.

### Step 2 Insert the Ethernet cable into LAN Port:

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



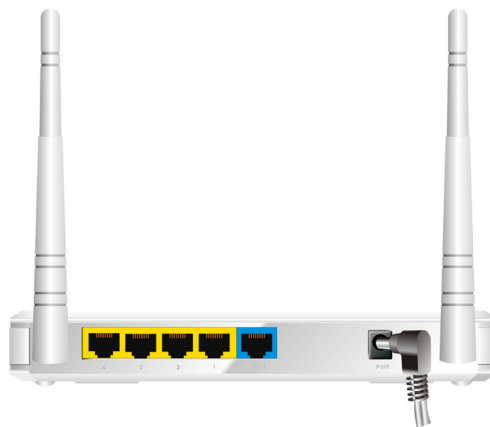
**Step 3 Insert the Ethernet patch cable into Wired WAN port:**

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



**Step 4. Power on Router:**

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

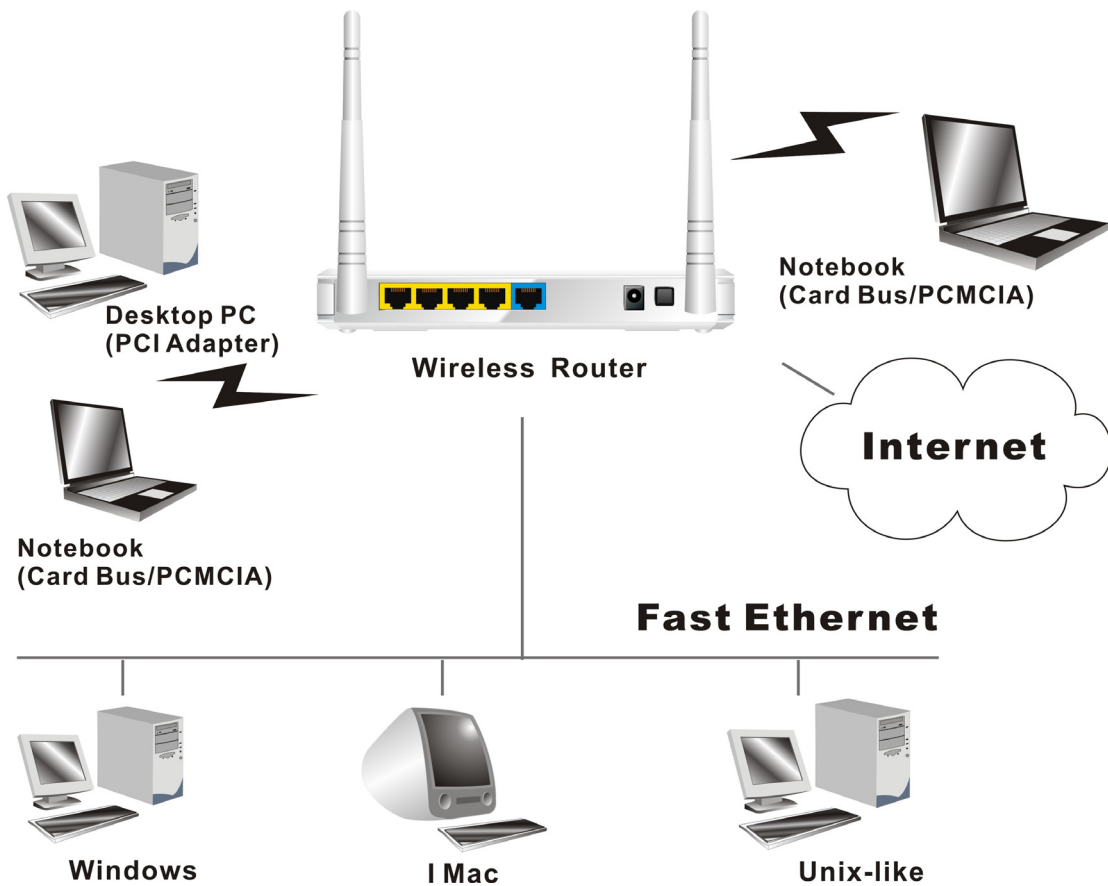


**Step 5. Complete the setup.**

5.1. When complete, the Status LED will flash.

## Chapter 2 Making Configuration

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



## 2.1 Login to Configure from Wizard

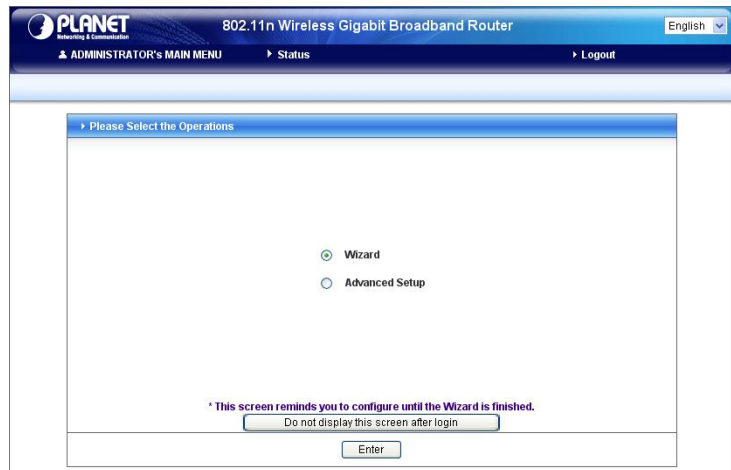
Configure the settings by the following steps:

2.1 Open web browser, type the default IP address (<http://192.168.0.1>)

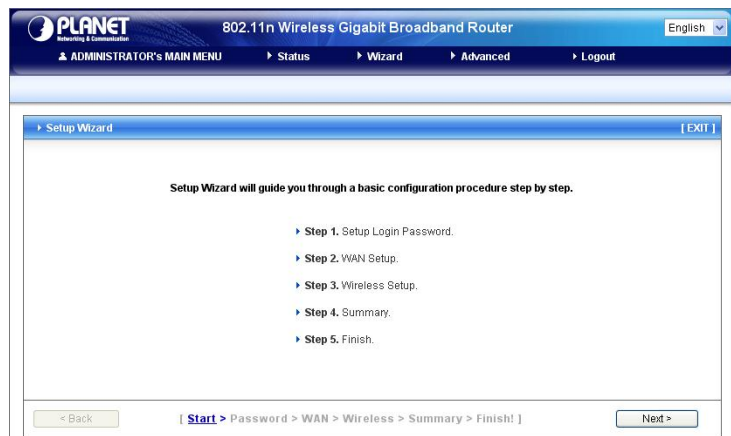
System Password: "admin"



2.2 Select "Wizard", and then click "Enter".



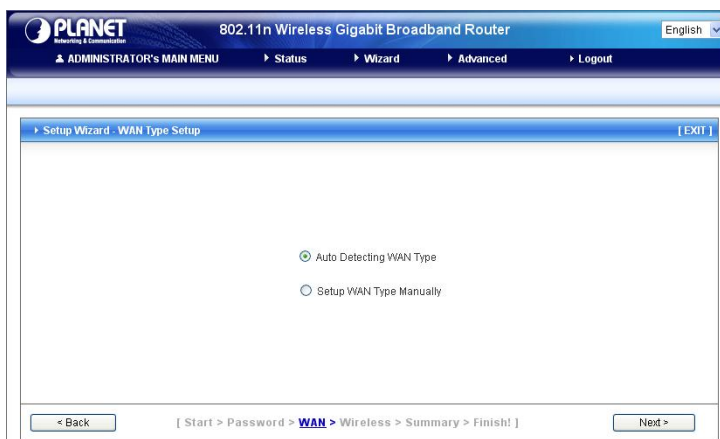
2.3 Start to configure Internet setting by click "Next >" button.



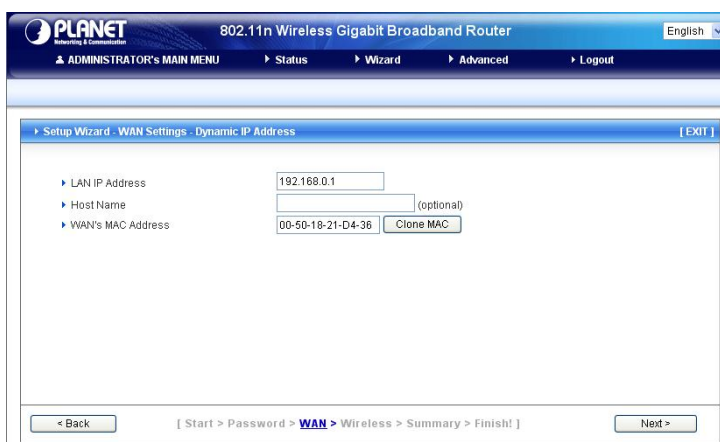
2.4 Modify the Old Password by entering a new one. Click "Next >" button if you don't want to change the password.



2.5 Select “Auto Detecting WAN Type” and then click “Next >” button.



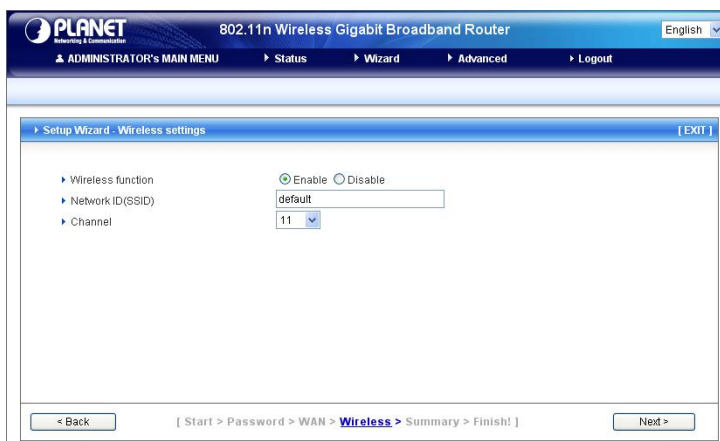
2.6 Click “Next >” to continue the setting.



Example, the Dynamic WAN type is detected.

2.7 Modify the Wireless settings.

Click “Next >” if setting by default. (Strongly suggest changing the SSID to protect your wireless network.)





## 2.8 Setup the Wireless Security.

Click “Next >” if setting by default. (Strongly suggest configuring the security to protect your wireless network.)

The screenshot shows the 'Setup Wizard - Wireless Security' page. At the top, there is a navigation bar with 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area has a 'Security' dropdown menu set to 'None'. At the bottom, there are buttons for '< Back' and 'Next >', along with a breadcrumb trail: '[ Start > Password > WAN > **Wireless** > Summary > Finish! ]'.

2.9 Make sure all the settings are configured correctly, and then click “Apply Settings” button.

**You can ignore the wan connection test by uncheck the “Do you want to proceed the network testing?”**

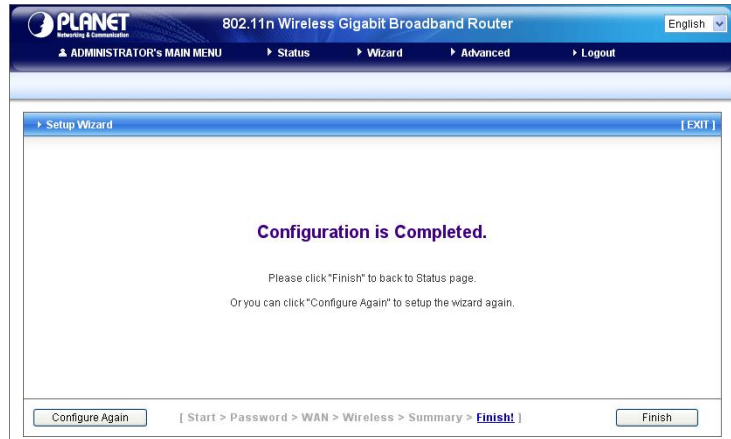
The screenshot shows the 'Setup Wizard - Summary' page. It displays a table of configuration details for confirmation. At the bottom, there is a checkbox for 'Do you want to proceed the network testing?' which is checked. Buttons for '< Back' and 'Apply Settings' are visible, along with the breadcrumb trail: '[ Start > Password > WAN > Wireless > **Summary** > Finish! ]'.

Please confirm the information below.	
WAN Type	Dynamic IP Address
Host Name	-
WAN's MAC Address	00-50-18-21-D4-36
Wireless	Enable
SSID	default
Channel	11
Security	None

2.10 Wait for the system applying the settings automatically.

The screenshot shows the 'Setup Wizard - WAN Connection Test' page. The main content area contains the text: 'System is applying the settings. Please wait a moment...'. At the bottom, there are buttons for '< Back' and 'Next >', along with the breadcrumb trail: '[ Start > Password > WAN > Wireless > **Summary** > Finish! ]'.

2.11 Click **Finish** to complete the Setup.  
Or you can click **Configure Again** to setup the wizard again.



## 2.2 System Status

The screenshot displays the administrator interface for a Planet 802.11n Wireless Gigabit Broadband Router. The top navigation bar includes the Planet logo, the router model name, a language dropdown set to English, and menu options for Administrator's Main Menu, Status, Wizard, Advanced, and Logout.

The main content area is divided into three sections:

- System Status:** A table showing WAN configuration details.
 

Item	WAN Status	Sidenote
IP Address	210.66.155.72	Static IP
Subnet Mask	255.255.255.0	
Gateway	210.66.155.94	
Domain Name Server	168.95.1.1, 8.8.8.8	
MAC Address	00-30-4F-21-D4-36	
- Wireless Status:** A table showing WLAN configuration details.
 

Item	WLAN Status	Sidenote
Wireless mode	Enable	
SSID	default	
Channel	11	
Security	None	
MAC Address	00-30-4F-21-D4-37	
- Statistics Information:** A table showing WAN traffic statistics.
 

Statistics of WAN	Inbound	Outbound
Octets	44789	5464
Unicast Packets	99	73
Non-unicast Packets	304	2

Below the statistics table are four buttons: View Log..., Clients List..., NAT Status..., and Refresh. At the bottom, the device time is shown as Mon Jun 01 00:21:10 2009, followed by the copyright notice: Copyright © 2010 Planet Technology corporation, All rights reserved.

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

### WAN 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.

### Statistics of WAN:

Enables you to monitor inbound and outbound packets

## 2.3 Advanced

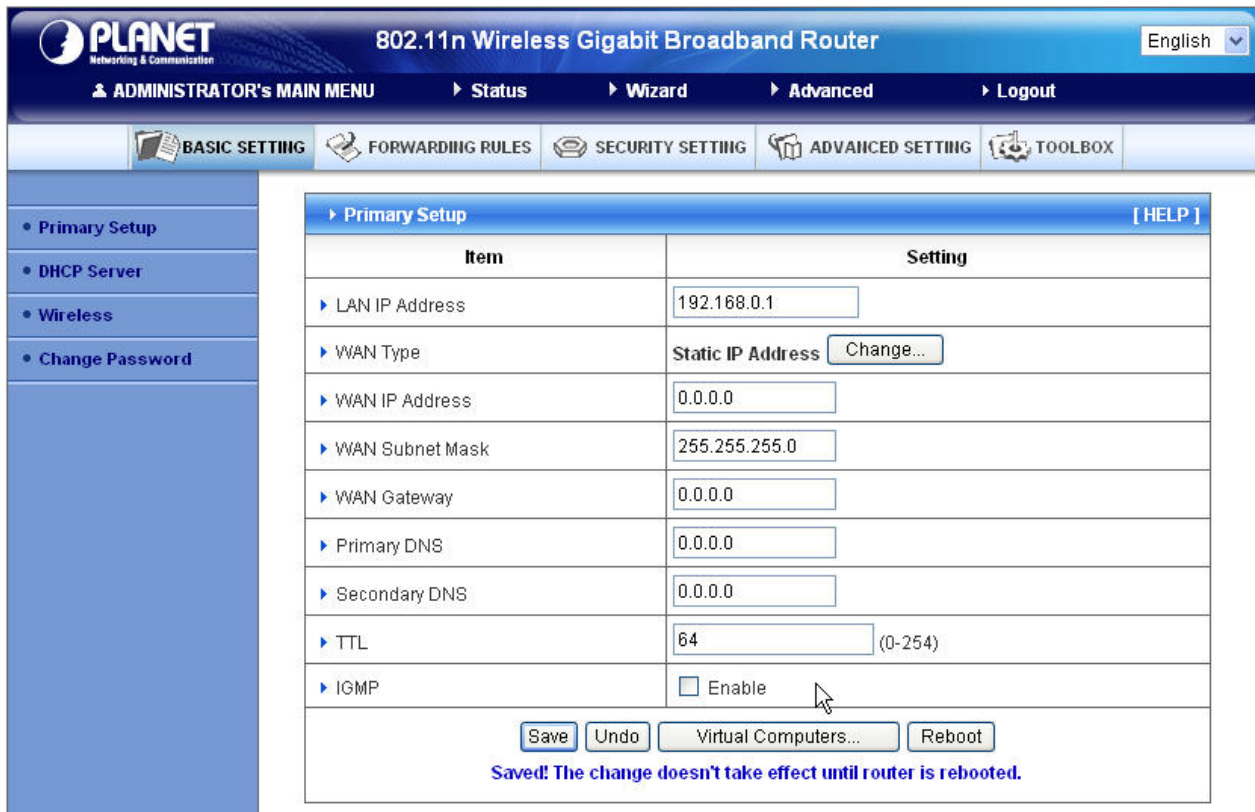
### 2.3.1 Basic Setting

Please Select "Advanced Setup" to Setup

The screenshot displays the web interface for a Planet 802.11n Wireless Gigabit Broadband Router. The top navigation bar includes the Planet logo, the router model name, and a language dropdown set to English. Below this is a main menu with options: ADMINISTRATOR's MAIN MENU, Status, Wizard, Advanced, and Logout. A secondary menu contains icons for BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING, and TOOLBOX. On the left side, a vertical sidebar lists: Primary Setup, DHCP Server, Wireless, and Change Password. The main content area is titled 'Basic Setting' and contains a list of configuration options:

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

### 2.3.1.1 Primary Setup – WAN Type, Virtual Computers



PLANET 802.11n Wireless Gigabit Broadband Router

ADMINISTRATOR'S MAIN MENU | Status | Wizard | Advanced | Logout

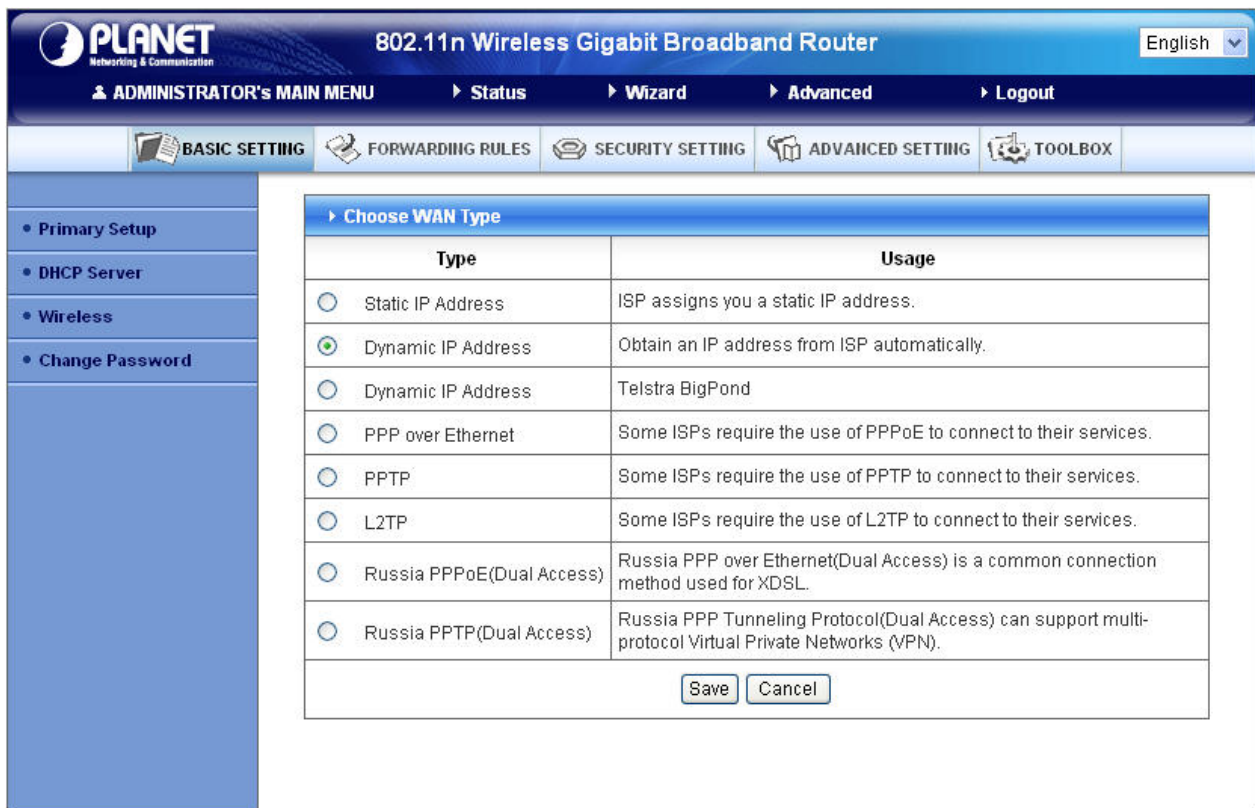
BASIC SETTING | FORWARDING RULES | SECURITY SETTING | ADVANCED SETTING | TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

Item	Setting
LAN IP Address	192.168.0.1
WAN Type	Static IP Address <input type="button" value="Change..."/>
WAN IP Address	0.0.0.0
WAN Subnet Mask	255.255.255.0
WAN Gateway	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
TTL	64 (0-254)
IGMP	<input type="checkbox"/> Enable

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

Click “Change”



PLANET 802.11n Wireless Gigabit Broadband Router

ADMINISTRATOR'S MAIN MENU | Status | Wizard | Advanced | Logout

BASIC SETTING | FORWARDING RULES | SECURITY SETTING | ADVANCED SETTING | TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

Type	Usage
<input type="radio"/> Static IP Address	ISP assigns you a static IP address.
<input checked="" type="radio"/> Dynamic IP Address	Obtain an IP address from ISP automatically.
<input type="radio"/> Dynamic IP Address	Telstra BigPond
<input type="radio"/> PPP over Ethernet	Some ISPs require the use of PPPoE to connect to their services.
<input type="radio"/> PPTP	Some ISPs require the use of PPTP to connect to their services.
<input type="radio"/> L2TP	Some ISPs require the use of L2TP to connect to their services.
<input type="radio"/> Russia PPPoE(Dual Access)	Russia PPP over Ethernet(Dual Access) is a common connection method used for XDSL.
<input type="radio"/> Russia PPTP(Dual Access)	Russia PPP Tunneling Protocol(Dual Access) can support multi-protocol Virtual Private Networks (VPN).

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: Telstra BigPond (Australia's ISP)
  - 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
  - G. Russia PPPoE(Dual Access): Russia PPP over Ethernet(Dual Access) is a common connection method used for XDSL.
  - H. Russia PPTP(Dual Access): Russia PPP Tunneling(Dual Access) can support multi-protocol Virtual Private Network(VPN).

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

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

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

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

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

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

PPPoE Account and Password: the account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it empty.

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

Maximum Idle Time: the amount of time of inactivity before disconnecting your PPPoE session.

Set it to zero or enable Auto-reconnect to disable this feature.

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

Connection Control: There are 3 modes to select:

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

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

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

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

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

My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned to you.

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.

Connection ID: optional. Input the connection ID if your ISP requires it.

Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will connect to ISP automatically, after system is restarted or connection is dropped.

Connection Control: There are 3 modes to select:

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

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

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

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

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

For example: Use Static

My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned to you.

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.

Connection ID: optional. Input the connection ID if your ISP requires it.

Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or enable

Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will connect to ISP automatically, after system is restarted or connection is dropped.

Connection Control: There are 3 modes to select:

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

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

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

### **Russia PPPoE(Dual Access)**

This mode only activate for Russia ISP that support dual layer Access to the Internet.

Please check with your ISP for the detail setting.

### **Russia PPTP(Dual Access)**

This mode only activate for Russia ISP that support dual layer Access to the Internet.

Please check with your ISP for the detail setting.

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

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.



## 2.3.1.2 DHCP Server

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a tree view with 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'DHCP Server' and contains a table with the following items and settings:

Item	Setting
DHCP Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Lease Time	0 Minutes
IP Pool Starting Address	100
IP Pool Ending Address	199
Domain Name	
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Primary WINS	0.0.0.0
Secondary WINS	0.0.0.0
Gateway	0.0.0.0 (optional)

At the bottom of the table are three buttons: 'Save', 'Undo', and 'Clients List...'.

1. **DHCP Server:** Choose “Disable” or “Enable.”
2. **Lease time:** This is the length of time that the client may use the IP address it has been Assigned by dhcp server.
3. **IP pool starting Address/ IP pool starting Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.
4. **Domain Name:** Optional, this information will be passed to the client.
5. **Primary DNS/Secondary DNS:** This feature allows you to assign DNS Servers
6. **Primary WINS/Secondary WINS:** This feature allows you to assign WINS Servers
7. **Gateway:** The Gateway Address would be the IP address of an alternate Gateway.  
This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.
8. **DHCP Client List:** List connected DHCP Clients.

### 2.3.1.3 Wireless

The screenshot shows the configuration interface for a Planet 802.11n Wireless Gigabit Broadband Router. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a tree view with 'Primary Setup', 'DHCP Server', 'Wireless' (highlighted), and 'Change Password'. The main content area is titled 'Wireless Setting' and contains a table of configuration items.

Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Turn off Wireless depend as Schedule Rule	(00)Always <input type="radio"/> Enable <input checked="" type="radio"/> Disable <input type="button" value="Schedule Setting"/>
Network ID(SSID)	default
Wireless Mode	<input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only <input type="radio"/> 11n only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	11
WDS	<input type="button" value="Enter..."/>
WPS	<input type="button" value="Enter..."/>
Security	None

At the bottom of the configuration area are buttons for 'Save', 'Undo', and 'Wireless Client List...'.

Wireless settings allow you to set the wireless configuration items.

**Wireless:** The user can enable or disable wireless function.

**Schedule Setting:** The device can turn off Wireless depend as Schedule.

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

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

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

## WPS (WiFi Protection Setup)

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

The screenshot displays the administrator interface for a Planet 802.11n Wireless Gigabit Broadband Router. The page is titled "Wi-Fi Protected Setup" and is part of the "SECURITY SETTING" menu. The interface includes a navigation bar with options like "ADMINISTRATOR'S MAIN MENU", "Status", "Wizard", "Advanced", and "Logout". A sidebar on the left lists menu items: "Primary Setup", "DHCP Server", "Wireless", and "Change Password".

Item	Setting
▶ WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Setup	<input checked="" type="radio"/> Current AP PIN <input type="radio"/> Configure Wireless Station
▶ Current PIN of the device	<input type="text" value="26264547"/> <input type="button" value="Generate New PIN"/>
▶ WPS state	Idle
▶ WPS status	Configured <input type="button" value="Release"/>

At the bottom of the configuration area, there are three buttons:

## 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.

## Hybrid Mode

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

The screenshot shows the administrator interface for a Planet 802.11n Wireless Gigabit Broadband Router. The main content area is titled "WDS Setting" and includes a table of scanned APs and configuration options.

**WDS Setting** [ HELP ]

Item	Setting
AP Mode:	AP Only
Remote AP MAC MAC 1	<input type="text"/>
MAC 2	<input type="text"/>
MAC 3	<input type="text"/>
MAC 4	<input type="text"/>

Scanned AP's MAC: --- Select one ---  Remote AP MAC: --

SSID	Channel	MAC Address
CHCEL	1	00-18-E7-F0-DB-0A
CL-WLAN	1	00-1A-1E-CE-E6-90
ADW-4401	1	00-30-4F-00-98-50
ADN-4100	6	00-30-4F-F4-BA-81
Qurtoba	7	00-30-4F-01-00-02
juntion_wap	7	00-04-E2-67-5A-03
	10	00-1F-F3-05-AB-35
3Com	11	00-12-A9-D0-82-32
darren1124	11	00-1F-1F-19-B1-61
Narnia	11	00-13-49-36-A8-EE
LAI-STAR	11	00-24-01-A9-F4-A0
CHTN_T07AW	11	00-14-A4-46-C1-3F
HOME-1	11	00-1F-1F-A4-20-BC

**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.

**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

**WPA**

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

Select Encryption and RADIUS Shared Key

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

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

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

### **WPA2-PSK (AES)**

1. Select Pre-share Key Mode

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

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

2. Fill in the key, Ex 12345678

### **WPA2 (AES)**

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

Select RADIUS Shared Key

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

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

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

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

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

1. Select Pre-share Key Mode

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

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

2. Fill in the key, Ex 12345678

### **WPA/WPA2**

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server

The router will detect automatically which Security type(Wpa-psk version 1 or 2) the client uses to encrypt. IP address or the 802.1X server's domain-name.

Select RADIUS Shared Key

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

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

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

## Wireless Client List

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'Wireless Client List' and contains a table with two columns: 'Connected Time1' and 'MAC Address'. The table lists three entries, all with a connection time of 'Sun May 31 23:37:24 2009'. The MAC addresses are '00-13-02-BA-26-7D', '00-18-DE-AC-6E-CE', and '00-18-DE-DD-F4-6E'. At the bottom of the table are 'Back' and 'Refresh' buttons.

Connected Time1	MAC Address
Sun May 31 23:37:24 2009	00-13-02-BA-26-7D
Sun May 31 23:37:24 2009	00-18-DE-AC-6E-CE
Sun May 31 23:37:24 2009	00-18-DE-DD-F4-6E

## 2.3.1.4 Change Password

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface for the 'Change Password' page. The navigation and sidebar elements are identical to the previous screenshot. The main content area is titled 'Change Password' and contains a table with two columns: 'Item' and 'Setting'. The table has three rows: 'Old Password', 'New Password', and 'Reconfirm', each with an adjacent text input field. At the bottom of the table are 'Save' and 'Undo' buttons.

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

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

## 2.3.2 Forwarding Rules

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router web interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this, a secondary menu contains 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar lists 'Virtual Server', 'Special AP', and 'Miscellaneous'. The main content area is titled 'Forwarding Rules' and contains the following information:

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

### 2.3.2.1 Virtual Server

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router web interface, specifically the 'Virtual Server' configuration page. The top navigation bar and secondary menu are identical to the previous screenshot. The left sidebar lists 'Virtual Server', 'Special AP', and 'Miscellaneous', with 'Virtual Server' being the active selection. The main content area is titled 'Virtual Server' and includes a '[ HELP ]' link. It features a 'Well known services' dropdown menu (currently set to '-- select one --') and a 'Schedule rule' dropdown menu (currently set to '(00)Always'). Below these is a 'Copy to ID' dropdown menu. The main configuration area is a table with 10 rows, each representing a virtual server entry. The table has the following columns: ID, Server IP, Service Ports, Protocol, Enable, and Schedule Rule#. At the bottom of the table are 'Next >>', 'Save', and 'Undo' buttons.

ID	Server IP	Service Ports	Protocol	Enable	Schedule Rule#
1	192.168.0. <input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
2	192.168.0. <input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
3	192.168.0. <input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
4	192.168.0. <input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
5	192.168.0. <input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
6	192.168.0. <input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
7	192.168.0. <input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
8	192.168.0. <input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
9	192.168.0. <input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
10	192.168.0. <input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>



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**.

### 2.3.2.2 Special AP

The screenshot shows the 'Special Applications' configuration page in the router's web interface. The page has a sidebar on the left with 'Special AP' selected. The main content area contains a table with 8 rows for configuring applications. Each row has columns for ID, Trigger, Incoming Ports, and Enable. The 'Trigger' column contains the value '65535' for all rows. The 'Incoming Ports' column contains the value '0' for all rows. The 'Enable' column contains a checkbox for each row, all of which are currently unchecked. At the bottom of the table are 'Save' and 'Undo' buttons.

ID	Trigger	Incoming Ports	Enable
1	65535	0	<input type="checkbox"/>
2	65535	0	<input type="checkbox"/>
3	65535	0	<input type="checkbox"/>
4	65535	0	<input type="checkbox"/>
5	65535	0	<input type="checkbox"/>
6	65535	0	<input type="checkbox"/>
7	65535	0	<input type="checkbox"/>
8	65535	0	<input type="checkbox"/>

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

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

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

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

### 2.3.2.3 Miscellaneous Items

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this, there are tabs for 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar has a menu with 'Virtual Server', 'Special AP', and 'Miscellaneous' (which is selected). The main content area displays the 'Miscellaneous Items' configuration table.

Item	Setting	Enable
IP Address of DMZ Host	192.168.0. <input type="text"/>	<input type="checkbox"/>
Super DMZ(IP Passthrough)	<input type="text"/>	<input type="checkbox"/>
Non-standard FTP port	<input type="text"/>	
UPnP setting		<input checked="" type="checkbox"/>
Xbox Support		<input checked="" type="checkbox"/>

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

#### 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.**

#### Super DMZ (IP Pass through)

Super DMZ (IP Pass through) is a useful feature if a host computer or server on the Local Area Network needs to have access into it from the internet with a real public IP address. With IP Pass through configured, all IP traffic, not just TCP/UDP, is forwarded back to the host computer. This can be necessary with certain types of software that do not function reliably through Network Address Translation.

#### Non-standard FTP port

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

#### Xbox Support

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

## UPnP Setting

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



## 2.3.3 Security Settings

A screenshot of the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The interface is in English and shows the "ADMINISTRATOR's MAIN MENU" with options for Status, Wizard, Advanced, and Logout. The "SECURITY SETTING" tab is selected, and the "Security Setting" page is displayed. The page contains a list of security features: Packet Filters, Domain Filters, URL Blocking, Internet Address Control, and Miscellaneous. Each feature has a brief description of its function.

**Planet** Networking & Communication  
802.11n Wireless Gigabit Broadband Router  
English

ADMINISTRATOR's MAIN MENU | Status | Wizard | Advanced | Logout

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

**Security Setting**

- **Packet Filters**
  - 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 Filters**
  - Let you prevent users under this device from accessing specific URLs.
- **URL Blocking**
  - URL Blocking will block LAN computers to connect to pre-defined websites.
- **Internet Address Control**
  - The device provides "Administrator MAC Control" for specific MAC to access the device or Internet without restriction. It also provides 3 features to access Internet: MAC Control by host, Group MAC Control and Interface Access Control depend as user-defined time Schedule.
- **Miscellaneous**
  - Remote Administrator Host: 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.
  - Administrator Time-out: The amount of time of inactivity before the device will automatically close the Administrator session. Set this to zero to disable it.
  - Discard PING from WAN side: When this feature is enabled, hosts on the WAN cannot ping the Device.

### 2.3.3.1 Packet Filters

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The top navigation bar includes 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main menu is divided into 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar shows 'Packet Filters' selected, with other options like 'Domain Filters', 'URL Blocking', 'Internet Access Control', and 'Miscellaneous'. The main content area is titled 'Outbound Packet Filter' and contains the following configuration options:

- Item:** Outbound Filter
- Setting:**  Enable
- Policy:**
  - Allow all to pass except those match the following rules.
  - Deny all to pass except those match the following rules.
- Block List:** -- select one --
- Schedule rule:** (00)Always  ID --

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

At the bottom of the configuration area are buttons for 'Save', 'Undo', and 'Inbound Filter...'.

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:**

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main menu tabs are 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar lists 'Packet Filters', 'Domain Filters', 'URL Blocking', 'Internet Access Control', and 'Miscellaneous'. The main content area is titled 'Inbound Packet Filter' and contains the following configuration options:

- Enable
- Allow all to pass except those match the following rules.
- Deny all to pass except those match the following rules.
- Schedule rule: (00)Always (dropdown) Copy to ID -- (dropdown)

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

Buttons at the bottom: Save, Undo, Outbound Filter...

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

(1.2.3.10-1.2.3.20) Remote hosts can do everything (block nothing) Others are all blocked.

**Example 2:**

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The top navigation bar includes 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a list of menu items: 'Packet Filters', 'Domain Filters', 'URL Blocking', 'Internet Access Control', and 'Miscellaneous'. The main content area is titled 'Inbound Packet Filter' and includes a '[ HELP ]' link. It features a table with columns 'Item' and 'Setting'. The 'Inbound Filter' is currently disabled. There are two radio buttons for filtering rules: 'Allow all to pass except those match the following rules.' (selected) and 'Deny all to pass except those match the following rules.'. Below this is a 'Schedule rule' dropdown set to '(00)Always' and a 'Copy to ID' dropdown set to '--'. A table with 8 rows follows, with columns 'ID', 'Source IP', 'Destination IP : Ports', 'Enable', and 'Schedule Rule#'. All 'Enable' checkboxes are unchecked. At the bottom are 'Save', 'Undo', and 'Outbound Filter...' buttons.

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

Others are all allowed.

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

**Outbound Filter:**

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

**Example 1:**

Router LAN IP is 192.168.12.254

The screenshot shows the 'Outbound Packet Filter' configuration page. The 'Enable' checkbox is checked. Below it, there are radio buttons for 'Allow all to pass except those match the following rules.' (selected) and 'Deny all to pass except those match the following rules.'. There are also dropdown menus for 'Block List' (set to '-- select one --') and 'Schedule rule' (set to '(00)Always'). A 'Copy to ID' dropdown is also present.

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

Buttons at the bottom: Save, Undo, Inbound Filter...

(192.168.12.100-192.168.12.149) Located hosts are only allowed to send mail (port 25), receive mail (port 110), and browse Internet (port 80); port 53 (DNS) is necessary to resolve the domain name.

(192.168.12.10-192.168.12.20) Located hosts can do everything (block nothing)  
Others are all blocked.

Example 2:

Router LAN IP is 192.168.12.254

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a tree view with 'Packet Filters' selected. The main content area is titled 'Outbound Packet Filter' and includes a '[ HELP ]' link. It features a table with columns 'Item' and 'Setting'. The 'Outbound Filter' is currently disabled. There are radio buttons for 'Allow all to pass except those match the following rules.' (selected) and 'Deny all to pass except those match the following rules.'. Below these are dropdown menus for 'Block List' (set to '-- select one --') and 'Schedule rule' (set to '(00)Always'). A 'Copy to ID' dropdown is also present. A table with 8 rows follows, with columns 'ID', 'Source IP', 'Destination IP : Ports', 'Enable', and 'Schedule Rule#'. All 'Enable' checkboxes are unchecked. At the bottom are 'Save', 'Undo', and 'Inbound Filter...' buttons.

(192.168.12.100 and 192.168.12.119) Located Hosts can do everything except read net news (port 119) and transfer files via FTP (port 21)

Others are allowed

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



## 2.3.3.2 Domain filters

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router web interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains 'Packet Filters', 'Domain Filters' (highlighted), 'URL Blocking', 'Internet Access Control', and 'Miscellaneous'. The main content area is titled 'Domain Filter' and contains the following configuration options:

- Domain Filter:**  Enable
- Log DNS Query:**  Enable
- Privilege IP Addresses Range:** From  To

Below these options is a table with 10 rows for defining domain filter rules:

ID	Domain Suffix	Action	Enable	Schedule Rule#
1	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
9	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
10	* (all others)	<input type="checkbox"/> Drop <input type="checkbox"/> Log	-	<input type="text" value="0"/>

At the bottom of the table are 'Save' and 'Undo' buttons.

### 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:

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The top navigation bar includes 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a tree view with 'Domain Filters' selected. The main content area is titled 'Domain Filter' and contains a configuration table.

Item		Setting		
Domain Filter		<input type="checkbox"/> Enable		
Log DNS Query		<input type="checkbox"/> Enable		
Privilege IP Addresses Range		From <input type="text" value="0"/> To <input type="text" value="0"/>		
ID	Domain Suffix	Action	Enable	Schedule Rule#
1	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
9	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
10	* (all others)	<input type="checkbox"/> Drop <input type="checkbox"/> Log	-	<input type="text" value="0"/>

At the bottom of the table are 'Save' and 'Undo' buttons.

In this example:

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

### 2.3.3.3 URL Blocking

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The top navigation bar includes 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a tree view with 'Packet Filters', 'Domain Filters', 'URL Blocking' (highlighted), 'Internet Access Control', and 'Miscellaneous'. The main content area is titled 'URL Blocking' and includes a '[ HELP ]' link. It features a table with columns 'ID', 'URL', 'Enable', and 'Schedule Rule#'. The 'Enable' column contains checkboxes, and the 'Schedule Rule#' column contains input boxes with the value '0'. At the bottom of the table are 'Save' and 'Undo' buttons.

ID	URL	Enable	Schedule Rule#
1	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
9	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
10	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>

**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 it 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.

PLANET Networking & Communication 802.11n Wireless Gigabit Broadband Router English

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Packet Filters
- Domain Filters
- URL Blocking
- Internet Access Control
- Miscellaneous

URL Blocking [HELP]

Item		Setting	
URL Blocking		<input type="checkbox"/> Enable	
ID	URL	Enable	Schedule Rule#
1	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
9	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
10	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>

Save Undo

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

### 2.3.3.4 Internet Access Control

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

#### Administrator MAC Control

Regardless the MAC access configuration of administrator, specific MAC can access the device.

The screenshot shows the web management interface of a Planet 802.11n Wireless Gigabit Broadband Router. The interface is in English and includes a navigation menu with options like Administrator's MAIN MENU, Status, Wizard, Advanced, and Logout. The main menu is divided into sections: BASIC SETTING, FORWARDING RULES, SECURITY SETTING (selected), ADVANCED SETTING, and TOOLBOX. Under SECURITY SETTING, the 'Internet Access Control' option is highlighted. The configuration page for 'Administrator MAC Control' is displayed, featuring a table with columns for ID, MAC Address, and Enable. There are three rows for ID 1, 2, and 3, each with an empty MAC Address input field and an unchecked 'Enable' checkbox. A 'DHCP clients' dropdown menu is set to '--- Select one ---', and a 'Copy to ID' dropdown is set to '--'. Below the table are 'Save' and 'Undo' buttons. The 'Internet Access Control' section below shows 'Access Control Type' with three radio button options: 'MAC Access Control', 'Group MAC Access Control', and 'Interface Access Control'. A 'Next >>' button is at the bottom.

This device can record 3 sets. When the host(should be admin) logs Web management, the device will record MAC address of this host. Before this host configures Internet Access Control , Suggest end-user to enable this feature, first.

## 1. MAC control

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a list of menu items: 'Packet Filters', 'Domain Filters', 'URL Blocking', 'Internet Access Control' (highlighted with a mouse cursor), and 'Miscellaneous'. The main content area is titled 'MAC Address Control' and includes a '[ HELP ]' link. It features several settings: 'MAC Address Control' (checked 'Enable'), 'Connection control' (unchecked), and 'Association control' (unchecked). Below these are fields for 'DHCP clients' and 'Schedule rule'. At the bottom is a table with columns for ID, MAC Address, IP Address, C, A, and Schedule Rule#. The table contains four rows, each with a MAC address field, an IP address field (192.168.0.), and a '0' in the Schedule Rule# column. At the bottom of the page are buttons for '<< Previous', 'Next >>', 'Save', and 'Undo'.

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

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

**Connection control** Check "Connection control" to enable the controlling of which wired and wireless clients can connect to this device. If a client is denied to connect to this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect to this device.

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

**Control table**

ID	MAC Address	IP Address	C	A	Schedule Rule#
1	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>

"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:

<b>MAC Address</b>	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.
<b>C</b>	When " <b>Connection control</b> " is checked, check " <b>C</b> " will allow the corresponding client to connect to this device.
<b>A</b>	When " <b>Association control</b> " is checked, check " <b>A</b> " 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:**

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The main menu includes: ADMINISTRATOR'S MAIN MENU, Status, Wizard, Advanced, Logout. The sub-menu includes: BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING, TOOLBOX. The left sidebar shows: Packet Filters, Domain Filters, URL Blocking, Internet Access Control (selected), Miscellaneous. The main content area is titled "MAC Address Control" and contains the following settings:

- MAC Address Control:  Enable
- Connection control:  Wireless and wired clients with **C** checked can connect to this device; and **allow** unspecified MAC addresses to connect.
- Association control:  Wireless clients with **A** checked can associate to the wireless LAN; and **deny** unspecified MAC addresses to associate. **Note: Association control has no effect on wired clients.**

Additional settings include: DHCP clients: --- Select one ---; Schedule rule: (00)Always; Copy to: ID --.

ID	MAC Address	IP Address	C	A	Schedule Rule#
1	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>

Buttons at the bottom: << Previous, Next >>, Save, Undo.

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" --> 192.168.12.100
  - ID 3 - "00-98-76-54-32-10" --> 192.168.12.101
 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 (192.168.12.101), 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.

## 2. Group MAC Access Control

Administrator can define hosts in which Group to allow Internet. For example, Father and Mother are in Group1 without limitation and hosts Brother and Sister are in Group2 to access according as Schedule Rule2.

For example,

Schedule Rule 1 sets “always” everyday with limitation.

Schedule Rule 2 sets 08:00~23:00 Monday ~ Friday.

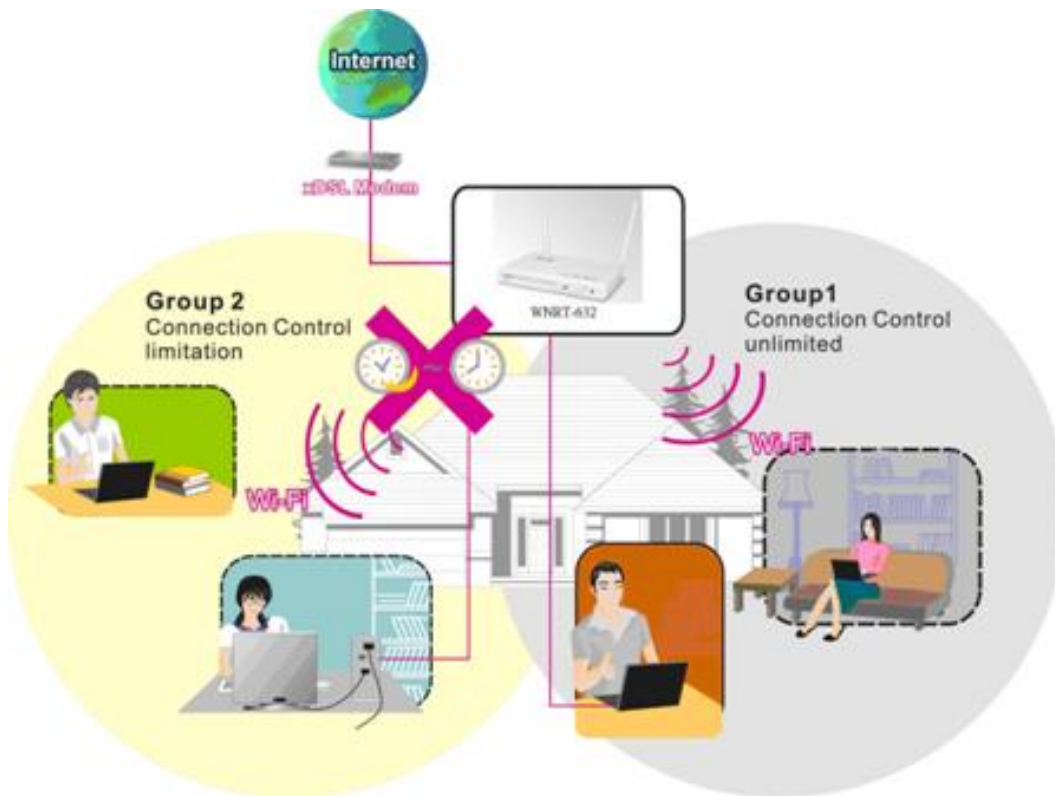
The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a list of settings: 'Packet Filters', 'Domain Filters', 'URL Blocking', 'Internet Access Control', and 'Miscellaneous'. The main content area is titled 'Group MAC Access Control' and contains a table with the following structure:

Item	Setting
Group MAC Access Control	<input type="checkbox"/> Enable

Below the table are 'Save' and 'Undo' buttons. Underneath is a section titled 'Add Member to Group List' with the following form fields:

Add MAC Address -  << Copy --- Select one ---

to Group  and apply schedule rule  Add



### 3. Interface Access Control

The device defines 5 Interfaces as Lan1,Lan2, Lan3,Lan4 and WiFi. The device allows different interface to access Internet by time schedule

For example,

Schedule Rule 1 sets “always” everyday with limitation.

Schedule Rule 2 sets 08:00~23:00 Monday ~ Friday.

Administrator can set guests in Lan3 and Lan4 to access Internet according as Schedule Rule

2. Set Friends in Lan1 ,Lan2 and WiFi according as Schedule Rule 1.

**PLANET** Networking & Communication  
**802.11n Wireless Gigabit Broadband Router** English

ADMINISTRATOR's MAIN MENU    ▶ Status    ▶ Wizard    ▶ Advanced    ▶ Logout

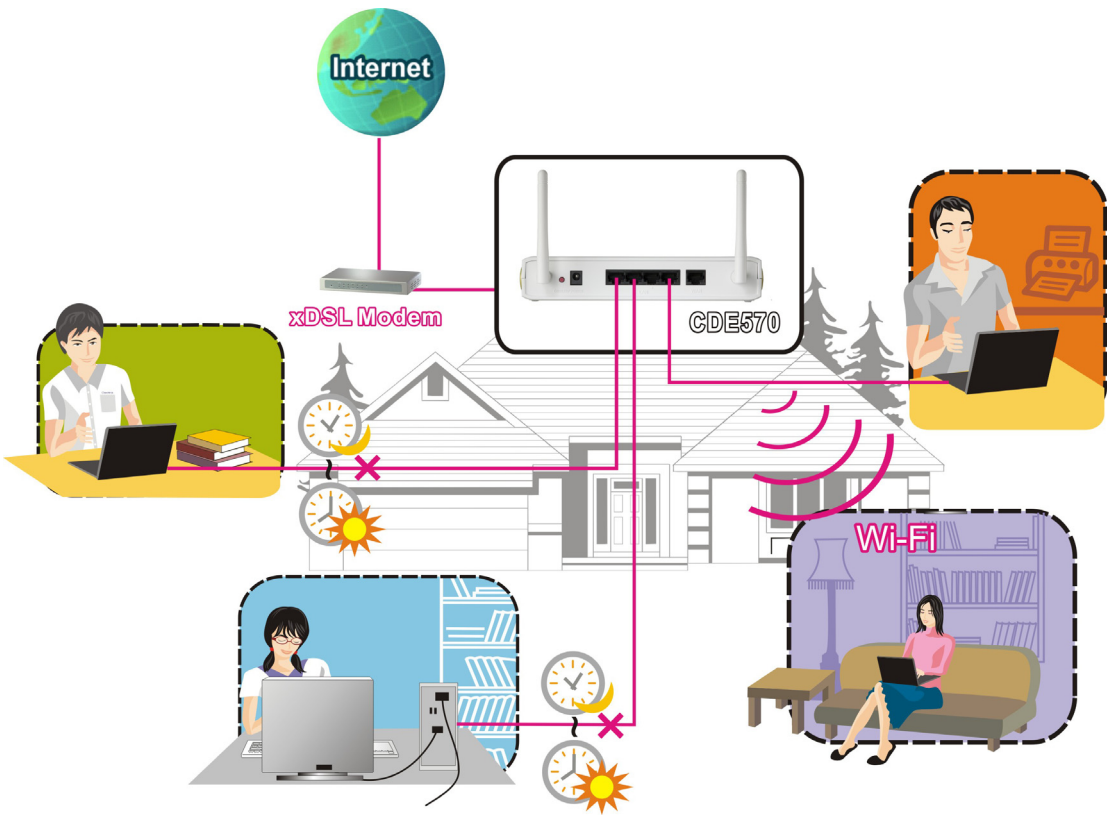
BASIC SETTING    FORWARDING RULES    SECURITY SETTING    ADVANCED SETTING    TOOLBOX

- Packet Filters
- Domain Filters
- URL Blocking
- Internet Access Control
- Miscellaneous

**Interface Access Control** [ HELP ]

Item	Setting	
Interface Access Control	<input type="checkbox"/> Enable	
Interface	Schedule Rule	Deny
Port 1	(00)Always	<input checked="" type="checkbox"/>
Port 2	(00)Always	<input checked="" type="checkbox"/>
Port 3	(00)Always	<input checked="" type="checkbox"/>
Port 4	(00)Always	<input checked="" type="checkbox"/>
Wireless	(00)Always	<input checked="" type="checkbox"/>

Save    Undo



### 2.3.3.5 Miscellaneous Items

The screenshot shows the PLANET 802.11n Wireless Gigabit Broadband Router web interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar lists configuration categories: 'Packet Filters', 'Domain Filters', 'URL Blocking', 'Internet Access Control', and 'Miscellaneous'. The 'Miscellaneous' category is selected, displaying a table of settings:

Item	Setting	Enable
▶ Remote Administrator Host / Port	0.0.0.0 / 88	<input type="checkbox"/>
▶ Administrator Time-out	600 seconds (0 to disable)	
▶ Discard PING from WAN side		<input type="checkbox"/>
▶ SPI mode		<input type="checkbox"/>
▶ DoS Attack Detection		<input type="checkbox"/>
▶ VPN PPTP Pass-Through		<input checked="" type="checkbox"/>
▶ VPN IPsec Pass-Through		<input checked="" type="checkbox"/>

At the bottom of the table are 'Save' and 'Undo' buttons.

#### 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.

## VPN IPSec Pass-Through

It is a setting/feature on routers which is required to implement secure exchange of packets at the IP layer and allow IPSec tunnels to pass through the router.

## VPN PPTP Pass-Through

It is a setting/feature on routers which is required in order to connect to a Remote PPTP VPN account.

## 2.3.4 Advanced Settings

The screenshot displays the web-based configuration interface for a Planet 802.11n Wireless Gigabit Broadband Router. The top navigation bar includes the Planet logo, the router model name, a language dropdown set to English, and menu items for Administrator's Main Menu, Status, Wizard, Advanced, and Logout. Below this is a secondary menu with icons for Basic Setting, Forwarding Rules, Security Setting, Advanced Setting (which is highlighted), and Toolbox. On the left side, a vertical sidebar lists various configuration categories: System Time, System Log, Dynamic DNS, QoS Rule, SNMP, Routing, and Schedule Rule. The main content area is titled 'Advanced Setting' and contains a list of configuration options with brief descriptions:

- System Time**: 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**: To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).
- QoS Rule**: Quality of Service can provide different priority to different users or data flows, or guarantee a certain level of performance.
- SNMP**: Gives a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.
- Routing**: 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.
- Schedule Rule**: Apply schedule rules to Packet Filters and Virtual Server.

## 2.3.4.1 System Time

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar lists various settings, with 'System Time' selected. The main content area is titled 'System Time' and contains the following configuration options:

Item	Setting
System Time	Monday, June 01, 2009 12:22:52 AM
<input type="radio"/> Get Date and Time by NTP Protocol	<input type="button" value="Sync Now!"/>
Time Server	time.nist.gov
Time Zone	(GMT-08:00) Pacific Time (US & Canada)
<input type="radio"/> Set Date and Time using PC's Date and Time	
PC Date and Time	Friday, September 17, 2010 10:45:36 AM
<input checked="" type="radio"/> Set Date and Time manually	
Date	Year: 2009, Month: Jun, Day: 01
Time	Hour: 0 (0-23), Minute: 0 (0-59), Second: 0 (0-59)
Daylight Saving	<input type="radio"/> Enable, <input checked="" type="radio"/> Disable
Start	Month: Jan, Day: 01, Hour: 00
End	Month: Jan, Day: 01, Hour: 00

At the bottom of the configuration area are 'Save' and 'Undo' buttons.

### 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.

## 2.3.4.2 System Log

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a list of menu items: 'System Time', 'System Log' (highlighted with a mouse cursor), 'Dynamic DNS', 'QoS Rule', 'SNMP', 'Routing', and 'Schedule Rule'. The main content area is titled 'System Log' and contains a table with the following items and settings:

Item	Setting	Enable
IP Address of Syslog Server	192.168.0. <input type="text"/>	<input type="checkbox"/>
E-mail Alert	<input type="button" value="Send Mail Now"/>	<input type="checkbox"/>
• SMTP Server IP/Port	<input type="text"/>	
• E-mail addresses	<input type="text"/>	
• E-mail Subject	<input type="text"/>	
• User name	<input type="text"/>	
• Password	<input type="text"/>	
Log Type	<input checked="" type="checkbox"/> System Activity <input checked="" type="checkbox"/> Debug Information <input checked="" type="checkbox"/> Attacks <input checked="" type="checkbox"/> Dropped Packets <input checked="" type="checkbox"/> Notice	

At the bottom of the configuration area, there are three buttons: 'View Log...', 'Save', and 'Undo'.

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

### IP Address for Syslog

Host IP of destination where syslog 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 concatenated 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.

### 2.3.4.3 DDNS Service

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a list of menu items: 'System Time', 'System Log', 'Dynamic DNS' (highlighted with a mouse cursor), 'QoS Rule', 'SNMP', 'Routing', and 'Schedule Rule'. The main content area is titled 'Dynamic DNS' and contains a table with the following structure:

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

At the bottom of the table are 'Save' and 'Undo' buttons.

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.



## 2.3.4.4 SNMP

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

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

### Enable SNMP

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

### Get Community

Setting the community of GetRequest your device will response.

### Set Community

Setting the community of SetRequest your device will accept.

### IP 1, IP 2, IP 3, IP 4

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

### SNMP Version

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

## 2.3.4.5 Routing

The screenshot shows the PLANET 802.11n Wireless Gigabit Broadband Router administrator interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this, there are tabs for 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a menu with items like 'System Time', 'System Log', 'Dynamic DNS', 'QoS Rule', 'SNMP', 'Routing', and 'Schedule Rule'. The 'Routing' item is selected and highlighted.

The main content area is titled 'Routing Table' and includes a '[ HELP ]' link. It contains the following settings:

- Dynamic Routing:**  Disable  RIPv1  RIPv2
- Static Routing:**  Disable  Enable

Below these settings is a table for configuring static routing rules:

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

At the bottom of the table are 'Save' and 'Undo' buttons.

**Routing Tables** allow you to determine which physical interface address to use for outgoing IP data grams. If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.

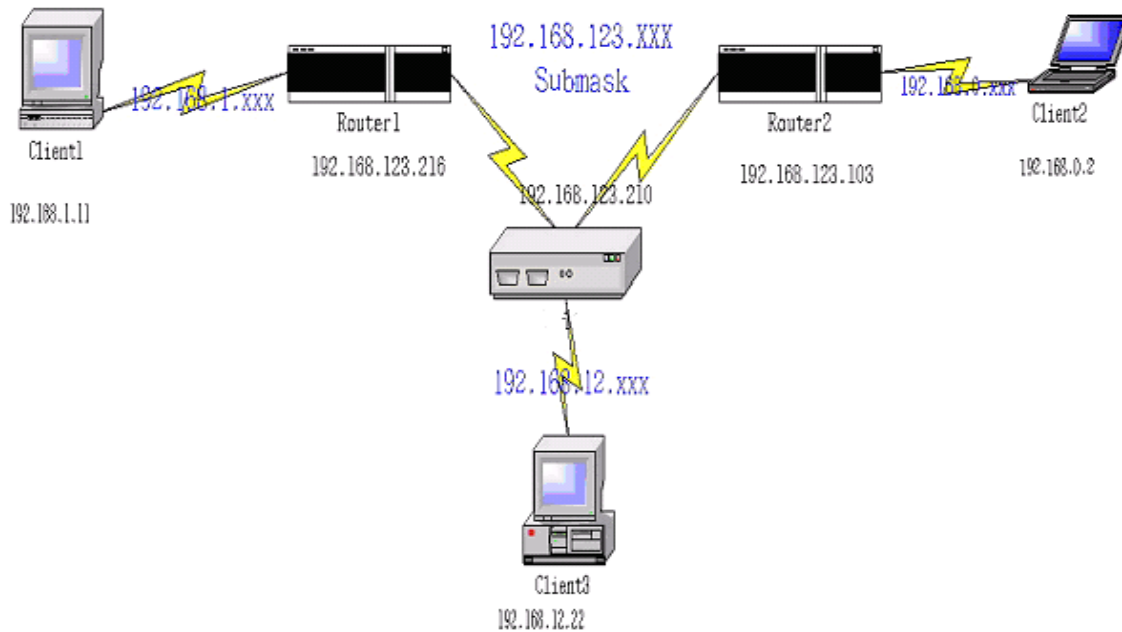
Routing Table settings are settings used to setup the functions of static.

### Dynamic Routing

Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnet in your network. Otherwise, please select RIPv1 if you need this protocol.

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

**Example:**



Configuration on NAT Router

Destination	SubnetMask	Gateway	Hop	Enabled
192.168.1.0	255.255.255.0	192.168.123.216	1	✓
192.168.0.0	255.255.255.0	192.168.123.103	1	✓

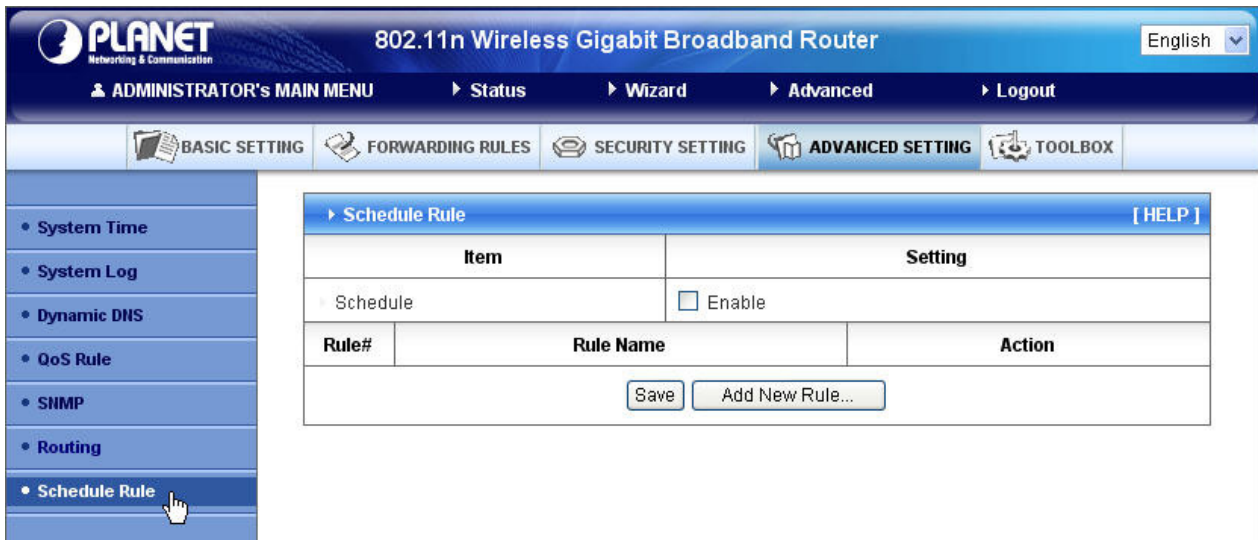
So if, for example, the client3 wanted to send an IP data gram to 192.168.0.2, it would use the above table to determine that it had to go via 192.168.123.103 (a gateway).

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.

### 2.3.4.6 Schedule Rule



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

#### Schedule Enable

Selected if you want to Enable the Scheduler.

#### Edit

To edit the schedule rule.

#### Delete

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

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

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

### 2.3.4.7 QoS Rule

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a list of configuration options: 'System Time', 'System Log', 'Dynamic DNS', 'QoS Rule' (highlighted), 'SNMP', 'Routing', and 'Schedule Rule'. The main content area is titled 'QoS Rule' and contains a table with columns: ID, Local IP, Remote IP : Ports, QoS Priority, Enable, and Schedule Rule#. There are 8 rows in the table, each with input fields for the first five columns and a '0' in the 'Schedule Rule#' column. Above the table, there are controls for 'Well known services' (a dropdown menu) and 'Schedule rule' (a dropdown menu set to '(00)Always' and a 'Copy to ID' dropdown). A 'QoS Control' section has an 'Enable' checkbox. At the bottom of the configuration area are 'Save' and 'Undo' buttons.

**Local IP:**

Please input Client IP, ex:192.168.12.33.

**Remote Priority:**

Please input Global IP and port, ex:168.96.2.3 and port 21

## 2.3.5 Toolbox

The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The top navigation bar includes the Planet logo, the router model name, and a language dropdown set to English. Below this is the 'ADMINISTRATOR's MAIN MENU' with links to Status, Wizard, Advanced, and Logout. A secondary menu contains icons for BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING, and TOOLBOX. The left sidebar lists menu items: View Log, Firmware Upgrade, Backup Setting, Reset to Default, Reboot, and Miscellaneous. The main content area displays the 'Toolbox' section with a list of functions:

- View Log**
  - View the system logs.
- Firmware Upgrade**
  - Prompt the administrator for a file and upgrade it to this device.
- Backup Setting**
  - Save the settings of this device to a file.
- Reset to Default**
  - Reset the settings of this device to the default values.
- Reboot**
  - Reboot this device.
- Miscellaneous**
  - MAC Address for Wake-on-LAN: Let you to power up another network device remotely.
  - Domain Name or IP address for Ping Test: Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

### 2.3.5.1 View Log

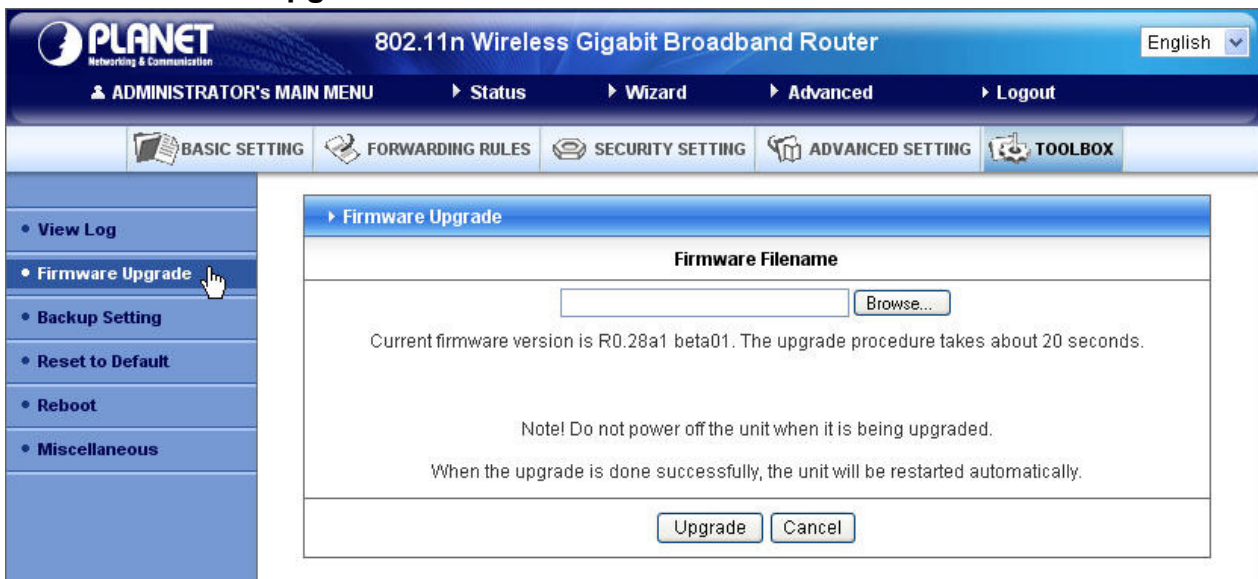
The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface with the 'View Log' function selected. The left sidebar shows 'View Log' highlighted with a mouse cursor. The main content area displays the 'System Log' section with a table of log entries:

System Log	
Item	Info
WAN Type	Static IP Address (R0.28a1 beta01)
Display time	Mon Jun 01 00:35:06 2009
Time	Log

Below the table are three buttons: Refresh, Download, and Clear logs.

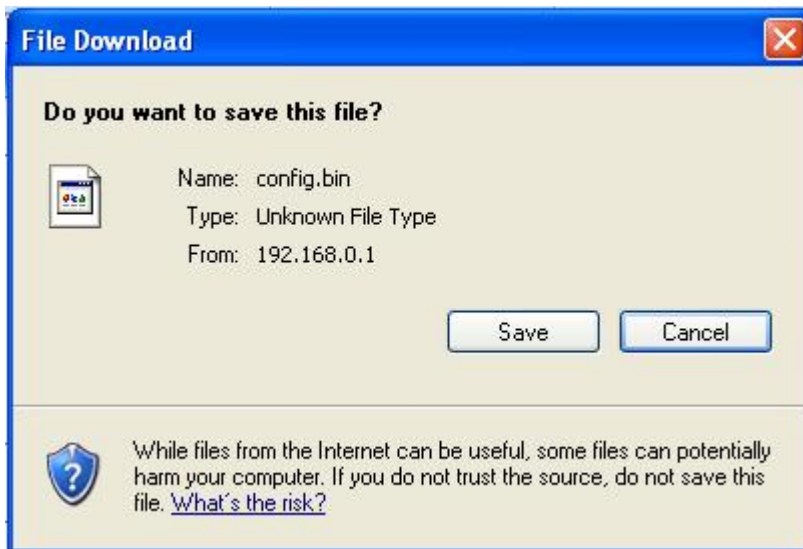
You can View system log by clicking the **View Log** button.

### 2.3.5.2 Firmware Upgrade



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

### 2.3.5.3 Backup Setting



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

### 2.3.5.4 Reset to default



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

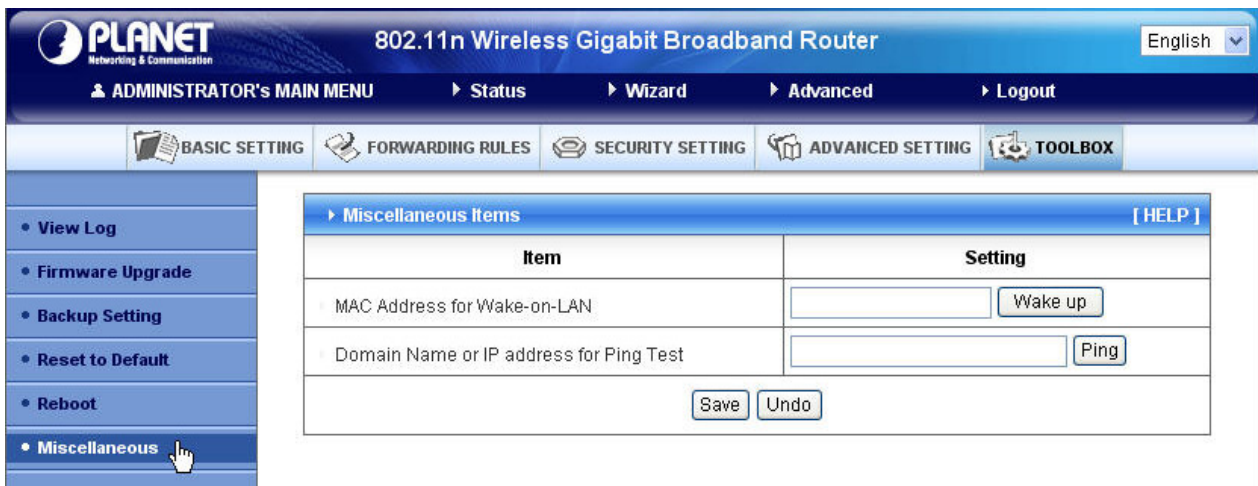
### 2.3.5.5 Reboot



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



## 2.3.5.6 Miscellaneous Items



The screenshot shows the Planet 802.11n Wireless Gigabit Broadband Router administrator interface. The top navigation bar includes the Planet logo, the router model name, a language dropdown set to English, and menu items for Administrator's Main Menu, Status, Wizard, Advanced, and Logout. Below this is a secondary menu with icons for Basic Setting, Forwarding Rules, Security Setting, Advanced Setting, and Toolbox. On the left side, a vertical menu lists various system functions: View Log, Firmware Upgrade, Backup Setting, Reset to Default, Reboot, and Miscellaneous (which is currently selected and highlighted with a mouse cursor). The main content area displays the 'Miscellaneous Items' configuration page, which includes a table with two columns: 'Item' and 'Setting'. The table contains two rows: one for 'MAC Address for Wake-on-LAN' with a text input field and a 'Wake up' button, and another for 'Domain Name or IP address for Ping Test' with a text input field and a 'Ping' button. At the bottom of the table are 'Save' and 'Undo' buttons. A '[ HELP ]' link is located in the top right corner of the table area.

### MAC Address for Wake-on-LAN

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

### Domain Name or IP Address for Test

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

# Appendices and Index

## 802.1x Setting

### 1. Equipment Details

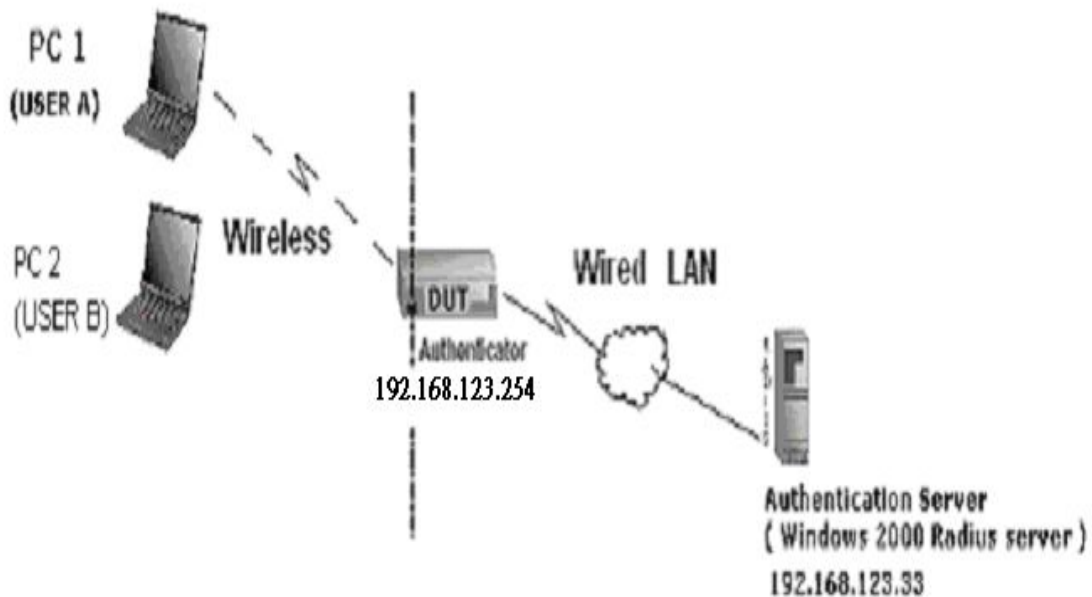


Figure 1: Testing Environment (Use Windows 2000 Radius Server)

#### PC1:

Microsoft Windows XP Professional without Service Pack 1.

#### PC2:

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

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

Note. Windows 2000 RADIUS server only supports PEAP after upgrade to service pack 3 and

HotFix Q313664 (You can get more information from

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

## 2. DUT

### Configuration:

- 1.Enable DHCP server.
- 2.WAN setting: static IP address.
- 3.LAN IP address: 192.168.0.1/24.
- 4.Set RADIUS server IP.
- 5.Set RADIUS server shared key.
- 6.Configure WEP key and 802.1X setting.

The following test will use the inbuilt 802.1X authentication method such as ,EAP\_TLS, PEAP\_CHAPv2(Windows XP with SP1 only), and PEAP\_TLS(Windows XP with SP1 only) using the Smart Card or other Certificate of the Windows XP Professional.

## 3. DUT and Windows 2000 Radius Server Setup

### 3-1-1. Setup Windows 2000 RADIUS Server

We have to change authentication method to MD5\_Challenge or using smart card or other certificate on RADIUS server according to the test condition.

### 3-1-2. Setup DUT

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

### 3-1-3. Setup Network adapter on PC

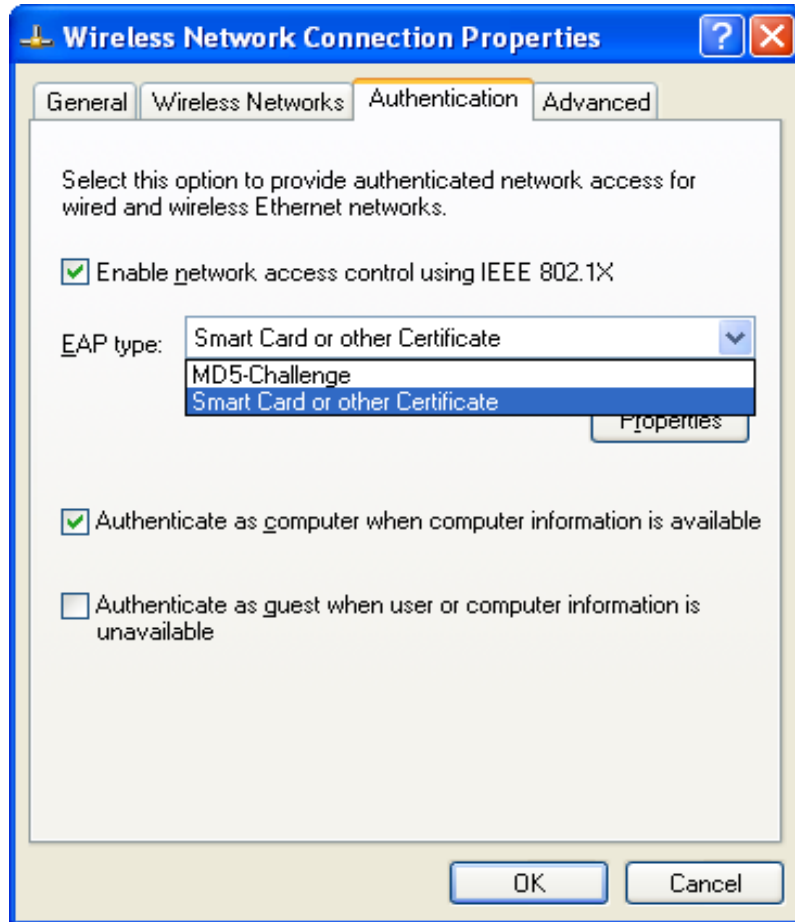
- 1.Choose the IEEE802.1X as the authentication method. (Fig 2)

#### Note.

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

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

3. If choosing to use a smart card or certificate as the EAP type, we select to use a certificate on this computer. (Fig 3)
4. We will change EAP type to fit the variable test condition.



**Figure 2: Enable IEEE 802.1X access control**

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

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

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

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

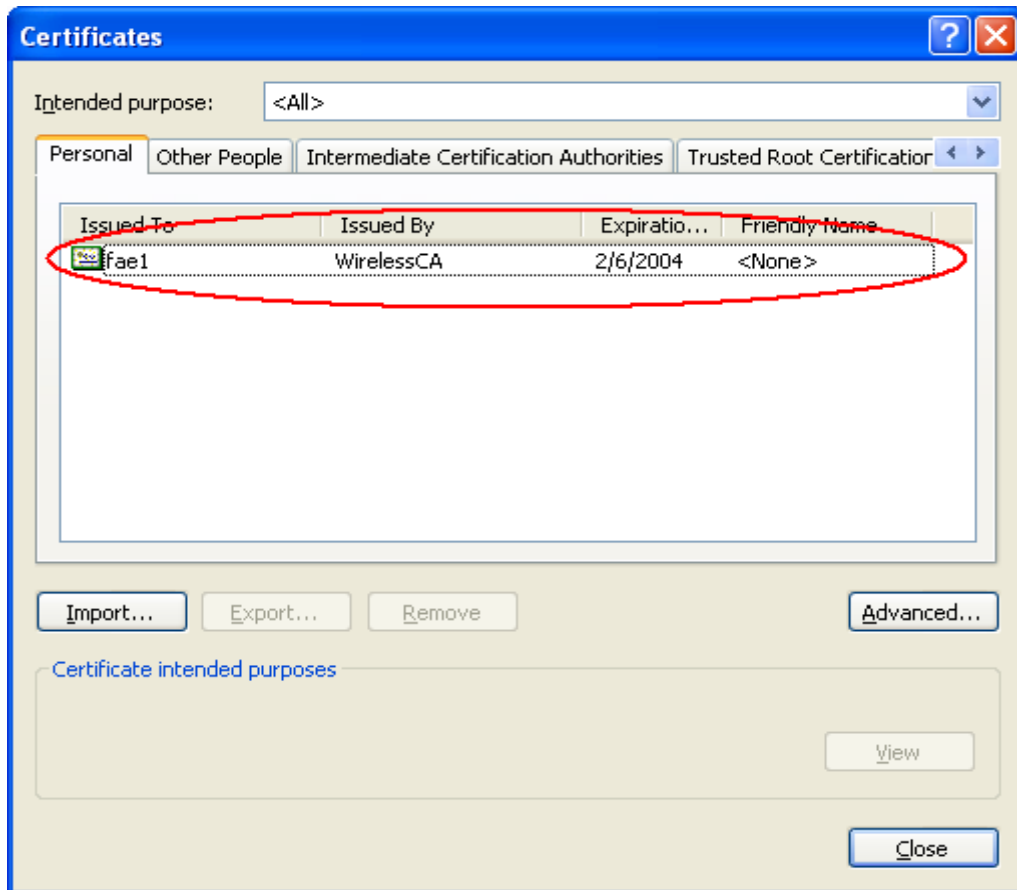


Figure 4: Certificate information on PC1

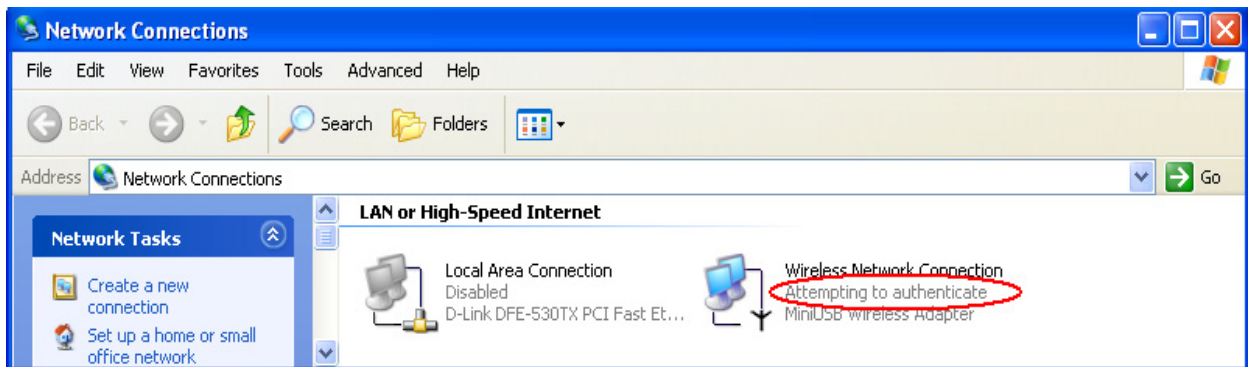
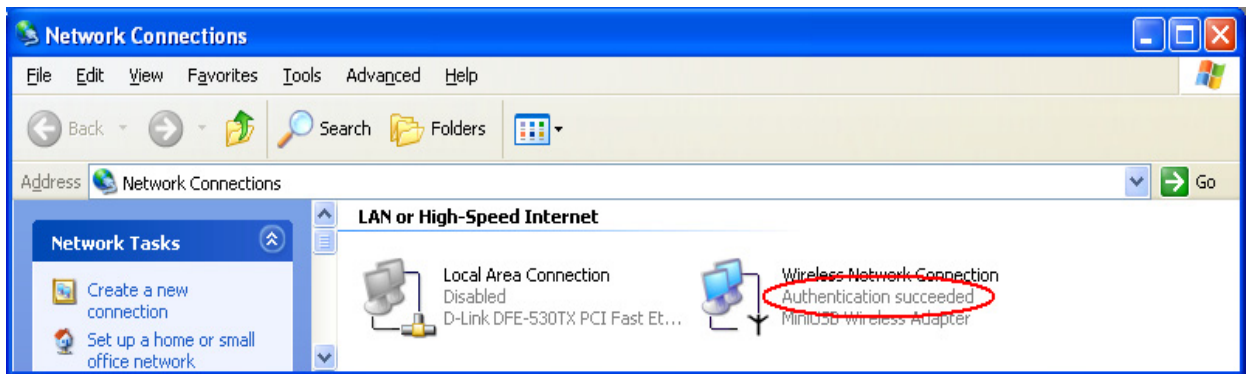


Figure 5: Authenticating



**Figure 6: Authentication success**

#### 4.2 DUT authenticate PC2 using PEAP-TLS.

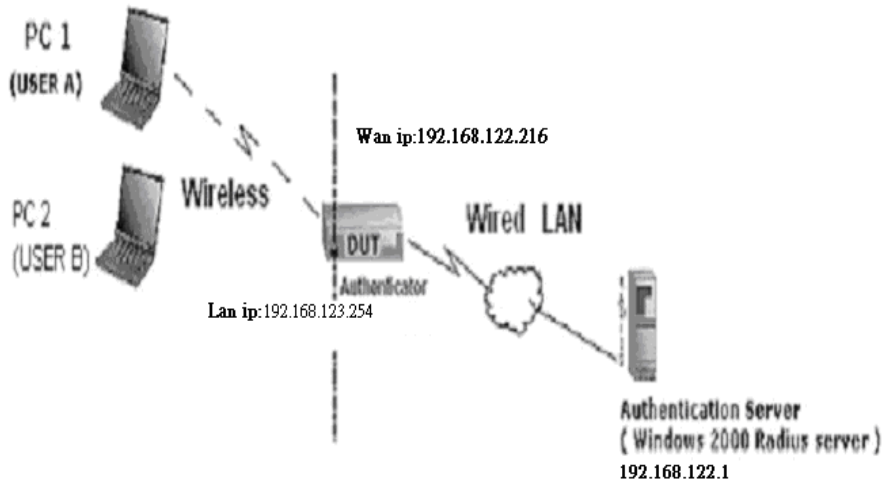
1. PC2 choose the SSID of DUT as the Access Point.
2. Set authentication type of wireless client and RADIUS server both to PEAP\_TLS.
3. Disable the wireless connection and enable again.
4. The DUT will send the user's certificate to the RADIUS server, and then send the message of authentication result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

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

#### Note.

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

# WPA Settings



Wireless Router: LAN IP: 192.168.0.1

WAN IP: 192.168.122.216

Radius Server: 192.168.122.1

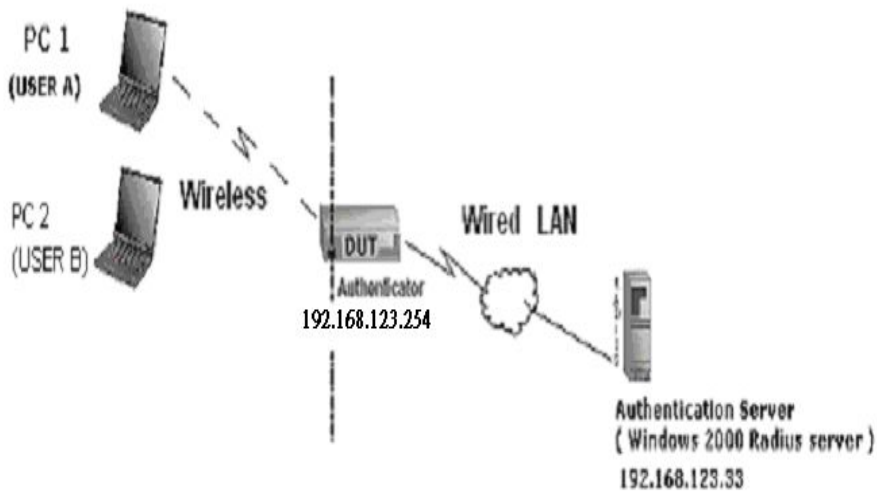
UserA : XP Wireless Card:Ti-11g

Tool: Odyssey Client Manager

Refer to: [www.funk.com](http://www.funk.com)

Download: [http://www.funk.com/News&Events/ody\\_c\\_wpa\\_preview\\_pn.asp](http://www.funk.com/News&Events/ody_c_wpa_preview_pn.asp)

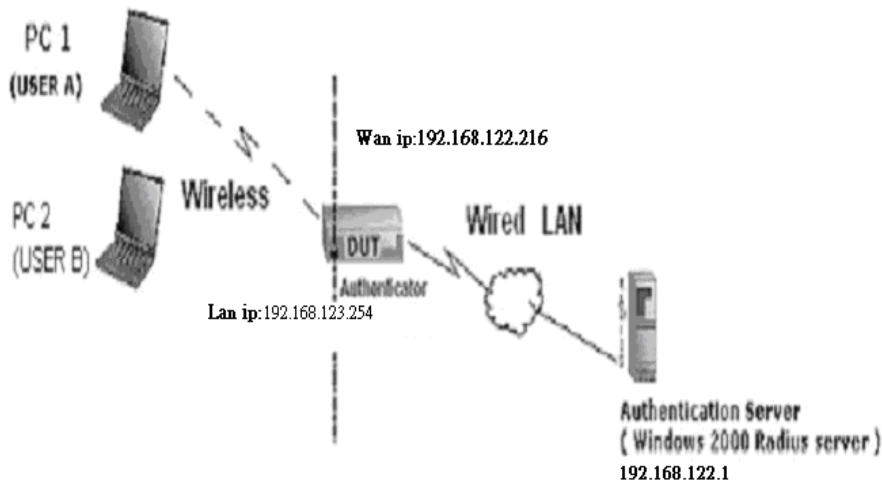
Or Another Configuration:





## 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



2. Then, Install this certificate and finish.

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

Network ID(SSID)	123kk
Channel	8
Security	WPA

#### 802.1X Settings

RADIUS Server IP	192.168.122.1
RADIUS port	1812
RADIUS Shared Key	costra

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

**Add Profile**

Profile name: 1

User Info | Authentication | ITLS Settings | PEAP Settings

Login name: fae1

Password

- Permit login using password
- use Windows password
- prompt for password
- use the following password:  
fae1
- Unmask

Certificate

- Permit login using my certificate:  
fae1

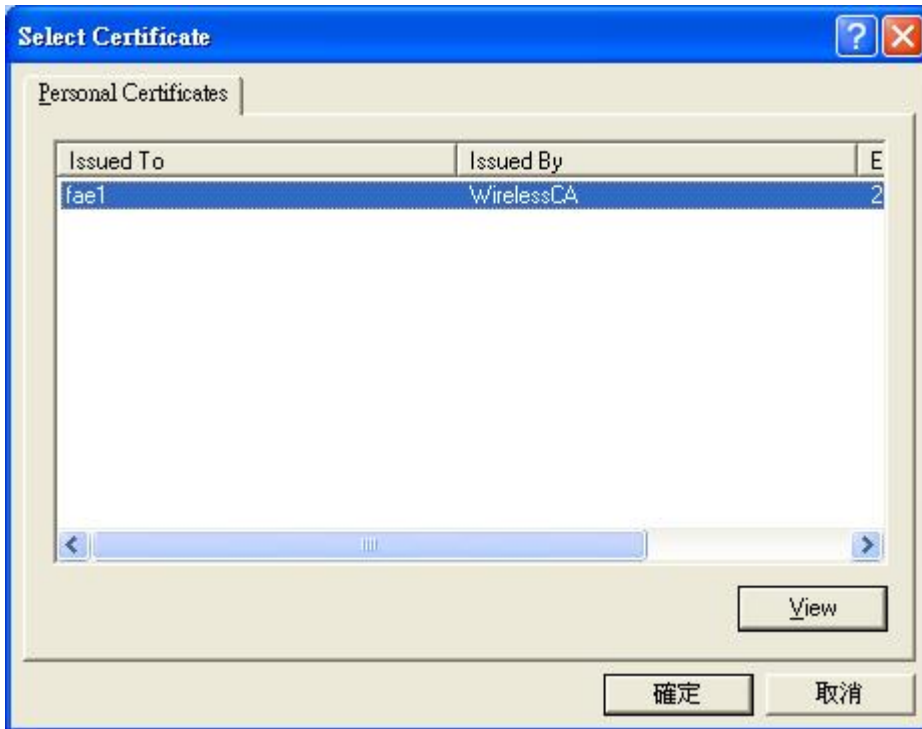
View ... Browse ...

OK Cancel

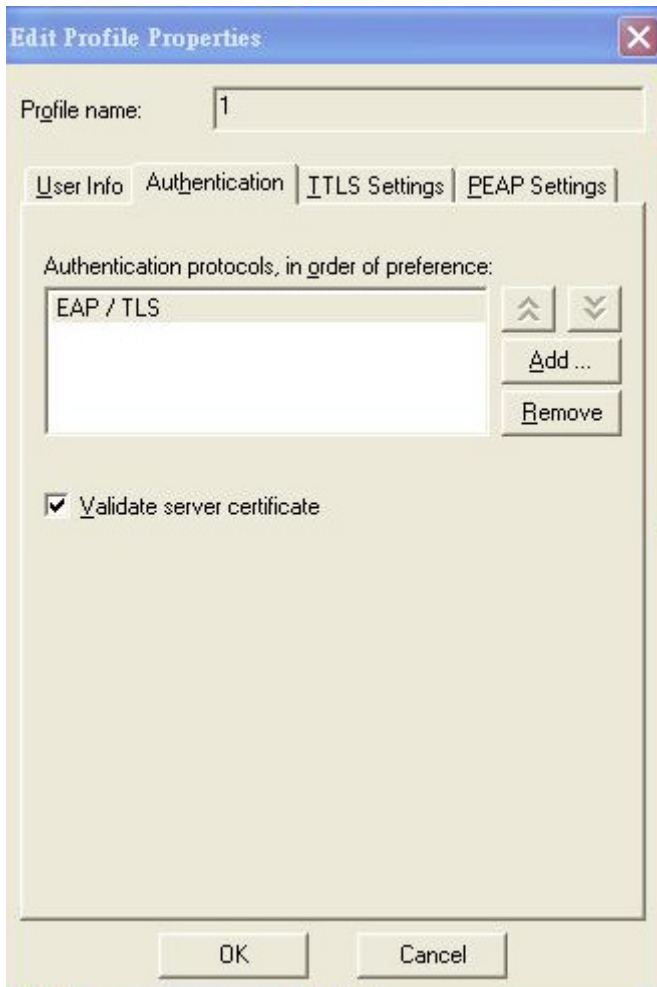
Login name and password are fae1 and fae1.

Remember that you get certificate from Radius in Step1.

5. Then Choose "certificate" like above.



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



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

**Network Properties**

Network

Network name (SSID): 123kk

Connect to any available network Scan ...

Description (optional):

Network type: Access point (infrastructure mode)

Channel: default channel

Association mode: WPA

Encryption method: TKIP

Authentication

Authenticate using profile: 1

Keys will be generated automatically for data privacy

Pre-shared key (WPA)

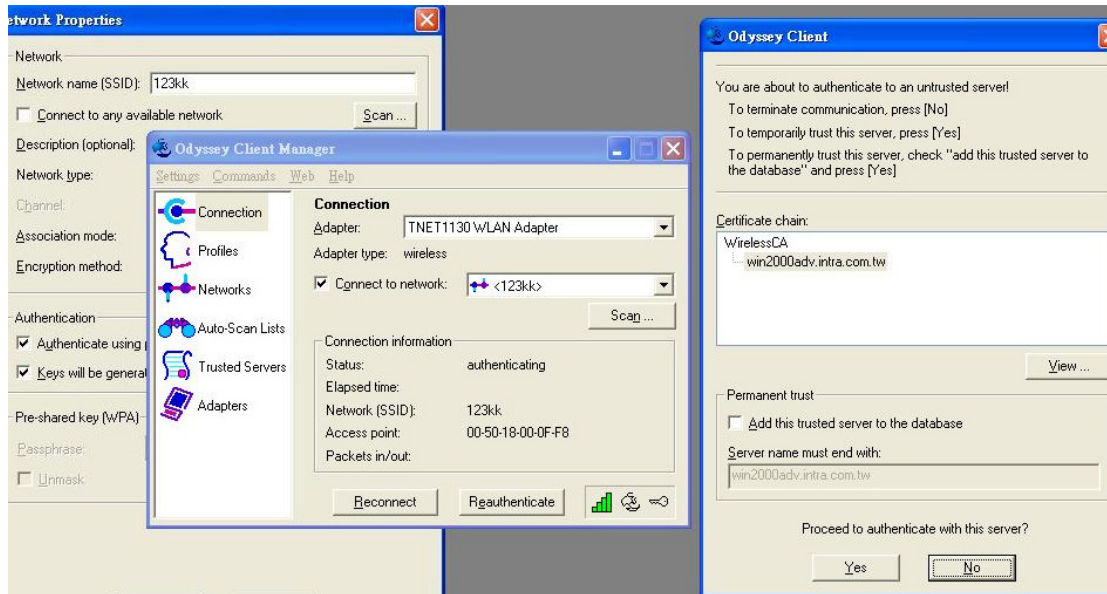
Passphrase: [masked]

Unmask

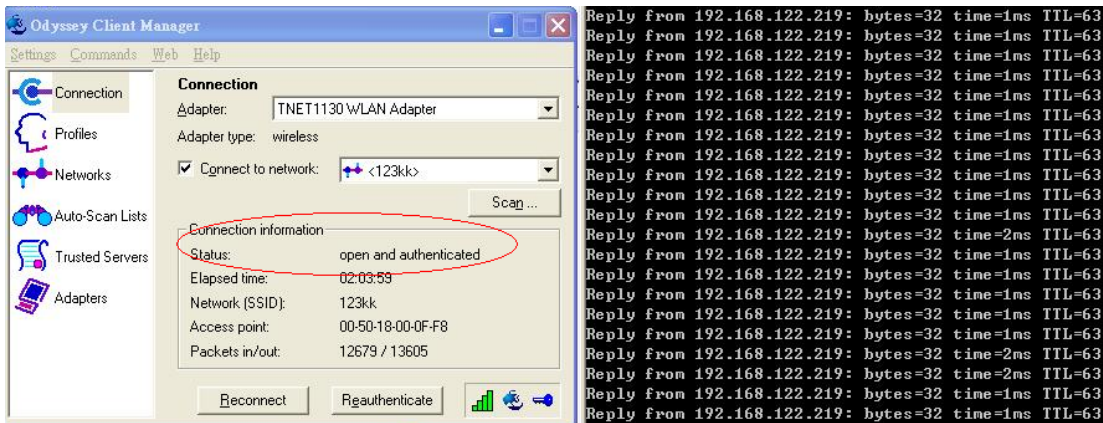
OK Cancel

8. Back to Connection and Select "123kk.

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



9.Result:



Method 2:

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

<http://192.168.122.1/certsrv>

account:fae1

passwd:fae1



2. Then Install this certificate and finish.

3. Setting on the router and client:

Router:

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

#### 802.1X Settings

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

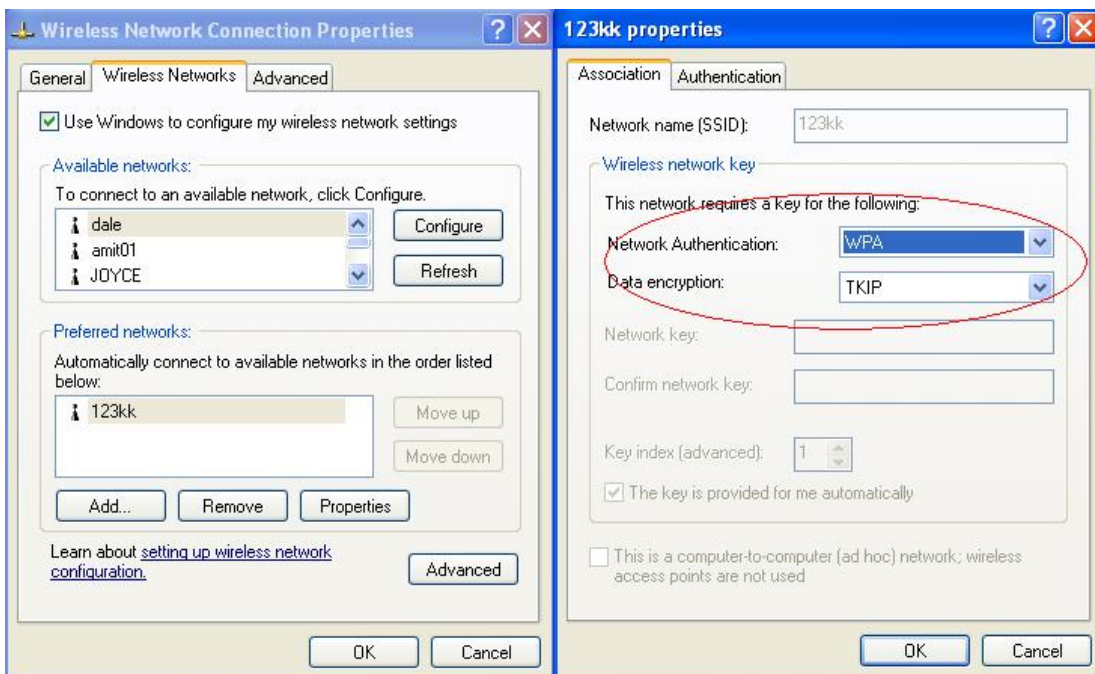
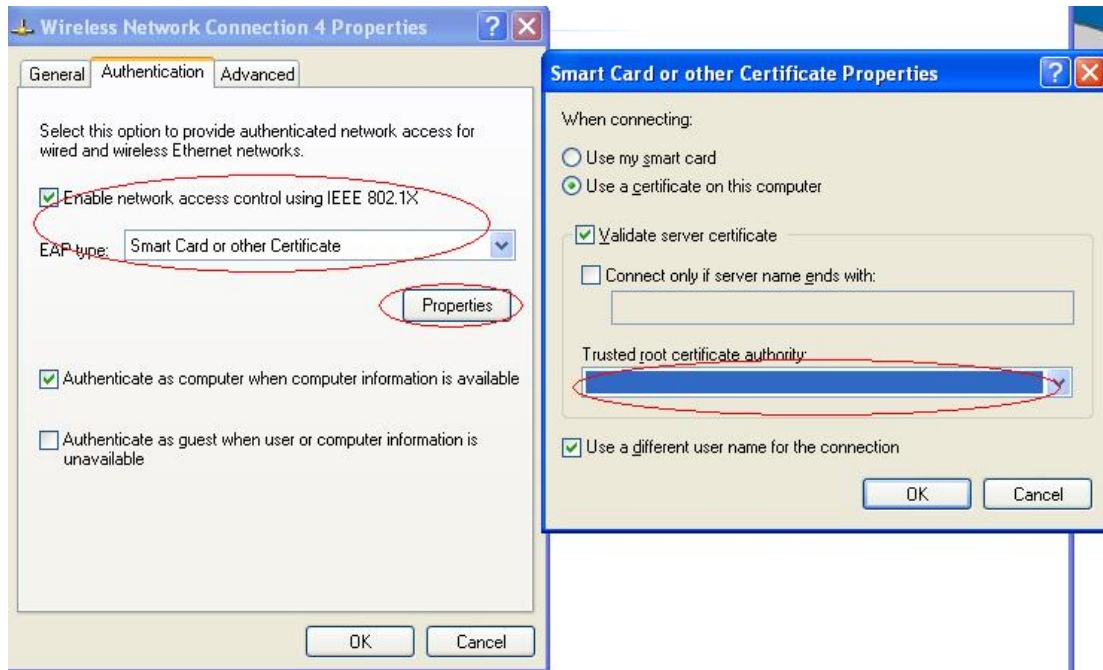
Client:

Go to "Network Connection" and select wireless adapter.

Choose "View available Wireless Networks" like below:

Advanced → choose "123kk"

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



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



# FAQ and Troubleshooting

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

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

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



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

```
C:\>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    IP Address . . . . . : 192.168.123.115
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.123.254
```

If yes, please execute Browser, like Mozilla and key 192.168.0.1 in address.

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

```
C:\>ipconfig /release
Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\>ipconfig /renew
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    IP Address . . . . . : 192.168.123.115
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.123.254
```

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



## **2. Why can I not connect the router even if the cable is plugged in Lan port and the led is light?**

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

If not, please check How blinking Status led shows.

There are many abnormal symptoms as below:

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

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

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

## **3. How to reset to factory default?**

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

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

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

**A:** Make sure that the network cable from DSL or Cable modem is plugged in Wan port of Router and that the network cable from Lan port of router is plugged in Ethernet adapter. Then, please check which wan type you use. If you are not sure, please call the isp. Then please go to this page to input the information [isp](#) [is](#) assigned.

▶ Choose WAN Type	
Type	Usage
<input type="radio"/> Static IP Address	ISP assigns you a static IP address.
<input checked="" type="radio"/> Dynamic IP Address	Obtain an IP address from ISP automatically.
<input type="radio"/> Dynamic IP Address	Telstra BigPond
<input type="radio"/> PPP over Ethernet	Some ISPs require the use of PPPoE to connect to their services.
<input type="radio"/> PPTP	Some ISPs require the use of PPTP to connect to their services.
<input type="radio"/> L2TP	Some ISPs require the use of L2TP to connect to their services.
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

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

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

**How do I connect router by using wireless?**

**1. How to start to use wireless?**

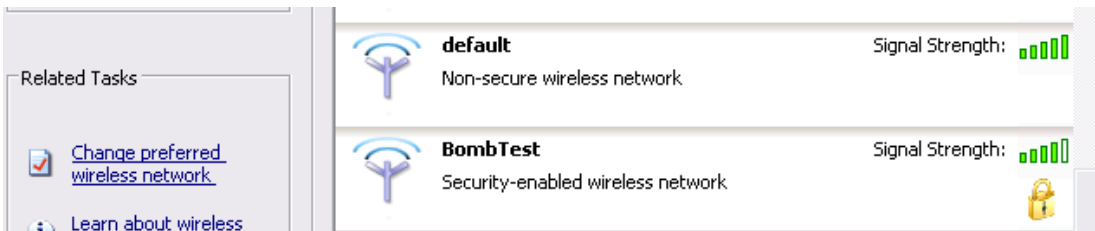
**A:** First, make sure that you already installed wireless client device in your computer. Then check the Configuration of wireless router. The default is as below:

Wireless Setting [ HELP ]	
Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Turn off Wireless depend as Schedule Rule	(00)Always <input type="radio"/> Enable <input checked="" type="radio"/> Disable <input type="button" value="Schedule Setting"/>
Network ID(SSID)	default
Wireless Mode	<input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only <input type="radio"/> 11n only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	11
WDS	<input type="button" value="Enter..."/>
WPS	<input type="button" value="Enter..."/>
Security	None
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Wireless Client List..."/>	

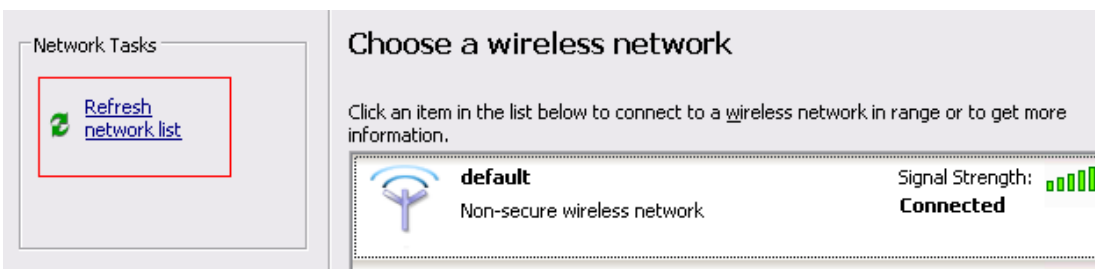
About wireless client, you will see wireless icon:



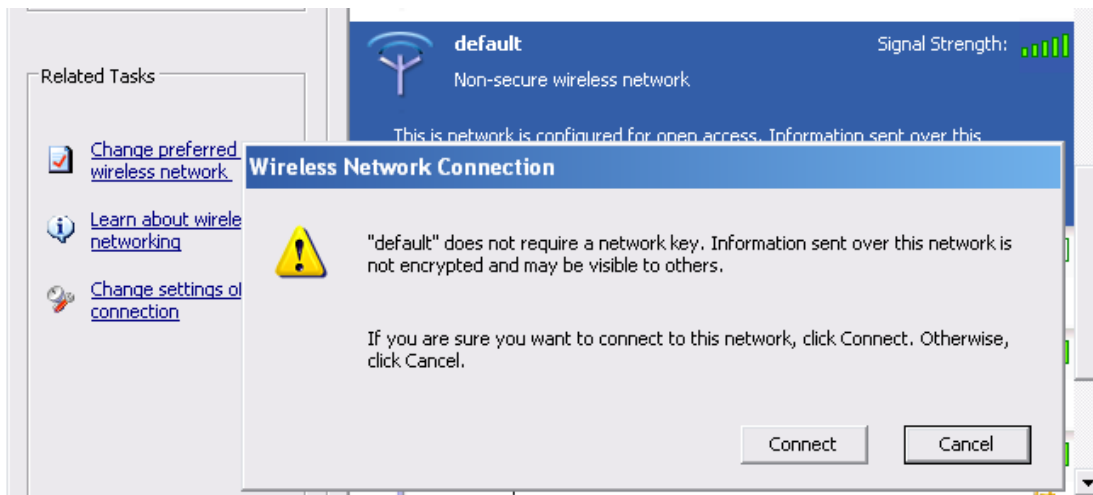
Then click and will see the ap list that wireless client can be accessed:



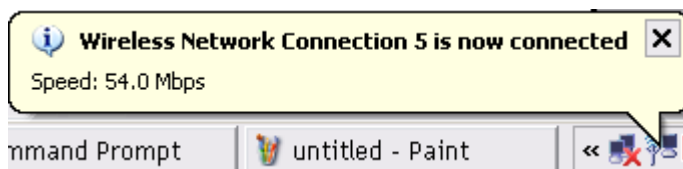
If the client can not access your wireless router, please refresh network list again. However, I still can not fine the device which ssid is "default", please refer to Q3.



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



If successfully, the computer will show



and get ip from router:

```

Ethernet adapter Wireless Network Connection 5:

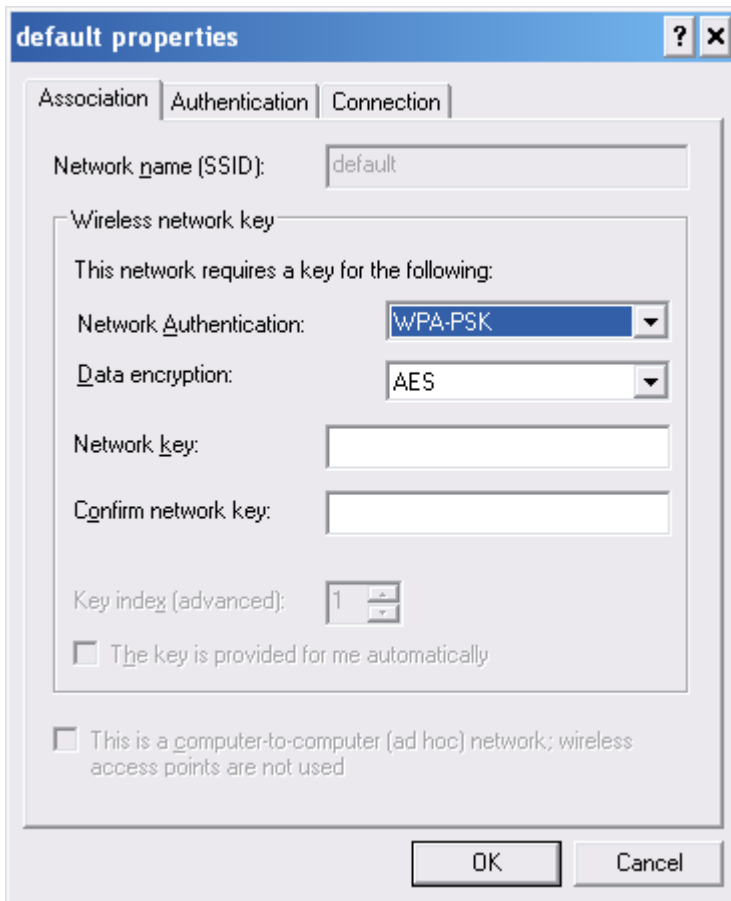
    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.123.165
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.123.254
  
```

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

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



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



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

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