



802.11n Wireless Broadband Router

WNRT-626

User's Manual

Copyright

Copyright © 2009 by 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.

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 Router

Model: WNRT-626v2

Rev: 1.0 (July. 2009)

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION	6
1.1 PACKAGE CONTENTS	6
1.2 FEATURES	6
1.3 SPECIFICATION	6
CHAPTER 2 HARDWARE INSTALLATION / NETWORK SETUP	8
2.1 HARDWARE INSTALLATION	8
2.2 LED INDICATORS	10
2.3 NETWORK SETUP	11
CHAPTER 3 INTRODUCTION TO WEB CONFIGURATION	13
3.1 WEB LOGIN.....	13
3.2 OPERATION MODE.....	14
3.3 INTERNET SETTINGS	14
3.3.1 WAN.....	14
3.3.2 LAN	20
3.3.3 DHCP clients.....	21
3.3.4 Advanced Routing.....	22
3.3.5 QoS.....	23
CHAPTER 4 WIRELESS SETTINGS	24
4.1 BASIC	24
4.2 ADVANCED WIRELESS SETTINGS.....	27
4.3 SECURITY	29
4.4 WPS.....	30
4.5 STATION LIST	31
CHAPTER 5 FIREWALL	32
5.1 MAC/IP/PORT FILTERING	32
5.2 PORT FORWARDING	33
5.3 DMZ	34
5.4 SYSTEM SECURITY SETTINGS	35
5.5 CONTENT FILTERING	36

CHAPTER 6 ADMINISTRATION	37
6.1 MANAGEMENT	37
6.2 MANAGEMENT UPLOAD FIRMWARE	38
6.3 SETTING MANAGEMENT	38
6.4 STATUS	39
6.5 STATISTIC	40
6.6 SYSTEM LOG	41

Chapter 1 Introduction

Thank you for purchasing WNRT-626. This manual guides you on how to install and properly use the WNRT-626 in order to take full advantage of its features.

1.1 Package Contents

Make sure that you have the following items:

- WNRT-626 x 1
- Ethernet Cable x 1
- Power Adapter x 1
- CD-ROM (included user's manual) x 1
- Quick Installation Guide x 1



If any of the above items are missing, please contact your supplier for support

1.2 Features

- IEEE 802.11n (Draft 2.0) wireless technology compliant with 802.11b/g standard
- Capable of up to 150Mbps data rate
- Supports Wi-Fi Protected Setup (WPS)
- Supports 64/128-bit WEP, WPA –TKIP(PSK), WPA2-AES(PSK), 802.1x
- AP / Station-Infrastructure / Bridge (WDS) / Repeater modes supported
- Equipped with four LAN ports (10/100M) and one WAN port (10/100M), Auto-MDI/MDI-X supported
- Supports DHCP Server
- System status monitoring includes Active DHCP Client, Security Log and Device/Connection Status
- Web-based GUI for and Wizard setup for easily configuration
- Remote Management allows configuration and upgrades from a remote site
- Supported Internet types: Dynamic / Static IP / PPPoE / PPTP / L2TP
- MAC / IP filter access control, URL blocking ; SPI firewall + DoS prevention protection
- Supports UPnP function

1.3 Specification

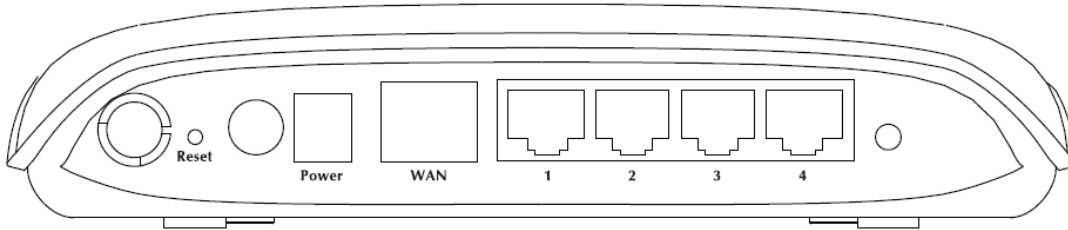
Standard	IEEE 802.11b/g, 802.11n Draft 2.0, IEEE802.3u
Frequency range	2.4 ~ 2.4835GHz
Radio Technology	IEEE 802.11b: DQPSK, DBPSK, DSSS, and CCK IEEE 802.11 g: BPSK, QPSK, 16QAM, 64QAM IEEE 802.11n: MCS0-MCS7
WAN Port	1 x 100Base-TX, Auto-MDI/MDI-X
LAN Port	4 x 100Base-TX, Auto-MDI/MDI-X
Antenna connector	1 x Fixed 3dBi Dipole Antenna
Data Encryption	64 bit / 128 bit WEP, WPA-PSK, WPA, WPA2, 802.1x encryption
Frequency	2.400GHz - 2.483GHz
Output Power	802.11b: Typ. 18dBm@Normal Temp Range; 802.11g: Typ. 15dBm@Normal Temp Range; 802.11n: Typ. 15dBm@Normal Temp Range.

Data Rate	11Mbps Max @802.11b 54Mbps Max @802.11g 150Mbps Max @802.11n
Receiver Sensitivity	1 Mbps:-94 dBm, 2 Mbps:-91 dBm, 5.5 Mbps:-89 dBm, 11 Mbps:-85 dBm; 6 Mbps:-90 dBm, 9 Mbps:-89 dBm; 12 Mbps:-86 dBm, 18 Mbps:-84 dBm; 24 Mbps:-81 dBm, 36 Mbps:-77 dBm; 48 Mbps:-73 dBm, 54 Mbps:-72 dBm, 150Mbps:-77dBm
Session	3000
LED Indicators	PWR, WLAN, WPS, WAN * 1, LAN * 4

Chapter 2 Hardware Installation / Network Setup

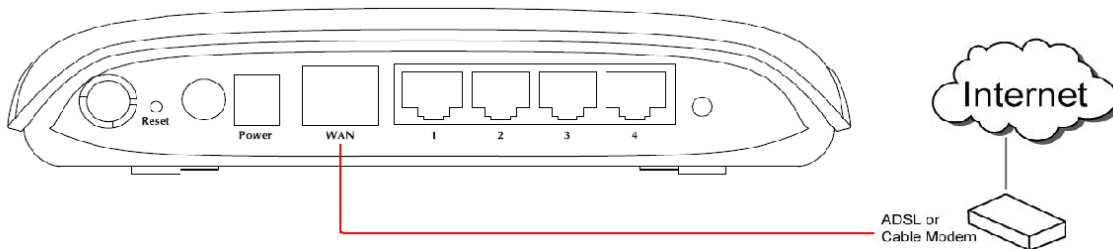
Please follow the below instruction to build the wireless network connection between WNRT-626 and your computers.

2.1 Hardware Installation

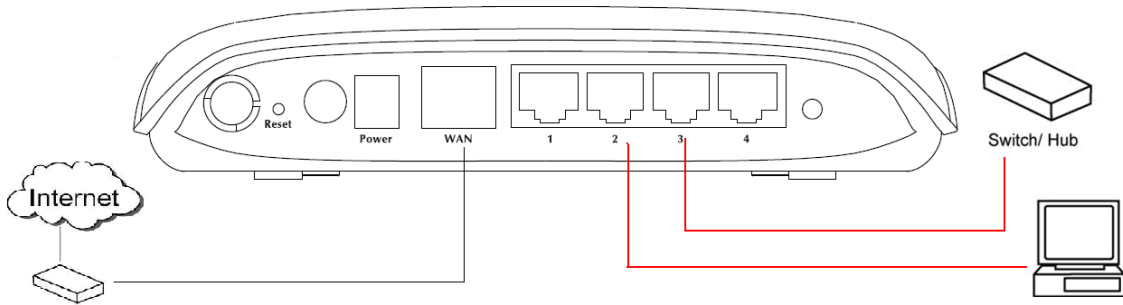


Interface	Function
Reset	Resets to the factory defaults. To restore factory defaults, keep the device powered on and push a paper clip into the hole. Press down the button over 5 seconds and then release.
ON/OFF	Power on or off.
Power	Interface that connects to the power adapter. 12 V DC, 500mA
WAN	Ethernet RJ-45 interfaces that connect to the Internet.
LAN 1~4	Ethernet RJ-45 interfaces that connect to the Ethernet interface of the computer or Ethernet devices.
WPS	WPS on or off switch.

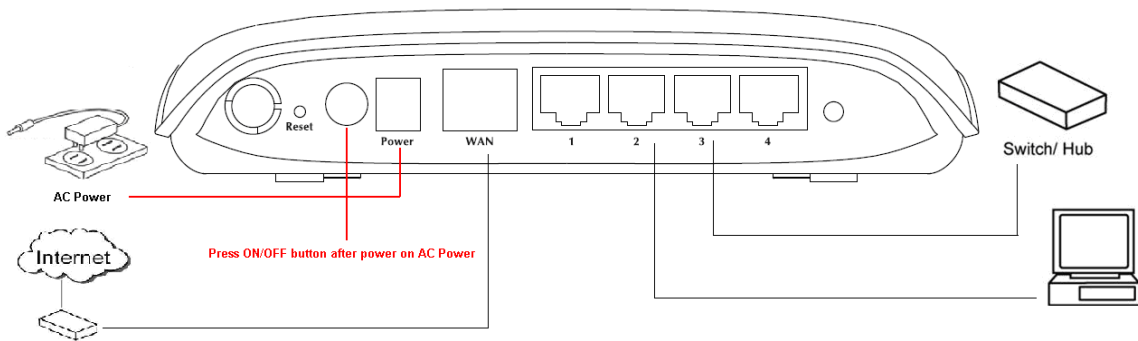
- 1. Locate an optimum location for the WNRT-626.** The best place for your WNRT-626 is usually at the center of your wireless network, with line of sight to all of your mobile stations.
- 2. Adjust the antennas of WNRT-626.** Try to adjust them to a position that can best cover your wireless network. The antenna's position will enhance the receiving sensitivity.
- 3. Connect xDSL/Cable Modem to WAN port of WNRT-626.** Usually, this cable would be provided with your modem. If no cable was supplied with your modem, please use a RJ-45 Ethernet cable




- 4. Connect all of your network devices to LAN port of WNRT-626.** Connect all your computers, network devices (network-enabled consumer devices other than computers, like game console, or switch / hub). Connect one of the LAN ports on WNRT-626 to your LAN switch/hub or a computer with a RJ-45 cable.



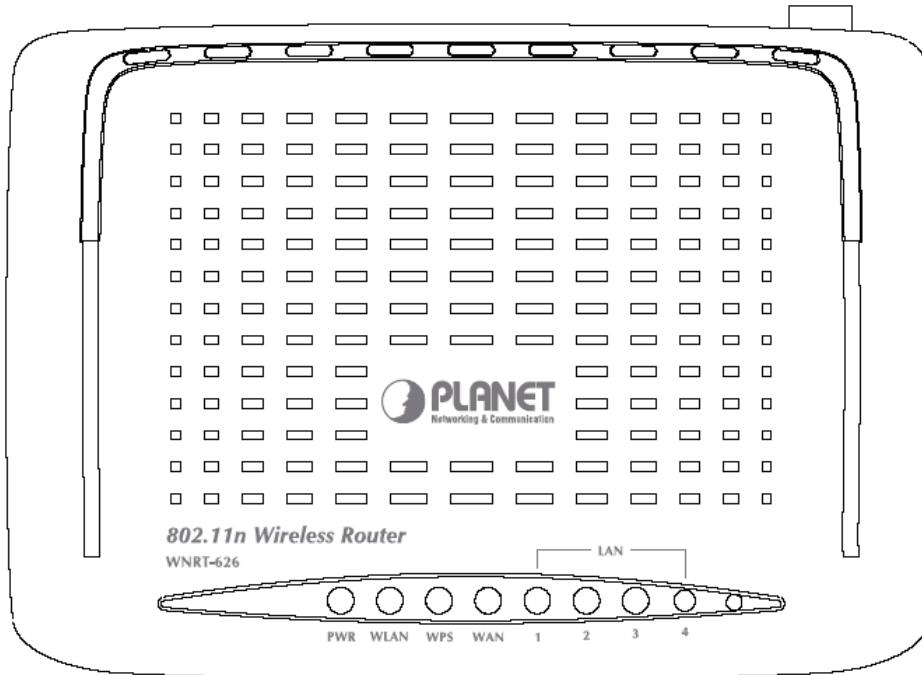
5. Plug in power adapter and connect to power source, then press ON/OFF button. After power on, WNRT-626 will start to operate.



6. Please check all LEDs on the front panel. 'PWR' LED should be steadily on. WAN and LAN LEDs should be on if the computer / network device connected to the respective port of the router is powered on and correctly connected. If PWD LED is not on, or any LED you expected is not on, please recheck the cabling, or jump to 'Troubleshooting' for possible reasons and solution.

- | | |
|---|--|
|  | <ol style="list-style-type: none"> 1. ONLY use the power adapter supplied with the WNRT-626. Otherwise, the product may be damaged. 2. If you want to reset WNRT-626 to default settings, press and hold the Reset button over 5 seconds and release. And then wait for WNRT-626 restart. |
|---|--|

2.2 LED Indicators

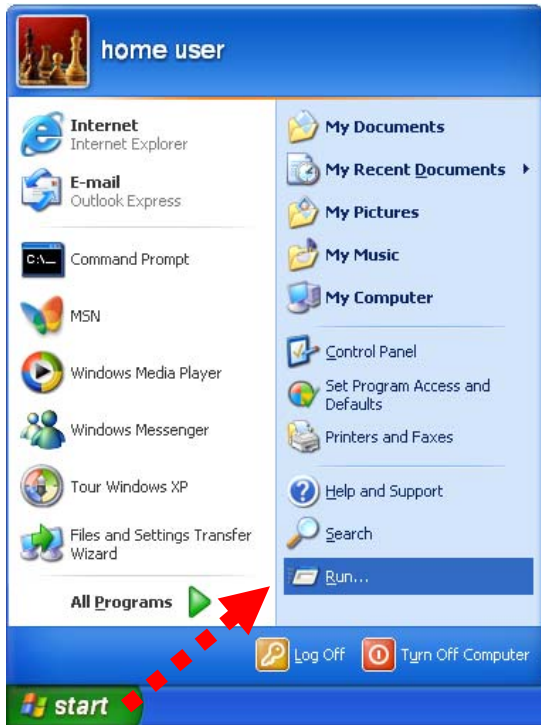


LEDs	Color	Status	Description
PWR	Green	On	The device is powered on, and it is running normally.
		Off	The device is powered off.
	Red	On	The device is power on and initializing.
WLAN	Green	On	WLAN radio is on.
		Blinks	Data is being transmitted through WLAN.
		Off	WLAN radio is off.
WPS	Green	On	WPS client registration is successful.
		Blinks	WPS client registration window is currently open.
		Off	WPS is not available, or WPS is not enabled or initialized.
WAN	Green	On	The device has successful Ethernet connections.
		Blinks	The device is receiving or sending data on WAN.
		Off	The WAN is not connected.
LAN 1~4	Green	On	The device has successful Ethernet connections.
		Blinks	The device is receiving or sending data on LAN.
		Off	The LAN is not connected.

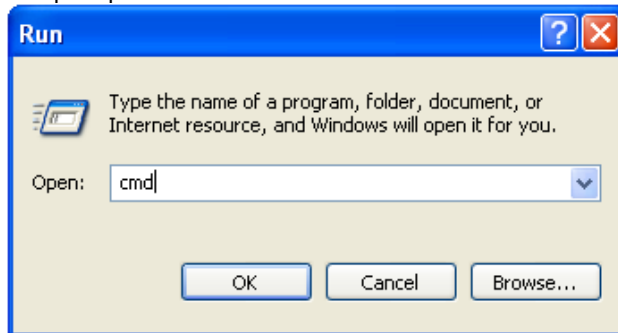
2.3 Network Setup

After you install your WNRT-626, the TCP/IP settings should be set to obtain an IP address from a DHCP server (WNRT-626) automatically. To verify your IP address, please follow the steps below:

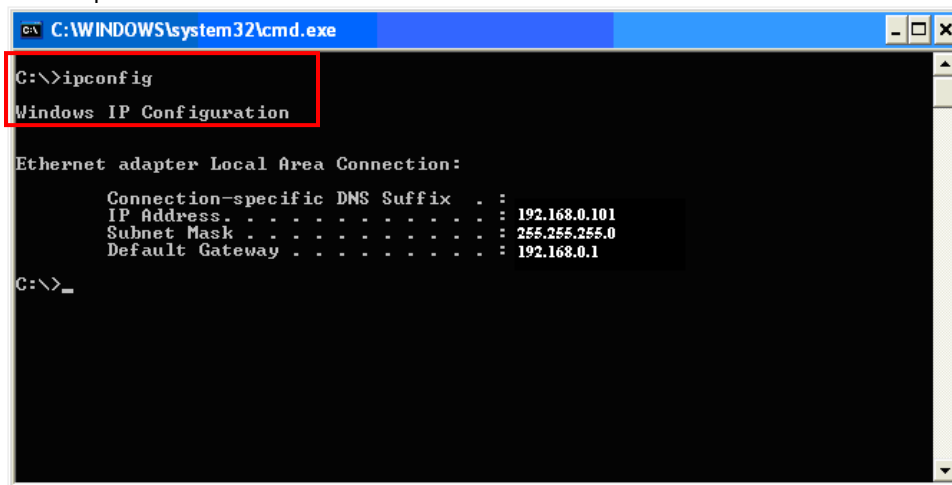
1. Click on **Start > Run**.



2. In the run box type "**cmd**" and click OK. (Windows VistaR users type cmd in the Start .Search box.)At the prompt.



3. Type "**ipconfig**" and press **Enter**. It will display the IP address, subnet mask, and the default gateway of adapter.



```
C:\WINDOWS\system32\cmd.exe
C:\>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address . . . . . : 192.168.0.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

C:\>_
```

4. If the address is **0.0.0.0**, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.

Assign a static IP address

If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

1. - **Windows Vista**® - Click on Start > Control .Panel > Network .and .Internet >Network .and .Sharing .Center > Manage Network Connections.
- **Windows**® **XP** - Click on Start > Control .Panel > Network Connections.
- **Windows**® **2000** - From the desktop, right-click My Network Places > Properties.
2. Right-click on the Local Area Connection which represents your network adapter and select Properties.
3. Highlight Internet .Protocol .(TCP/IP) and click Properties.
4. Click Use .the .following .IP .address and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.
Example: If LAN IP address of WNRT-626 is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.0.1).
Set Primary DNS the same as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.
5. Click OK twice to save your settings.

Chapter 3 Introduction to Web Configuration

3.1 Web Login

WNRT-626 with an assigned IP address allows you to monitor and configure via web browser (e.g., MS Internet Explorer or Netscape).

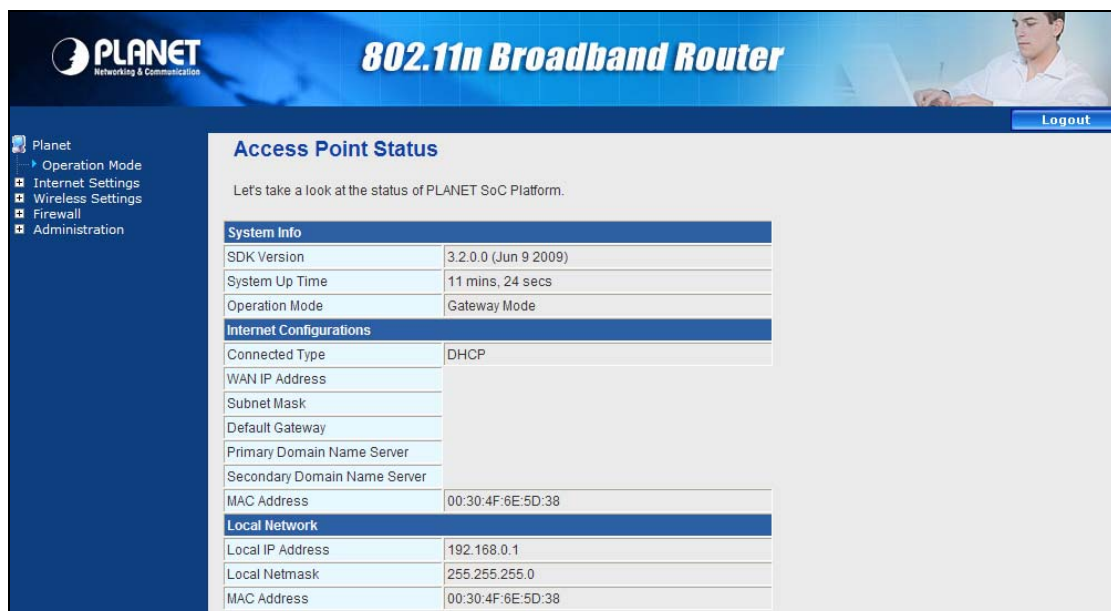
1. Open your web browser.
2. Enter the IP address of your WNRT-626 in the address field (default IP address is **http://192.168.0.1**).
3. Please enter your User Name and Password in the dialog box, and then click "OK". Default User name and password as below:

User Name: **admin**

Password: **admin**



4. Then you will see the WNRT-626 HOME screen as below.



System Info	
SDK Version	3.2.0.0 (Jun 9 2009)
System Up Time	11 mins, 24 secs
Operation Mode	Gateway Mode

Internet Configurations	
Connected Type	DHCP
WAN IP Address	
Subnet Mask	
Default Gateway	
Primary Domain Name Server	
Secondary Domain Name Server	
MAC Address	00:30:4F:6E:5D:38

Local Network	
Local IP Address	192.168.0.1
Local Netmask	255.255.255.0
MAC Address	00:30:4F:6E:5D:38

3.2 Operation Mode

Choose **Operation Mode** and the following page appears. In this page, you can configure the operation mode according to your practice.

- **Bridge:** All Ethernet and wireless interfaces are bridged into a single bridge interface.
- **Gateway:** The first Ethernet interface is treated as WAN interface. The other Ethernet interfaces and the wireless interface are bridged together treated as LAN interfaces. If the device is in Gateway operation mode, you can enable or disable NAT. Gateway is the default operation mode.
- **WISP:** All the Ethernet ports are bridged together and the wireless interface of this router will connect to ISP's Access Point. The NAT is enabled and PCs in Ethernet ports share the same IP to ISP through wireless LAN. The connection type can be setup in WAN page by using PPPoE, DHCP client, PPTP/L2TP client or static IP.



If you select **Bridge operation mode**, WAN configuration in Internet Settings are not available. (Firewall functions on the left page are not available.)

Operation Mode Configuration

You may configure the operation mode suitable for you environment.

Bridge:
In this mode, all Ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

Gateway:
In this mode, the device is supposed to connect to Internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP/L2TP client or static IP.

WISP:
In this mode, all Ethernet ports are bridged together and the wireless interface of this router will connect to ISP's Access Point. The NAT is enabled and PCs in Ethernet ports share the same IP to ISP through wireless LAN. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP/L2TP client or static IP.

NAT Enabled

After finishing setting, click **Apply** to save the settings and make the new configuration take effect. Click **Cancel** to close without saving.

3.3 Internet Settings

3.3.1 WAN

The WAN Settings screen allows you to specify the type of Internet connection. The WAN settings offer the following selections for the router's WAN port, **STATIC (fixed IP)**, **DHCP (Auto config)**, **PPPoE (ADSL)**, **L2TP**, and **PPTP**.

Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: DHCP (Auto config) ▾

MAC Clone

Enabled Disable ▾

STATIC (fixed IP)
 DHCP (Auto config)
 PPPoE (ADSL)
 L2TP
 PPTP

➤ **STATIC (FIXED IP)**

Select **STATIC (fixed IP)** in the **WAN Connection Type** drop-down list and the following page appears.

Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: STATIC (fixed IP) ▾

Static Mode

IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Default Gateway	<input type="text"/>
Primary DNS Server	<input type="text"/>
Secondary DNS Server	<input type="text"/>

MAC Clone

Enabled Disable ▾

Static Mode

- **IP Address:** Enter the IP address of WAN port.
- **Subnet Mask:** Enter IP subnet mask of WAN port.
- **Default Gateway:** Enter the default gateway address of WAN port.
- **Primary DNS Server:** Primary DNS Server of WAN port.
- **Secondary DNS Server:** Secondary DNS Server of WAN port.

MAC Clone

MAC Clone provides WAN to connect to a MAC address.

- **Enabled:** Enable or disable MAC clone.

After finishing setting, click **Apply** to save the settings and make the new configuration take effect. Click **Cancel** to close without saving.

➤ **DHCP (AUTO CONFIG)**

Select **DHCP (Auto config)** in the **WAN Connection Type** drop-down list and the following page appears. If the WAN connection type is set to **DHCP**, the device automatically obtains the IP address, gateway and DNS address from the DHCP server on WAN interface.

The screenshot shows a configuration window titled "WAN Connection Type" with a dropdown menu set to "DHCP (Auto config)". Below this, there is a section for "MAC Clone" with a dropdown menu set to "Disable". At the bottom, there are "Apply" and "Cancel" buttons.

MAC Clone

MAC Clone provides WAN to connect to a MAC address.

- **Enabled:** Enable or disable MAC clone.

After finishing setting, click **Apply** to save the settings and make the new configuration take effect. Click **Cancel** to close without saving.

➤ **PPPOE (ADSL)**

Select **PPPoE (ADSL)** in the **WAN Connection Type** drop-down list and the following page appears. If the WAN connection type is set to **PPPoE (ADSL)**, you can configure the following parameters to PPPoE dial up.

The screenshot shows a configuration window titled "Wide Area Network (WAN) Settings" with a dropdown menu set to "PPPoE (ADSL)". Below this, there is a section for "PPPoE Mode" with fields for "User Name" (pppoe_user), "Password", and "Verify Password". There is also a "Keep Alive" dropdown menu and a "Keep Alive Mode" section with "Redial Period" (60 seconds) and "On demand Mode: Idle Time" (5 minutes). At the bottom, there is a "MAC Clone" section with a dropdown menu set to "Disable" and "Apply" and "Cancel" buttons.

PPPoE Mode

- **User Name:** User name of PPPoE account
- **Password:** Password of PPPoE account
- **Verify Password:** Enter the password of PPPoE account again.
- **Operation Mode:** It provides two types of operation modes.
 - **Keep Alive** means keeping on-line mode. You can set the redial period in the field. When the redial period expires, AP will execute dial-up again to keep online.
 - **On Demand** means executing dial-up on demand. Within the preset idle time, if AP does not detect the flow of the user continuously, AP automatically stops the PPPOE connection. Once it detects the flow (e.g., accessing a webpage), the router restarts the PPPOE dial-up.

MAC Clone

- **Enabled:** Enable or disable.

After finishing setting, click **Apply** to save the settings and make the new configuration take effect. Click **Cancel** to close without saving.

➤ L2TP

Select **L2TP** in the **WAN Connection Type** drop-down list and the following page appears. There are two address modes: **Static** and **Dynamic**.

1. If you select **Static** in the **Address Mode** field, the page shown in the following figure appears.

The screenshot displays the L2TP configuration interface. At the top, 'WAN Connection Type' is set to 'L2TP'. Below this, the 'L2TP Mode' section contains the following fields: 'Server IP' (10.10.10.123), 'User Name' (l2tp_user), 'Password' (masked with dots), 'Address Mode' (Static), 'IP Address' (10.10.10.254), 'Subnet Mask' (255.255.255.0), and 'Default Gateway' (10.10.10.253). The 'Operation Mode' is set to 'Keep Alive', with sub-fields for 'Keep Alive Mode: Redial Period' (60 seconds) and 'On demand Mode: Idle Time' (5 minutes). The 'MAC Clone' section at the bottom has 'Enabled' set to 'Disable'. 'Apply' and 'Cancel' buttons are located at the bottom of the form.

2. If you select **Dynamic** in the **Address Mode** field, the page shown in the following figure appears.

The screenshot shows a configuration window for WAN Connection Type. At the top, 'WAN Connection Type' is set to 'L2TP'. Below this is a section titled 'L2TP Mode' with the following fields: 'Server IP' (10.10.10.123), 'User Name' (l2tp_user), 'Password' (masked with dots), 'Address Mode' (Dynamic), and 'Operation Mode' (Keep Alive). Under 'Operation Mode', there are two sub-fields: 'Keep Alive Mode: Redial Period' (60 seconds) and 'On demand Mode: Idle Time' (5 minutes). Below the L2TP Mode section is a section titled 'MAC Clone' with an 'Enabled' field set to 'Disable'. At the bottom of the window are 'Apply' and 'Cancel' buttons.

L2TP Mode

- **Server IP:** Address of L2TP server.
- **User Name:** The user name of L2TP account.
- **Password:** The password of L2TP account.
- **IP Address:** IP address of WAN port.
- **Subnet Mask:** Subnet mask of WAN port.
- **Default Gateway:** The default gate way of WAN port.
- **Operation Mode:** It provides two types of operation modes.
 - **Keep Alive** means keeping on-line mode. You can set the redial period in the field. When the redial period expires, AP will execute dial-up again to keep online.
 - **On Demand** means executing dial-up on demand. Within the preset idle time, if AP does not detect the flow of the user continuously, AP automatically stops the PPPOE connection. Once it detects the flow (e.g., accessing a webpage), the router restarts the PPPOE dial-up.

MAC Clone

- **Enabled:** Enable or disable.

After finishing setting, click **Apply** to save the settings and make the new configuration take effect. Click **Cancel** to close without saving.

➤ **PPTP**

Select **PPTP** in the **WAN Connection Type** drop-down list and the following page appears. There are two address modes: **Static** and **Dynamic**.

WAN Connection Type:		PPTP
PPTP Mode		
Server IP	10.10.10.123	
User Name	pptp_user	
Password	●●●●●●●●	
Address Mode	Static	
IP Address	10.10.10.254	
Subnet Mask	255.255.255.0	
Default Gateway	10.10.10.253	
Operation Mode	Keep Alive	
	Keep Alive Mode: Redial Period	60 seconds
	On demand Mode: Idle Time	5 minutes
MAC Clone		
Enabled	Disable	
Apply		Cancel

PPTP Mode

- **Server IP:** Address of PPTP server.
- **User Name:** The user name of PPTP account.
- **Password:** The password of PPTP account.
- **IP Address:** IP address of WAN port.
- **Subnet Mask:** Subnet mask of WAN port.
- **Default Gateway:** The default gate way of WAN port.
- **Operation Mode:** It provides two types of operation modes.
 - **Keep Alive** means keeping on-line mode. You can set the redial period in the field. When the redial period expires, AP will execute dial-up again to keep online.
 - **On Demand** means executing dial-up on demand. Within the preset idle time, if AP does not detect the flow of the user continuously, AP automatically stops the PPPOE connection. Once it detects the flow (e.g., accessing a webpage), the router restarts the PPPOE dial-up.

MAC Clone

- **Enabled:** Enable or disable.

After finishing setting, click **Apply** to save the settings and make the new configuration take effect. Click **Cancel** to close without saving.

3.3.2 LAN

This page allows you may enable or disable networking functions and configure their parameters according to your practice.

Local Area Network (LAN) Settings

You may enable/disable networking functions and configure their parameters as your wish.

LAN Setup	
IP Address	<input type="text" value="192.168.0.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
LAN 2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
LAN2 IP Address	<input type="text"/>
LAN2 Subnet Mask	<input type="text"/>
MAC Address	00:30:4F:6E:5D:38
DHCP Type	Server <input type="button" value="v"/>
Start IP Address	<input type="text" value="192.168.0.100"/>
End IP Address	<input type="text" value="192.168.0.200"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Primary DNS Server	<input type="text" value="192.168.1.1"/>
Secondary DNS Server	<input type="text" value="192.168.1.1"/>
Default Gateway	<input type="text" value="192.168.1.1"/>
Lease Time	<input type="text" value="86400"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>

- **IP Address:** Enter the IP address of LAN port.
- **Subnet mask:** Enter the subnet mask of LAN port.
- **LAN2:** The second IP switch of LAN port. You can enable or disable this function.
- **LAN2 IP Address:** The second IP address of LAN port.
- **LAN2 Subnet Mask:** The second IP Subnet Mask of LAN port.
- **MAC Address:** MAC address of LAN port (Read-only).
- **DHCP Type:** You can select **Server** or **Disable**. If you select Disable, the DHCP service of LAN port is disabled. After selecting Server, you can set the following items.
- **Start IP Address:** The first IP address that DHCP server assigns.
- **End IP Address:** The last IP address that DHCP server assigns.
- **Subnet Mask:** The subnet mask of dynamic IP.
- **Primary DNS Server:** The primary DNS server address.
- **Secondary DNS Server:** The secondary DNS Server address.
- **Default Gateway:** The default gateway that DHCP server assigns.
- **Lease Time:** Lease time of the IP address.

- **Statically Assigned:** Assign IP to the assigned MAC address. Enter the assigned MAC address and IP in the corresponding fields.
- **802.1d Spanning Tree:** Spanning Tree Protocol. You can select Enable or Disable.
- **LLTD:** Link Layer Topology Discovery Protocol. You can select Enable or Disable.
- **IGMP Proxy:** You can select Enable or Disable.
- **IGMP Snooping:** You can select Enable or Disable.
- **UPNP:** Universal Plug and Play (UPNP). You can select Enable or Disable.
- **Router Advertisement:** You can select Enable or Disable.
- **PPPoE Relay:** You can select Enable or Disable.
- **DNS Proxy:** You can select Enable or Disable.

After finishing setting, click **Apply** to save the settings and make the new configuration take effect. Click **Cancel** to close without saving.

3.3.3 DHCP clients

You can view the information about DHCP clients in the page.

DHCP Client List		
You could monitor DHCP clients here.		
DHCP Clients		
MAC Address	IP Address	Expires in
00:30:40:11:22:33	192.168.0.100	23:44:34

3.3.4 Advanced Routing

You can add or delete routing rules, enable or disable dynamic routing protocol in the page.

Static Routing Settings

You may add and remote custom Internet routing rules, and/or enable dynamic routing exchange protocol here.

Add a routing rule

Destination	<input type="text"/>
Range	Host <input type="button" value="v"/>
Gateway	<input type="text"/>
Interface	LAN <input type="button" value="v"/> <input type="text"/>
Comment	<input type="text"/>

Current Routing table in the system:

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN (br0)	
2	192.168.0.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN (br0)	

Add a routing rule

- **Destination:** Enter the legal destination IP address.
- **Range:** Destination IP address is a host address or the network address.
- **Gateway:** Enter the specific gateway.
- **Interface:** The interface for this route. You can select LAN, WAN and Custom.
- **Comment:** Add the description of this route.

After finishing the setting above, click **Apply** to make the new routing rule take effect. Otherwise, click **Reset** to cancel the new routing rule.

Current Routing table in the system

You can delete or reset the routing rules.

Dynamic Routing Settings

You can enable or disable the **RIP**.

After finishing the setting above, click **Apply** to make the new routing rule take effect. Otherwise, click **Reset** to cancel the new routing rule.

3.3.5 QoS

You may set up rules to provide Quality of Service (QoS) guarantee for some specific applications. In the page, you can enable or disable Quality of Service. After enabling QoS, you can set upload bandwidth and download bandwidth.

Quality of Service Settings

You may setup rules to provide Quality of Service guarantees for specific applications.

QoS Setup	
Quality of Service	Enable ▾
Upload Bandwidth:	User defined ▾ <input type="text"/> Bits/sec
Download Bandwidth:	User defined ▾ <input type="text"/> Bits/sec

- **Upload Bandwidth:** You can select the proper bandwidth in the drop-down list. The value is from **64K** to **60M**. You can also set the bandwidth by selecting **User defined** and enter the proper bandwidth in the field.
 - **Download Bandwidth:** You can select the proper bandwidth in the drop-down list. The value is from **64K** to **60M**. You can also set the bandwidth by select **User defined** and enter the proper bandwidth in the field.
- fter finishing the setting above, click **Submit** to save the new configuration.

Chapter 4 Wireless Settings

4.1 Basic

You can configure the minimum number of wireless settings for communication, such as network name (SSID) and channel.

Basic Wireless Settings

You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

Wireless Network	
Radio On/Off	<input type="button" value="RADIO OFF"/>
Network Mode	11b/g/n mixed mode ▾
Network Name(SSID)	default
Multiple SSID1	<input type="text"/>
Multiple SSID2	<input type="text"/>
Multiple SSID3	<input type="text"/>
Multiple SSID4	<input type="text"/>
Multiple SSID5	<input type="text"/>
Multiple SSID6	<input type="text"/>
Multiple SSID7	<input type="text"/>
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
BSSID	00:30:4F:6E:5D:38

Wireless Network

- **Radio On/Off:** Enable or disable the wireless LAN.
- **Network Mode:** There are 6 modes: 11b only, 11g only, 11b/g mixed mode, and 11b/g/n mixed mode.
- **Network Name (SSID):** The service set identification (SSID) is a unique name to identify the router in the wireless LAN. Wireless stations associating to the router must have the same SSID. Enter a descriptive name. Its length is up to 32 characters.
- **Multiple SSID 1/2/3/4/5/6/7:** There are 7 multiple SSIDs. Enter their descriptive names that you want to use.
- **Broadcast Network Name (SSID):** Select **Enable** to allow the SSID broadcast on the network, so that the STA can find it. Otherwise, the STA can not find it.

- **AP Isolation:** Enable or disable AP Isolation. When many clients connect to the same access point, they can access each other. If you want to disable the access between clients which connect the same access point, you can enable this function.
- **MBSSID AP Isolation:** Enable or disable MBSSID AP Isolation.
- **BSSID:** Basic Service Set Identifier. This is the assigned MAC address of the station in the access point. This unique identifier is in Hex format and can only be edited when Multi BSSID is enabled in the previous screen.
- **Frequency (Channel):** A channel is the radio frequency used by wireless device. Channels available depend on your geographical area. You may have a choice of channels (for your region) and you should use a different channel from an adjacent AP to reduce the interference. The Interference and degrading performance occurs when radio signals from different APs overlap.

Wireless Distribution System (WDS)

WDS Mode: There are four options, including **Disable**, **Lazy Mode**, **Bridge Mode**, and **Repeater**

Mode.

➤ **Disable**

Select Disable to disable the WDS mode.

➤ **Lazy Mode**

Wireless Distribution System(WDS)	
WDS Mode	Lazy Mode ▼
Phy Mode	CCK ▼
EncrypType	NONE ▼

- **WDS Mode:** Select Lazy Mode.
- **Phy Mode:** It provides 4 options, including **CCK**, **OFDM**, **HTMIX**, and **GREENFIELD**.
- **Encryp Type:** It provides 4 options, including **None**, **WEP**, **TKIP**, and **AES**.

➤ **Bridge Mode/ Repeater Mode**

Wireless Distribution System(WDS)	
WDS Mode	Bridge Mode ▼
Phy Mode	CCK ▼
EncrypType	NONE ▼
AP MAC Address	<input type="text"/>
AP MAC Address	<input type="text"/>
AP MAC Address	<input type="text"/>
AP MAC Address	<input type="text"/>

- **WDS Mode:** Select **Bridge Mode** or **Repeater Mode**.
- **Phy Mode:** It provides 4 options, including CCK, OFDM, HTMIX, and GREENFIELD.
- **Encrypt Type:** It provides 4 options, including **None, WEP, TKIP, and AES**.
- **AP MAC Address:** It provides 4 AP MAC Address. Enter the MAC address of the other APs.

WDS (Wireless Distribution System) allows access points to communicate with one another wirelessly in a standardized way. It can also simplify the network infrastructure by reducing the amount of cabling required. Basically the access points will act as a client and an access point at the same time.

WDS is incompatible with WPA. Both features cannot be used at the same time. A WDS link is bi-directional, so the AP must know the MAC address of the other AP, and the other AP must have a WDS link back to the AP.

Dynamically assigned and rotated encryption key are not supported in a WDS connection. This means that WPA and other dynamic key assignment technologies may not be used. Only Static WEP keys may be used in a WDS connection, including any STAs that are associated with a WDS repeating AP.

Enter the MAC address of the other APs that you want to link to and click enable.

Supports up to 4 point to multipoint WDS links, check Enable WDS and then enable on the MAC addresses.

Example of a WDS topology:

AP1 <-- WDS --> Master AP (our AP) <-- WDS --> AP3 <-- WDS --> AP4

HT Physical Mode	
Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel BandWidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> Long <input checked="" type="radio"/> Auto
MCS	Auto ▾
Reverse Direction Grant(RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extension Channel	2457MHz (Channel 10) ▾
Aggregation MSDU(A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Auto Block ACK	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Decline BA Request	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

HT Physical Mode

- **Operation Mode:** Select Mixed Mode or Green Field.
- **Channel Bandwidth:** Select 20 or 20/40.
- **Guard Interval:** Select Long or Auto.
- **MCS:** Select the proper value between 0 and 15 or 32. Auto is the default value.
- **Reverse Direction Grant (RDG):** Select Disable or Enable.
- **Extension Channel:** Select the proper extension channel in the drop-down list.
- **Aggregation MSDU (A-MSDU):** Select Disable or Enable.
- **Auto Block ACK:** Select Disable or Enable.
- **Decline BA Request:** Select Disable or Enable.

Other	
HT TxStream	2 ▾
HT RxStream	2 ▾

Other

- **HT TxStream:** You can select 1 or 2 in the drop-down list.
- **HT RxStream:** You can select 1 or 2 in the drop-down list.

After finishing the settings above, click **Apply** to save the settings and make the new configuration take effect.

4.2 Advanced Wireless Settings

This page makes more detailed settings for the AP. **Advanced Wireless Settings** page includes items that are not available in the **Basic Wireless Settings** page, such as basic data rates, beacon interval, and data beacon rate.

Advanced Wireless Settings

Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon Interval, Control Tx Rates and Basic Data Rates.

Advanced Wireless	
BG Protection Mode	Auto <input type="button" value="v"/>
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	50 (range 1 - 100, default 100)
Short Preamble	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Short Slot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Tx Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Pkt_Aggregate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Country Code	None <input type="button" value="v"/>

Advanced Wireless

- **BG Protection Mode:** It provides 3 options, including Auto, On, and Off. The default BG protection mode is **Auto**.
- **Beacon Interval:** The interval time range is between 20ms and 999ms for each beacon transmission. The default value is 100ms.
- **Date Beacon Rate (DTM):** The DTM range is between 1 ms and 255 ms. The default value is 1ms.
- **Fragment Threshold:** This is the maximum data fragment size (between 256 bytes and 2346 bytes) that can be sent in the wireless network before the router fragments the packet into smaller data frames. The default value is 2346.

- **RTS Threshold:** Request to send (RTS) is designed to prevent collisions due to hidden node. A RTS defines the biggest size data frame you can send before a RTS handshake invoked. The RTS threshold value is between 1 and 2347. The default value is 2347.
If the RTS threshold value is greater than the fragment threshold value, the RTS handshake does not occur. Because the data frames are fragmented before they reach the RTS size.
- **Tx Power:** The Tx Power range is between 1 and 100. The default value is 100.
- **Short Preamble:** Select Disable or Enable.
- **Short Slot:** Select Disable or Enable.
- **Tx Burst:** Select Disable or Enable.
- **Pkt_Aggregate:** Select Disable or Enable.
- **Country Code:** Select the region which area you are. It provides six regions in the drop-down list.

Wi-Fi Multimedia	
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DLS Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Parameters	<input type="button" value="WMM Configuration"/>

Wi-Fi Multimedia

- **WMM Capable:** Enable or disable WMM.
- **APSD Capable:** Enable or disable APSD.
- **WMM Parameter:** Click WMM Configuration button to pop up WMM Parameters of Access Point page. You can configure WMM parameters in the page.

Multicast-to-Unicast Converter	
Multicast-to-Unicast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Multicast-to-Unicast Converter

Multicast-to-Unicast Converter: Enable or disable Multicast-to-Unicast Converter.

After finishing the settings above, click **Apply** to save the settings and make the new configuration take effect. Click **Cancel** to close without saving.

4.3 Security

Choose **Wireless Settings>Security** and the following page appears. It allows you to modify the settings to prevent the unauthorized accesses.

Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID

SSID choice: default

"default"

Security Mode: Disable

Access Policy

Policy: Disable

Add a station Mac:

Apply Cancel

Select SSID

SSID choice: Select SSID in the drop-down list.

Security

Security Mode: There are 11 options, including **Disable**, **OPEN**, **SHARED**, **WEPAUTO**, **WPA**, **WPA-PSK**, **WPA2**, **WPA2-PSK**, **WPAPSKWPA2PSK**, **WPA1WPA2**, and **802.1X**.

[EXAMPLE]

Take 802.1x for example. Select 802.1x in the **Security Mode** down-list. The page shown in the following page appears.

"default"

Security Mode: 802.1X

802.1x WEP

WEP: Disable Enable

Radius Server

IP Address: []

Port: 1812

Shared Secret: []

Session Timeout: 0

Idle Timeout: []

- **WEP:** Disable or enable WEP.

Radius Server

- **IP Address:** Enter the IP address of Radius Server.
- **Port:** The default port of the RADIUS server for authentication is 1812. You need not change this value unless your network administrator instructs you to do so with additional information.
- **Shared Secret:** Enter a password as the key to be shared between the external authentication server and the access point. The key is not send over the network. This key must be the same on the external authentication server and your router.
- **Session Timeout:** Set the time interval for session. Enter the proper value in the field.
- **Idle Timeout:** Set the idle time interval. Enter the proper value in the field.

Access Policy	
Policy	Disable ▾
Add a station Mac:	<input type="text"/>

Access Policy

- **Policy:** There are three options, including Disable, Allow, and Reject. You can choose Disable, Allow or Reject. Select Allow, only the clients whose MAC address is listed can access the router. Select Reject, the clients whose MAC address is listed are denied to access the router.
- **Add a station MAC:** If you want to add a station MAC, enter the MAC address of the wireless station that are allowed or denied access to your router in this address field.

After finishing the settings above, click **Apply** to save the settings and make the new configuration take effect. Click **Cancel** to close without saving.

4.4 WPS

You can enable or disable the WPS function in this page.

Wi-Fi Protected Setup	
You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.	
WPS Config	
WPS:	Enable ▾
<input type="button" value="Apply"/>	Disable Enable

Select **Enable** in the WPS drop-down list. Click **Apply** and the following page appear.

WPS Config

WPS: ▼

WPS Summary

WPS Current Status:	Idle
WPS Configured:	No
WPS SSID:	default
WPS Auth Mode:	Open
WPS Encryp Type:	None
WPS Default Key Index:	1
WPS Key(ASCII)	
AP PIN:	72328248

WPS Progress

WPS mode PIN PBC

PIN

WPS Status

WSC: Idle

WPS Summary

It displays the WPS information, such as WPS Current Status, WPS Configured, and WPS SSID. Reset OOB: Reset to out of box (OoB) configuration

WPS Progress

- **WPS mode:** There are two way for you to enable WPS function: **PIN, PBC**. You can use a push button configuration (PBC) on the Wi-Fi router. If there is no button, enter a 4- or 8-digit PIN code. Each STA supporting WPS comes with a hard-coded PIN code.
- **PIN:** If you select PIN mode, you need enter the PIN number in the field.

WPS Status

It displays the information about WPS status.

4.5 Station list

Through this page, you can easily identify the connected wireless stations. It automatically observes the ID of connected wireless station (if specified), MAC address, SSID, and current status.

Station List

You could monitor stations which associated to this AP here.

Wireless Network							
MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
00-30-40-56-12-3f	1	1	1 31	7	20M	1	0

Chapter 5 Firewall

5.1 MAC/IP/Port Filtering

You may set up firewall rules to protect your network from malicious activity on the Internet. It is also convenient for you to delete these settings.

MAC/IP/Port Filtering Settings

You may setup firewall rules to protect your network from virus, worm and malicious activity on the Internet.

Basic Settings

MAC/IP/Port Filtering:

Default Policy -- The packet that don't match with any rules would be:

MAC/IP/Port Filter Settings

MAC address:

Dest IP Address:

Source IP Address:

Protocol:

Dest Port Range: -

Source Port Range: -

Action:

Comment:

(The maximum rule count is 32.)

Current MAC/IP/Port filtering rules in system:

No.	MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
Others would be accepted									-


Basic Settings

- **MAC/IP/Port Filtering:** Enable or disable the MAC/IP/Port filtering function.
- **Default Policy:** The Packet that does not match any rules would be dropped or accepted.

MAC/IP/Port Filter Settings

- **MAC Address:** Enter the MAC address that matches the source address of the packet (optional).
- **Dest IP Address:** Enter the IP address that matches the destination address of the packet (optional).

- **Source IP Address:** Enter the IP address that matches the source address of the packet (optional).
- **Protocol:** There are 4 options, including none, TCP, UDP and ICMP.
- **Dest Port Range:** After setting a valid protocol, you may enter the UPD or TCP destination port range.
- **Source Port Range:** After setting a valid protocol, you may enter the UPD or TCP source port range.
- **Action:** Select **Drop** or **Accept** in the drop down list.
- **Comment:** Add description for this rule.

 The maximal rule number you can add is 32.

Click **Apply** to make the configuration take effect. Click **Reset** to cancel the new configuration.

Current MAC/IP/Port filtering rules in system:									
No.	MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
Others would be accepted									-
Delete Selected					Reset				

Current MAC/IP/Port filtering rules in system

If you want to delete some rules in the table above, select the rules, and then click **Delete Selected**.

Otherwise, click **Reset**.

5.2 Port Forwarding

This page allows you to set virtual server to provide services on the Internet.

Virtual Server Settings

You may setup Virtual Servers to provide services on Internet.

Virtual Server Settings

Virtual Server Settings	Disable ▾
IP Address	<input type="text"/>
Port Range	<input type="text"/> - <input type="text"/>
Protocol	TCP&UDP ▾
Comment	<input type="text"/>


(The maximum rule count is 32.)

Current Virtual Servers in system:

No.	IP Address	Port Range	Protocol	Comment
Delete Selected				
Reset				

Virtual Server Settings

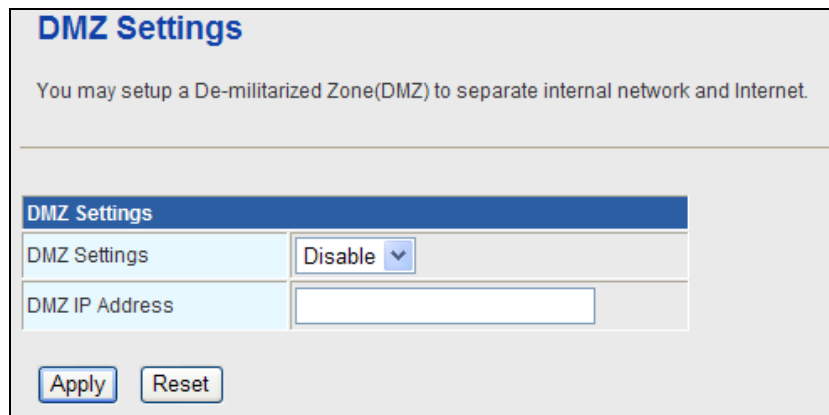
- **Virtual Server Settings:** Enable or disable this function. After selecting **Enable**, you can set the following parameters.
- **IP Address:** Enter the virtual server IP address in internal network.
- **Port Range:** Set the port range of virtual server.
- **Protocol:** There are 3 options, including none, TCP& UDP, TCP, and UDP.
- **Comment:** Add description for this rule.

	The maximal rule number you can add is 32.
---	--

Click **Apply** to make the configuration take effect. Click **Reset** to cancel the new configuration.

5.3 DMZ

This page allows you to set a De-militarized Zone (DMZ) to separate internal network and Internet.



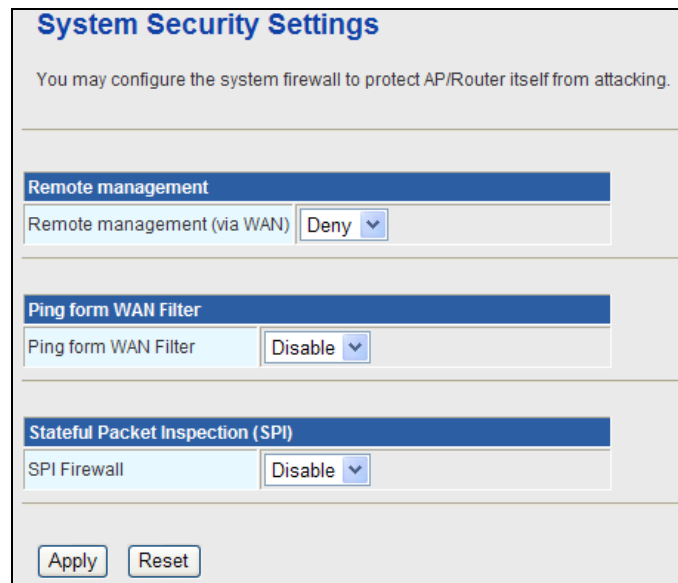
DMZ Settings	
DMZ Settings	Disable ▾
DMZ IP Address	<input type="text"/>

- **DMZ Settings:** Enable or disable this function. After selecting **Enable**, you can set the DMZ IP address.
- **DMZ IP Address:** Enter the DMZ host IP address.

Click **Apply** to make the configuration take effect. Click **Reset** to cancel the new configuration.

5.4 System Security Settings

Choose **Firewall > System Security** and the following page appears. This page allows you to configure the system firewall to protect AP from attacking.



The screenshot shows the 'System Security Settings' configuration page. At the top, there is a title 'System Security Settings' and a subtitle 'You may configure the system firewall to protect AP/Router itself from attacking.' Below this, there are three main sections, each with a blue header bar and a light blue input field with a dropdown menu:

- Remote management**: The input field is labeled 'Remote management (via WAN)' and the dropdown menu is set to 'Deny'.
- Ping from WAN Filter**: The input field is labeled 'Ping from WAN Filter' and the dropdown menu is set to 'Disable'.
- Stateful Packet Inspection (SPI)**: The input field is labeled 'SPI Firewall' and the dropdown menu is set to 'Disable'.

At the bottom of the page, there are two buttons: 'Apply' and 'Reset'.

Remote Management

Remote management (via WAN): Deny or allow remote management through web.

Ping from WAN Filter

Ping from WAN Filter: You may select enable or disable to determine whether to filter the ping package which comes from the external network.

Stateful Packet Inspection (SPI)

SPI Firewall: You may disable or enable the SPI firewall.

Click **Apply** to make the configuration take effect. Click **Reset** to cancel the new configuration.

5.5 Content Filtering

Choose **Firewall > Content Filtering** and the following page appears. You can set content filter to restrict the improper content access.

The screenshot shows the 'Content Filter Settings' page. At the top, it says 'You can setup Content Filter to restrict the improper content access.' Below this is the 'Webs Content Filter' section, which includes a 'Filters:' label, three checkboxes for 'Proxy', 'Java', and 'ActiveX', and 'Apply' and 'Reset' buttons. The 'Webs URL Filter Settings' section follows, containing a table of 'Current Webs URL Filters' with columns for 'No' and 'URL', and 'Delete' and 'Reset' buttons. Below the table is the 'Add a URL filter:' section, which has a 'URL:' label, an input field, and 'Add' and 'Reset' buttons.

Current Webs URL Filters:	
No	URL

Add a URL filter:	
URL:	<input type="text"/>

Current Webs URL Filters: If you want to delete some filters in the table above, select the rules, and then click **Delete**. Otherwise, click **Reset**.

Add a URL filter

URL: Enter a URL filter.

Click **Add** to add a URL filter. Otherwise, click **Reset** to cancel the URL filter.

Chapter 6 Administration

6.1 Management

Choose **Administration > Management**, and the following page appears. You may configure administrator account and password, NTP settings, and dynamic DNS settings in the page.

The screenshot shows a web interface titled "System Management" with a subtitle: "You may configure administrator account and password, NTP settings, and Dynamic DNS settings here." The interface is divided into four sections:

- Language Settings:** A dropdown menu for "Select Language" is set to "English". Below it are "Apply" and "Cancel" buttons.
- Administrator Settings:** Two input fields: "Account" (containing "admin") and "Password" (containing "*****"). Below are "Apply" and "Cancel" buttons.
- NTP Settings:** "Current Time" is "Sat Jan 1 01:43:07 UTC 2000" with a "Sync with host" button. "Time Zone:" is a dropdown menu set to "(GMT-11:00) Midway Island, Samoa". "NTP Server" is an input field with examples: "ex: time.nist.gov", "ntp0.broad.mit.edu", "time.stdtime.gov.tw". "NTP synchronization(hours)" is an empty input field. Below are "Apply" and "Cancel" buttons.
- DDNS Settings:** "Dynamic DNS Provider" is a dropdown menu set to "None". Below are input fields for "Account", "Password", and "DDNS". Below are "Apply" and "Cancel" buttons.

Administrator Settings

- **Account:** Enter the username of the administrator in the field.
- **Password:** Enter the password of the administrator in the field.

NTP Settings

- **Current Time:** Display the current date and time. Click **Sync with host**, the current time is synchronized by your PC which is connected to AP.
- **Time Zone:** Select the proper time zone in the drop-down list.
- **NTP Server:** Enter the IP address or domain name of NTP server.
- **NTP Synchronization (hours):** Enter the time interval for synchronization.

DDNS Settings

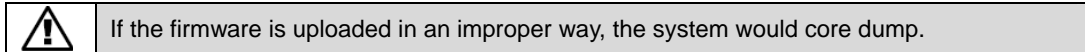
- **Dynamic DNS Provider:** Select the proper dynamic DNS provider in the drop-down list. After selecting a dynamic DNS provider, you are allowed to set the following parameters.

- **Account:** Enter the username of DDNS provider in the field.
- **Password:** Enter the password of DDNS provider in the field.
- **DDNS:** Enter the domain name of your device.

Click **Apply** to make the configuration take effect. Click **Cancel** to cancel the new configuration.

6.2 Management Upload Firmware

Choose **Administration > Upload Firmware** and the following page appears. In this page, you may upgrade the correct new version firmware to obtain new functionality. It takes about 1 minute to upload upgrade flash.



Upgrade Firmware

Upgrade the PLANET SoC firmware to obtain new functionality. **It takes about 1 minute to upload upgrade flash and be patient please. Caution! A corrupted image will hang up the system.**

Update Firmware

Location: Browser..

Apply

Update Firmware

Location: Click **Browse** to select the firmware file, and click **Apply** to upgrade the firmware.

6.3 Setting Management

Choose **Administration > Settings Management** and the following page appears. You may save system settings by exporting them to a configuration file, restore them by importing the file, or reset them to the factory default.

Settings Management

You might save system settings by exporting them to a configuration file, restore them by importing the file, or reset them to factory default.

Export Settings

Export Button Export

Import Settings

Settings file location 瀏覽...

Import Cancel

Load Factory Defaults

Load Default Button Load Default

Export Settings

Export Button: Click the **Export** to export the settings.

Import Settings

Settings file location: Click **Browse** to select the configuration file, and then click **Import** to upload the configuration file. Click **Cancel** to cancel the uploading operation.

Load Factory Defaults

Load Default Button: Click **Load Default** to make AP return to the default settings.

6.4 Status

Choose **Administration > Status** and the following page appears. It displays the information about AP status, including system information, Internet configurations, and local network.

Access Point Status


Let's take a look at the status of PLANET SoC Platform.

System Info	
SDK Version	3.2.0.0 (May 31 2009)
System Up Time	1 hour, 55 mins, 27 secs
Operation Mode	Gateway Mode

Internet Configurations	
Connected Type	DHCP
WAN IP Address	
Subnet Mask	
Default Gateway	
Primary Domain Name Server	
Secondary Domain Name Server	
MAC Address	00:30:4F:6E:5D:38

Local Network	
Local IP Address	192.168.0.1
Local Netmask	255.255.255.0
MAC Address	00:30:4F:6E:5D:38

Ethernet Port Status



6.5 Statistic

Choose **Administration > Statistics** and the following page appears. This page shows all the statistics information about your AP.

Statistic	
Take a look at the PLANET SoC statistics	
Memory	
Memory total:	29412 kB
Memory left:	13948 kB
WAN/LAN	
WAN Rx packets:	0
WAN Rx bytes:	0
WAN Tx packets:	690
WAN Tx bytes:	403716
LAN Rx packets:	10378
LAN Rx bytes:	678938
LAN Tx packets:	8322
LAN Tx bytes:	1567917
All interfaces	
Name	eth2
Rx Packet	15278
Rx Byte	2585997
Tx Packet	22547
Tx Byte	4236152
Name	lo
Rx Packet	14
Rx Byte	2249
Tx Packet	14
Tx Byte	2249
Name	eth2.1

6.6 System Log

Choose **Administration > System Log** and the following page appears. You are allowed to view and clear the system log in this page.

System Log

Syslog:

Remote System Log Settings

Enable

IP Address

System Log

```
Jan 1 00:06:52 PlanetAP syslog.info syslogd started: BusyBox v1.12.1
Jan 1 00:06:52 PlanetAP user.notice kernel: klogd started: BusyBox v1.12.1 (200
Jan 1 00:06:55 PlanetAP user.debug kernel: eth2.2: no IPv6 routers present
Jan 1 00:06:56 PlanetAP user.debug kernel: ra0: no IPv6 routers present
Jan 1 00:06:57 PlanetAP user.debug kernel: br0: no IPv6 routers present
```

Click **Refresh** to refresh the log. Click **Clear** to clear the log.