P-6101C (DSL-100HN-T1A v2)

User Manual

802.11n wireless ADSL2+ 4port router

Version: 1.13
Original: 6/2012

預設登入資訊	
IP Address	http://192.168.1.1
Username	user
Password	user

Wireless Parameters:

SSID: ____________________

Key : ____________________

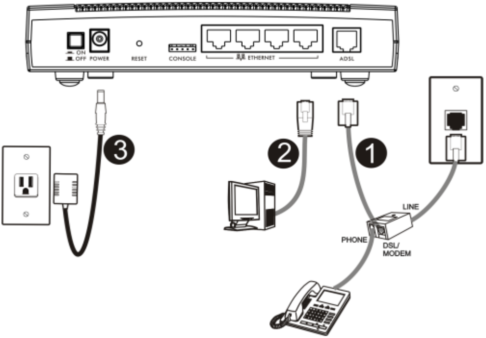
In order to avoid hacker to attache the wireless AP,WPA2-PSK and AES authentication method is suggested (see Page 8) and change the user password

ZyXEL

Introduction

P-6101Cis802.11n ADSL2+wireless 4 port router and provide high-rate internet service。Its internal switch can connect at most 4 pcs.IEEE 802.11n wireless (AP) can provide wireless internet service.
This Manual will provide the steps how to set P-6101C for Internet services and you need to have the account info provided by the ISP.

Hardware Connection



1. ADSL： Please connect the telephone line to the wall jack to get the Internet service. If you need to use the attached ADSL splitter, first connect one side of the telephone line to the Ethernet port, then the other side

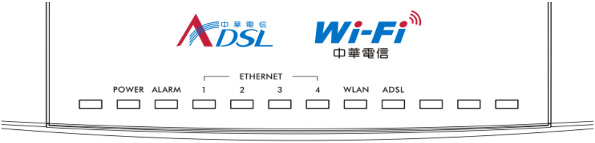
to the Splitter, then connect the Splitter line port to the wall jack of the telephone

Splitter has three interfaces：

- LINE：Connect to the Phone wall jack
- MODEM：Connect to the device’ s ADSL jack
- PHONE：Connect to Phone

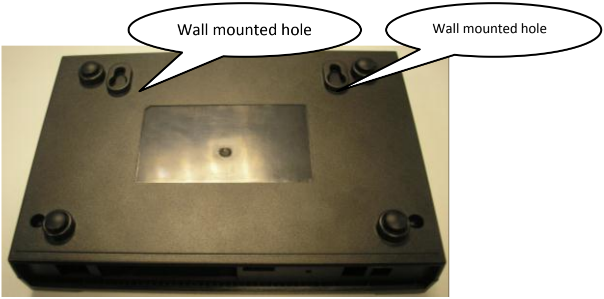
2. ETHERNET： Use Ethernet Cable to connect the Ethernet ports to PC or STB (Set-Top- Box) in order to connect to the Internet and get VOD.
3. POWER：ON/OFF to power on/shut off P-6101C
4. CONSOLE: Management Port for engineering usage

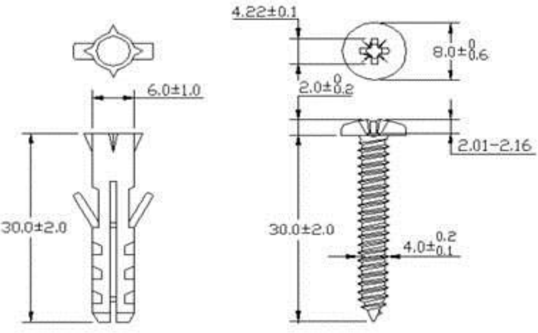
Check LED



If LED cannot be on, please plug off the power and re-check the hardware

Wall Mounted Function





If you want to mount this product onto the wall, please follow below step.

Step 1: use screws (Dimension:4.0mm) fix bracket into the wall
Step 2: put equipment mount on bracket

Product Spec

- Anntena : 1* Embedded Antenna
- Band : 2.4 GHz (11g/n) USA (FCC): 2.412 to 2.462 GHz
- Max. output power :
  a. 11b/g 54Mbps 15dbm
  6Mbps 19dbm
  b. 11g/n 20MHz 15dbm
  40MHz 15dbm
- Wired transfer rate : 10/100Mbps （full-duplex/half-duplex）
- LAN : 4*port
- WLAN:
  a. Max. transfer rate : 150Mbps
  b. WMM support
  c. WEP support
  d. WPA/WPA2-PSK support
  e. WPA2 support
  f. WPA/WPA2-Enterprise Support

ADSL Spec

- ADSL line code: DMT modulation

- Handshake protocol: ITU-T Rec. G.994.1
- SNR margin: display real-time SNR margin for both upstream and downstream on demand
- ATM transmission convergence: ITU-T G.992.5 Annex K.
- Spectra bound should be configurable
- Spectra Mask:

  - Transmitter signal comply with Power Spectrum Density (PSD) mask specified in Annex A of ITU-T Rec. G.992.5 and the pass-band PSD ripple should be no greater than +1.0dB.

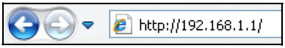
  - Support ITU-T G.992.5 Annex M

- Controllable spectrum bound: ITU-T G.992.5
- EOC and Overhead Channel Access：ITU-T Rec G.992.5 and ITU-T Rec G.997.1
- Latency path function: ITU-T Rec G.992.5
- Rate Adaptive modes: ITU-T Rec G.992.5 and ITU-T Rec G.997.1
- Selectable pilot subcarrier for downstream direction: ITU-T Rec G.992.5
- Power Management Link state (including L0,L2 and L3): specified in ITU Rec G.992.5 and L2, L3 should be configurable.
- Power Management: ITU-T Rec G.992.5 and the transitions between L0 and L2 states in downstream should comply with ITU-T Rec G.992.5 and ITU-T Rec G.997.1

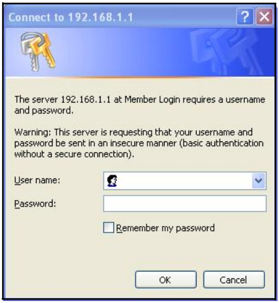
- The loop diagnostics function: ITU-T Rec G.992.5
- Seamless Rate Adaptation (SRA): On-line configuration specified in ITU-T Rec G.992.5
- Non-overlapped spectrum operation: ITU-T Rec G.992.5
- Trellis Coding: ITU-T Rec G.992.5
- Dying Gasp Message: ITU-T Rec G.992.5
- Backward compatibility: ADSL G.dmt and an ADSL2 line by auto-handshake technique
- Impulse Noise Protection: ITU-T Rec G.992.5
- Should show near-end Errored Second (ES), Severely Errored Second (SES) and Unavailable Second (UAS)
- Support to show near-end Code Violation
- Target Noise margin, Max. Noise Margin, Min. Noise Margin, Up-shift Noise Margin, Down-shift Noise Margin, Max. Interleaving Delay, Min.Net Date Rate, Max.Net Data Rate, INP_min, and the Max. normal transmit PSD for downstream should be supported and configurable.
- AAL 5 PVC supporting UBR, the configurable parameter shall include PCR and CDVT
- F5 End-to End OAM loopback function (ITU-T Rec.1.610)

WEB GUI Page

1. Type the blew IP in the browser「192.168.1.1」。



2. Type the username: user，Password: user. Enter OK



The server 192.168.1.1 at Member Login requires a username and password.

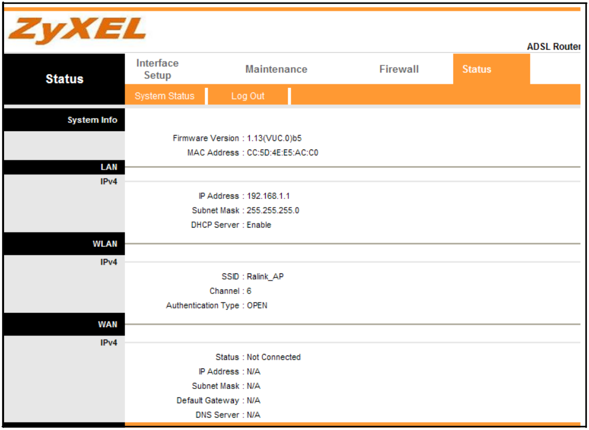
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name:

Password:

□ Remember my password

3. Main page



System Info

Firmware Version : 1.13(VUC.0)b5
MAC Address : CC:5D:4E:E5:AC:C0

LAN
IPv4

IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0
DHCP Server : Enable

WLAN
IPv4

SSID : Ralink_AP
Channel : 6
Authentication Type : OPEN

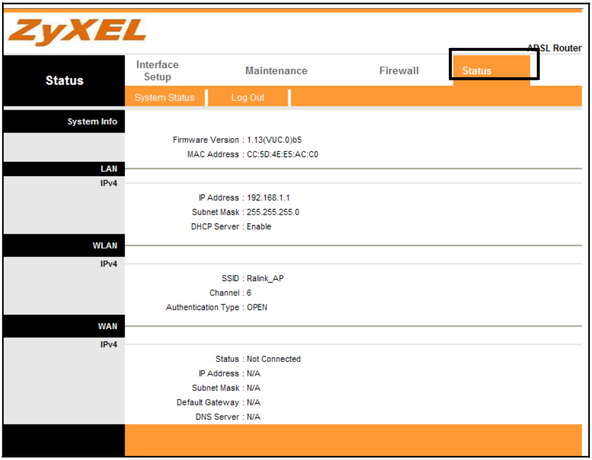
WAN
IPv4

Status : Not Connected
IP Address : N/A
Subnet Mask : N/A
Default Gateway : N/A
DNS Server : N/A

Basic Functions:

Status Page

Statuswill show info such as FW version, MAC, WAN, LAN, WLAN and so on



System Info

Firmware Version : 1.13(VUC.0)b5
MAC Address : CC:5D:4E:E5:AC:C0

LAN
IPv4

IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0
DHCP Server : Enable

WLAN
IPv4

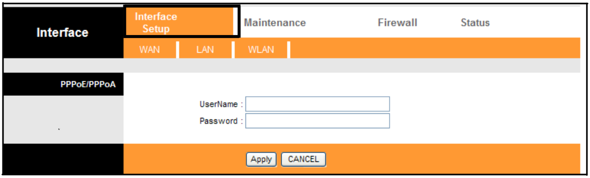
SSID : Ralink_AP
Channel : 6
Authentication Type : OPEN

WAN
IPv4

Status : Not Connected
IP Address : N/A
Subnet Mask : N/A
Default Gateway : N/A
DNS Server : N/A

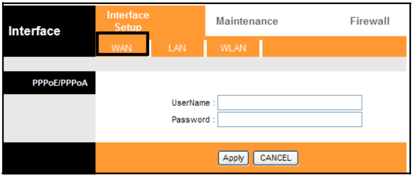
Interface Setup

You can set WAN\ LAN\WLAN under Interface Setup



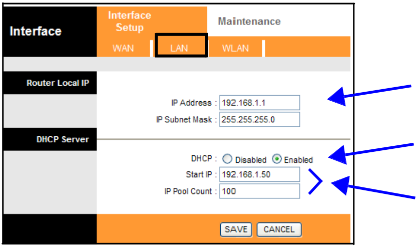
WAN

Make settings for the Internet services, ISP will provide you the related PPPoE/PPPoA account info. The device will automatically dial and your PC doesn’ t need to do any dial operation. With this setting, please refer to LAN/DHCP.



LAN

Set IP address of the LAN network and run DHCP server



IP Address : 192.168.1.1
IP Subnet Mask : 255.255.255.0

DHCP : ○ Disabled ● Enabled
Start IP : 192.168.1.50
IP Pool Count : 100

Current IP address

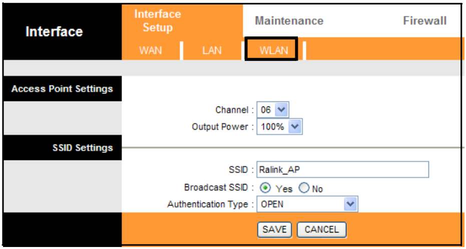
Choose Enabled to run DHCP server

IP Range

WLAN

WLAN Setting options:

- Channel: Wireless transfer channel
- Output Power: Adjust the wireless coverage
- SSID: Wireless AP Name，Type in English or Number
- Broadcast SSID: Choose Yes, when you search the wireless AP, will see the SSID name; If Choose No, will not see the SSID name, need to type the SSID to make the computer to connect to the device
- Authentication Type: Choose the secure authentication methods (WEP、WPAPSK、WPA2PSK)or unsecure authentication way(OPEN)。



Channel : 06

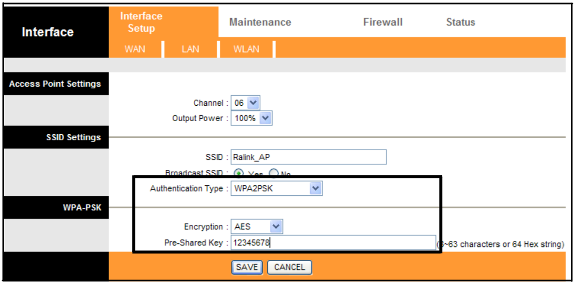
Output Power : 100%

SSID : Ralink_AP

Broadcast SSID : ● Yes ○ No

Authentication Type : OPEN

- Secure mode and pre-shared key : E.g. under Authentication Type , choose WPA2-PSK。Under Encryption and PreShared Key fill in the passwords



Channel : 06

Output Power : 100%

SSID : Ralink_AP

Broadcast SSID : ● Yes ○ No

Authentication Type : WPA2PSK

Encryption : AES

Pre-Shared Key : 12345678 (8~63 characters or 64 Hex string)

After this, click save button to save all the settings.

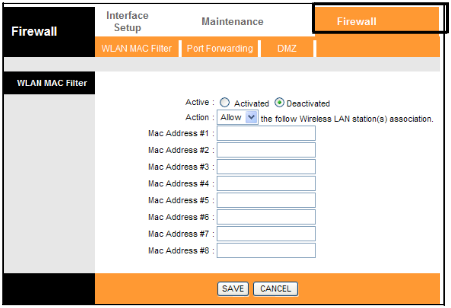
Test Wireless:

1. Wireless clients search the SSID of P-6101C
2. Choose the same authentication way as P-6101C and fill the same key
3. Get the LAN IP assigned by the device

If wireless clients can’t connect to the Internet, check the DSL connection and Internet account info

Firewall

Set the router to make the servers behind your router can be seen outside



Active : ○ Activated ● Deactivated

Action : Allow the follow Wireless LAN station(s) association.

Mac Address #1 :

Mac Address #2 :

Mac Address #3 :

Mac Address #4 :

Mac Address #5 :

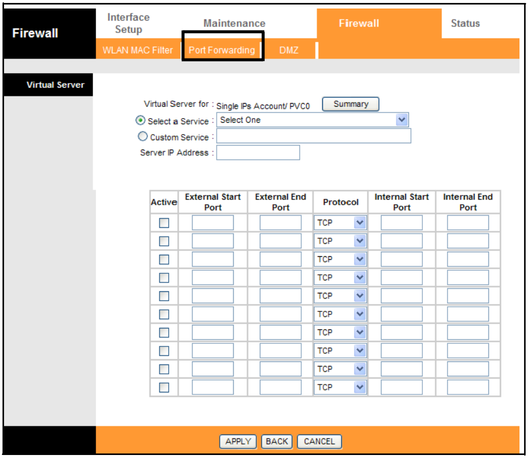
Mac Address #6 :

Mac Address #7 :

Mac Address #8 :

Port Forwarding

First, Interface Setup > WAN set PPPoE/ PPPoA account info



Virtual Server for : Single IPs Account/ PVC0

● Select a Service : Select One

○ Custom Service :

Server IP Address :

Active	External Start Port	External End Port	Protocol	Internal Start Port	Internal End Port
□			TCP		
□			TCP		
□			TCP		
□			TCP		
□			TCP		
□			TCP		
□			TCP		
□			TCP		
□			TCP		
□			TCP		

Then:

1. Select a Service : Choose the service you need and fill in the IP address of the Server

2. Check the port number of the server service , If correct, chooseActive , thenAPPLY。

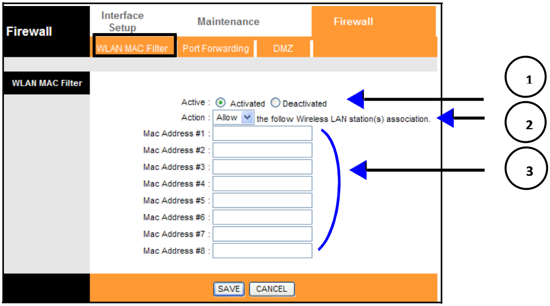
WLAN MAC Filter

MACfilter will deny or allow the corresponding wireless clients to connect to the router via wireless。

1. Choose Activated

2. Allow or Deny the corresponding wireless client

3. Fill in MAC address，then Click Save button.



Active : ● Activated ○ Deactivated

Action : Allow the follow Wireless LAN station(s) association.

Mac Address #1 :

Mac Address #2 :

Mac Address #3 :

Mac Address #4 :

Mac Address #5 :

Mac Address #6 :

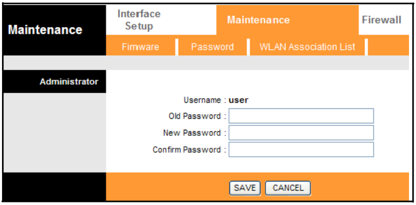
Mac Address #7 :

Mac Address #8 :

Password

Set password of the device in the below page

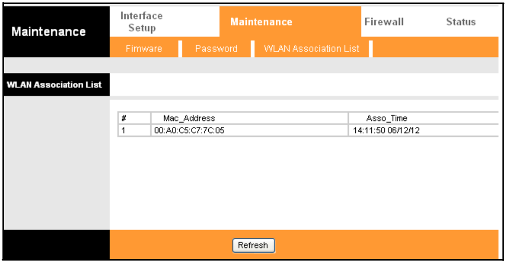
Step:Type the original password(user) , then type the new password , fill in twice , then click SAVE button.



Username : user
Old Password :
New Password :
Confirm Password :

WLAN Association List

In this page, you will see the wireless clients that are connected to the router with the info such as MAC address and time.



#	Mac_Address	Asso_Time
1	00:A0:C5:C7:7C:05	14:11:50 06/12/12

ATTENTION !

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

. This device may not cause harmful interference.

. This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device 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 device does cause harmful interference to radio/television reception, which can be determined by turning the device 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 the 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/TV technician for help.

FCC Radiation Exposure Statement

. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

. IEEE 802.11b or 802.11g or 802.11n(20MHz) operation of this product in the U.S.A. is firmware-limited to channels 1 through 11. IEEE 802.11n(40MHz)operation of this product in the U.S.A. is firmware-limited to channels 3 through 9.

. To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

The user manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. In cases where the manual is provided only in a form other than paper, such as on a computer disk or over the Internet, the information required by this section may be included in the manual in that alternative form, provided the user can reasonably be expected to have the capability to access information in that form.