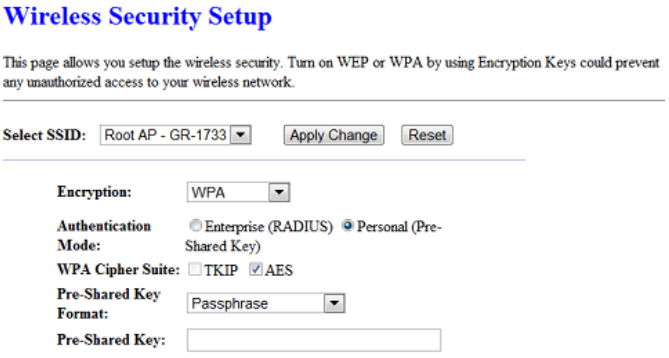
2. Encryption- WPA (WPA, WPA2, and WPA2 Mixed), WPA Authentication Mode

(1) Enterprise (RADIUS): Please fill in the RADIUS server Port, IP Address, and Password

(2) Personal (Pre-Shared Key): Pre-Shared Key type is ASCII Code; the length is between 8 to 63 characters. If the key type is Hex, the key length is 64 characters.



(3) Apply Change & Reset: Click on 'Apply Changes' to save setting data. Or click 'Reset' to reset all the input data.

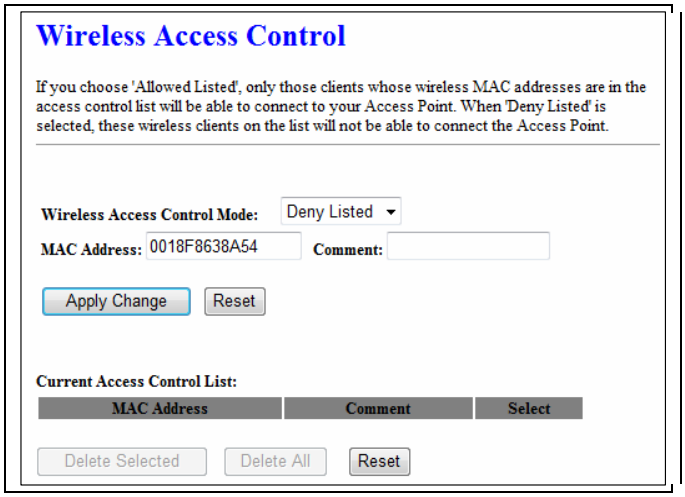
4.3 Wireless Access Control

Access Control allows user to block or allow wireless clients to access this router. Users can select the access control mode, then add a new MAC address with a simple comment and click on "Apply Change" to save the new addition. To delete a MAC address, select its

corresponding checkbox under the Select column and click on “Delete Selected” button.

Take the wireless card as the example.

(1) Please select Deny Listed in Wireless Access Control Mode first, and then fill in the MAC address what you plan to block in the MAC Address field. Click Apply Changes to save the setting.



(2) The MAC address what you set will be displayed on the Current Access Control List.

(3) The wireless client will be denied by the wireless router.

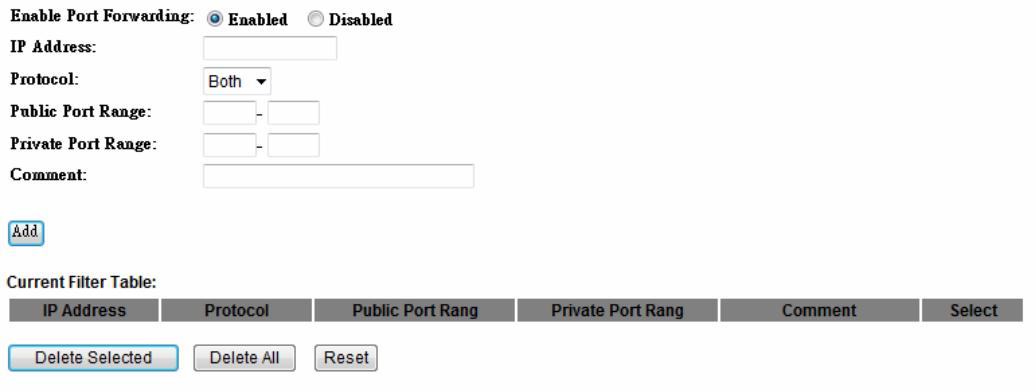
Chapter 5 Router Mode Security Setup

This section contains configurations for the BR485D's advanced functions such as: virtual server, DMZ, and Firewall to provide your network under a security environment.

5.1 NAT

5.1.1 Virtual Server

The Virtual Server feature allows users to create Virtual Servers by re-directing a particular range of service port numbers (from the WAN port) to a particular LAN IP address.

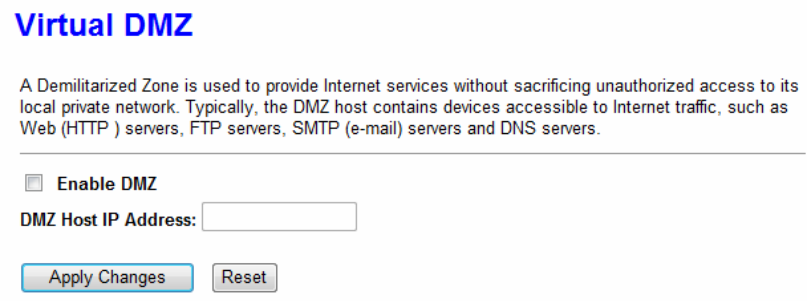


Item	Description
Enable Port Forwarding	Select to enable Port Forwarding service or not.
IP Address	Specify the IP address which receives the incoming packets.
Protocol	Select the protocol type.
Public Port Range	Enter the port number, for example 80-80.
Private Port Range	Enter the port number, for example 20-22.
Comment	Add comments for this port forwarding rule.
Add	Click on **Add** to enable the settings.
Current Port Forwarding Table	It will display all port forwarding regulation you made.
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.
Reset	Click **Reset** to cancel.

Please find the following figure to know that what the virtual server is. The web server is located on 192.168.1.100, forwarding port is 80, and type is TCP+UDP.

5.1.2 Virtual DMZ

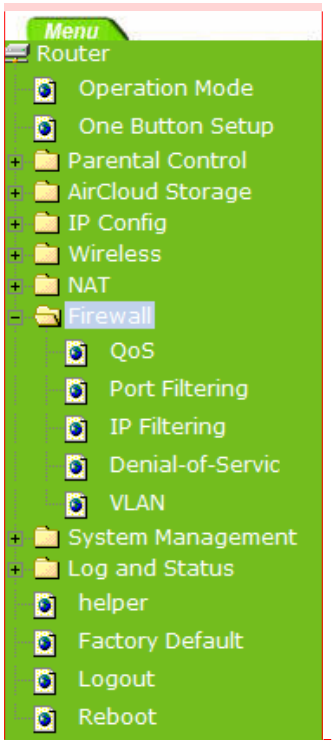
The DMZ feature allows one local user to be exposed to the Internet for special-purpose applications like Internet gaming or videoconferencing. When enabled, this feature opens all ports to a single station and hence renders that system exposed to intrusion from outside. The port forwarding feature is more secure because it only opens the ports required by that application.



Item	Description
Enable DMZ	It will enable the DMZ service if you select it.
DMZ Host IP Address	Please enter the specific IP address for DMZ host.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

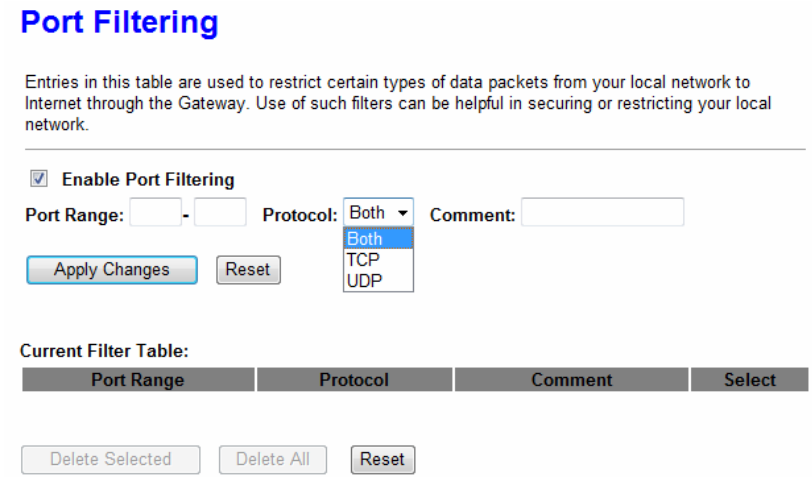
5.2 Firewall

註解 [J1]: 111



5.2.1 Port Filtering

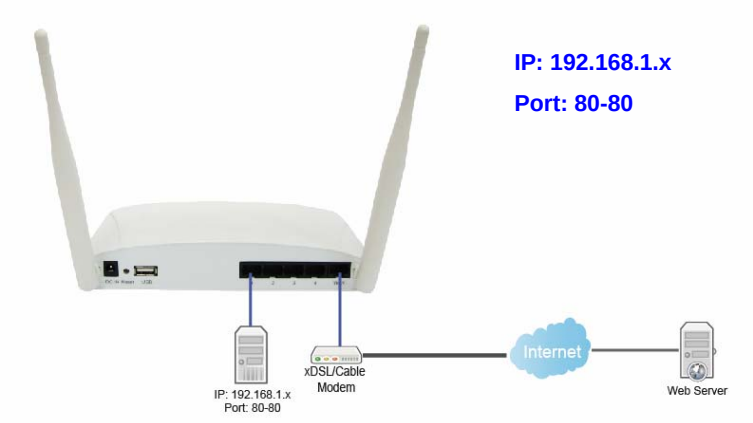
When enabled packets are denied access to Internet/filtered based on their port address.



Item	Description
Enable Port Filtering	Select Enable Port Filtering to filter ports.
Port Range	Enter the port number that needs to be filtered.

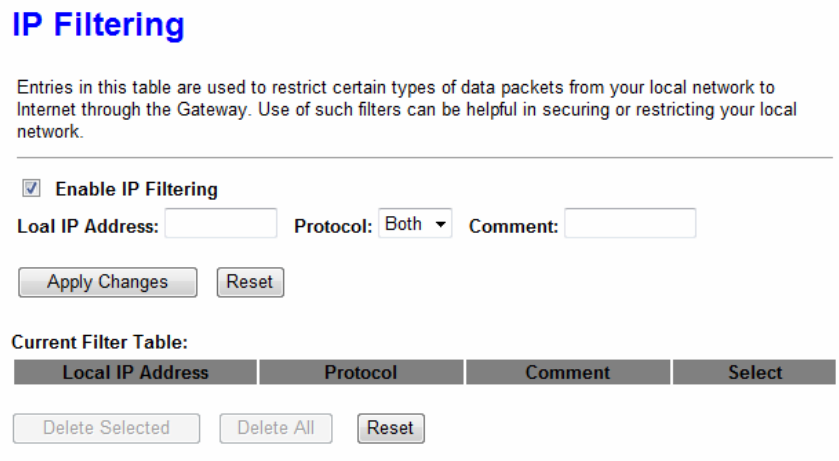
Protocol	Please select the protocol type of the port.
Comment	You can add comments for this regulation.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.
Reset	You can click **Reset** to cancel.

Port 80 has been blocked as the following illustrate.



5.2.2 IP Filtering

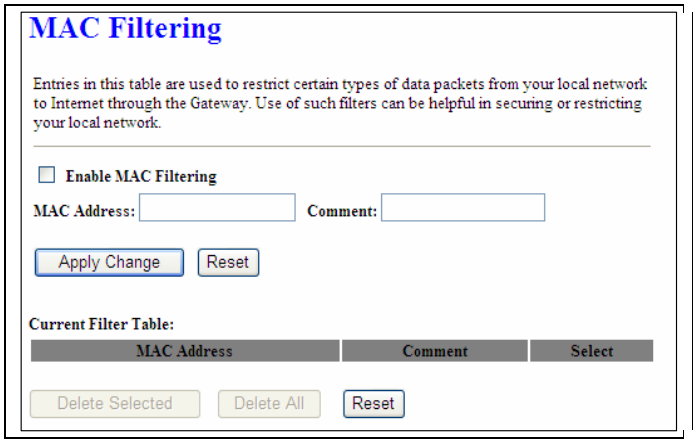
When enabled, LAN clients are blocked / filtered from accessing the Internet based on their IP addresses.



Item	Description
Enable IP Filtering	Please select Enable IP Filtering to filter IP addresses.
Local IP Address	Please enter the IP address that needs to be filtered.
Protocol	Please select the protocol type of the IP address
Comment	You can add comments for this regulation.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.
Reset	You can click **Reset** to cancel.

5.2.3 MAC Filtering

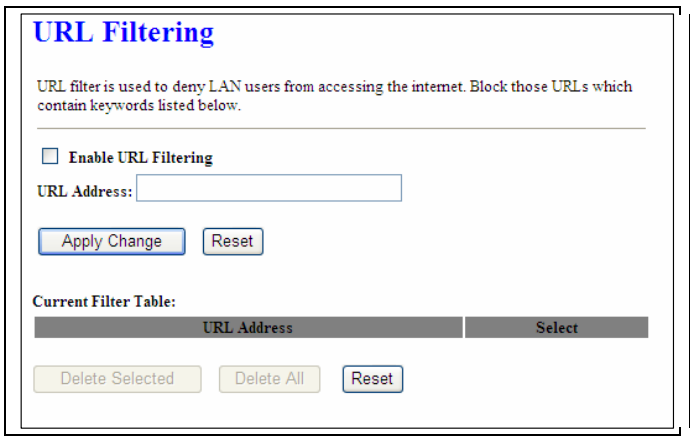
When enabled, filtering will be based on the MAC address of LAN computers. Any computer with its MAC address on this list will be blocked from accessing the Internet.



Item	Description
Enable MAC Filtering	Please select Enable MAC Filtering to filter MAC addresses.
MAC Address	Please enter the MAC address that needs to be filtered.
Comment	You can add comments for this regulation.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.
Reset	You can click **Reset** to cancel.

5.2.4 URL Filtering

URL Filtering is used to restrict users to access specific websites in internet



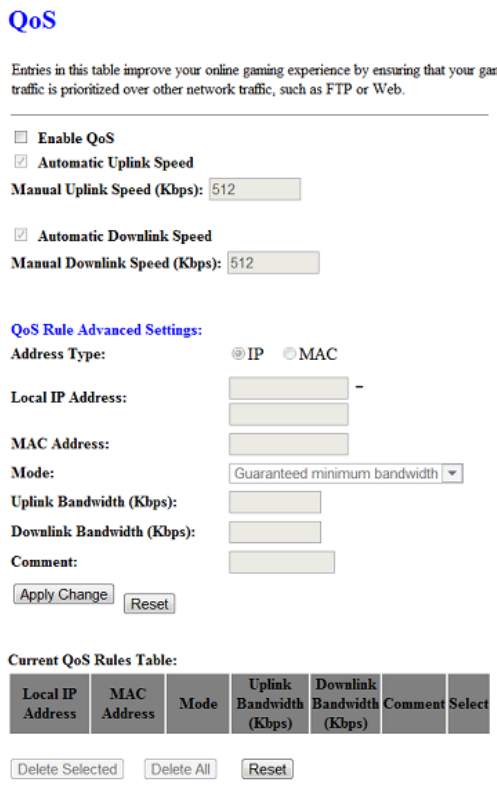
Item	Description
Enable URL Filtering	Please select Enable MAC Filtering to filter MAC addresses
URL Address	Please enter the MAC address that needs to be filtered.
Apply Changes & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.
Reset	You can click **Reset** to cancel.

Notes: This function will not be in effect when the Virtual Server is enabled. Please disable Virtual Server before activate the URL Filtering function.

5.2.5 QoS

The QoS can let you classify Internet application traffic by source/destination IP address and port number.

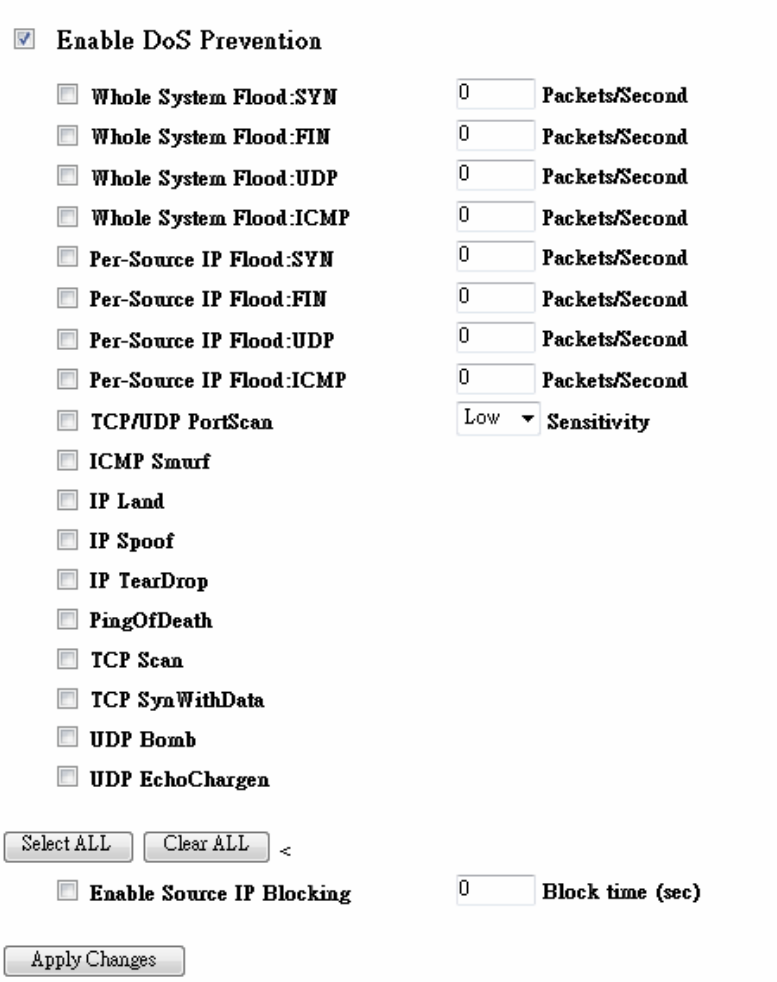
To assign priority for each type of application and reserve bandwidth can let you have a better experience in using critical real time services like Internet phone, video conference …etc.



Item	Description
Enable QoS	Check “Enable QoS” to enable QoS function for the WAN port. You also can uncheck “Enable QoS” to disable QoS function for the WAN port.
Automatic uplink speed / Manual Uplink Speed	Set the uplink speed by manual to assign the download or upload bandwidth by the unit of Kbps or check the Automatic uplink speed.
Automatic downlink speed / Manual Downlink Speed	Set the downlink speed by manual to assign the download or upload bandwidth by the unit of Kbps or check the Automatic downlink speed.

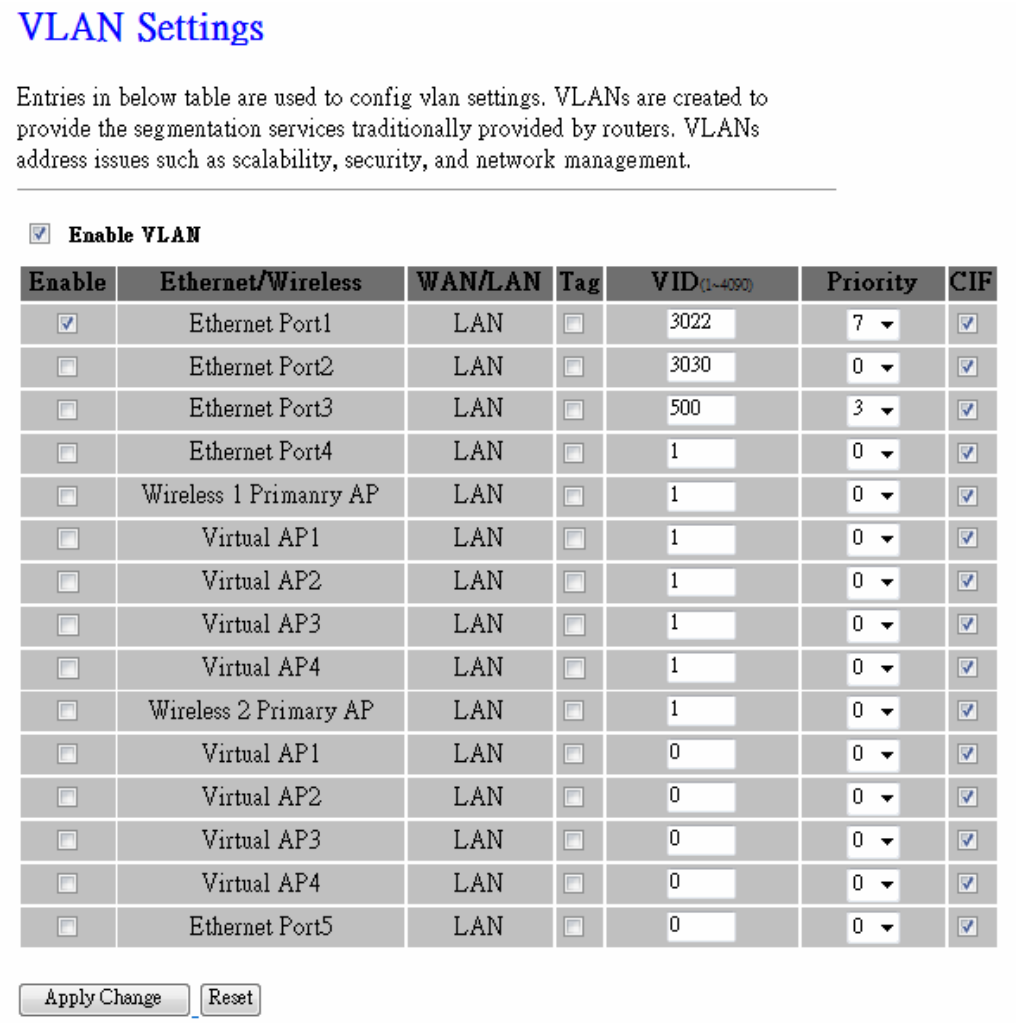
QoS Rule Advance Setting:	
Address Type	Set QoS by **IP** Address or **MAC** address
Local IP Address	Set local IP Address if the address type is by IP Address
MAC Address	Set MAC Address if the address type is by MAC Address
Mode	Select **Guaranteed minimum bandwidth** or **Restricted maximum bandwidth**
Bandwidth	Key in the bandwidth.
Comment	Write your comment here.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

5.2.6 Denial of Service



Item	Description
Enable DoS Prevention	Check “Enable DoS Prevention” to enable DoS function for prevention. You also can uncheck ““Enable DoS Prevention” to disable DoS function.

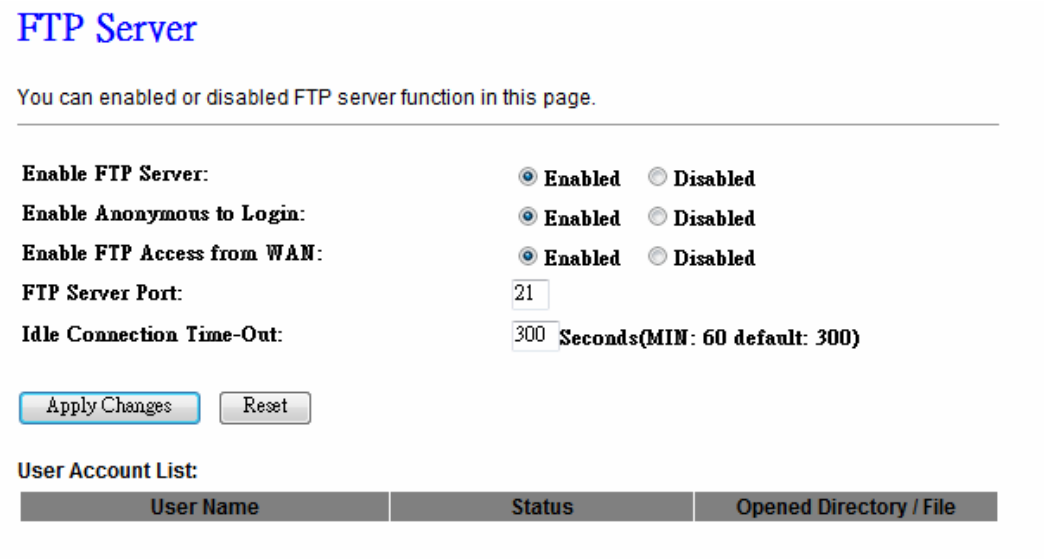
5.2.7 VLAN Settings



Item	Description
Tag	Add VLAN tag to packet
VID	Set VLAN ID（1~4096）
Priority	It indicates the frame priority level. Values are from 0 (best effort) to 7 (highest); 1 represents the lowest priority
CIF	Enable or Disable CIF

5.3 Server Setup

5.3.1 FTP



Item	Description
Enable FTP Server	FTP server start or stop
Enable Anonymous to Login	Agree anonymous account login to FTP server
Enable FTP Access from WAN	Allow user access device FTP server from WAN side（internet）
FTP Server Port	Default FTP server port is 21
Idle Connection Time-Out	FTP process should have an idle timeout, which will terminate the process and close the control connection if the server is inactive (i.e., no command or data transfer in progress) for a long period of time

Chapter 6 Advanced Setup

You can find advanced settings in this section.

Router Router Mode only.

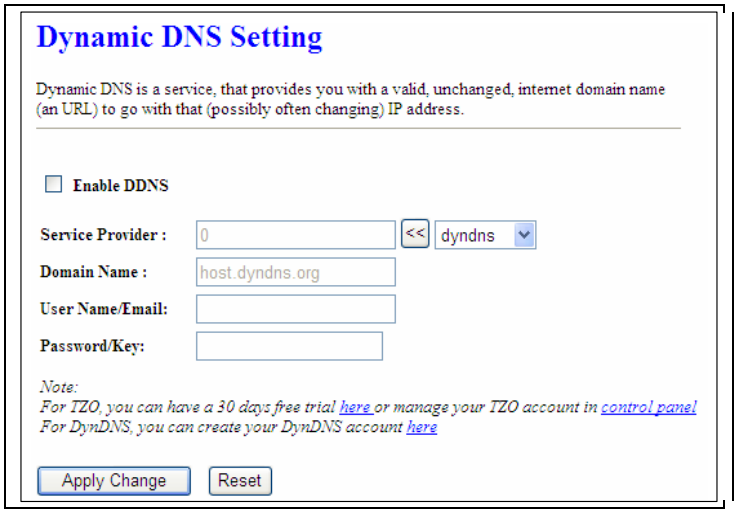
AP AP Mode only.

WiFi-AP WiFi AP Mode only.

6.1 Dynamic DNS Setting Router

You can assign a fixed host and domain name to a dynamic Internet IP address. Each time the router boots up, it will re-register its domain-name-to-IP-address mapping with the DDNS service provider. This is the way Internet users can access the router through a domain name instead of its IP address.

Note: make sure that you have registered with a DDNS service provider before enabling this feature.

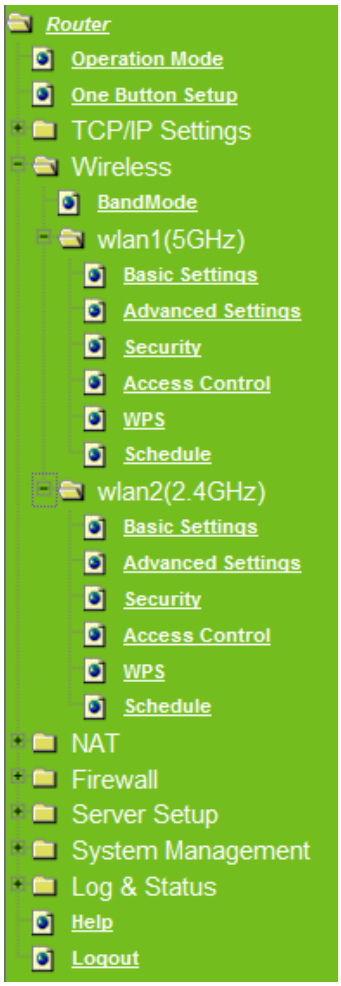


Please enter Domain Name, User Name/Email, and Password/Key. After entering, click on Apply Changes to save the setting, or you may click on Reset to clear all the input data.

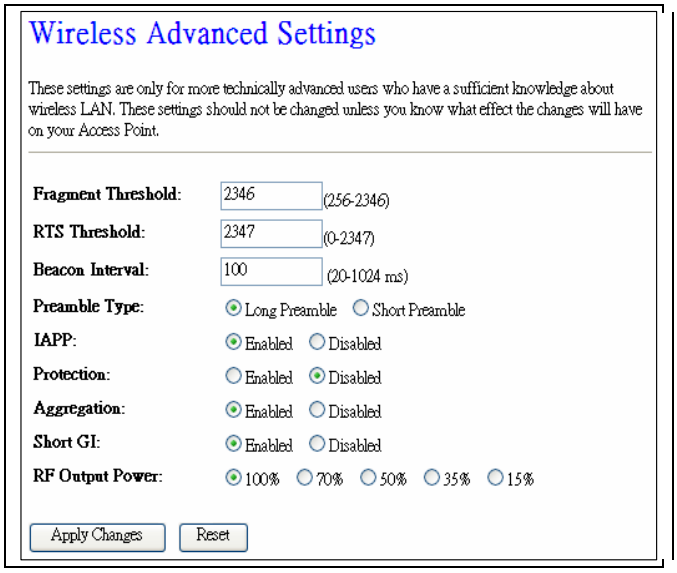
Item	Description
Enable/Disable DDNS	Select enable to use DDNS function. Each time your IP address to WAN is changed, and the information will be updated to DDNS service provider automatically.
Service Provider	Choose correct Service Provider from drop-down list, here including DynDNS, TZO, ChangeIP, Eurodns, OVH, NO-IP, ODS, Regfish embedded in BR485D.

User Name/Email	User name is used as an identity to login Dynamic-DNS service.
Password/Key	Password is applied to login Dynamic-DNS service.
Apply Changes & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

6.2 Wireless Advanced Setup



In Advanced Settings page, more 802.11 related parameters are tunable.



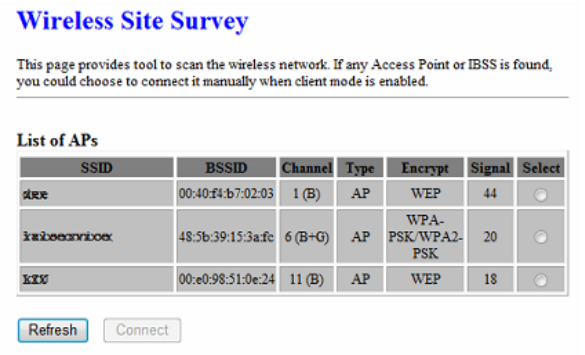
Item	Description
Fragment Threshold	To identify the maxima length of packet, the over length packet will be fragmentized. The allowed range is 256-2346, and default length is 2346.
RTS Threshold	This value should remain at its default setting of 2347. The range is 0~2347. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the present RTS threshold size, the RTS/CTS mechanism will not be enabled. The router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. Fill the range from 0 to 2347 into this blank.
Beacon Interval	Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. The allowed setting range is 20-1024 ms..
Preamble Type	PLCP is Physical layer convergence protocol and PPDU is PLCP protocol data unit during transmission, the PSDU shall be appended to a PLCP preamble and header to create the PPDU. It has 2 options: Long Preamble and Short Preamble.
IAPP	Inter-Access Point Protocol is a recommendation that describes an optional extension to IEEE 802.11 that provides wireless access-point communications among multivendor systems.
Protection	Please select to enable wireless protection or not.
Aggregation	Enable this function will combine several packets to one and transmit it. It can reduce the problem when mass packets are transmitting.
Short GI	Users can get better wireless transmission efficiency when they enable this function.
RF Output Power	Users can adjust RF output power to get the best wireless network environment. Users can choose from 100%, 70%, 50%, 35%, and

	15%.
Apply Changes & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

6.2.1 Wireless Site Survey WiFi-AP

This function provides users to search existing wireless APs or wireless base stations from ISP. You can connect to a wireless AP manually in Wi-Fi AP mode. The designed AP will appear on SSID column in Wireless Basic Setup page.

Please click on Refresh to refresh the list. Click Connect after select an existing AP to connect.



6.2.2 WPS Router AP

This page allows user to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client atomically synchronize it's setting and connect to the Access Point in a minute without any hassle. BR485D could support both Self-PIN or PBC modes, or use the WPS button (at real panel) to easy enable the WPS function.

PIN model, in which a PIN has to be taken either from a sticker label or from the web interface of the WPS device. This PIN will then be entered in the AP or client WPS device to connect.

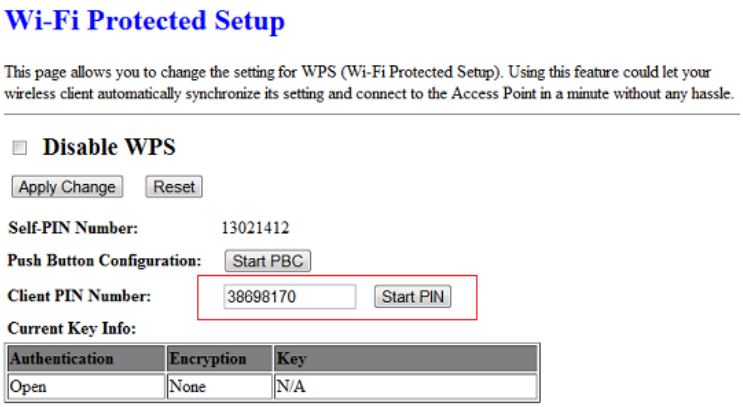
PBC model, in which the user simply has to push a button, either an actual or a virtual one, on both WPS devices to connect.

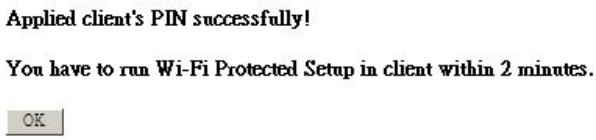
Please follow instructions below to enable the WPS function.

1. Setup Wireless LAN with WPS PIN :

(1). Get the WPS PIN number from wireless card and write it down.

(2). Fill in the PIN number from the wireless card in Client PIN Number field, and then click “Start PIN”.





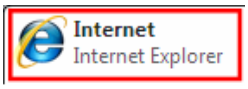
(3). Click PIN from Adapter Utility to complete the WPS process with the wireless router.

2. Start PBC:

(1). Press the WPS button (A) from BR485D and wait for Wireless/WPS LED light (B) changed into orange.

(2). Press the WPS button (C) from the adapter until the setup window shows up.

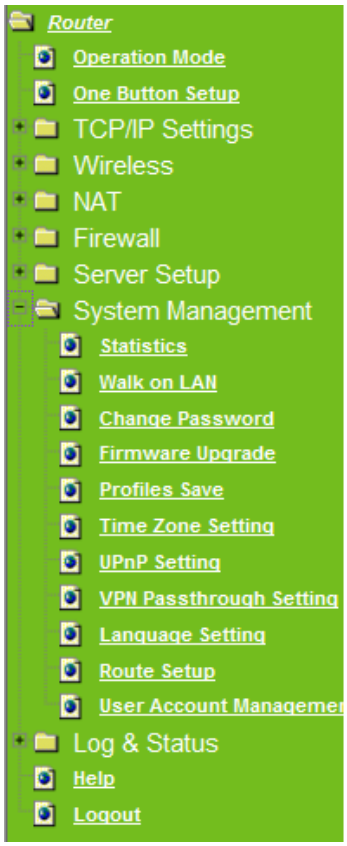
(3). Open a web browser to check the internet connection.



Please also refer to section 4.1.1 WPS setup for more details.

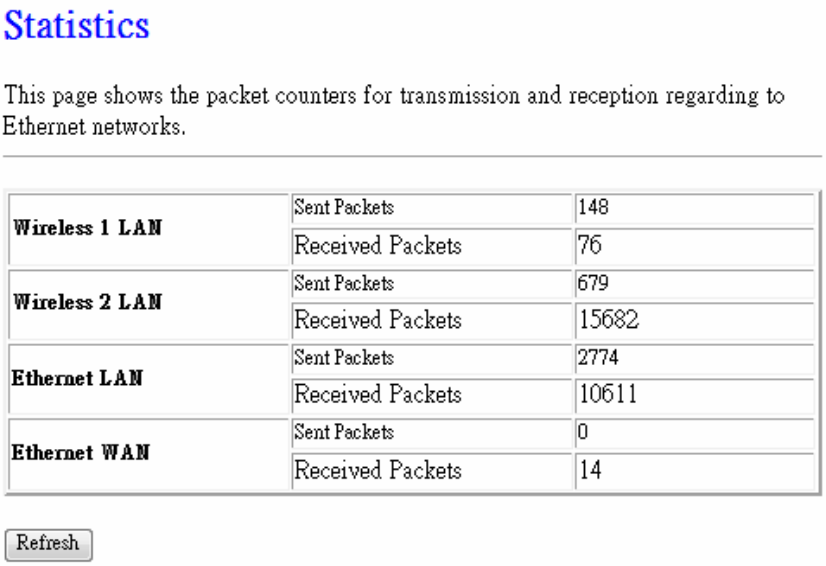
6.3 System Management

This section including **Change Password, Firmware Upgrade, Profiles Save, Time Zone Setting, UPnP Setting, VPN Passthrough Setting, and Language Setting**. It is easy and helpful for users making more detailed settings.



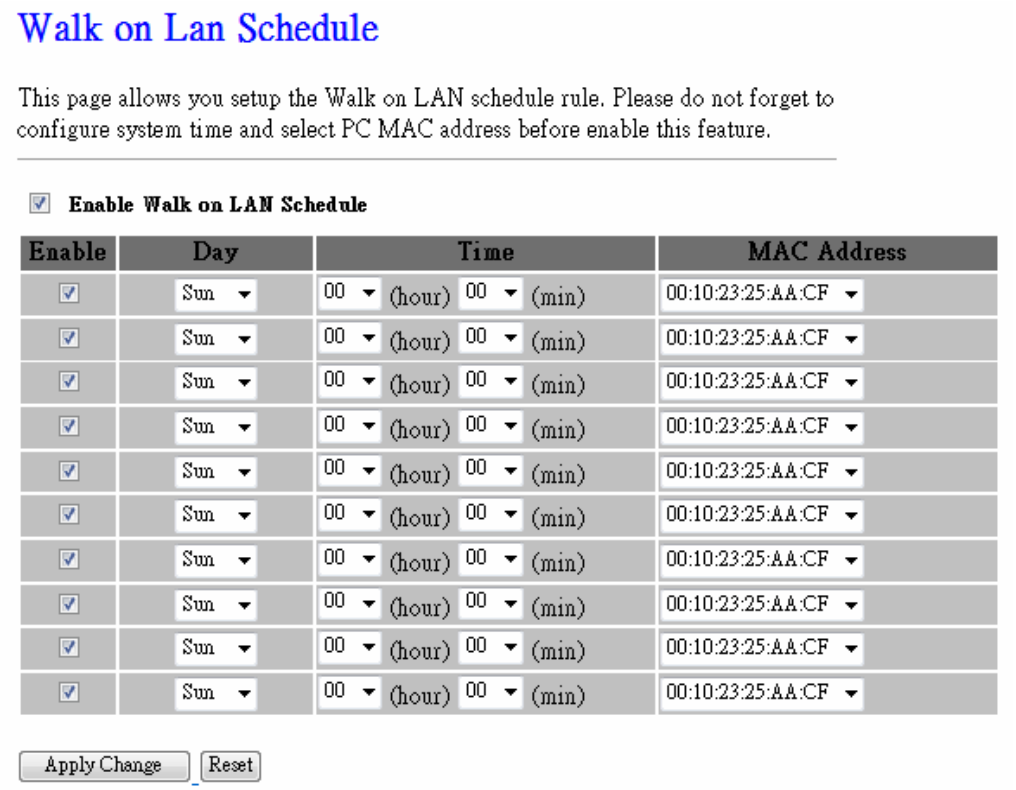
6.3.1 Statistics

It shows the packet counters for transmission and reception regarding to Ethernet networks



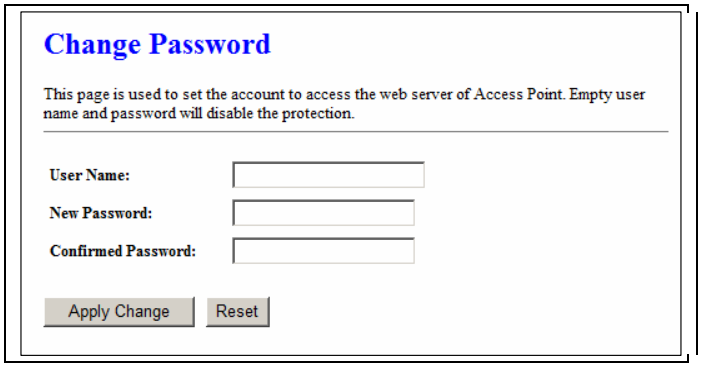
6.3.2 Walk on LAN Schedule

Switch your computer ON through your LAN or the Internet . To support WOL you must have a computer with Motherboard that supports WOL, as well as a Network Controller (NIC) supporting this function. Most of the newer Motherboard (circa 2002 and On), have an On Board NIC that supports WOL. Otherwise you need to install a PCI NIC that is WOL capable.



6.3.3 Change Password

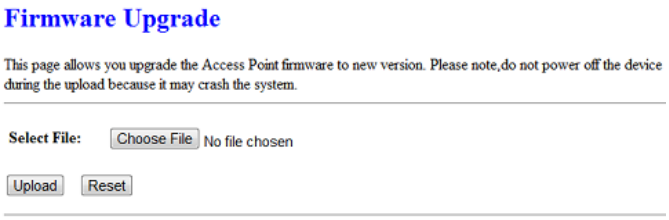
Users can set or change user name and password used for accessing the web management interface in this section.



Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

6.3.4 Firmware Upgrade

This function can upgrade the firmware of the router. There is certain risk while doing firmware upgrading. Firmware upgrade is not recommended unless the significant faulty is found and published on official website. If you feel the router has unusual behaviors and is not caused by the ISP and environment. You can check the website (http://www.amigo.com.tw) to see if there is any later version of firmware. Download the firmware to your computer, click Browser and point to the new firmware file. Click Upload to upgrade the firmware. You can't make any move unless the machine reboot completely.



Caution: To prevent that firmware upgrading is interrupted by other wireless signals and causes failure. We recommend users to use wired connection during upgrading.

Note: The firmware upgrade will not remove your previous settings.

λ **Reset button:**

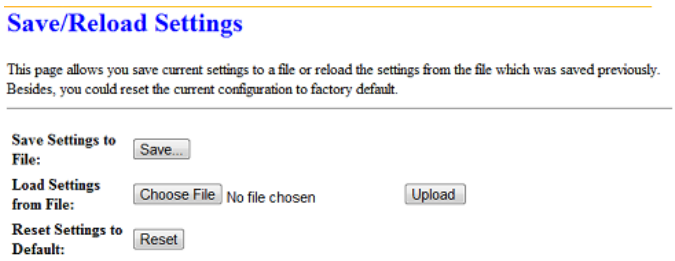
On the front of this router, there is a reset button. If you cannot login the administrator page by forgetting your password; or the router has problem you can't solve. You can push the reset button for 5 seconds with a stick. The router will reboot and all settings will be restored to factory default settings. If the problem still exists, you can visit our web site to see if there is any firmware for download to solve the problem.

6.3.5 Profile Save

Users can create a backup file that contains current router settings. This backup file can be used to restore router settings. This is especially useful in the event you need to reset the router to its default settings.

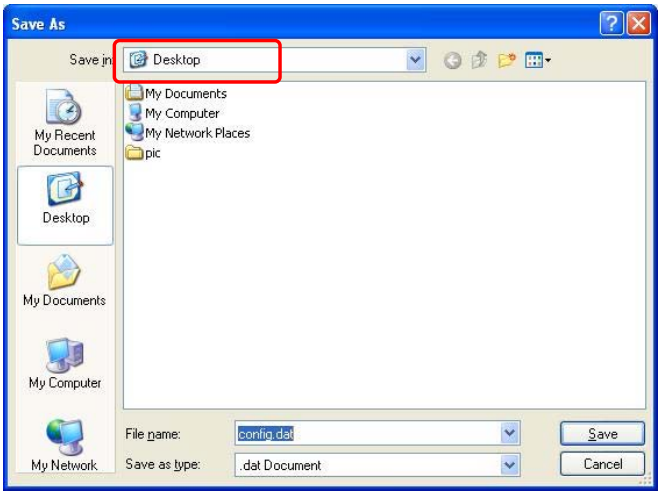
1. Save Configuration

(1). Click Save



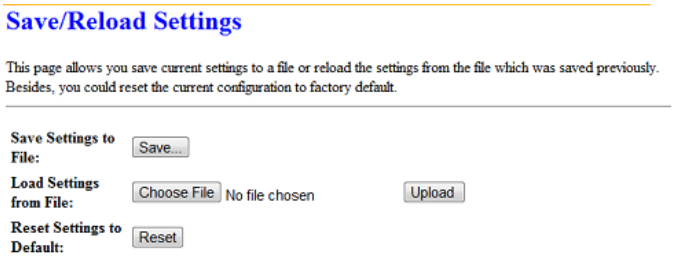
(2). Please click “Save” to save the configuration to your computer.

(3). Select the location which you want to save file, then click Save.

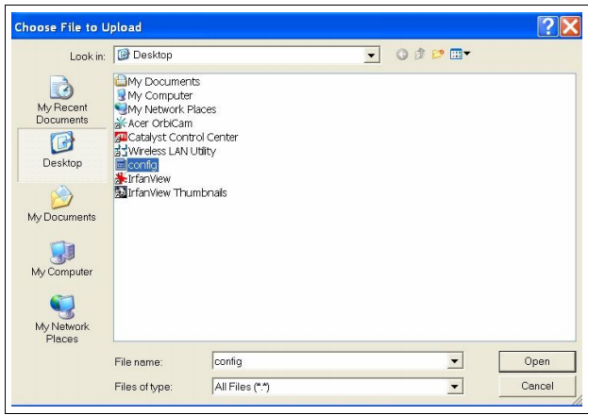


2. Load configuration file

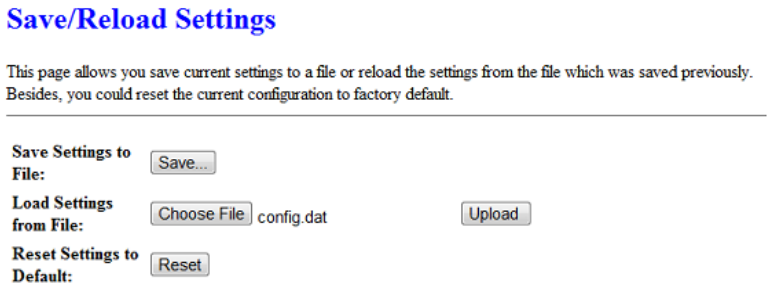
(1). Click Choose File



(2). Select configuration file then click Open



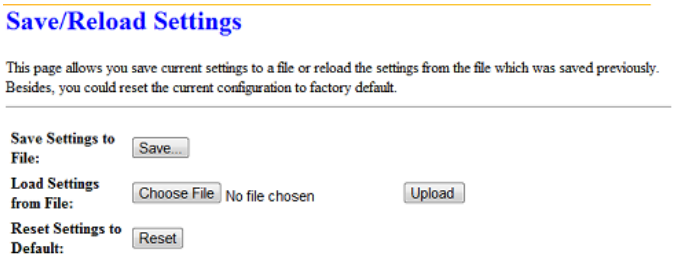
(3). Click Upload to upload configuration file to BR485D.



(4). After 90 seconds, BR485D will reboot automatically.

3. Reload factory default setting

(1). Please click Reset

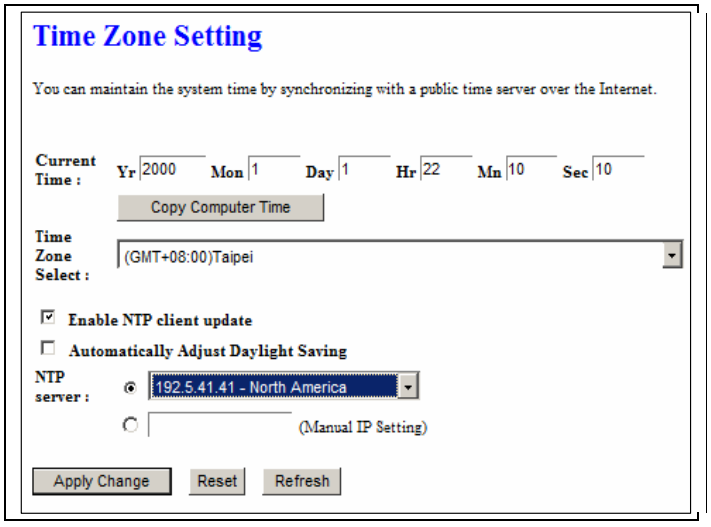


(2). Please click OK to start reload factory default setting to BR485D.

(3). After 90 seconds, BR485D will reboot automatically.

6.3.6 Time Zone Setting

Users can synchronize the local clock on the router to an available NTP server (optional). To complete this setting, enable NTP client update and select the correct Time Zone.

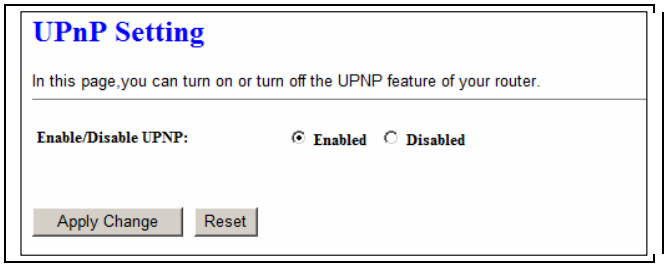


Item	Description
Current Time	Users can input the time manually.

Time Zone Select	Please select the time zone.
Enable NTP client update	Please select to enable NTP client update or not.
Automatically Adjust Daylight Saving	Please select to enable Automatically Adjust Daylight Saving or not.
NTP Server	Please select the NTP server from the pull-down list, or you can enter the NTP server IP address manually.
Apply Changes & Reset & Refresh	Please click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data. Or you may click on Refresh to update the system time on the screen.

6.3.7 UPnP Setting

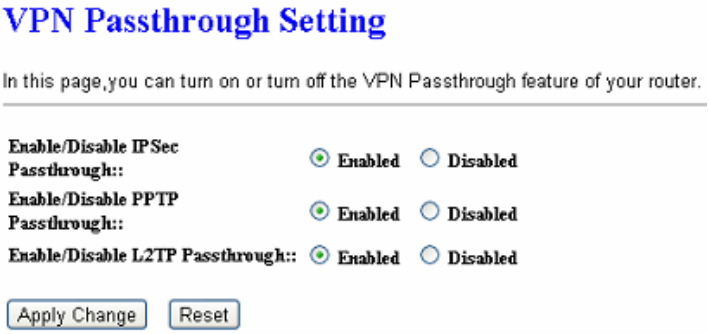
Universal Plug and Play (UPnP) is a standard of networking protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. BR485D supports UPnP function, and can cooperate with other UPnP devices. When you activate UPnP, please click My Network Places. Users will see an Internet Gateway Device icon. By click the icon, users can enter the GUI of the router. If you do not wish to use UPnP, you can disable it.



Enable/Disable UPnP: Select to enable or disable this function.

6.3.8 VPN Passthrough Setting

Virtual Private Networking (VPN) is typically used for work-related networking. For VPN tunnels, the router supports IPSec, Pass-through, PPTP Pass-through, and L2TP Pass-through.



Item	Description
IPSec Pass-through	Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the router, IPSec Pass-through is enabled by default. To disable IPSec Pass-through , select Disable
PPTP Pass-through	Point-to-Point Tunneling Protocol is the method used to enable VPN sessions to a Windows NT 4.0 or 2000 server. To allow PPTP tunnels to pass through the router, PPTP Pass-through is enabled by default. To disable PPTP Pass-through, select Disable.
L2TP Pass-through	To allow the L2TP network traffic to be forwarded to its destination without the network address translation tasks.
Apply Changes & Reset & Refresh	Please click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

6.3.9 Language Setting

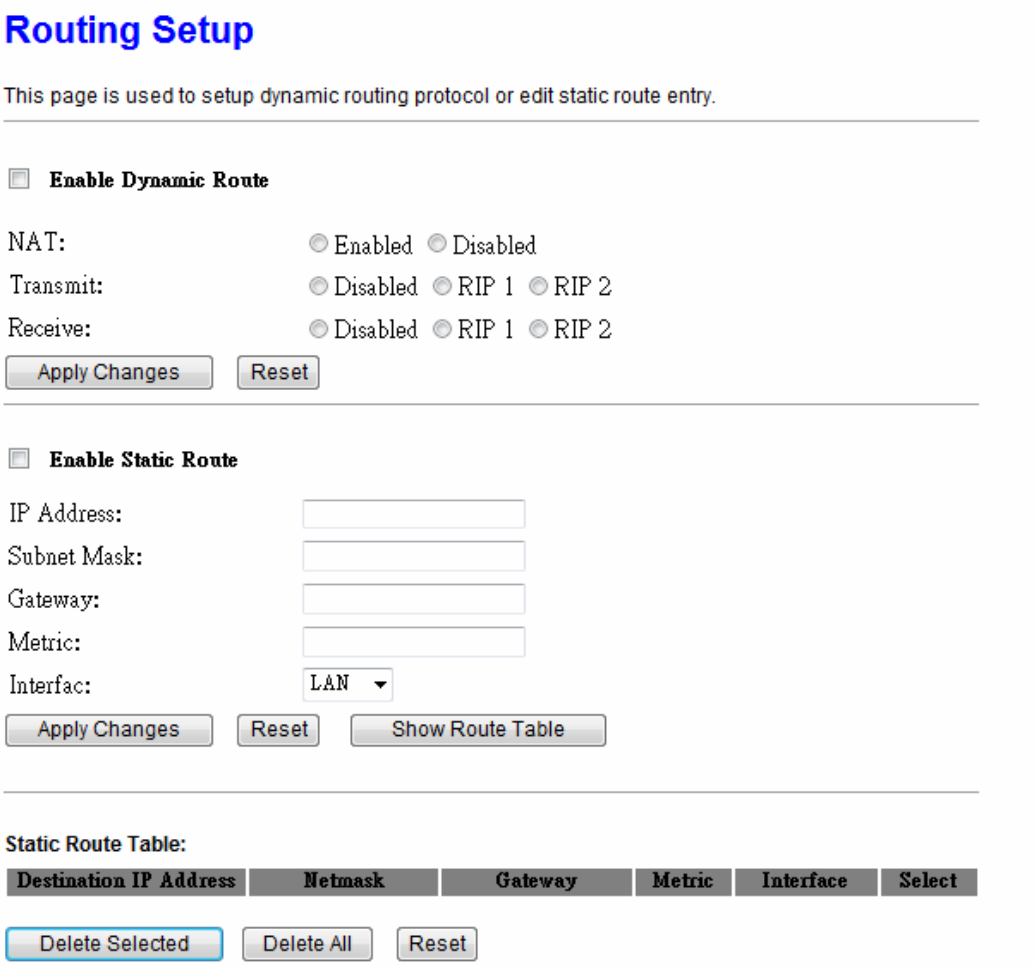
The BR485D provide 12 languages for Web GUI. You can select the language interface from the dropdown list and by following steps.

When you see the screen message change to the selected language, the setup is completed.

6.3.10 Routing Setup

Dynamic routing is is a distance-vector routing protocol, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15

Static routing is a data communication concept describing one way of configuring path selection of routers in computer networks. It is the type of routing characterized by the absence of communication between routers regarding the current topology of the network.This is achieved by manually adding routes to the router routing table.

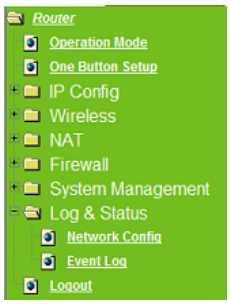


Item	Description
Enable Dynamic Route	Enable or Disable dynamic route
NAT	Enable or Disable NAT function
Transmit	There are 3 options： 1. Disable：do not send any RIP packet out 2. Send RIP1 packet out 3. Send RIP2 packet out
Receive	There are 3 options： 4. Disable：do not receive any RIP packet 5. Only receive RIP1 packet 6. Only receive RIP2 packet

Item	Description
Enable Static Route	Enable or Disable dynamic route
IP Address	Destination IP address
Subnet Mask	Destination IP subnet mask
Gateway	Gateway IP address for destination
Metric	Metric number on router's routing table
Interface	Static route rule for LAN or WAN interface

6.4 Log & Status

The category provides Network Config and Event Log status for users to know the operation status.



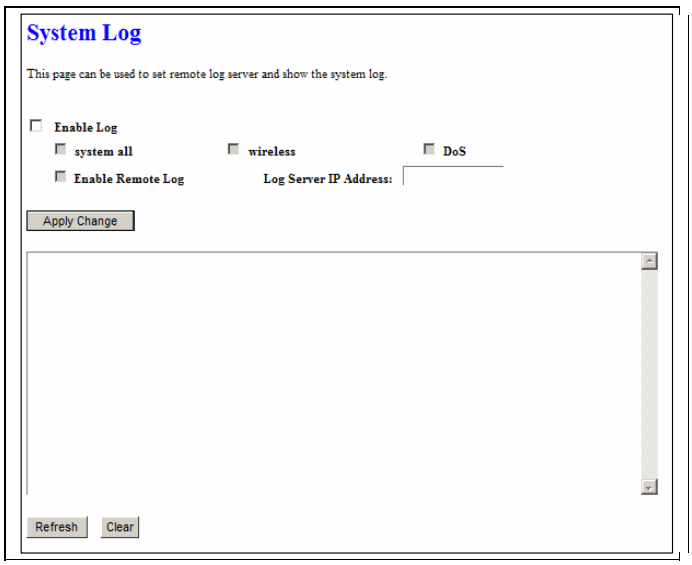
6.4.1 Network Config

Users can check the Internet status under this category, including Firmware version, Wireless setting, Connecting Time, WAN, TCP/IP …information.

System	
Uptime	0day:0h:33m:7s
Firmware Version	2007/04/25 Ver1.0.7 B05
RJ45 Port Define	LAN
Wireless 1 Configuration	
Mode	AP
Band	5 GHz (A+N)
SSID	11N_Broadband_Router_0d21ff
Channel Number	11
Encryption	Disabled
MAC Address	00:e0:4c:81:86:21
Associated Clients	0
Wireless 2 Configuration	
Mode	AP
Band	2.4 GHz (N)
SSID	11N_Broadband_Router_0d21ff
Channel Number	11
Encryption	Disabled
MAC Address	00:e0:4c:81:86:21
Associated Clients	0
LAN Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	Enabled
MAC Address	00:e0:4c:81:86:21
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
DNS 1	
DNS 2	
DNS 3	
	Connect Disconnect
USB Configuration	
USB Type	Storage
Name	PQI
Model	3100
FTP	

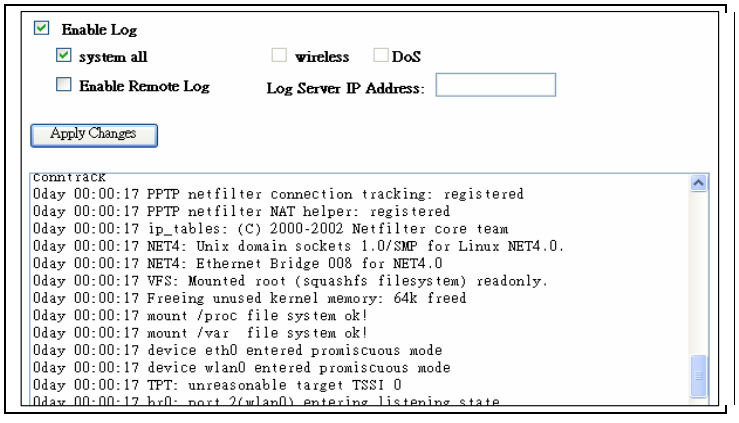
6.4.2 Event Log

You may enable the event log feature here.



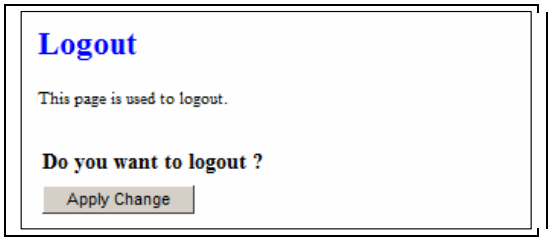
Item	Description
Enable Log	You may choose to enable Event Log or not.
System all, Wireless, & DoS	Please select the event you want to record.
Enable Remote Log	You may choose to enable the remote event log or not.
Log Server IP Address	Please input the log server IP Address.
Apply Changes & Refresh & Clear	Click on Apply Changes to save the setting data. Click on Refresh to renew the system time, or on Clear to clear all the record.

* The following figure is an example when users click Apply Changes to record the event log.



6.5 Logout

This function logs out the user.



Chapter 7 Samba Server

The BR485D is able to act as a Samba server to share the file on USB storage in local network.

7.1 How to use BR485D as a Samba server

1. Plug in the USB hard disk/Flash.

2. Star your web browser and input \\192.168.1.1.

3. Star “My Computer” and you will find a folder named “sda1”.

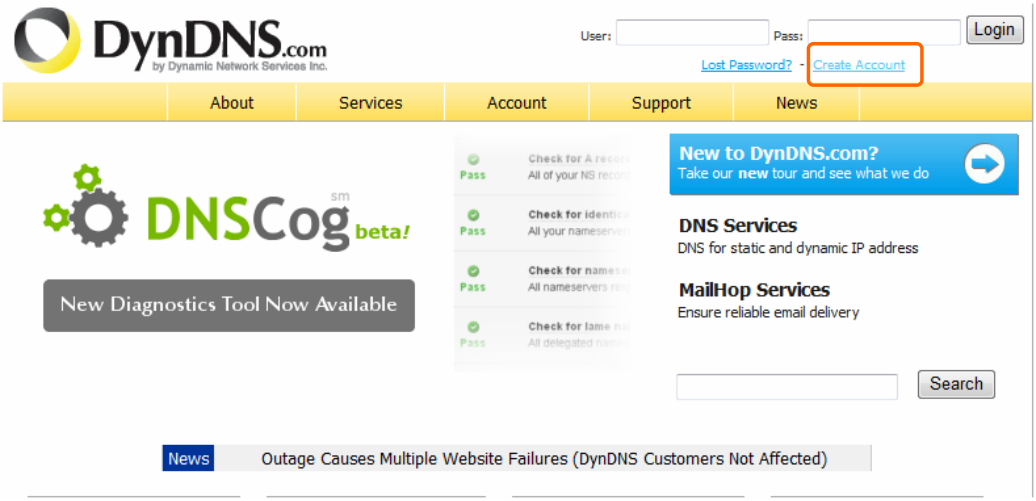
Chapter 8 DDNS Service Application

DDNS is a service changes the dynamic IP to the static IP. The settings of DDNS can solve the problem of being given the different IP by router every time. After setting the Router, your host name would correspond to your dynamic IP. Moreover, via the host name application, it could be easier for you to use FTP, Webcam and Printer remotely.

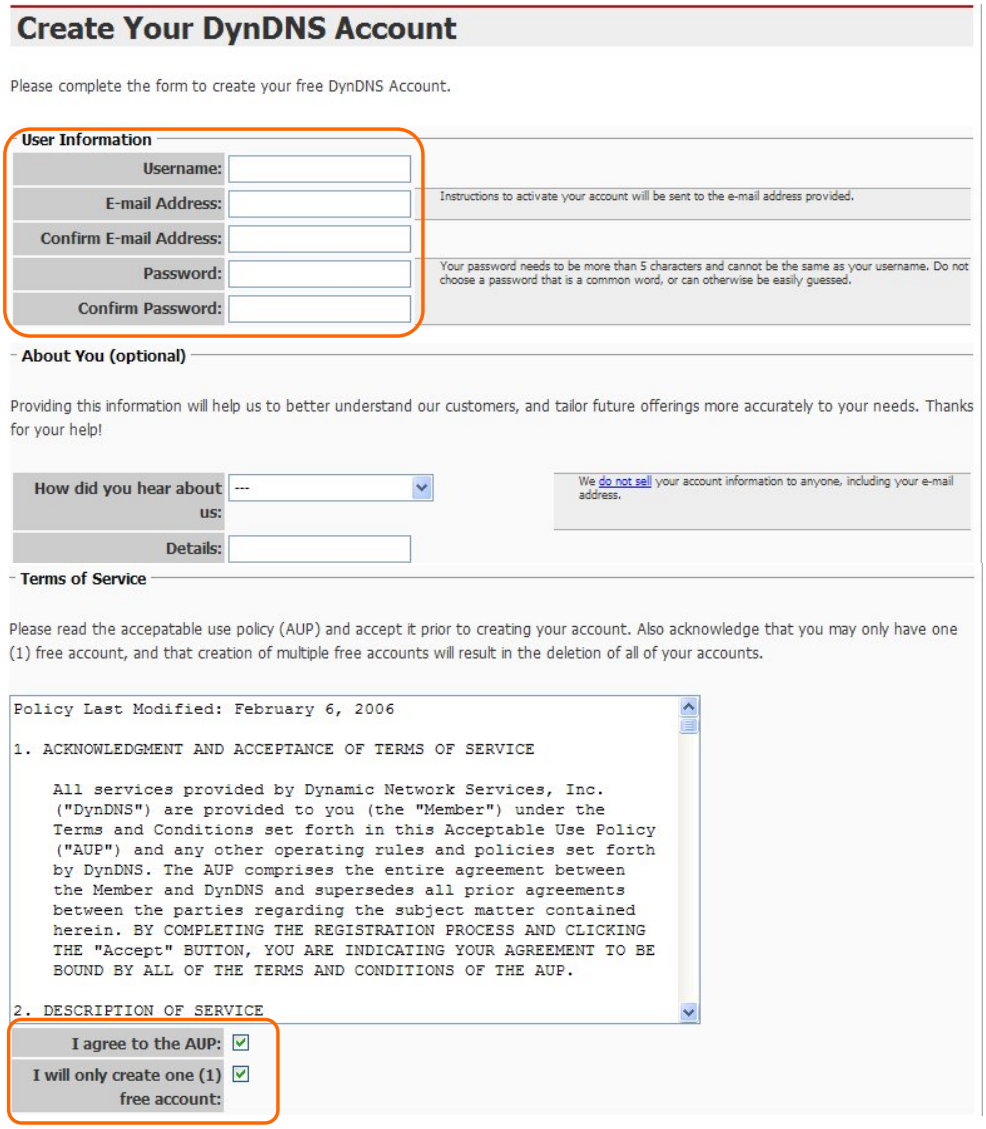
Dynamic DNS allows you to make an assumed name as a dynamic IP address to a static host name. Please configure the dynamic DNS below. Please select **Dynamic DNS** under the **IP Config** folder, and follow the instructions below to enter the **Dynamic DNS** page to configure the settings you want.

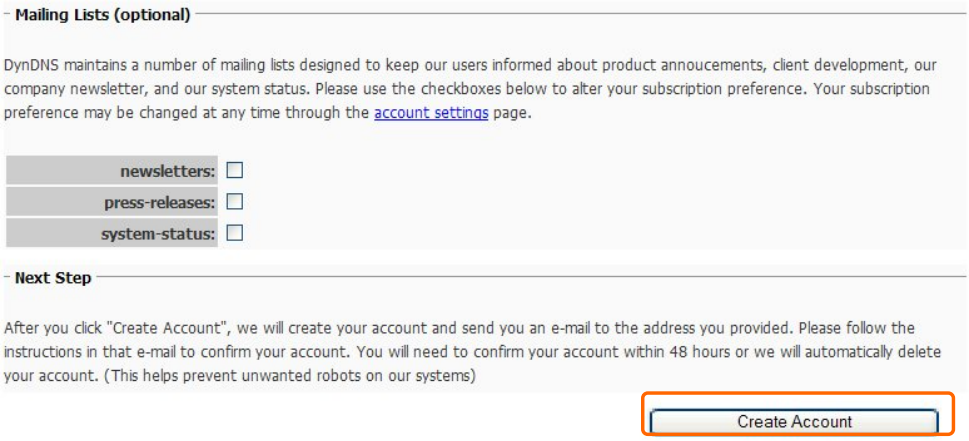
If you don't have a DDNS account, please follow the steps to complete your DDNS with Dynamic IP settings.

1. First access the Internet and fill http://www.dyndns.com/ into the address field of your web browser, then click **Create Account**.

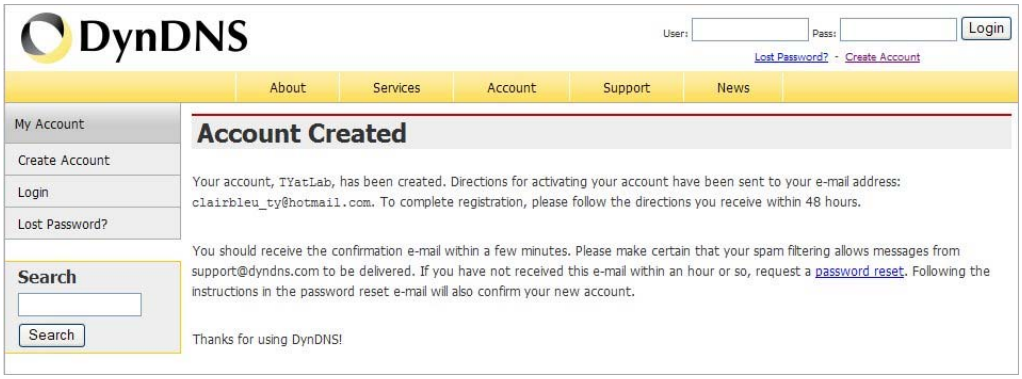


2. Fill in the form as required, and then click on **Create Account** button.

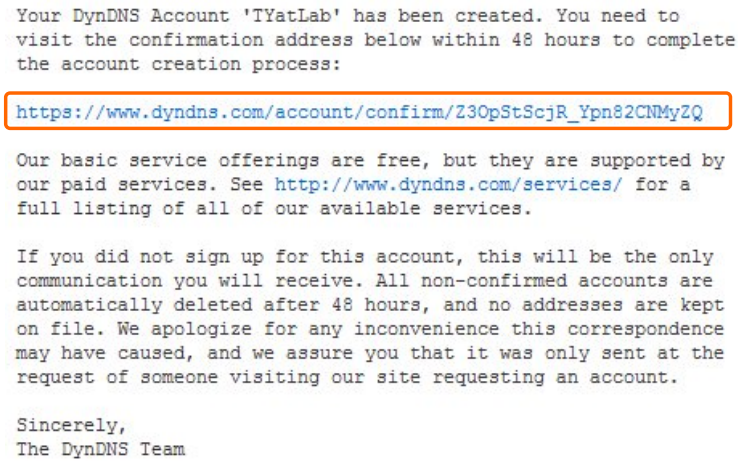




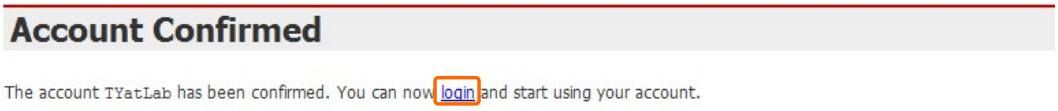
3. When you got this account created message, close it, and check your mailbox. You would get a mail from DynDNS website.



4. Click on the indicated address within your mail to confirm.

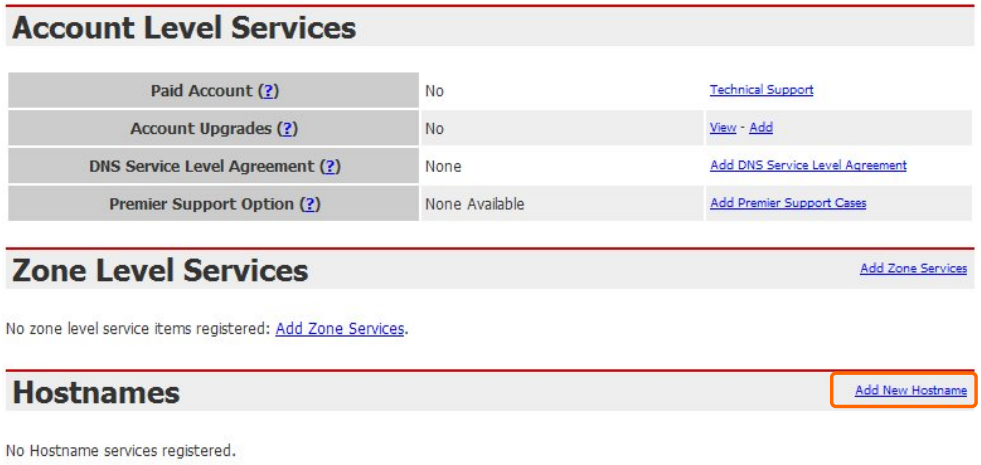


5. Click on **login.**

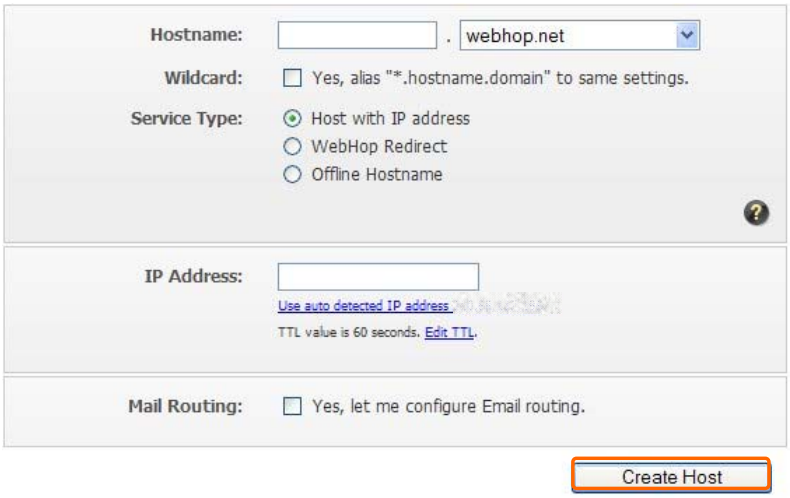


6. Click **My Services** after logging in.

7. Click **Add New Hostname**.



8. Put in your favorite hostname and service type, and then click **Create Host** after finished.



9. Your hostname has been created when you see the following page.

Chapter 9 Q & A

9.1 Installation

1. Q: Where is the XDSL Router installed on the network?

A: In a typical environment, the Router is installed between the XDSL line and the LAN. Plug the XDSL Router into the XDSL line on the wall and Ethernet port on the Hub (switch or computer).

2. Q: Why does the throughput seem slow?

A: To achieve maximum throughput, verify that your cable doesn't exceed 100 meter. If you have to do so, we advise you to purchase a bridge to place it in the middle of the route in order to keep the quality of transmitting signal. Out of this condition you would better test something else.

- Verify network traffic does not exceed 37% of bandwidth.
- Check to see that the network does not exceed 10 broadcast messages per second.
- Verify network topology and configuration.

9.2 LED

1. Why doesn't BR485D power up?

A: Check if the output voltage is suitable, or check if the power supply is out of order.

2. The Internet browser still cannot find or connect to BR485D after verifying the IP address and LAN cable, the changes cannot be made, or password is lost.

A: In case BR485D is inaccessible; you can try to restore its factory default settings. Please press the "Reset" button and keep it pressed for over 7 seconds and the light of STATUS will vanish. The LEDs will flash again when reset is successful.

3. Why does BR485D shut down unexpectedly?

A: Re-plug your power adapter. Then, check the STATUS indicator; if it is off, the internal flash memory is damaged. For more help, please contact with your provider.

9.3 IP Address

1. **Q: What is the default IP address of the router for LAN port?**

   A: The default IP address is 192.168.1.1 with subnet mask 255.255.255.0

2. **Q: I don't know my WAN IP.**

   A: There are two ways to know.

   Way 1: Check with your Internet Service Provider.

   Way 2: Check the setting screen of BR485D. Click on **Status & Log** item to select **Network Configuration** on the Main Menu. WAN IP is shown on the WAN interface.

3. **How can I check whether I have static WAN IP Address?**

   A: Consult your ISP to confirm the information, or check Network Configuration in BR485D 's Main Menu.

4. **Will the Router allow me to use my own public IPs and Domain, or do I have to use the IPs provided by the Router?**

   A: Yes, the Router mode allows for customization of your public IPs and Domain.

9.4 OS Setting

1. **Why can't my computer work online after connecting to BR485D?**

   A: It's possible that your Internet protocol (TCP/IP) was set to use the following IP address. Please do as the following steps. (Windows 2000 & XP) **Start**＞**Settings**＞ **Network and Dial-up Connections**＞double click on **Internet Protocol(TCP/IP)**＞ select **obtain IP address automatically**＞ Click on **OK** button. Then, open Internet browser for testing. If you still can't go online, please test something else below.

   - Verify network configuration by ensuring that there are no duplicate IP addresses.
   - Power down the device in question and ping the assigned IP address of the device. Ensure no other device responds to that address.
   - Check that the cables and connectors or use another LAN cable.

2. **Q: Why can't I connect to the router's configuration utility?**

A: Possible Solution 1: Make sure that your Ethernet connect properly and securely. Make sure that you've plugged in the power cord.

Possible Solution 2: Make sure that your PC is using an IP address within the range of 192.168.1.2 to 192.168.1.254. Make sure that the address of the subnet mask is 255.255.255.0. If necessary, the Default Gateway data should be at 192.168.1.1. To verify these settings, perform the following steps:

Windows 2000, or XP Users:

1. Click on Windows **Start** > click on **Run** > input **cmd** > click on **OK** button.
2. At the DOS prompt, type ipconfig/all.
3. Check the IP Address, Subnet Mask, Default Gateway data. Is this data correct? If the data isn't correct. Please input **ipconfig/release** > press **Enter** > input **ipconfig/renew** > press **Enter**.

Possible Solution 3: Verify the connection setting of your Web browser and verify that the HTTP Proxy feature of your Web browser is disabled. Make these verifications so that your Web browser can read configuration pages inside your router. Launch your Web browser.

Internet Explorer Users:

1. Click on **Tools** > **Internet Options** > **Connections tab**.
2. Select **never dial a connection**, click on **Apply** button, and then click on **OK** button.
3. Click on **Tools** and then click on **Internet Options**.
4. Click on **Connections** and then click on **LAN Settings**.
5. Make sure none of the check boxes are selected and click on **OK** button.
6. Click on OK button.

Netscape Navigator Users:

1. Click on **Edit** > **Preferences** > double-click **Advanced** in the Category window.
2. Click on **Proxies** > select **Direct connection to the Internet** > click on **OK** button.
3. Click on **Edit again** and then click on **Preferences**.
4. Under category, double-click on **Advanced** and then click on **Proxies**.
5. Select **Direct connection to the Internet** and click on **OK** button.
6. Click on **OK** button.

3. Q: Web page hangs, corrupt downloads, or nothing but junk characters is being displayed on the screen. What do I need to do?

A: Force your NIC to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your NIC as a temporary measure. (Please look at the Network Control Panel, in your Ethernet Adapter's Advanced Properties tab.)

4. Q: Why can't I connect to the Web Configuration?

A: you can remove the proxy server settings in your web browser.

9.5 BR485D Setup

1. Q: Why does BR485D's setup page shut down unexpectedly?

A: If one of the pages appears incompletely in BR485D 's setup pages, please click on Logout item on the Main Menu before shutting it down. Don't keep it working. Then, close Internet browser and open it again for going back to the previous page.

2. Q: I don't know how to configure DHCP.

A: DHCP is commonly used in the large local network. It allows you to manage and distribute IP addresses from 2 to 254 throughout your local network via BR485D . Without DHCP, you would have to configure each computer separately. It's very troublesome. Please Open **Internet browser** > Input **192.168.1.1 in the website blank field** > Select **DHCP Server under** the **IP Config Menu**. For more information, please refer to 3.3.2 (Router Mode) or 4.3.1 (AP Mode).

3. Q: How do I upgrade the firmware of BR485D ?

A: Periodically, a new Flash Code is available for BR485D on your product supplier's website. Ideally, you should update BR485D 's Flash Code using **Firmware Upgrade** on the **System Management** menu of BR485D Settings.

4. Q: Why is that I can ping to outside hosts, but cannot access Internet websites?

A: Check the DNS server settings on your PC. You should get the DNS servers settings from your ISP. If your PC is running a DHCP client, remove any DNS IP address setting. As the router assign the DNS settings to the DHCP-client-enabled PC.

5. Q: BR485D couldn't save the setting after click on Apply button?

A: BR485D will start to run after the setting finished applying, but the setting isn't written into memory. Here we suggest if you want to make sure the setting would be written into memory, please reboot the device via **Reboo**t under **System Management** directory**.**

9.6 Wireless LAN

1. Q: Why couldn’t my wireless notebook work on-line after checking?

A: Generally, Wireless networks can sometimes be very complicated to set up, particularly if you're dealing with encryption and products from different vendors. Any number of variables can keep your workstations from talking to each other. Let's go over some of more common ones.

For starters, verify that your router and your workstation are using the same SSID descriptions. SSID acts as a password when a mobile device tries to connect to the wireless network. The SSID also differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A workstation will not be permitted to connect to the network unless it can provide this unique identifier. This is similar to the function of your network's Workgroup or Domain name.

When you're experiencing conductivity problems, it is always best to keep things simple. So next you are going to do is that, please disable any WEP encryption you might have configured.

Successful implementation of encryption also includes the use of a shared key. A HEX key is the most common, but other formats are also used. This key identifies the workstation to the router as a trusted member of this network. Different manufacturers can implement this key technology in ways that might prevent them from working correctly with another vendor's products. So pay attention to detail is going to be the key to a successful installation.

Next make sure the router and the NIC are configured to use the same communications channel. There are normally 11 of them, and the default channel can also vary from vendor to vendor. You might also want to confirm that the router has DHCP services enabled and an address pool configured. If not, the NIC won't be able to pick up an IP address. I have run across a few access points that offer DHCP services but do not assign all of the needed IP information to the NIC. As a result, I was able to connect to the network, but could not browse the web. The point is, don't assume anything. Verify for yourself that all of the required settings are being received by the workstation.

Finally, you might want to keep the system you're trying to configure in the same room as the router, at least during the initial configuration, in order to minimize potential interference from concrete walls or steel beams.

2. Q: My PC can't locate the Wireless Access Point.

A: Check the following:

- Your PC is set to Infrastructure Mode. (Access Points are always in Infrastructure Mode.)
- The SSID on your PC and the Wireless Access Point are the same. Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup".
- Both your PC and the Wireless Access Point must have the same setting for WEP. The default setting for the Wireless Router is disabled, so your wireless station should also have WEP disabled.
- If WEP is enabled on the Wireless Router, your PC must have WEP enabled, and the key must match.
- If the Wireless Router's Wireless screen is set to Allow LAN access to selected Wireless Stations only, then each of your Wireless stations must have been selected, or access will be blocked.
- To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Access Point. Remember that the connection range can be as little as 100 feet in poor environments.

3. Q: Wireless connection speed is very slow.

A: The wireless system will connect at highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with following:

- Access Point location: Try adjusting the location and orientation of the Access Point.
- Wireless Channel: If interference is the problem, changing to another channel may show a marked improvement.
- Radio Interference: Other devices may be causing interference. You can experiment by switching other devices off, and see if this helps. Any "noisy" devices should be shielded or relocated.
- RF Shielding: Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Access Point.

4. Q: Some applications do not run properly when using the Wireless Router.

A: The Wireless Router processes the data passing through it, so it is not transparent. Use the Special Application feature to allow the use of Internet applications which do not function correctly. If this does solve the problem, you can use the DMZ function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.
- Only one (1) PC can use this feature.

5. Q: I can't connect to the Wireless Router to configure it.

A: Check the following:

- The Wireless Router is properly installed, LAN connections are OK, and it is powered ON.
- Make sure that your PC and the Wireless Router are on the same network segment.
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, make sure that it is using an IP Address within the range 192.168.1.129 to 192.168.1.253 and thus compatible with the Wireless Router's default IP Address of 192.168.1.254. Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Router. In Windows, you can check these settings by using Control Panel ~ Network to check the Properties for the TCP/IP protocol.

6. Q: The WinXP wireless interface couldn't communicate the WEP with BR485D's wireless interface.

A: The default WEP of WinXP is **Authentication Open System - WEP**, but the WEP of BR485D is only for **Shared Key - WEP**, it caused both sides couldn't communicate. Please select the WEP of WinXP from Authentication Open System to **Pre-shared Key - WEP**, and then the WEP wireless interface between WinXP and BR485D would be communicated.

9.7 Support

1. Q: What is the maximum number of IP addresses that the XDSL Router will support?

A: The Router will support to 253 IP addresses with NAT mode.

5. Q: Is the Router cross-platform compatible?

A: Any platform that supports Ethernet and TCP/IP is compatible with the Router.

9.8 Others

1. Q: Why does the router dial out for PPPoE mode very often?

A: Normally some of game, music or anti-virus program will send out packets that trigger the router to dial out, you can close these programs. Or you can set the idle time to 0, then control to dial out manually.

2. Q: What can I do if there is already a DHCP server in LAN?

A: If there are two DHCP servers existing on the same network, it may cause conflict and generate trouble. In this situation, we suggest to disable DHCP server in router and configure your PC manually.

9.9 USB Device

1. Q: How many USB devices can be connected to the Product?

A: BR485D has 1 USB ports.

Chapter 10 Appendices

10.1 Operating Systems

1. Microsoft：Windows 2000, XP, Vista, Windows 7.
2. Apple：Mac OS X 10.4.7, Leopard and the following related versions.
3. Linux：Redhat 9, Fedora 6 & 7, Ubuntu 7.04 and the following related versions.

10.2 Browsers

1. Internet Explorer ver. 6 and 7 and the following related versions.
2. FireFox ver. 2.0.0.11 and the following related versions.3.
3. Safari ver. 3.04 and the following related versions.

10.3 Communications Regulation Information

Should any consumers need to learn more information, services and supports, please contact the supplier of your product directly.