

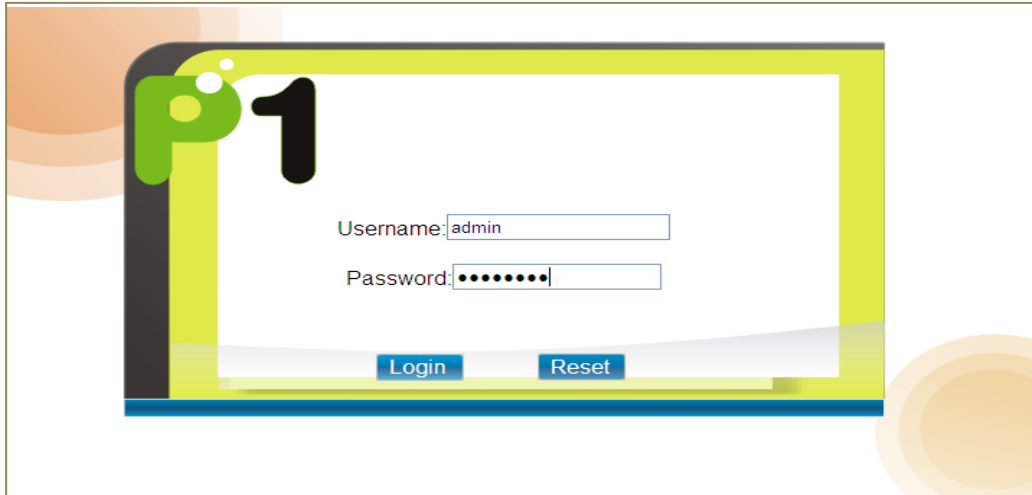
DV230 Web Based Configuration Troubleshooting Guide

1. Login settings

After getting a DHCP IP address from your P1 WIMAX Modem DV-230), open any Internet browser and type in the URL address: <http://10.1.1.254>

Username : admin

Password : admin123



Troubleshooting:

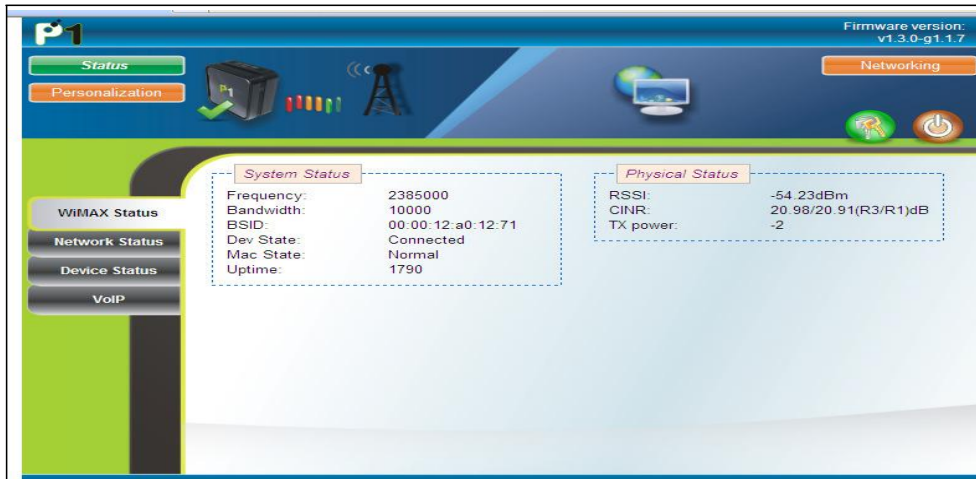
You cannot access the Customer Web GUI page

- Ensure you receive a DHCP IP from your Modem in the range of 10.1.1.x (excluding 10.1.1.254), subnet mask 255.255.255.0
- Check if you are able to ping to 10.1.1.254
- Go to START > RUN (Type: cmd) > COMMAND PROMPT (Type: ping 10.1.1.254)
- Check if your web browser has blocked the URL <http://10.1.1.254> or if this URL is under the Restricted List.

2. Status Guides

WiMAX Status

The following is the meaning of each status in the WiMAX Status Page:



Frequency	The WiMAX Radio Frequency channel that the Modem is connected to.
Bandwidth	The width of the WiMAX Radio Frequency channel.
BSID	The WiMAX Base station ID that the Modem is connected to.
State	Status of the Modem.
Uptime	The length of time that the Modem is powered up, starting when the power is turned ON.
RSSI	The signal strength of the WiMAX Radio Frequency channel that the Modem is connected to.
CINR	The signal quality of the WiMAX Radio Frequency channel that the Modem is connected to.
TX Power	The WiMAX Radio Frequency power that is transmitted from the Modem to the Base station.

Network Status

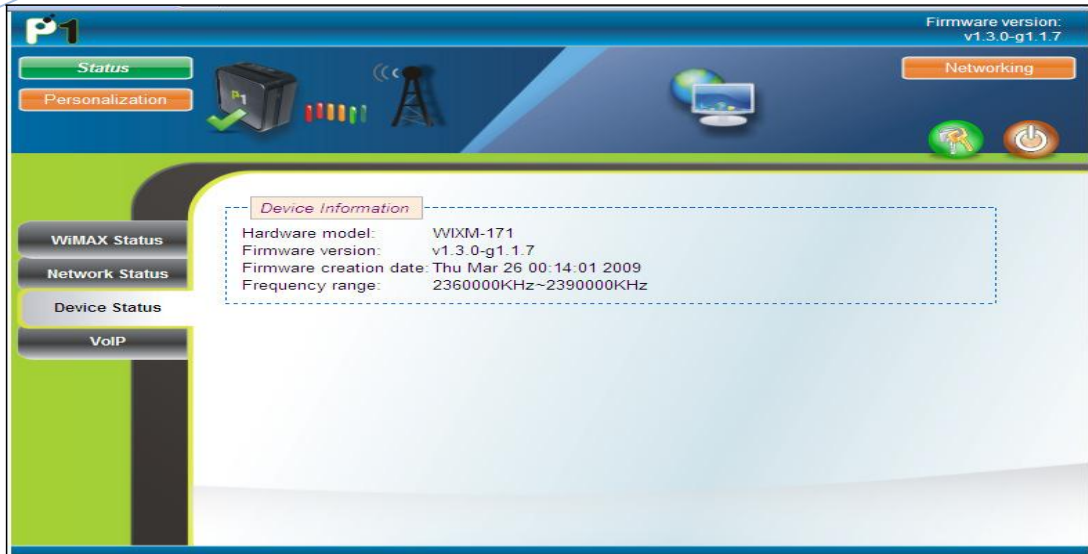
The following is the meaning of each status in the Network Status Page:



LAN Box	Network information on the Modem’s LAN side (connected from RJ-45 Port to user’s PC/Laptop).
WAN Box	Network information on the Modem’s WiMAX side. The IP is a Public IP.
DHCP Client List Box	Shows the information of the PC/Laptop, which is connected to the Modem’s LAN side DHCP Server.

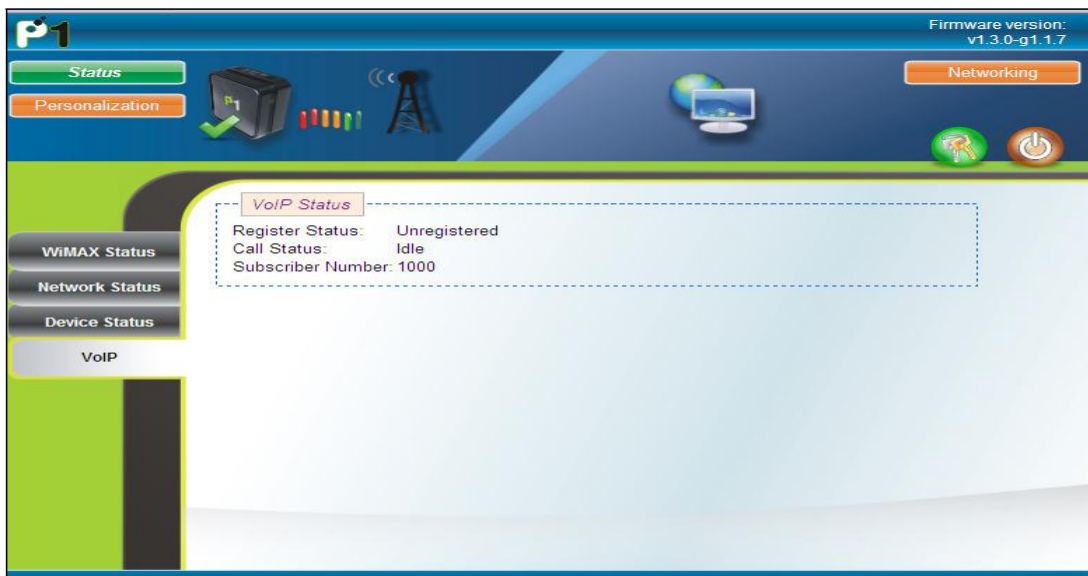
Device Status

The Device Status shows the Firmware Version, Hardware Model and WiMAX Frequency Range of the Modem.



VoIP Status

This page allows you to check your VoIP Status: Register Status, Call Status and Subscriber Number.



Field	Objective	Remark
Register Status	Indicates whether subscriber number is Registered or Unregistered	You status must be shown as Registered in order to make a call.
Call Status	Indicates current call status	
Subscriber Number	Indicates subscriber number	

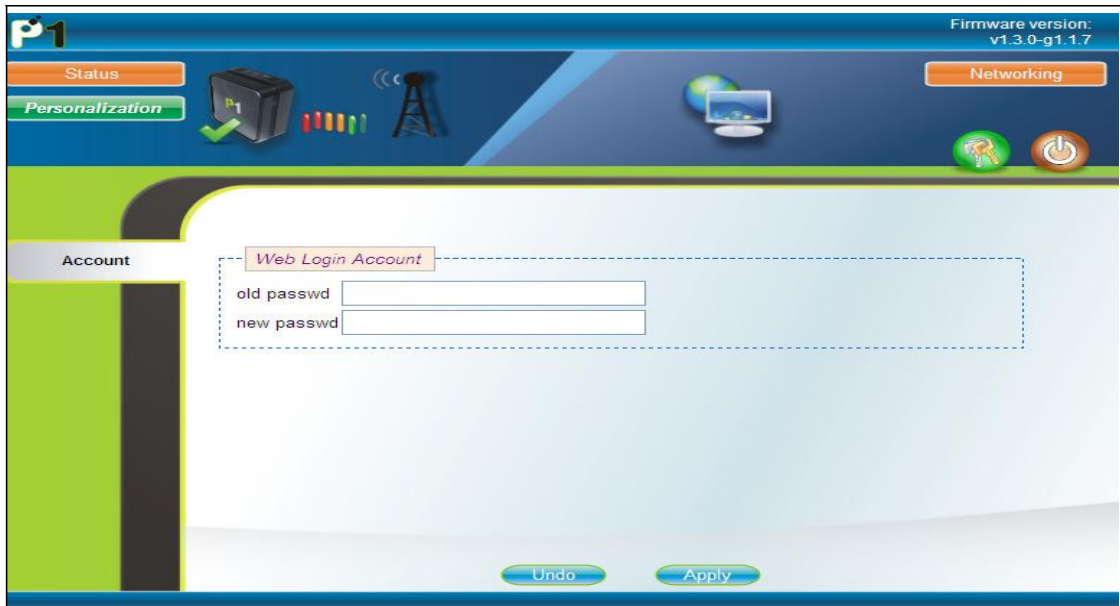


Troubleshooting:

- If your status is Unregistered, please check your WiMAX connectivity and ensure that your Modem is connected to P1's WiMAX service. If the problem persists, please call the P1 Care Line at 1300 03 1300.
- Alternatively, you can listen to the phone connected to your Modem to check its call status. A busy tone indicates an Unregistered status. A normal tone indicates a Registered Status.

3. Personalisation for Account

In the Account section, you can change their Password for their Web Login.



4. Networking

Networking - LAN

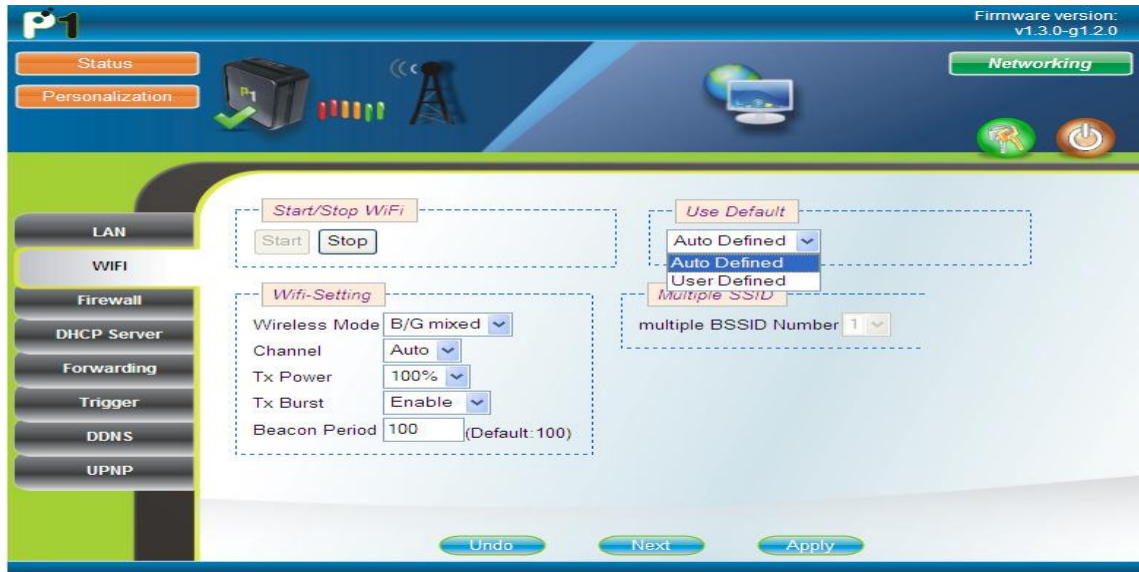
On this page, you can change the settings of the Modem's LAN IP Address and Subnet Mask according to the requirements of each individual user.



Networking - WiFi

This page allows some basic configuration such as start/stop WiFi and WiFi settings. Click the Next button to move to the next page.

Note: Ensure UF-230G USB WiFi adapter is inserted into the USB slot.



This page allows customised security settings to prevent unauthorised access to your WiFi connectivity. Example: Change his/her SSID and WEP Key. After all configurations are completed, press Apply. The device will then reboot itself.

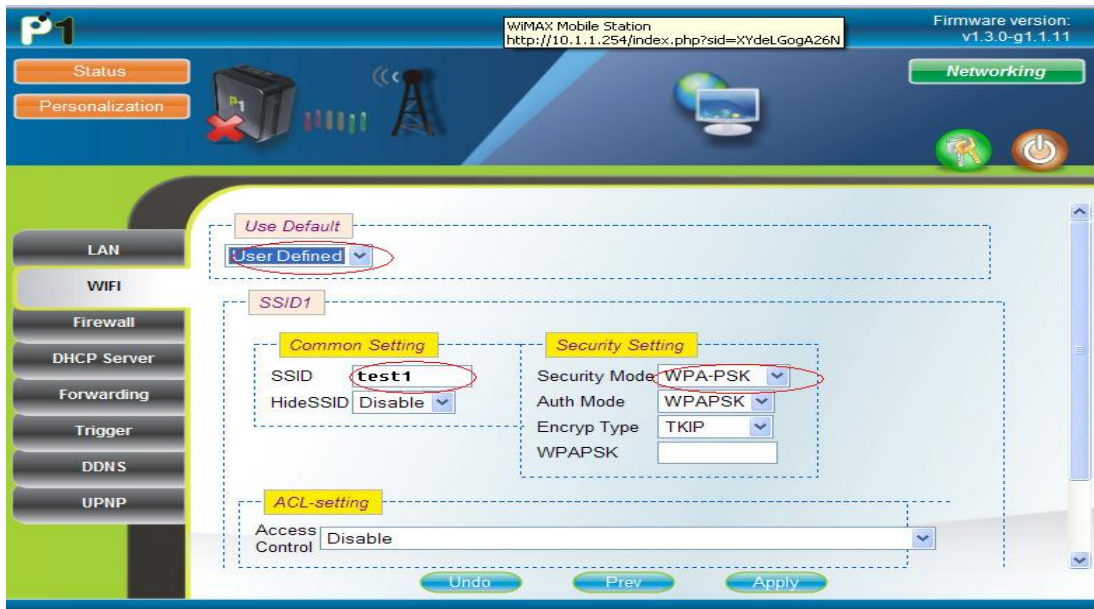


Wifi WPA/WPA2 security type setting:

- I. Access the Wifi security page by clicking at Networking, followed by Wifi, and then the Next buttons.



- II. Select User Defined in the Use Default Palette.
- III. Key in SSID in the SSID field. (In the picture below, “test1” was used)
- IV. In the Security Setting palette, select WPA-PSK from the Security Mode drop down list.



- V. Leave the Auth Mode selection to the default selection value which is WPAPSK.



- VI. For Encryp Type, choose either one of the three list offered in the drop down box, which is TKIP, AES or TKIPAES.
- VII. Next, key in your password in the WPAPSK text box. It can be 8-63 characters or 64 Hexadecimal values long.

Field	Objective	Remark
Use Default	Default setting or user define settings of the Wifi SSID and it's Security settings	Auto Defined: The wifi SSID and it's security settings will be as printed at the label of the USB wifi adapter. The default security mode will be WEP and the WEP key will also be printed at the label of the USB wifi adapter. User Defined: User will have full control to make any changes on the Wifi SSID and it's security settings.
Start/Stop WiFi	Enable and disable WiFi Connectivity	Default value is enable
Wireless Mode	Allows B,G and B/G mixed	Default value is B/G mixed
Channel	Channel 9, 10, 11 and Auto	Default value is Auto
Tx Power	Transmitted power from WiFi in percentage value	Select 100% for maximum transmit power if WiFi is weak
Tx Burst	Transmit signal in occasional burst mode	Enable by default
Beacon Period	Defines how often DV230 will send out wireless beacon	Default value is 100
Multiple BSSID Number	Allows maximum of 2 SSID	Default value enable 1 SSID
SSID	Insert SSID name	Accepts a maximum of 29 alphanumeric characters. (symbols may cause error when trying to connect or doing settings to the SSID. Confirm symbols that causes error are #, &, “)
Hide SSID	Hide/Unhide broadcast of SSID name	



Security Mode	Enable security to prevent unauthorized access	7 modes - Disable, WEP, WPA, WPA-PSK, WPA2, WPA2-PSK,
WEP	Enter key string in hexadecimal or ASCII format	<p>802.1X</p> <p><u>64bit</u></p> <p>-5 ASCII characters (A-Z or a mixture of A-Z and 0-9)</p> <p>-10 Hexadecimal characters (0-9, A-F or mixture of both 0-9 & A-F only)</p> <p><u>128bit</u></p> <p>-13 ASCII characters (A-Z or a mixture of A-Z and 0-9)</p> <p>-26 Hexadecimal characters (0-9,A-F or mixture of both 0-9 & A-F only)</p>
WPA/WPA2	Uses external Radius Server in conjunction with TKIP and AES for authentication	<p>8-63 ASCII Characters (Can be mixture of A-Z & 0-9)</p> <p>8-64 Hexadecimal (Can be mixture of 0-9 & A-F only)</p>
802.1x	Utilizes Radius Server for authentication and dynamic WEP key generation for data encryption	
WPA-PSK/WPA2-PSK		<p>8-63 ASCII Characters (Can be mixture of A-Z & 0-9)</p> <p>8-64 Hexadecimal (Can be mixture of 0-9 & A-F only)</p>
Authentication Mode	Open/Shared for WEP	
Encryption Type	TKIP, AES, TKIPAES for WPA mode	
Access control	Prevent user from accessing WiFi by filtering MAC address	

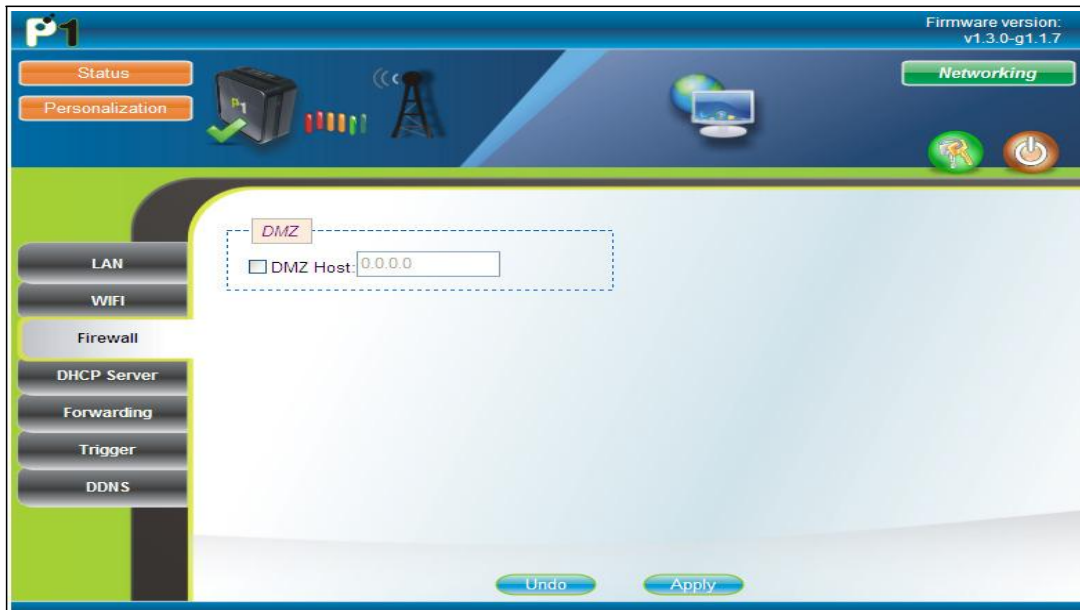
Troubleshooting:

No	Description	Suggested Solution
1.	Your laptop/desktop cannot detect the Modem's WiFi Signal/SSID.	I. Ensure that the modem is switched on and that the USB WiFi Adapter is properly plugged into the modem. II. Make sure that user "start" the wifi at "networking -> Wifi" at Web GUI. In addition, Disable the Hide SSID option. III. Check that your laptop/desktop has its WiFi function turned on. Ensure that it can detect WiFi 11 frequencies and is able to support B, G and B/G mix mode. IV. To ensure that it is not an issue of weak service signals, position your laptop/desktop near to the Modem. V. Make sure that the SSID you are searching for through the WiFi search network menu matches the SSID that has been set in the Modem.
2.	Your laptop/desktop can detect the Modem's WiFi signal and SSID but unable to connect to it.	I. Ensure that you are connected to the correct SSID. II. Check your WiFi Security Mode as some security modes may require Radius Server Authentication. III. Ensure you key in the correct and matching security key/mode in the laptop/desktop and Modem. IV. Disable Access Control at the P1 W1MAX Modem (DV-230) WiFi tab on the web GUI.
3.	You are connected to the Modem's WiFi SSID but unable to get an IP or has limited connection.	I. Check that you have keyed in the correct and matching security key mode in the laptop/desktop and Modem II. Check that the Modem's DHCP server is enabled at Networking -> DHCP Server. Ensure that the DHCP IP range is bigger than the amount of desktop/laptop connected to it via wired or wireless to DV230. III. Disable Access Control at the P1



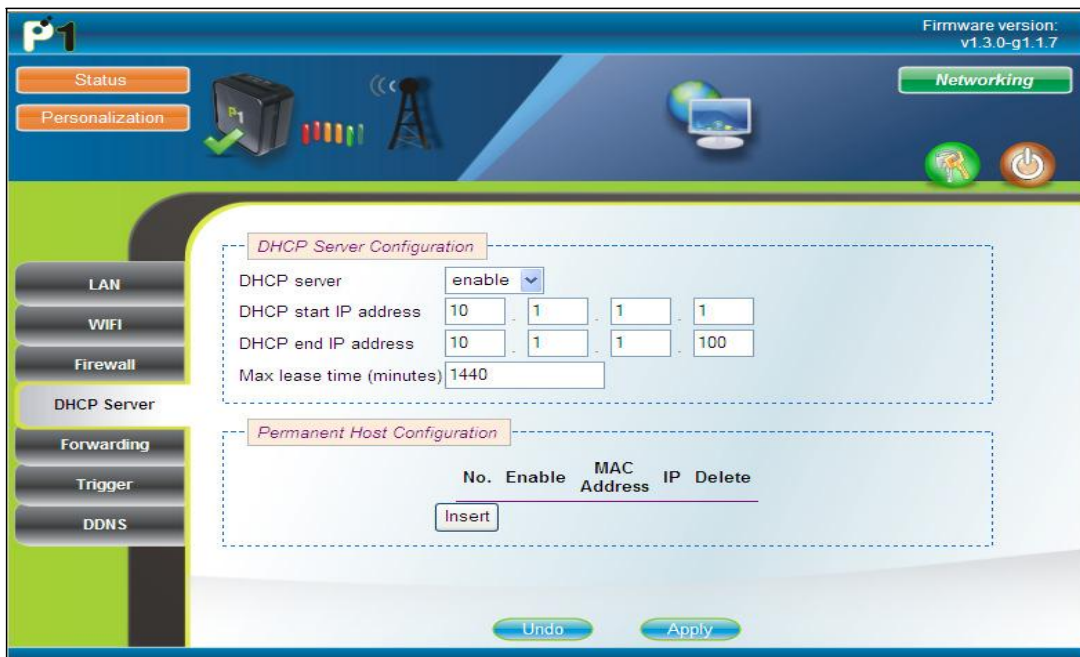
		WIMAX Modem (DV-230) WiFi tab on the web GUI.
4.	You are connected to the Modem's WiFi SSID and can an IP but cannot browse the Internet.	<ol style="list-style-type: none"> I. Set your laptop's/desktop's Network Wireless Connection to Obtain IP automatically and Obtain DNS server address automatically. II. Ensure that your Modem is connected to WIMAX service by checking your Modem's LED lights. III. Check for proxy settings that disables your connection in your Web browser. IV. User may have to click Repair on their WiFi Network Connection for Windows OS or a similar function for other operating systems. V. Check whether you can ping to the Modem. The gateway for your laptop/desktop should have the same IP as the LAN IP for your Modem. VI. Disable Access Control at the P1 WIMAX Modem (DV-230) WiFi tab on the web GUI.
5.	You experience irregular or slow browsing when connected through WiFi.	<ol style="list-style-type: none"> I. Check whether you can ping to the Modem. The gateway for your laptop/desktop should have the same IP as the LAN IP for your Modem. II. To ensure that it is not an issue of weak service signals, position your laptop/desktop near to the Modem. III. Try changing the WiFi Channel to a different channel as it may be due to WiFi Interference. IV. Do a ping and speed test check via wired to the Modem to determine if it is a WIMAX network congestion issue.

Networking - Firewall



Networking - DHCP server

In this section, you can set the Modem's LAN DHCP Server settings.



The settings for the DHCP Server is as below:

- By default the DHCP Server settings are enabled and the default DHCP IP range is from 10.1.1.1 to 10.1.1.100
- You can either Enable or Disable the Modem's DHCP Server.
- You can also change the DHCP Starting IP, DHCP Ending IP, auto obtain DNS IP from ISP or manually set DNS IP, change the Domain Name and

the DHCP max lease time.

- Users can also have a permanent DHCP IP bind to a PC/Laptop Network Interface Card MAC address under Permanent Host Configuration.
- After keying the settings, you have to click Apply and reboot for the new settings to take effect.

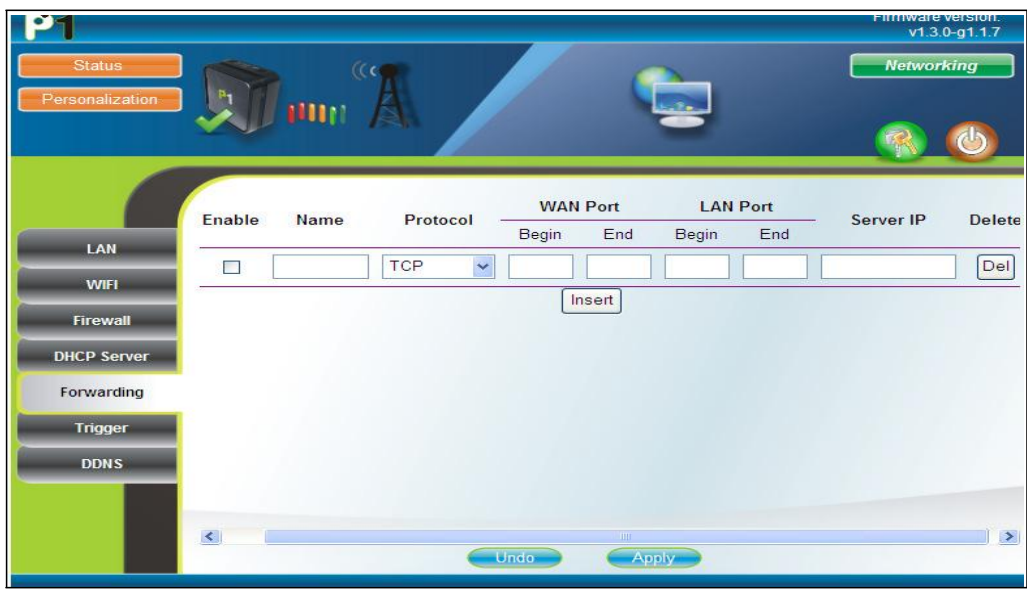
Troubleshooting:

- If your PC/Laptop cannot get an IP from the Modem, please check whether the Modem’s DHCP Server has been Enabled.
- If you cannot browse the Internet or certain websites, ensure that you set the Primary DNS to tick the From ISP option as certain users may change the DNS configurations.
- If you cannot bind the PC/Laptop NIC MAC, check whether it is bind to the correct MAC Address by typing ipconfig/all in the Command Prompt for Windows OS. The MAC Address should be in the format of 00:11:22:33:44:55

Note: If you change the range of the Default LAN IP from 10.1.1.254 to 192.168.1.254, the DHCP Server will change the DHCP Start IP address to 192.168.1.1 and DHCP End IP address to 192.168.1.100 accordingly.

Networking - Forwarding

Port Forwarding helps you to open up a Port in the DV-230 so that support certain Online Games, Host a Web Server or FTP Server, and etc.



WAN Port	It shows the range of Ports for incoming data from the Modem’s Public IP; should it be Open for the Port Forwarding rule.
Server IP	It shows which computer is connected to the Modem’s

Address	Server IP Address for Port Forwarding.
LAN PORT	This is the range of Ports that the incoming data should be forwarded to on the LAN Side.
Protocol	The Internet Protocol that is allowed to be Port Forwarded in the Incoming data of the WAN Side.
Enable	Tick this if you want to Enable this Port Forwarding Rule
Delete	Click on this if you want to Delete this Port Forwarding Rule
Insert	Insert another row of Port Forwarding Rules
Apply	To Save the Port Forwarding Rule or to Save the changes that has been done. After this, you will need to reboot the Modem.

Troubleshooting:

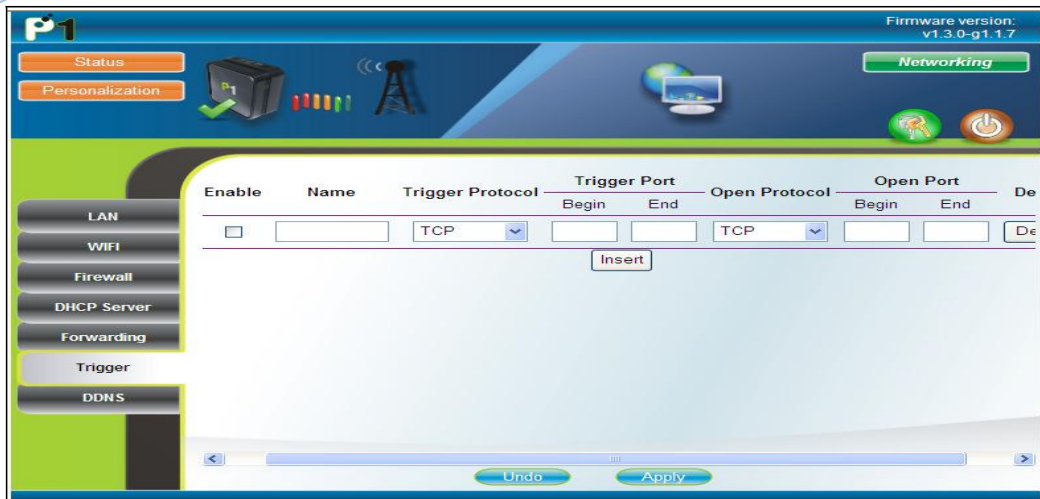
If you are not able to set Port Forwarding or make it work:

- Make sure the Port Forwarding range in both “WAN” and “LAN” is not more or equal to 900. For example the range must be 30000 to 30899, and not 30000 to 30900.
- Make sure the intended computer IP for the Port Forwarding on the LAN Side is the same IP as you set in the Web GUI Server IP Address
- Make sure that the intended computer has turned off any Firewall programs and allow the Ports that have been set in the Modem Port Forwarding rule.
- A Port can only be used by ONE program at a time. This means that you can only use Port 500 on ONE computer on the Modem at a time. Using Port 500 on two computers at the same time would violate the ONE program rule, and your data would get messed up.
- Make sure you know and set the correct Ports for “WAN” and “LAN” in your Port Forwarding rules as this is always the common mistake.

Networking - Trigger

Port Triggering is Port Forwarding with an ON/OFF switch for the Ports that have been forwarded. This ON/OFF switch is turned ON or OFF by data flowing out of a Trigger Port.

Port Triggering is a little more secured than Port Forwarding because the incoming Ports are not open all the time. They are only open when a program is actively using the Trigger Port.



Note: Most Port Triggering setups DO NOT require you to enter a LAN IP Address to forward the incoming Ports to. This means that any computer on the network can use your Port Triggering setup. If two computers try to use the Port Triggering setup at the same time you will run into problems.

Name	Is an Identifier of the Port Triggering rule.
Trigger Port	It is the range of Ports that will be triggered ON/OFF when there is outgoing data that uses that range of Ports from your Modem's Public IP side.
Open Port	It is the range of Ports that incoming data will be forwarded to when outgoing data triggers the Port Triggering rule in the Modem.
Trigger Protocol	It is the Internet Protocol that is allowed to be Port Forwarded in the Incoming data of the WAN Side.
Open Protocol	It is the Internet Protocol that is allowed to be Port Forwarded in the Incoming data of the LAN Side.
Enable	Tick this if you want to Enable this Port Forwarding Rule
Delete	Click on this if you want to Delete this Port Forwarding Rule
Insert	Insert another row of Port Forwarding Rules
Apply	To Save the Port Forwarding Rule or to Save the changes that has been done. After this, you will need to reboot your Modem.

Troubleshooting:

- Make sure that the intended computer has turned OFF any Firewall programs and allow the Ports that have been set in the Modem's Port Triggering rule.
- A Port can only be used by one program at a time. This means that you can only use Port 500 on one computer with the Modem at a time. Using Port 500 on two computers at the same time would violate the



one program rule, and your data would get messed up.

- Make sure you know and set the correct Ports for “Triggering Port” and “Forwarding Port” in your Port Triggering rule as this is always the common mistake.
- The Port that you set for Port Triggering is constantly sending data out to WAN. The length of time that the Modem keeps those Ports open needs to be taken into account. If the Modem times out between the gaps of outgoing data to WAN, the Port Forwarding connection will be severed.

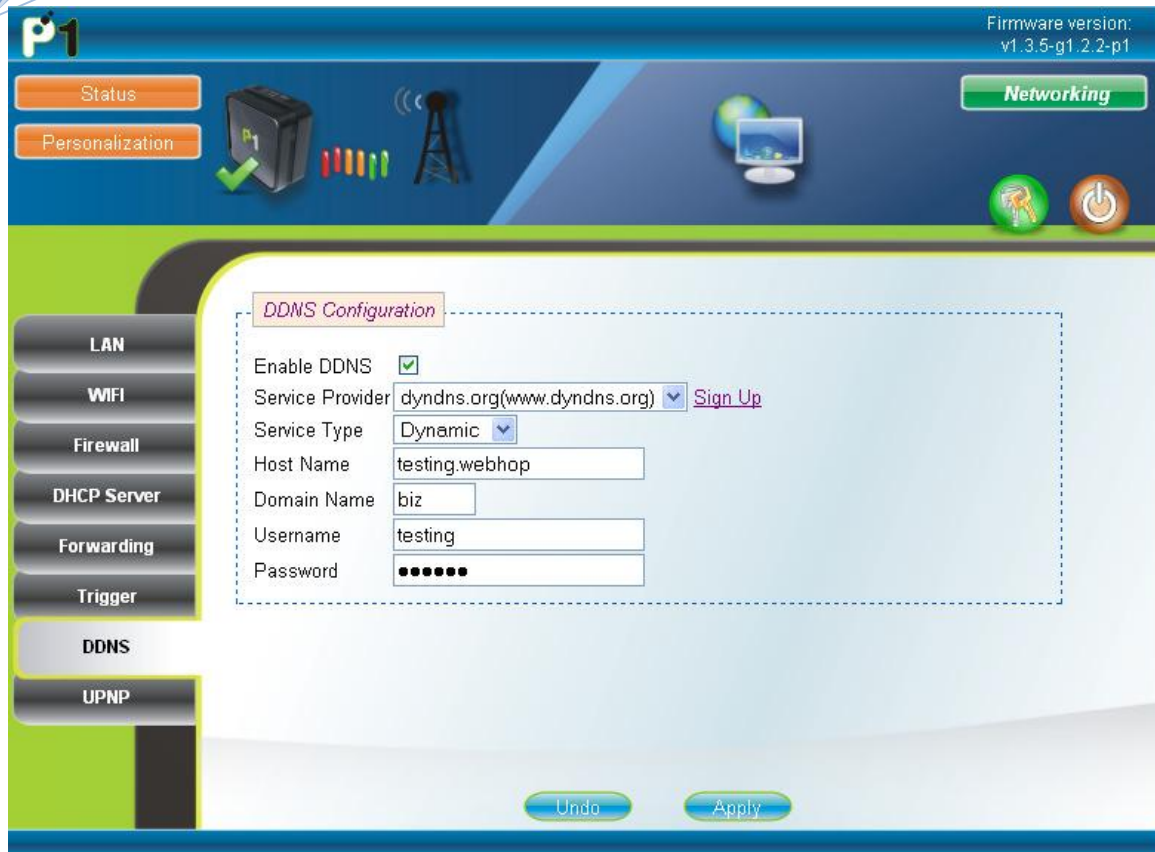
EXAMPLE: What happens when you are trying to download a very large file? The Modem that you have set up with Port Triggering may not keep sending data out of the trigger Port. When that happens, the Modem closes the incoming Ports, and your download is interrupted.

Networking - DDNS

Dynamic Domain Name Server (DDNS) allows you to create a host name that points to your Dynamic Public IP or Static Public IP address or URL.

Settings:

- Tick on the “Enable DDNS” to enable this feature.
- On the “Service Provider” column, select the DDNS Service Provider Name that you sign up for in this service.
- Create an account with either “dyndns.org” or “tzo.com”
- Create and customize your own host name and select the domain name of your choice at “dyndns.org” or “tzo.com”
- The correct setting at DV230 is as the screenshot below



- Host Name setting should be the customize name like “testing” or “johnnie” or “June” as shown above. It should be followed by a “.” (dot) like “webhop” or “dyndns” or “homelinux” that have to be chosen from the dyndns.org or tzo.com website.
- Domain Name setting is the end of chosen domain from the website like “com” or “net” or “org” or “cc”
- You will also have to key in the username and password of your account on dyndns.org or tzo.com at the DV230 username and password field.
- Click “Apply” and reboot your Modem to Save the changes.
- Once everything is complete, DV230 will update the IP of your created hostname every time the DV230 is connected to the internet or the DV230 obtains a new public IP.

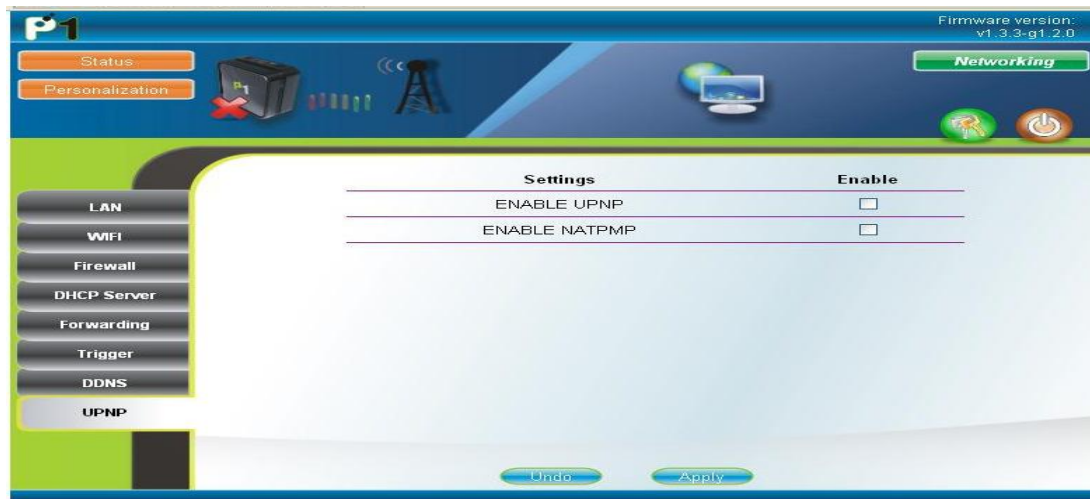
Troubleshooting:

- Make sure that your Username, Password & Host Name is correct and is the same as the account that you have created with the DDNS Service Provider.
- Certain DDNS Service Providers do not instantly link the Host Name that you have created in the Modem, it would take between 5 minutes to 30 minutes for the DDNS Service Provider to update.
- The Modem will automatically update the DDNS Service Provider when the DDNS configurations have been set, on every Reboot, when you

connect to the Internet or if there is a change of Public IP assigned to it.

Networking - UPNP

There are 2 options that can be enabled under this setting tab which are UPNP and NATPM.



UPNP

Explanation:

Universal Plug and Play (UPnP) is a set 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. UPnP supports zero-configuration networking.

How it works:

UPnP devices are "plug-and-play" in that when connected to a network they automatically join a network, obtain an IP address, announcing their network address and supported device and services types, enabling clients that recognize those types to immediately begin using the device. Devices can leave the network automatically without leaving any unwanted state information behind.

Usage:



Just tick the box under “ENABLE UPNP” to enable it. Devices which support UPnP are printers, scanners, WLAN access points, media servers and many more.

NAT-PMP

Explanation:

NAT Port Mapping Protocol (NAT-PMP) is introduced by Apple Computer in June 2005. NAT-PMP allows a computer in a private network (behind a NAT router) to automatically configure the router to allow parties outside the private network to contact itself. NAT-PMP runs over UDP. It essentially automates the process of port forwarding.

How it works:

In NAT-PMP is a method for retrieving the public IP address of a NAT gateway, thus allowing a client to make this public IP address and port number known to peers that may wish to communicate with it.

Usage:

Just tick the box under “ENABLE NATPMP” to enable it. Products that support this protocol includes MAC OS X, limewire, uTorrent, Nicecast and many more.