D-Link®

DVG-G5402SP
VoIP Wireless Router

User’s Manual

Version 1.0

(10 June 2008)

Warranty: please contact your D-Link Authorized Reseller or the D-Link Branch Office nearest your place of purchase for information about the warranty offered on your D-Link product.

Information in this document is subject to change without notice.

FCC Warning

This equipment 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 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 communication. 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:

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

CE Mark Warning

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

Warnung!

Dies ist ein Produkt der Klasse B. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase B. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe B. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe B. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

Contents

1. Introduction

1-1 Product Overview

The DVG-G5402SP is designed to carry both voice and facsimile over the IP network and wirelessly share Internet access. It uses the industry standard SIP call control protocol so as to be compatible with free registration services or VoIP service providers' systems. As a standard user agent, it is compatible with all common Soft Switches and SIP proxy servers. While running optional server software, the VoIP Router can be configured to establish a private VoIP network over the Internet without a third-party SIP Proxy Server.

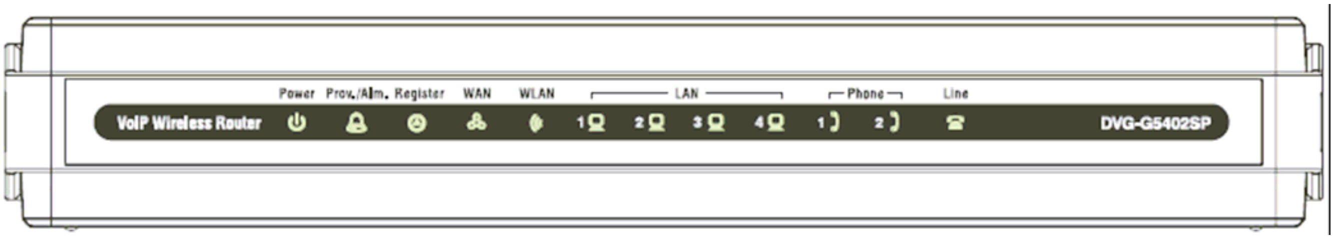
The DVG-G5402SP can be seamlessly integrated into an existing network by connecting to a phone set and fax machine. With only a broadband connection such as an ADSL bridge/router, a Cable Modem or a leased-line router, the VoIP Router allows you to use voice and fax services over IP in order to reduce the cost of all long distance calls.

The DVG-G5402SP is also an 802.11b/g wireless access point. Allow wireless clients to connect to it and share your broadband Internet connection. A built-in 4-port switch makes it possible to connect up to 4 Ethernet-enabled computers or devices to also share your Internet connection.

The DVG-G5402SP can be configured a fixed IP address or it can have one dynamically assigned by DHCP or PPPoE. It adopts either the G.711, G.726, G.729A or G.723.1 voice compression format to save network bandwidth while providing real-time, toll quality voice transmission and reception.

1-2 Hardware Description

Front Panel



Power: Power LED. A steady light indicates a proper connection to a power source.

Prov./Alm.: A blinking light indicates the VoIP Router is attempting to connect with the Provisioning server. Once the service connects, the LED will turn off. The LED will light solid if the self-test or boot-up fails.

Register: The Register LED will turn on when the VoIP Router is connected to a VoIP service provider. The LED will turn off if not connected to a service provider.

WAN: When a connection is established the 10 or 100 LED will light up solid. The LED will blink to indicate activity. If the 10 or 100 LED does not light up when a cable is connected, verify the cable connections and make sure your devices are powered on.

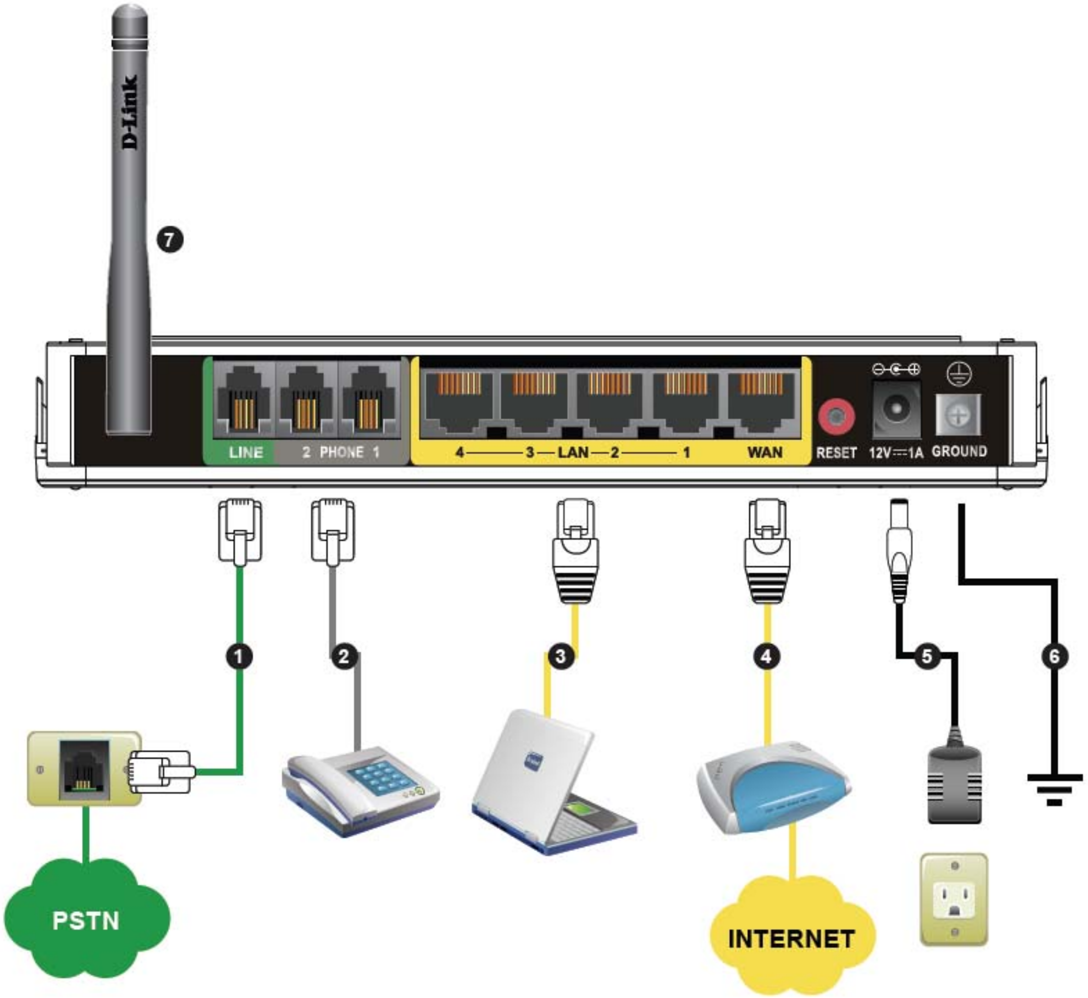
WLAN: A steady light indicates a wireless connection. A blinking light indicates that the VoIP Router is receiving/transmitting from/to the wireless network.

LAN: When a connection is established the 10 or 100 LED (bottom) will light up solid on the appropriate port. The LEDs will blink to indicate activity. If the 10 or 100 LED does not light up when a cable is connected, verify the cable connections and make sure your devices are powered on.

Phone: This LED displays the VoIP status and Hook/Ringing activity on the phone port that is used to connect your normal telephone(s). If a phone connected to a phone port is off the hook or in use, this LED will light solid. When a phone is ringing, the indicator will blink.

Line: Light on means the line is in use (off-hook), and vice versa.

Rear Panel



1. **Line:** Connect to your original telephone line on the wall jack with RJ-11 cable.
2. **Phone Port (1-2):** Connect to your phones using standard phone cabling (RJ-11).
3. **LAN:** Connect to your Ethernet enabled computers using Ethernet cabling.
4. **WAN:** Connect to your broadband modem using an Ethernet cable.
5. **Power Receptor:** Receptor for the provided power adapter.
6. **Ground:** A conducting connection with the earth. Connect with the ground so as to make the earth a part of an electrical circuit using metal wire.
7. **Antenna:** Connect to a wireless network.

WARNING: DO NOT (1) connect the phone ports to each other (FXS to FXS) or (2) connect any phone port directly to a PSTN line (FXS to PSTN) or to an internal PBX line (FXS to PBX extension). Doing so may damage your VoIP Router.

Use Reset Button to restore factory default settings:

1. **Power on.**
2. **Press and hold the reset button for 5 seconds.**
3. **Release the reset button. Factory settings will be restored.**

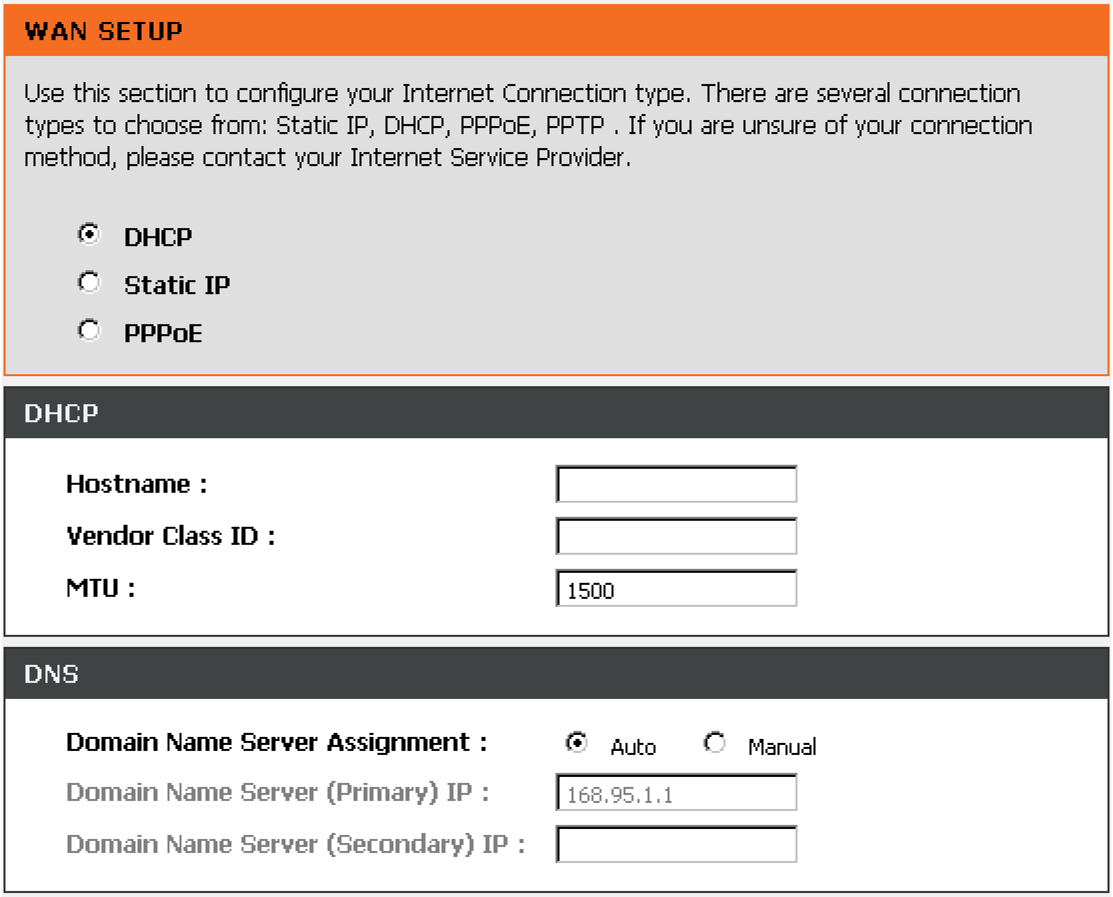
2. VoIP Router Web Configuration (continued)

During configuration, please follow the Setup Hint for some specific procedure in case the VoIP Router fails to make the changes active.

Situation 1: (example: Internet Setup)

Setup Hint:

1. Select DHCP WAN Setup.
2. Click "Apply".
3. Click "Save and Restart" to make change take effect.



WAN SETUP

Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP . If you are unsure of your connection method, please contact your Internet Service Provider.

● DHCP
○ Static IP
○ PPPoE

DHCP

Hostname :	
Vendor Class ID :	
MTU :	1500

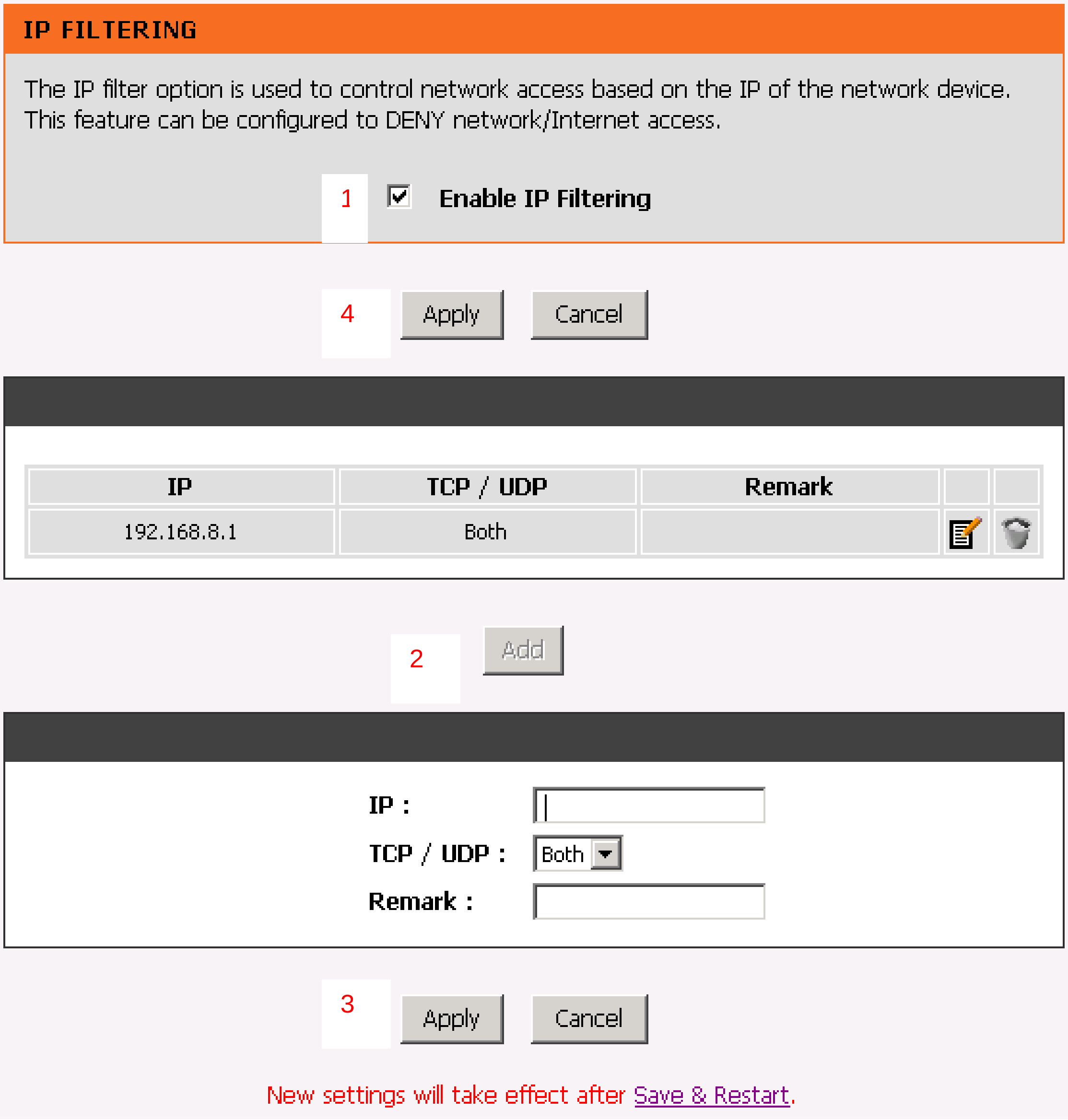
DNS

Domain Name Server Assignment :	● Auto ○ Manual
Domain Name Server (Primary) IP :	168.95.1.1
Domain Name Server (Secondary) IP :	

Situation 2: (example: Enable IP Filtering)

Setup Hint:

1. Click "Enable IP Filtering" check box to open the main screen.
2. Click "Add" to enter an entry.
3. After Adding an entry, you have to click "Apply".
4. Don't forget to click "Apply" which in the filed of "Enable IP Filtering".
5. After settings, save and reboot.



IP FILTERING

The IP filter option is used to control network access based on the IP of the network device. This feature can be configured to DENY network/Internet access.

1 ☑ Enable IP Filtering

IP	TCP / UDP	Remark		
192.168.8.1	Both		📝	🗑

IP : |

TCP / UDP : Both ▾

Remark :

New settings will take effect after Save & Restart.

2-1 SETUP

2-1-1 Internet Setup

WAN (Wide Area Network) Settings are used to connect to your ISP (Internet Service Provider). The WAN settings are provided to you by your ISP and oftentimes referred to as "public settings". Please select the appropriate option for your specific ISP.

IP Configuration (Setting WAN Port)

There are five methods of obtaining a WAN port IP address:

1. DHCP, which means a Dynamic IP (Cable Modem)
2. Static IP
3. PPPoE (dial-up ADSL)

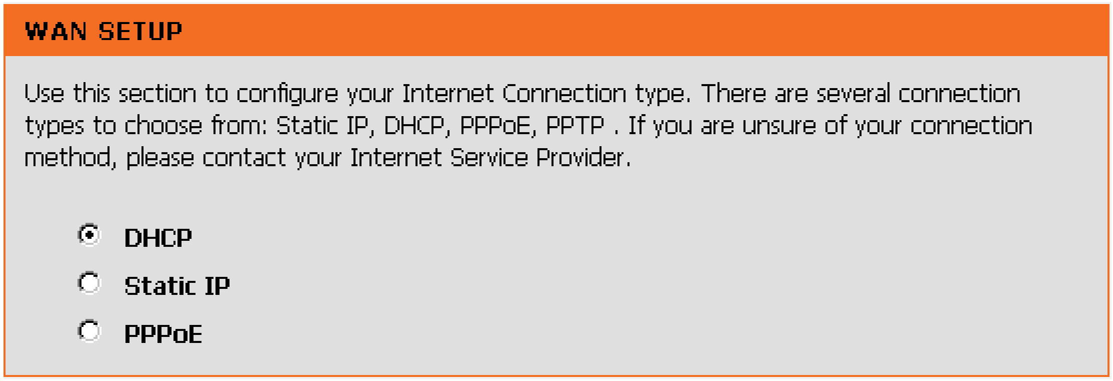
Methods for using DHCP and PPPoE for obtaining an IP address may vary. If you are not familiar with creating a network connection, please contact your local ISP.

After selecting the suitable option, click **Accept** at the bottom of the screen to save the settings.

You need to save the changes and restart the VoIP Router to make the changes active. Saving the settings: Click **MAINTENANCE** and select **Save/Restart** in **System** from the left menu. Tick **Save Settings** and **Restart**, then click **Accept**. Wait for about 40 seconds before the VoIP Router obtaining an IP address by the method you selected.

Note: When the system has obtained a new IP address, and you are using a WAN port to enter the Web Configuration Screen, the new IP address has to be used before you can get connected to the VoIP Router. The same principle applies to the next two settings.

SETUP → Internet Setup



WAN SETUP

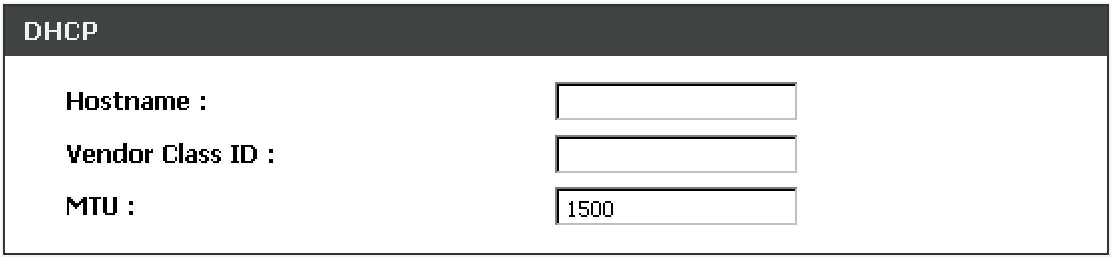
Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP . If you are unsure of your connection method, please contact your Internet Service Provider.

● DHCP

○ Static IP

○ PPPoE

SETUP → Internet Setup

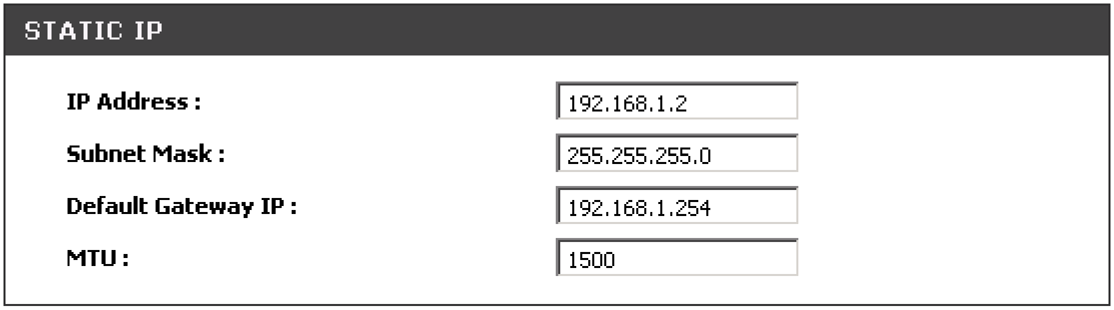


DHCP

Hostname :	
Vendor Class ID :	
MTU :	1500

DHCP: Select this option if your ISP (Internet Service Provider) provides you an IP address automatically. Cable modem providers typically use dynamic assignment of IP Address. The Host Name field is optional but may be required by some Internet Service Providers.

SETUP → Internet Setup

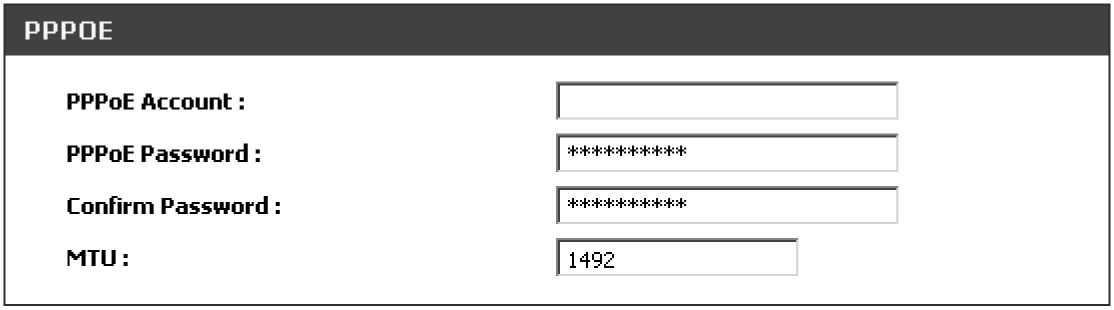


STATIC IP

IP Address :	192.168.1.2
Subnet Mask :	255.255.255.0
Default Gateway IP :	192.168.1.254
MTU :	1500

Static IP: Select this option if your ISP (Internet Service Provider) provides you a Static IP address. Enter the **IP address**, **Subnet Mask** and **Default Gateway IP**.

SETUP → Internet Setup

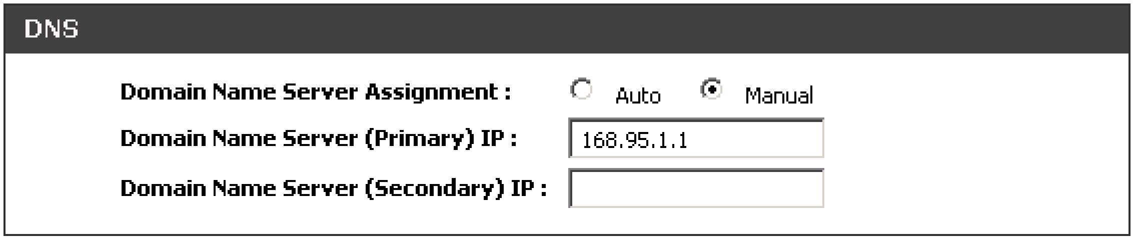


PPPOE

PPPoE Account :	
PPPoE Password :	**********
Confirm Password :	**********
MTU :	1492

PPPoE: Select this option if your ISP requires you to use a PPPoE (Point-to-Point Protocol over Ethernet) connection. Enter the **PPPoE Account**, **PPPoE Password** and re-enter Password to confirm.

SETUP → Internet Setup



DNS

Domain Name Server Assignment :	○ Auto ● Manual
Domain Name Server (Primary) IP :	168.95.1.1
Domain Name Server (Secondary) IP :	

Domain Name Server Assignment: Select **Auto** or **Manual** to get the IP address of Domain Name Server assigned by ISP or manually.

Domain Name Server IP: Enter the primary and secondary IP address of Domain Name Server if Domain Name Server Assignment is **Manual**. Otherwise, the VoIP Router will not be able to access hosts using hostnames instead of IPs.

2-1-2 Wireless Setup

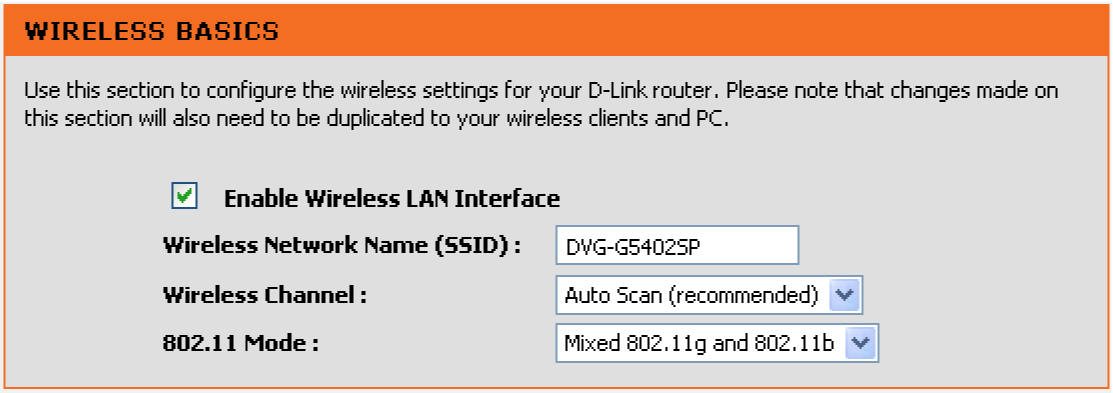
This section instructs you how to setup your wireless network on the VoIP Router device.

Setup Hint:

1. Every device in the same wireless network must use the same SSID.
2. To avoid wireless network overlap, a specific and different channel is needed.
3. Make sure security used by every device in the same wireless network is compatible with the wireless AP.

2-1-2-1 Wireless Basic

SETUP -> Wireless Setup -> Wireless Basic



WIRELESS BASICS

Use this section to configure the wireless settings for your D-Link router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

☑ Enable Wireless LAN Interface

Wireless Network Name (SSID) : DVG-G5402SP

Wireless Channel : Auto Scan (recommended)

802.11 Mode : Mixed 802.11g and 802.11b

Enable Wireless LAN Interface: Enable wireless basic settings on LAN interface.

Wireless Network Name (SSID): SSID is the name of your wireless network. All wireless-equipped devices share the same SSID to communicate with each other. It must be unique to identify separated wireless network. For security, you should change the default SSID to a special ID.

Wireless Channel: Select a clear and appropriate channel for your wireless network. A device on your wireless network must use a specific channel to transmit and receive data. If wireless network has overlap, change a different channel number.

802.11 Mode: The VoIP Router can operate in 2.4GHz ISM band with different speed of wireless connection, Select the wireless band of your network.

802.11b only - Allow all 802.11B compliant wireless devices to associate with the wireless AP.

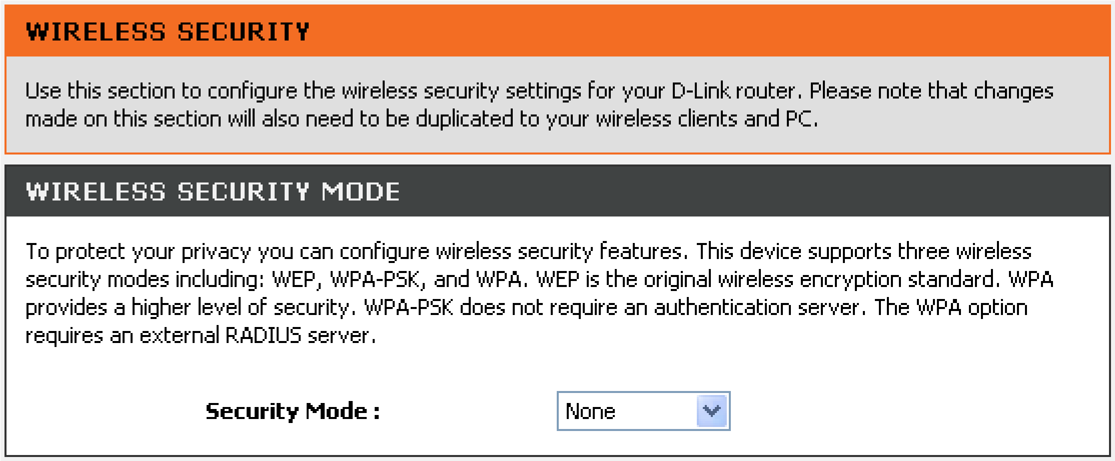
802.11g only - Allow all 802.11G compliant wireless devices to associate with the wireless AP.

Mixed 802.11g and 802.11b - Allow a mix of both IEEE802.11b and IEEE802.11g compliant wireless devices to associate with the wireless AP.

2-1-2-2 Wireless Security

This section introduces you different ways of wireless security you can setup. It is important to enable secure algorithm to protect your data from eavesdropping by unauthorized wireless users.

SETUP -> Wireless Setup -> Wireless Security



WIRELESS SECURITY

Use this section to configure the wireless security settings for your D-Link router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

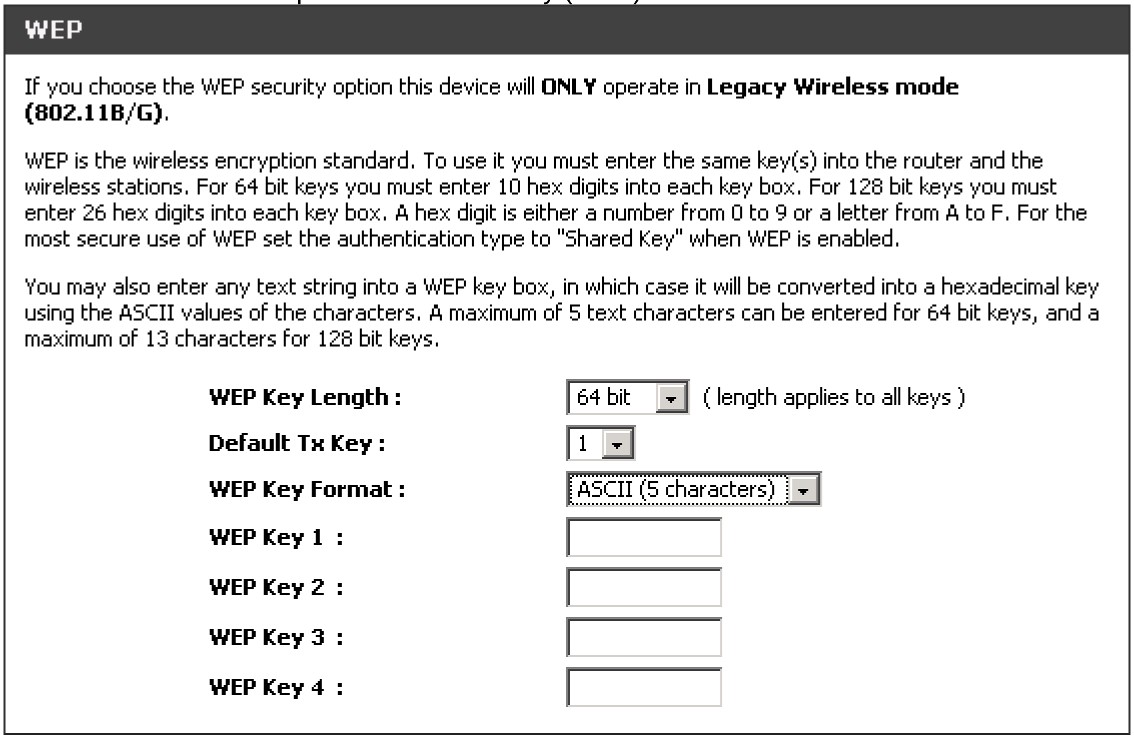
WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA-PSK, and WPA. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

Security Mode : None

Security Mode: Select the encryption/authentication type: None, WEP, WPA, WPA2 and WPA2 Mixed.

SETUP -> Wireless Setup -> Wireless Security (WEP)



WEP

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**.

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length : 64 bit (length applies to all keys)

Default Tx Key : 1

WEP Key Format : ASCII (5 characters)

WEP Key 1 :

WEP Key 2 :

WEP Key 3 :

WEP Key 4 :

WEP Key Length: Select 64-bit or 128-bit data encryption.

Default Tx Key: You can select one of the keys as active key at a time.

WEP Key Format: Select the preferred WEP Key Format according to which WEP encryption you choose. When WEP 64bits is enabled, you can select ASCII (5 characters) and Hex (10 characters). When WEP 128bits is enabled, you can select ASCII (13 characters) and Hex (26 characters).

WEP Key 1 – 4: You can manually input key value from Key1 to Key4. Type a character sting and apply changes.

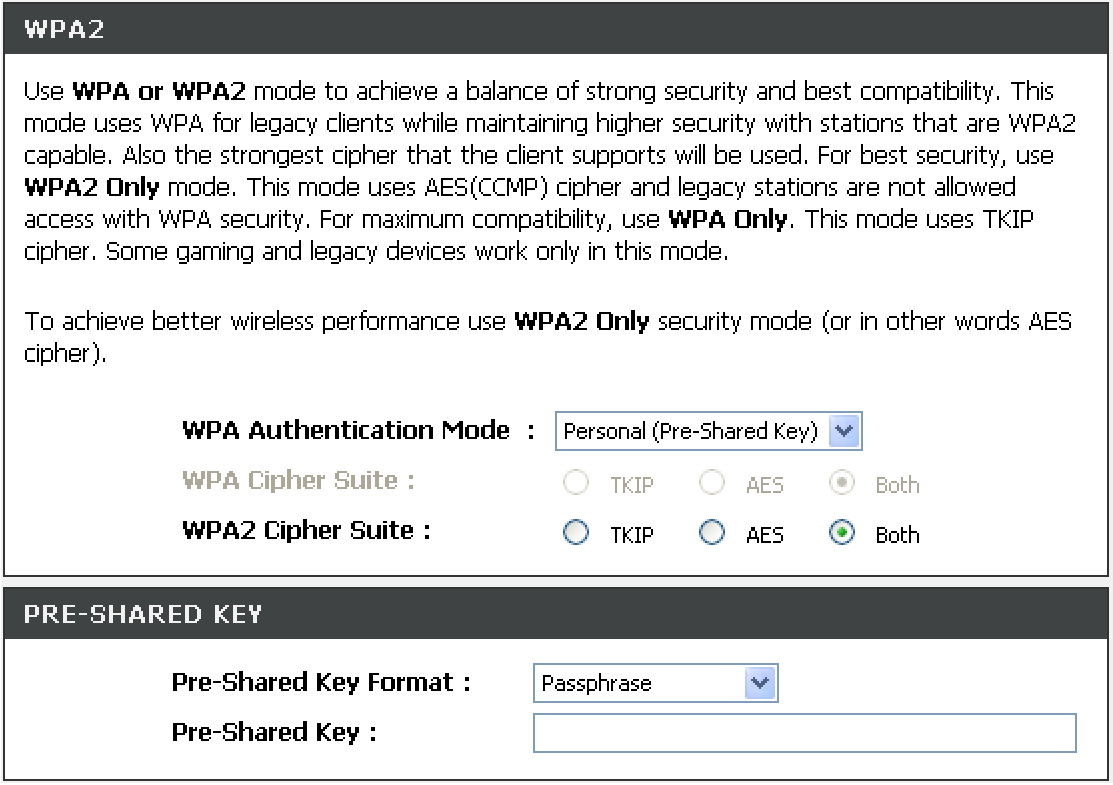
For a 64-bit WEP key - Enter 5 characters (ASCII sting) or 10 hexadecimal characters (“0-9”, “A-F”).

For a 128-bit WEP key - Enter 13 characters (ASCII sting) or 26 hexadecimal characters (“0-9”, “A-F”).

WPA Authentication Mode

The wireless network can use WPA Authentication to verify whether a wireless device is allowed to access your Access Point or not. You can choose to use Enterprise (RADIUS) method or Personal (Pre-Shared Key). The encryption mechanism used for RADIUS and WPA-PSK is the same. The difference between the two is that WPA-PSK uses a specific characters sting like password instead of a user-authentication.

SETUP -> Wireless Setup -> Wireless Security (WPA-PSK)



WPA2

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Authentication Mode : Personal (Pre-Shared Key)

WPA Cipher Suite : ○ TKIP ○ AES ● Both

WPA2 Cipher Suite : ○ TKIP ○ AES ● Both

PRE-SHARED KEY

Pre-Shared Key Format : Passphrase

Pre-Shared Key :

Select the type of WPA-PSK (WPA-PSK, WPA2-PSK, WPA2 Mixed-PSK), choose the proper security mode according to your wireless network.

WPA Authentication Mode: Select **Personal (Pre-Shared Key).**

WPA Cipher Suite: WPA Cipher Suite is used for the configuration of WPA or WPA2 Mixed.

> **TKIP -** TKIP is the security protocol used in WPA. The length of TKIP encryption is longer than WEP encryption that increases the complexity of decoding for crackers.

AES - The most powerful encryption algorithm that is commonly used in WPA.

WPA2 Cipher Suite: WPA2 Cipher Suite is used for the configuration of WPA2 or WPA2 Mixed.

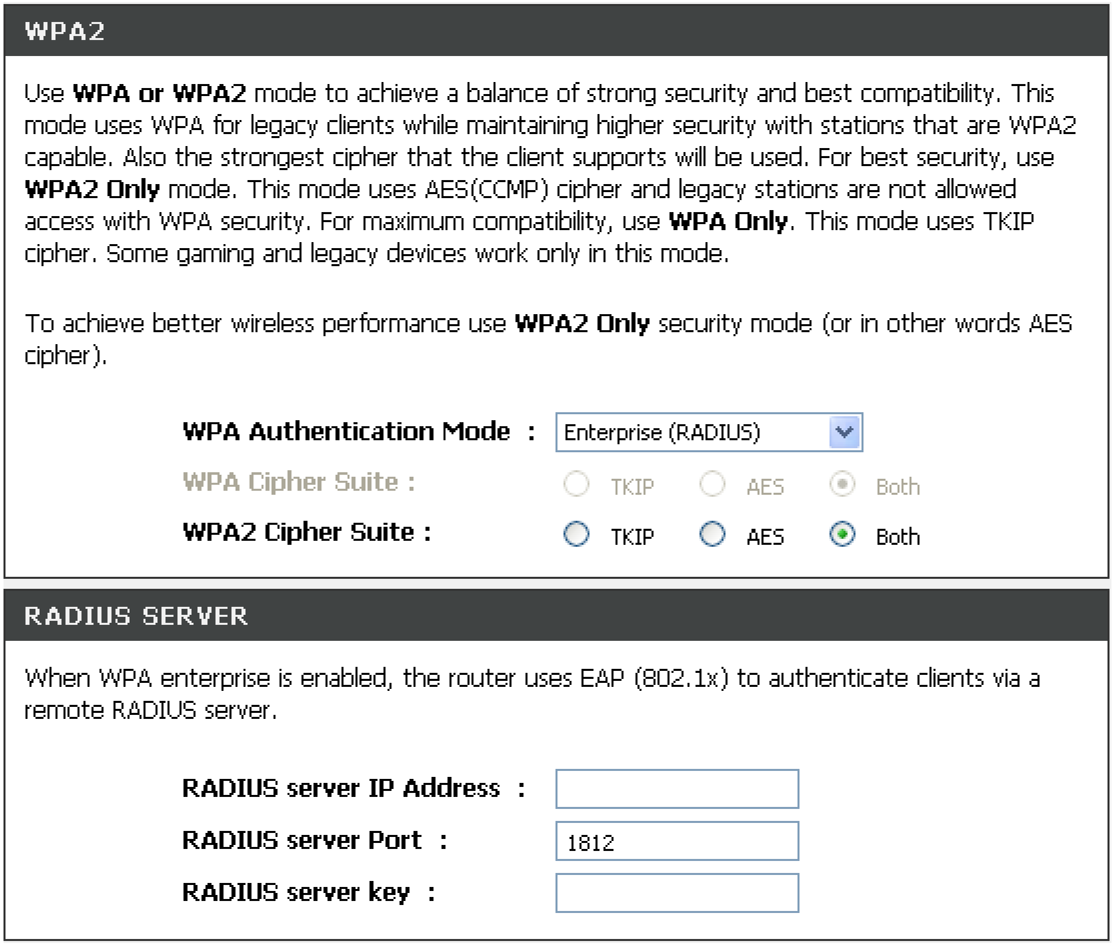
TKIP - TKIP is the security protocol used in WPA. The length of TKIP encryption is longer than WEP encryption that increases the complexity of decoding for crackers.

AES - The most powerful encryption algorithm that is commonly used in WPA.

Pre-Shared Key Format: Select the Format of Pre-Shared Key. You can select Passphrase or Hex (64 characters) by entering a character string ranging from “A-Z” and “0-9”.

Pre-Shared Key: Enter a key of 8-64 characters long in the Pre-Shared Key filed. Make sure this key is exactly the same on all other wireless stations.

SETUP -> Wireless Settings -> Wireless Security (WPA)



WPA2

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Authentication Mode : Enterprise (RADIUS)

WPA Cipher Suite : ○ TKIP ○ AES ● Both

WPA2 Cipher Suite : ○ TKIP ○ AES ● Both

RADIUS SERVER

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

RADIUS server IP Address :

RADIUS server Port : 1812

RADIUS server key :

Select the type of WPA (WPA, WPA2, WPA2 Mixed), choose the proper security mode according to your wireless network.

WPA Authentication Mode: Select **Enterprise (RADIUS).**

WPA Cipher Suite: WPA Cipher Suite is used for the configuration of WPA or WPA2 Mixed.

TKIP - TKIP is the security protocol used in WPA. The length of TKIP encryption is longer than WEP encryption that increases the complexity of decoding for crackers.

AES - The most powerful encryption algorithm that is commonly used in WPA.

WPA2 Cipher Suite: WPA2 Cipher Suite is used for the configuration of WPA2 or WPA2 Mixed.

TKIP - TKIP is the security protocol used in WPA. The length of TKIP encryption is longer than WEP encryption that increases the complexity of decoding for crackers.

AES - The most powerful encryption algorithm that is commonly used in WPA.

RADIUS Server:

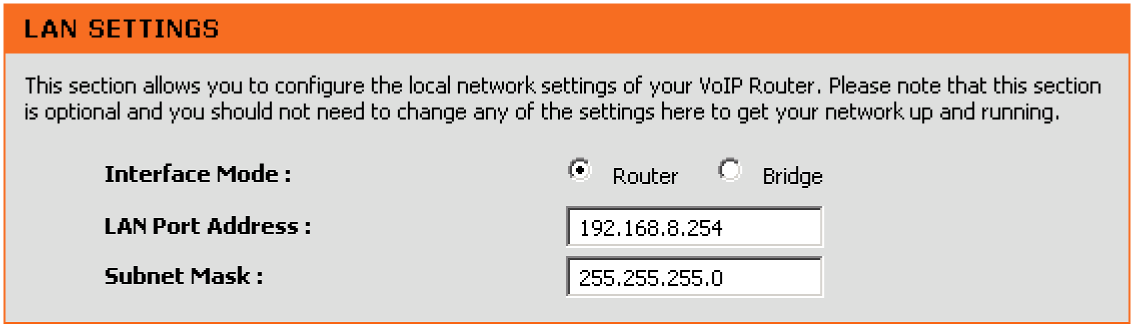
RADIUS server Port - Enter the port number of the authentication RADIUS server. Keep the default value: 1812 unless the server required change to another number.

RADIUS server IP Address - Enter the IP address of the authentication RADIUS server.

RADIUS server key - Enter the password such as a security Key.

2-1-3 LAN Setup

SETUP → LAN Setup



LAN SETTINGS

This section allows you to configure the local network settings of your VoIP Router. Please note that this section is optional and you should not need to change any of the settings here to get your network up and running.

Interface Mode : ● Router ○ Bridge

LAN Port Address : 192.168.8.254

Subnet Mask : 255.255.255.0

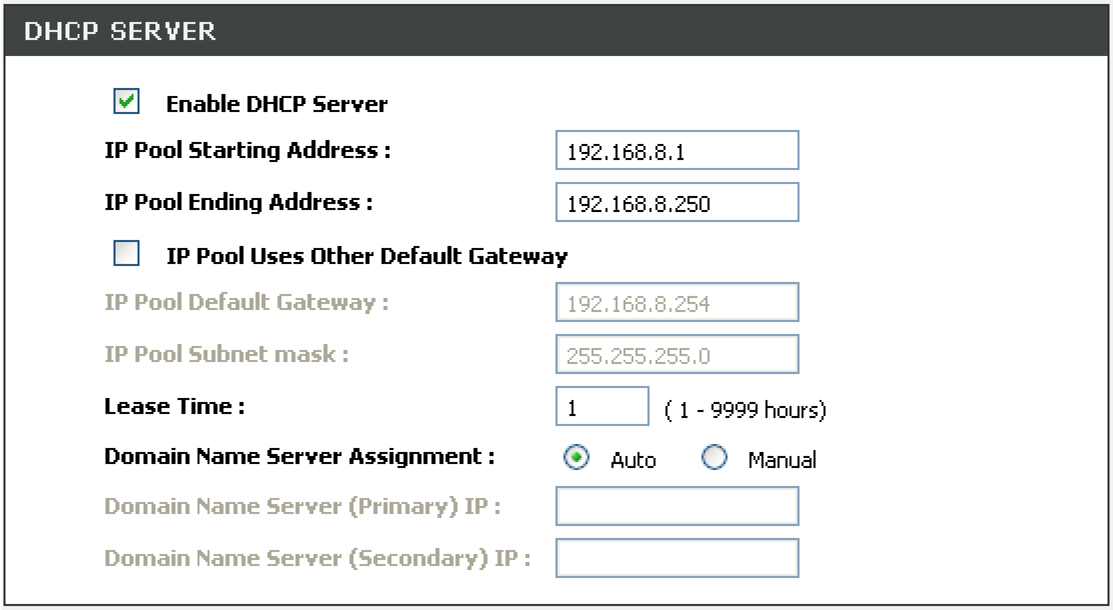
Interface Mode: Select the VoIP Router serving as a **Router** with NAT or **Bridge** between WAN port and LAN port without NAT.

Note: It is still accessible if LAN Interface Mode is Bridge.

LAN Port Address: Enter the LAN IP address of the VoIP Router. It is also the default gateway for DHCP clients.

Subnet Make: Enter the subnet mask for DHCP clients.

SETUP → LAN Setup



DHCP SERVER

☑ Enable DHCP Server

IP Pool Starting Address :	192.168.8.1
IP Pool Ending Address :	192.168.8.250

□ IP Pool Uses Other Default Gateway

IP Pool Default Gateway :	192.168.8.254
IP Pool Subnet mask :	255.255.255.0
Lease Time :	1 (1 - 9999 hours)
Domain Name Server Assignment :	● Auto ○ Manual
Domain Name Server (Primary) IP :	
Domain Name Server (Secondary) IP :	

Enable DHCP Server: This variable is to assign the IP address for the devices connected to LAN port of the VoIP Router.

IP Pool Starting Address: Enter the starting IP address for the DHCP server's IP assignment.

IP Pool Ending Address: Enter the ending IP address for the DHCP server's IP assignment.

IP Pool Uses Other Default Gw: Check the box to assign different default gateway for DHCP clients.

IP Pool Default Gateway: Enter the new default gateway that is different from LAN IP of the VoIP Router.

IP Pool Subnet mask: Enter the new subnet mask.

Lease Time: Enter the length of time for the IP lease.

Domain Name Server Assignment: Select **Auto** or **Manual** to get the IP address of Domain Name Server assigned by ISP or manually.

Domain Name Server IP: Enter the primary and secondary IP address of Domain Name Server if Domain Name Server Assignment is **Manual**. Otherwise, the VoIP Router will not be able to access hosts using hostnames instead of IPs.

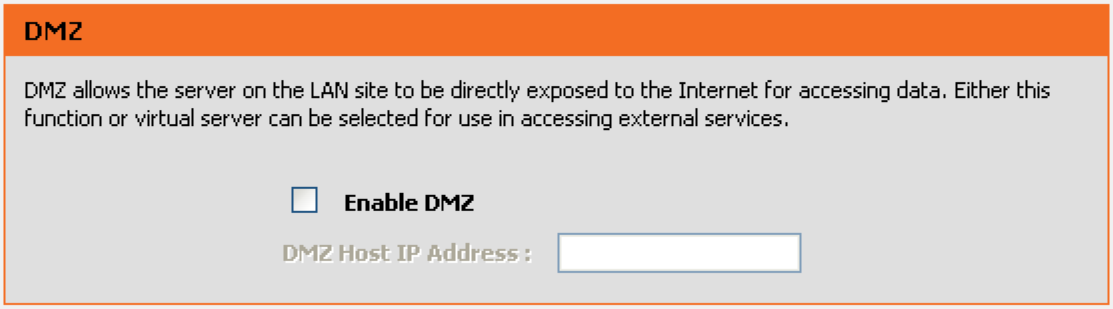
2-2 ADVANCED

2-2-1 Firewall and DMZ

2-2-1-1 DMZ

DMZ (Demilitarized Zone) allows the server on the LAN site to be directly exposed to the Internet for accessing data and to forward all incoming ports to the DMZ Host. Adding a client to the DMZ may expose that computer to a variety of security risks; so only use this option as a last resort.

ADVANCED → Firewall and DMZ → DMZ



DMZ

DMZ allows the server on the LAN site to be directly exposed to the Internet for accessing data. Either this function or virtual server can be selected for use in accessing external services.

☐ Enable DMZ

DMZ Host IP Address :

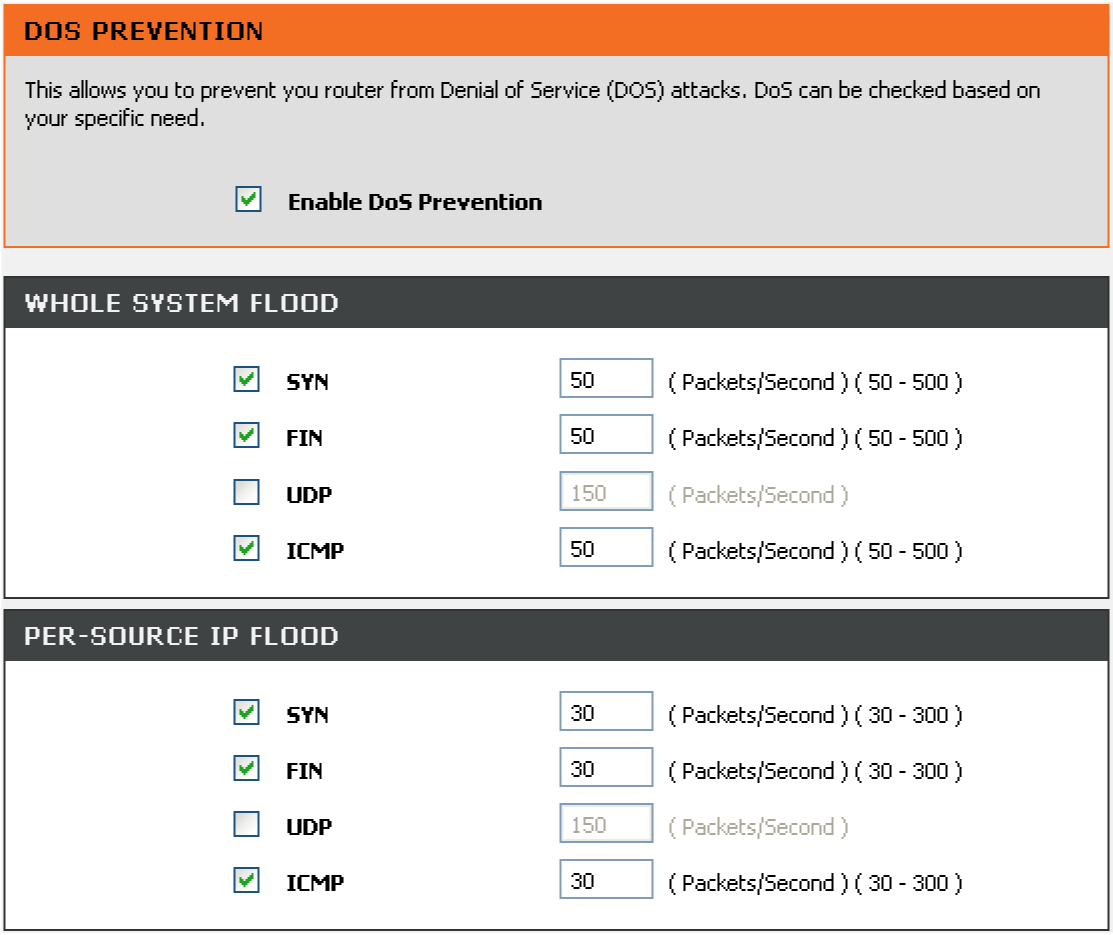
Enable DMZ: Check the box to enable DMZ feature.

DMZ Host IP Address: Enter the IP address of that computer as a DMZ Host with unrestricted Internet access.

Note: Either this function or virtual server can be selected for use in accessing external services.

2-2-1-2 DoS Prevention

ADVANCED → Firewall and DMZ → DoS Prevention



DOS PREVENTION

This allows you to prevent you router from Denial of Service (DOS) attacks. DoS can be checked based on your specific need.

☑ Enable DoS Prevention

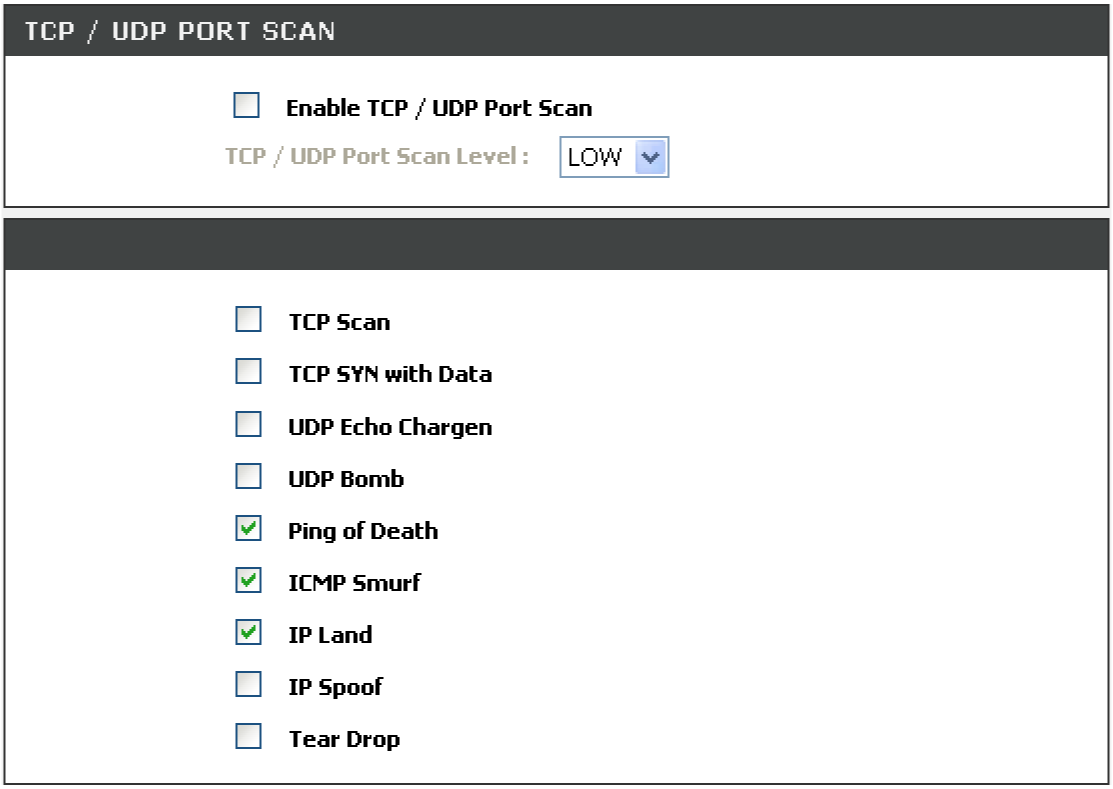
WHOLE SYSTEM FLOOD

☑	SYN	50	(Packets/Second) (50 - 500)
☑	FIN	50	(Packets/Second) (50 - 500)
□	UDP	150	(Packets/Second)
☑	ICMP	50	(Packets/Second) (50 - 500)

PER-SOURCE IP FLOOD

☑	SYN	30	(Packets/Second) (30 - 300)
☑	FIN	30	(Packets/Second) (30 - 300)
□	UDP	150	(Packets/Second)
☑	ICMP	30	(Packets/Second) (30 - 300)

ADVANCED → Firewall and DMZ → DoS Prevention



TCP / UDP PORT SCAN

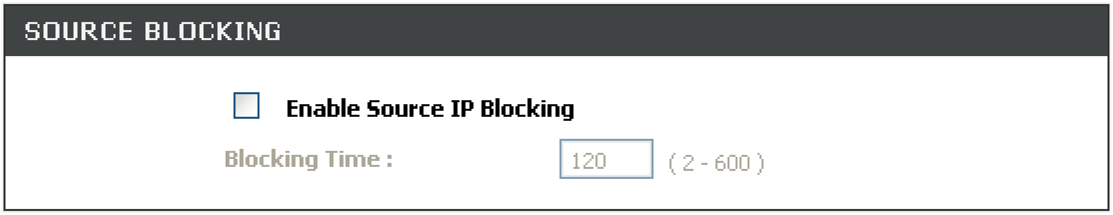
□ Enable TCP / UDP Port Scan

TCP / UDP Port Scan Level : LOW

- □ TCP Scan
- □ TCP SYN with Data
- □ UDP Echo Chargen
- □ UDP Bomb
- ☑ Ping of Death
- ☑ ICMP Smurf
- ☑ IP Land
- □ IP Spoof
- □ Tear Drop

Enable DoS Prevention: Check the box to prevent DoS attacks from WAN or LAN. There are various types of DoS attacking. Leave settings in this field to the default if you are not familiar with it.

ADVANCED → Firewall and DMZ → DoS Prevention



SOURCE BLOCKING

□ Enable Source IP Blocking

Blocking Time : 120 (2 - 600)

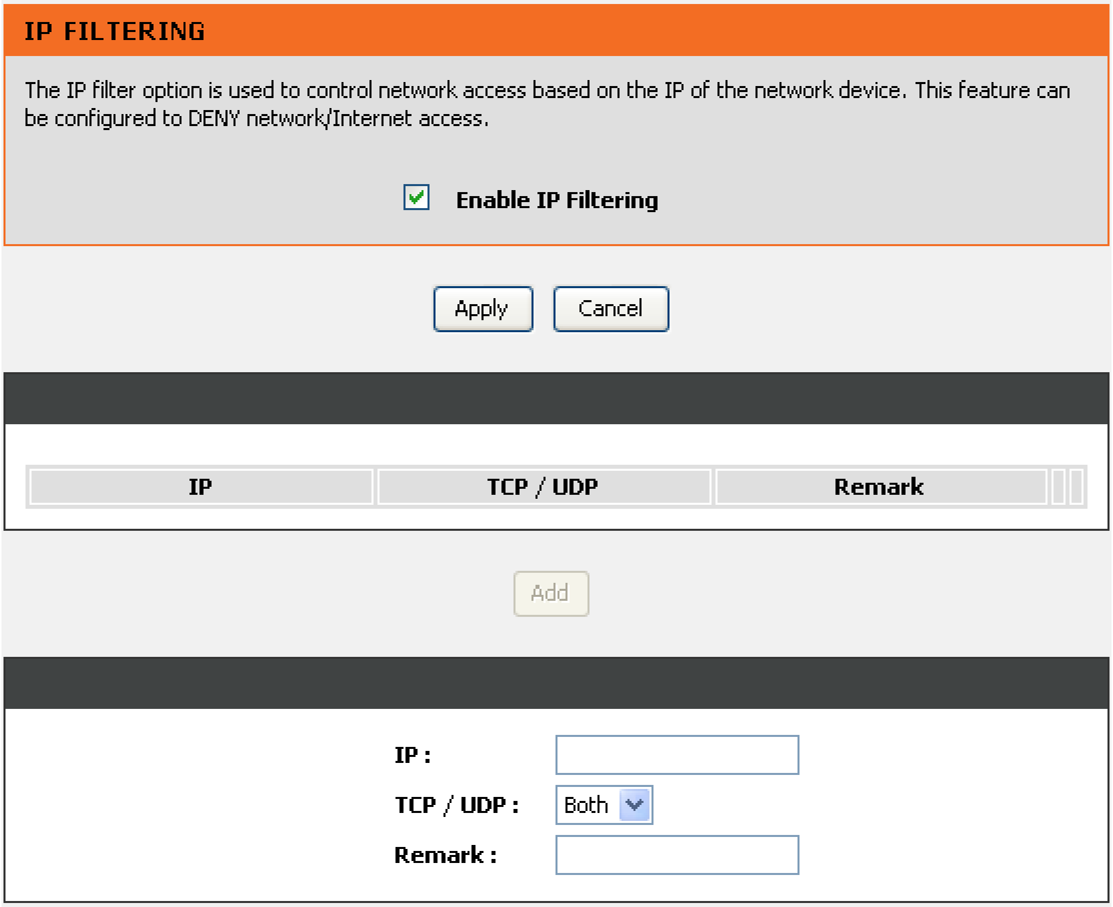
Enable Source IP Blocking: Check the box to block a particular IP address that detects the connection confirmed with the type of DoS attacking by the VoIP Router.

Blocking Time: Enter the blocking time to block the particular IP.

2-2-1-3 IP Filtering

Use IP Filters to deny particular LAN IP addresses from accessing the Internet. You can deny specific port numbers or all ports for a specific IP address. The screen will display well-known ports that are defined. To use them, click on the edit icon. You will only need to input the LAN IP address(es) of the computer(s) that will be denied Internet access.

ADVANCED → Firewall and DMZ→ IP Filtering



IP FILTERING

The IP filter option is used to control network access based on the IP of the network device. This feature can be configured to DENY network/Internet access.

☑ Enable IP Filtering

IP	TCP / UDP	Remark

IP :

TCP / UDP : Both

Remark :

Enable IP Filtering: Check the box to deny particular LAN IP addresses from accessing the Internet.

IP: Enter the IP address that you want to deny in this filed.

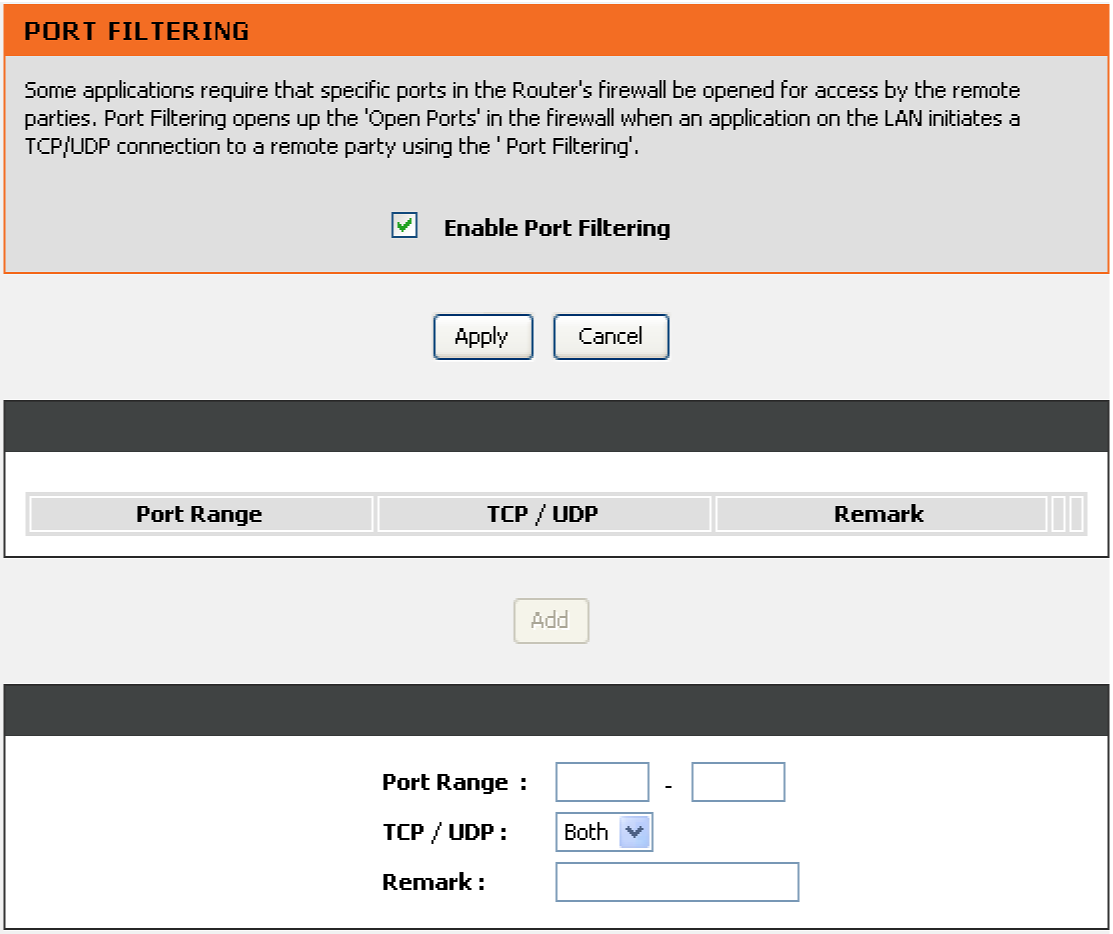
TCP/UDP: Select **TCP**, **UDP** or **Both** that will be used with the IP address that will be blocked.

Remark: Enter comments.

2-2-1-4 Port Filtering

Port filtering enables you to control all data that can be transmitted over routers. When the port used at the source end is within the defined scope, it will be filtered without transmission.

ADVANCED → Firewall and DMZ→ Port Filtering



PORT FILTERING

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Filtering opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the ' Port Filtering'.

☑ Enable Port Filtering

Port Range	TCP / UDP	Remark

Port Range : ______ - ______

TCP / UDP : Both

Remark : ______

Enable Port Filtering: This variable is to restrict certain types of data packets by port.

Port Range: Enter the port range that will be denied access to the Internet.

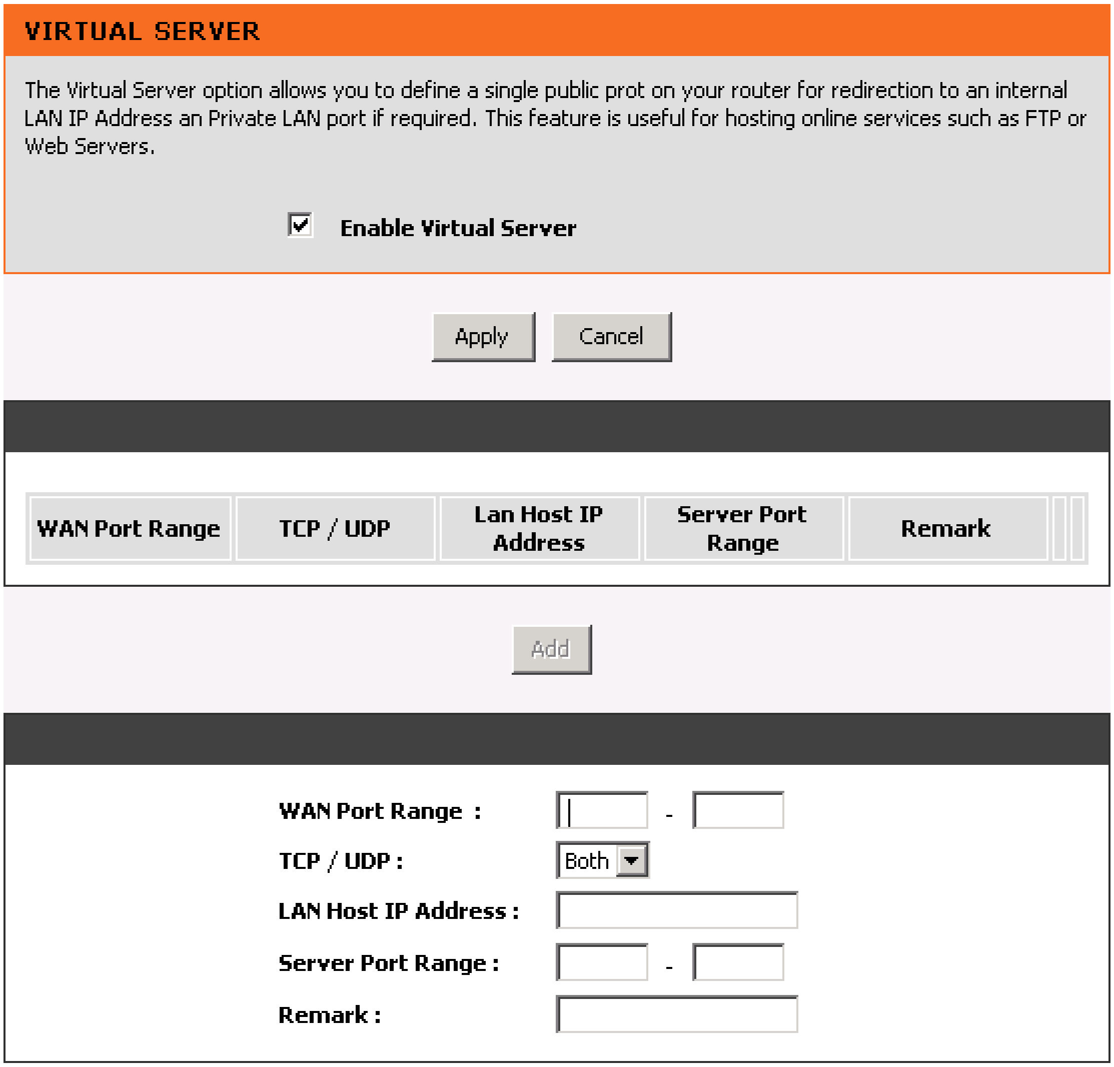
TCP/UDP: Select **TCP**, **UDP** or **Both** that will be used with the port that will be blocked.

Remark: Enter comments.

2-2-1-5 Virtual Server

Enable users on Internet to access the WWW, FTP and other services from your NAT. It is also known as port forwarding. When remote users are accessing Web or FTP servers through WAN IP address, it will be routed to the server with LAN IP address.

ADVANCED → Firewall and DMZ→ Virtual Server



VIRTUAL SERVER

The Virtual Server option allows you to define a single public prot on your router for redirection to an internal LAN IP Address an Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

☑ Enable Virtual Server

WAN Port Range	TCP / UDP	Lan Host IP Address	Server Port Range	Remark

WAN Port Range :	-
TCP / UDP :	Both
LAN Host IP Address :	
Server Port Range :	-
Remark :	

Enable Virtual Server: Check the box to enable port forwarding.

WAN Port Range: Enter the port range for the WAN side.

TCP/UDP: Select the communication protocols used by the server, **TCP**, **UDP** or **Both**.

LAN Host IP Address: Enter the IP address of the device that provides various services.

Server Port Range: Enter comments.

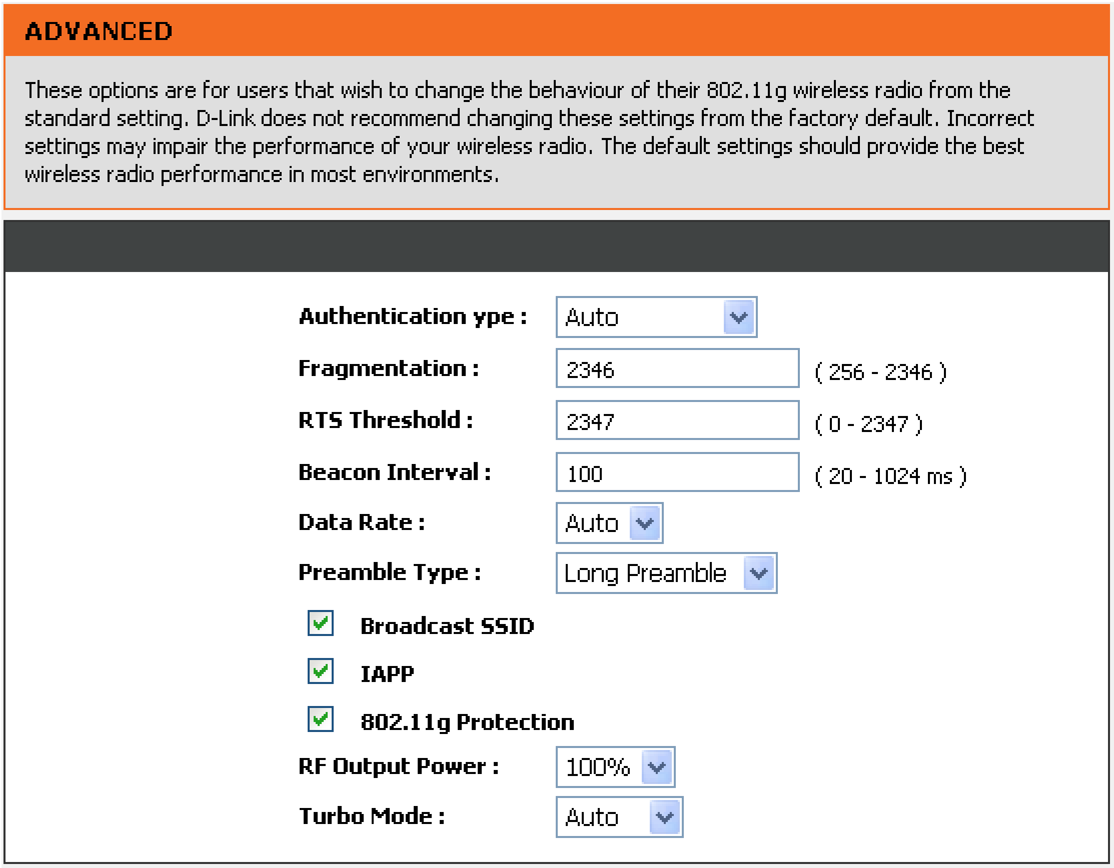
Remark: Enter comments.

2-2-2 Advanced Wireless

2-2-2-1 Advanced

This section introduces advanced configuration for the wireless access point. If you are not familiar with the following functions, keep the default parameters. In some cases, incorrect settings may reduce wireless performance.

ADVANCED -> Advanced Wireless -> Advanced



ADVANCED

These options are for users that wish to change the behaviour of their 802.11g wireless radio from the standard setting. D-Link does not recommend changing these settings from the factory default. Incorrect settings may impair the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.

Authentication ype :	Auto	
Fragmentation :	2346	(256 - 2346)
RTS Threshold :	2347	(0 - 2347)
Beacon Interval :	100	(20 - 1024 ms)
Data Rate :	Auto	
Preamble Type :	Long Preamble	

☑ Broadcast SSID

☑ IAPP

☑ 802.11g Protection

RF Output Power :	100%
Turbo Mode :	Auto

Authentication Type: Select the type of authentication.

Open System - Any wireless client can associate with the wireless access point but the client must have the same WEP key to exchange data.

Shared Key - Wireless clients must have the same WEP key to associate with wireless access point and exchange data.

Auto - Auto-detect the authentication type.

Fragmentation: A packet can be fragmented into small units to pass over a network medium that can not support the original packet size. If you encounter a busy network, a lower value of Fragment Threshold could improve performance. If the traffic flows are not very busy, a higher Fragment Threshold provides good network performance. In most case, keeping the default value=2346 is recommended.

RTS Threshold: RTS Threshold is a mechanism to implement in collision avoidance. In a large wireless network, two stations do not hear each other but can hear wireless access point. When the two send data to Access Point at the same time, it may result in data collision and a loss of messages for both wireless stations. In most case, keeping the default value=2347 is recommended.

Beacon Interval: The default value is **100**. The Beacon Interval indicates the frequency interval of target beacon transmission time which can be found in a packet body. The VoIP Router transmits the beacon packet to help a wireless client to identify the existence of nearby access point. If the beacon intervals are too long, it would be hard to access the network. If the beacon intervals are too short, the resources would be wasted.

Data Rate: IEEE802.11b supports Auto, 1, 2, 5.5, 11 Mbps signaling rate. IEEE802.11g supports Auto, 6, 9, 12, 18, 24, 36, 48, 54 Mbps signaling rate. The data rate will change automatically to get better throughput depending on range and environment of the wireless network.

Preamble Type: Preamble Type defines the length of the preamble which sends out with a packet format. Specify an appropriate preamble type for your network, if you do not know which one to select, keeping the default setting **Long Preamble** is recommended.

Broadcast SSID: Disable the SSID broadcast. This is to prevent users from seeing your wireless network.

IAPP: IAPP (Inter Access Point Protocol) provides the communication among access points in order to support mobile station roaming mechanism from one access point to another.

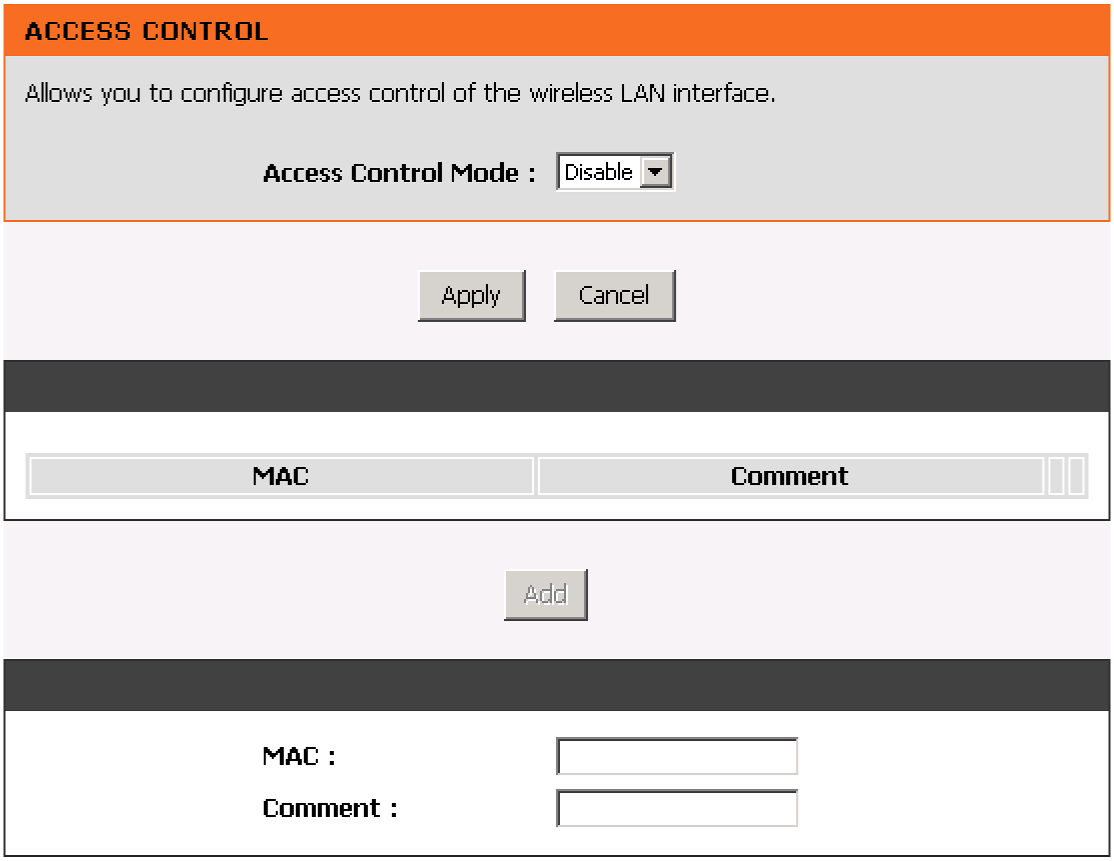
802.11g Protection: In 802.11b/g Mixed mode, it can be used for protection mechanism. The 802.11g OFDM traffic can keep the connection stable and avoid 802.11b interference. But that might cause the poor throughput.

RF Output Power: You can adjust the percentage of power 100, 50, 25, 10, 5 of your VoIP Router to change the coverage of wireless network. Keep the default value, 100% to reach full range.
Turbo Mode: The AP would identify the wireless station's chipset to improve the performance.

2-2-2-2 Access Control

The Access Control setting provides a service that you can control different access rights for different wireless clients connected to your VoIP Router. The local and remote stations are limited to access Internet through your Access Points using MAC address of wireless client. Choose the appropriate Access Control Services from Wireless Access Control Mode option.

ADVANCED -> Advanced Wireless -> Access Control



ACCESS CONTROL

Allows you to configure access control of the wireless LAN interface.

Access Control Mode : Disable

MAC	Comment

MAC :

Comment :

Access Control Mode--

Disable: The VoIP Router does not response to any access rules. You are not allowed to make configuration changes on this page.

Allow: When **Allow Listed** is enabled, only those wireless clients whose MAC addresses are in the Access Control List have rights to connect to your Access Point.

Deny: When **Deny Listed** is enabled, only those wireless clients whose MAC addresses are in the Access Control List will be blocked and restricted access to your Access Point.

MAC Address: Specify the MAC address which you want to allow/deny access your Access Point.

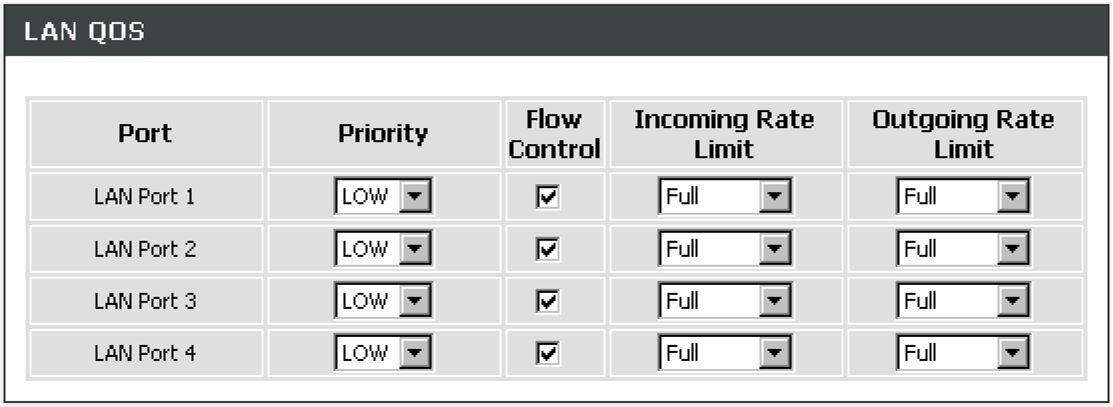
Comment: The space is reserved for comment or notation.

2-2-3 Advanced Network

2-2-3-1 QOS

LAN QoS

ADVANCED → Advanced Network → QoS



LAN QOS

Port	Priority	Flow Control	Incoming Rate Limit	Outgoing Rate Limit
LAN Port 1	LOW	☑	Full	Full
LAN Port 2	LOW	☑	Full	Full
LAN Port 3	LOW	☑	Full	Full
LAN Port 4	LOW	☑	Full	Full

Enable LAN QoS: Check the box to enable LAN QoS by Hardware.

Priority: Use the drop-down menu to select **Low** or **High** for the VoIP Router to deliver the packets from LAN interface when the packets arrive at the same time.

Flow Control: Check the box to limit incoming and outgoing rate.

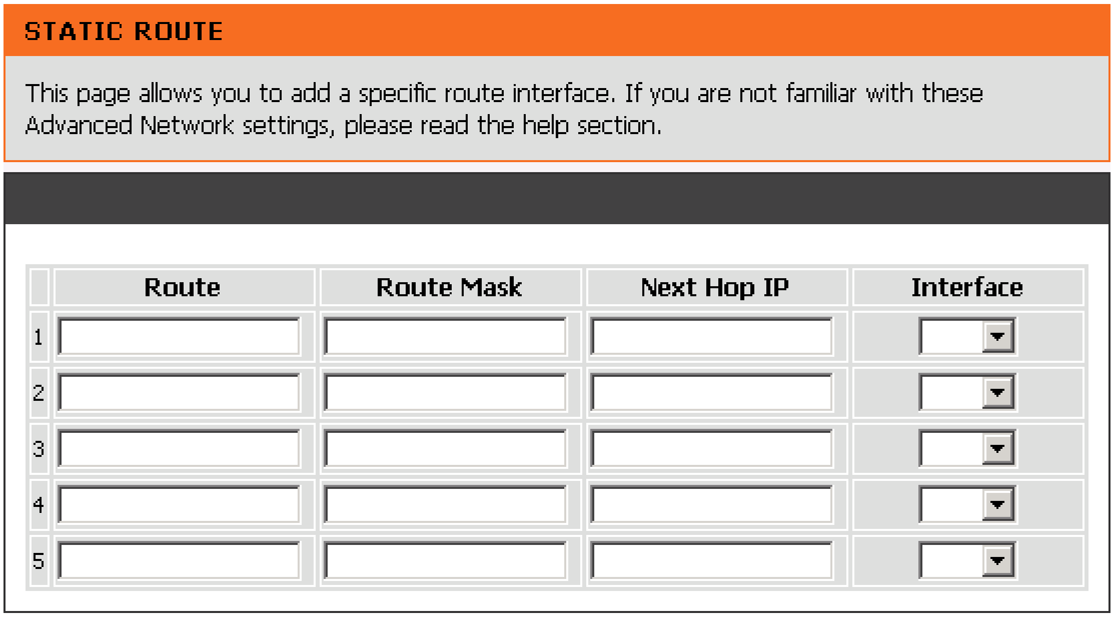
Incoming Rate Limit: Use the drop-down menu to select the proper rate limit for the specific LAN port. The flow is from LAN to WAN, and the rate limit can not exceed the real upstream bandwidth.

Outgoing Rate Limit: Use the drop-down menu to select the proper rate limit for the specific LAN port. The flow is from WAN to LAN, and the rate limit can not exceed the real downstream bandwidth.

2-2-3-2 Static Route

Build static routes within an internal network. These routes will not apply to the Internet.

ADVANCED → Advanced Network → Static Route



STATIC ROUTE

This page allows you to add a specific route interface. If you are not familiar with these Advanced Network settings, please read the help section.

	Route	Route Mask	Next Hop IP	Interface
1				
2				
3				
4				
5				

Route: Destination network of the route.

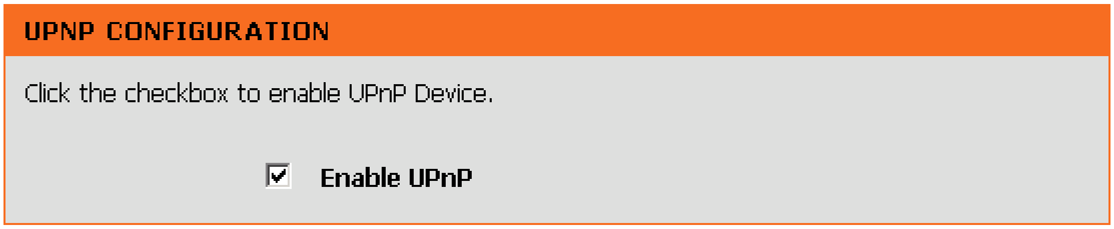
Route Mask: Subnet mask to apply on destination network.

Next Hop IP: The next hop IP address to the specified network.

Interface: The interface attached to this route.

2-2-3-3 UPnP

ADVANCED → Advanced Network → UPnP



UPNP CONFIGURATION

Click the checkbox to enable UPnP Device.

☑ Enable UPnP

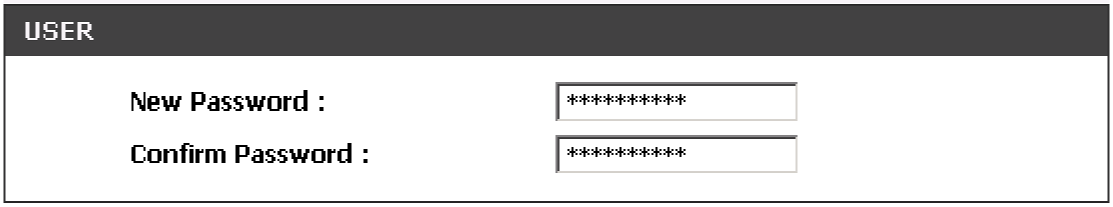
Enable UPnP: Check the box to enable the VoIP Router's IP traffic to pass through an Internet sharing device. This function only works when the Internet sharing device supports UPnP and has it enabled.

Note: The "Status → Current Status" page will show the status of UPnP.

2-3 MAINTENANCE

2-3-1 Device Management

MAINTENANCE → Device Management



USER

New Password : **********

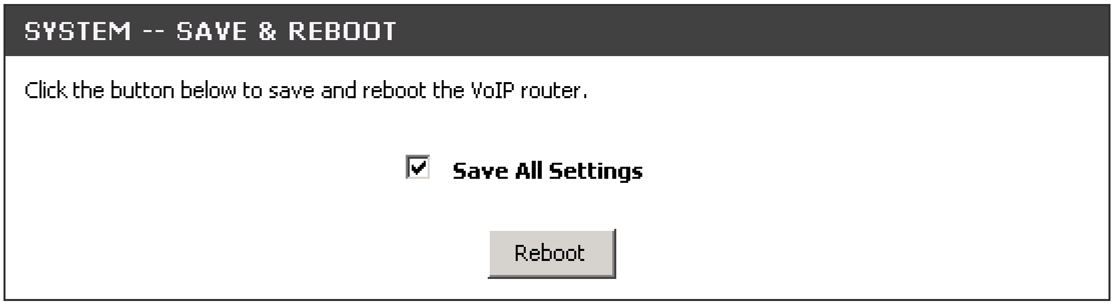
Confirm Password : **********

Password: By default there is no password configured. It is highly recommended that you create a password to keep your router secure.

2-3-2 Backup and Restore

Save and Reboot

MAINTENANCE → Backup and Restore



SYSTEM -- SAVE & REBOOT

Click the button below to save and reboot the VoIP router.

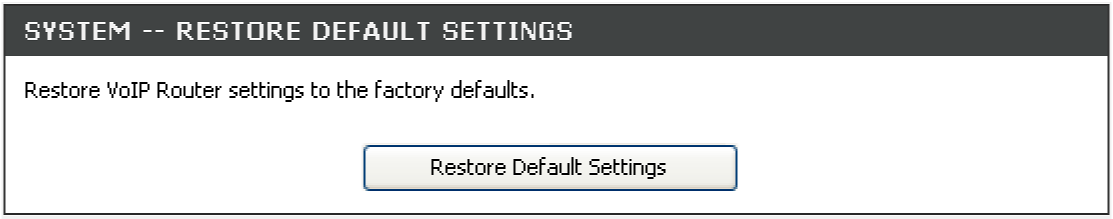
☑ Save All Settings

Save All Settings: Click the **Save All Settings** check box and reboot the system after completing changes. The new settings will take effect after the VoIP Router is restarted.

Restart: Click the **Reboot** button to reboot the system.

Restore Default Settings

MAINTENANCE → Backup and Restore



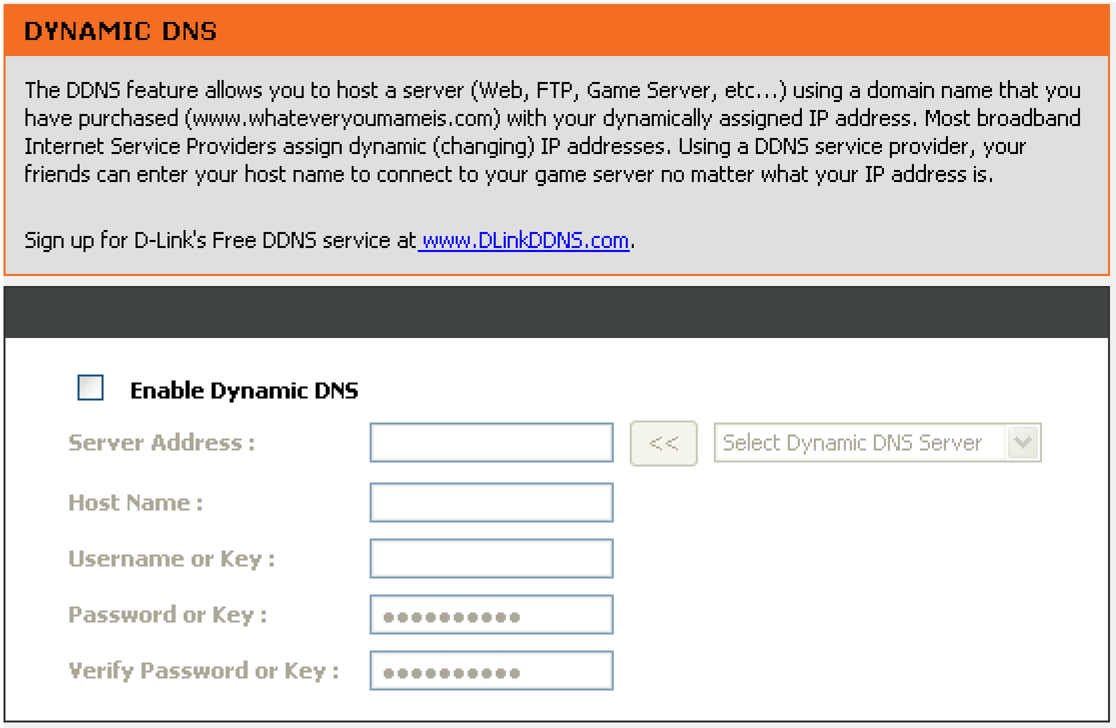
SYSTEM -- RESTORE DEFAULT SETTINGS

Restore VoIP Router settings to the factory defaults.

Select **Restore Default Settings** to reset the VoIP Router's settings back to the factory default settings.

2-3-3 Dynamic DNS

ADVANCED → Dynamic DNS



DYNAMIC DNS

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryoumameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.

Sign up for D-Link's Free DDNS service at www.DLinkDDNS.com.

□ Enable Dynamic DNS

Server Address : [ ] << Select Dynamic DNS Server

Host Name :

Username or Key :

Password or Key : ●●●●●●●●●●

Verify Password or Key : ●●●●●●●●●●

Enable Dynamic DNS: Check the box to enable DDNS function. It is only necessary when the VoIP Router is set up behind an Internet sharing device that uses a dynamic IP address and does not support DDNS.

Server address: Select a DDNS service from the drop and down arrow.

Hostname: Enter the URL of the system (or NAT) – applied from domain name registration providers (e.g. www.dyndns.org).

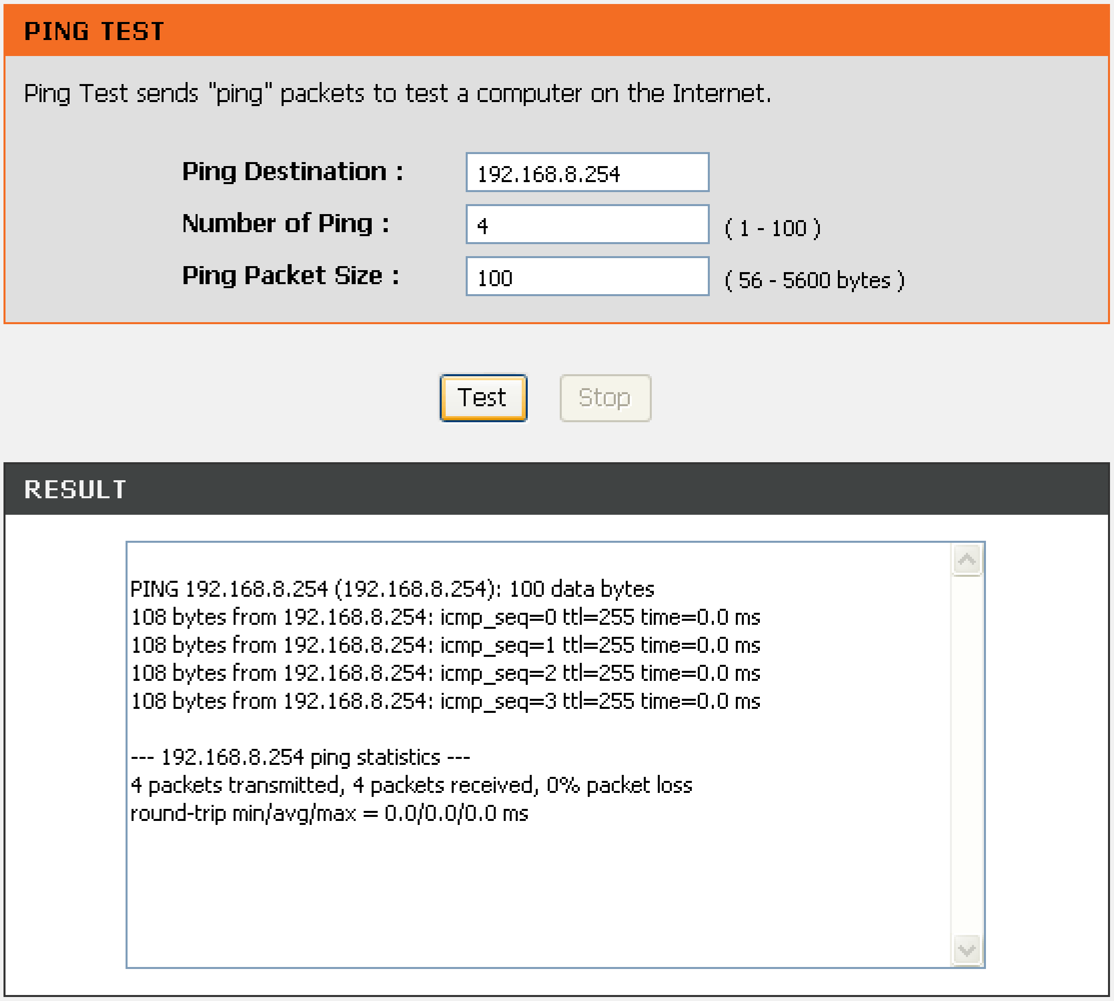
Username or Key/Password or Key: Enter the Login ID and password used to log-in to the DDNS server.

Note: If the VoIP Router is set up under NAT, then enter the hostname in the NAT IP/Domain that is the same as the Hostname of the DDNS.

2-3-4 Diagnostics

Use “Ping” to verify if a remote peer is reachable. Enter a remote IP address and click “Test” to ping the remote host. The result would be shown on **Result** Table

MAINTENANCE → Diagnostics



PING TEST

Ping Test sends "ping" packets to test a computer on the Internet.

Ping Destination :	192.168.8.254	
Number of Ping :	4	(1 - 100)
Ping Packet Size :	100	(56 - 5600 bytes)

RESULT

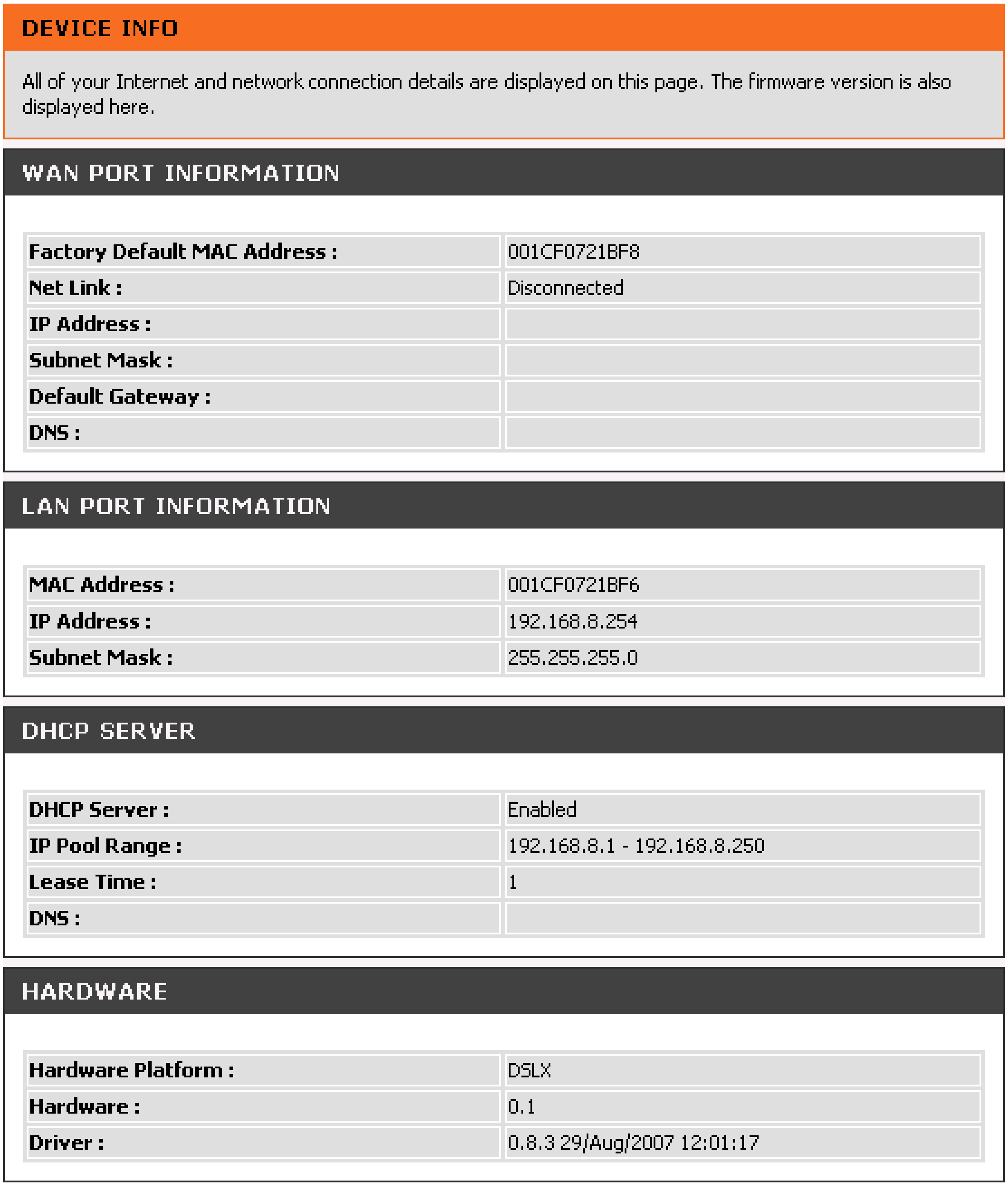
```
PING 192.168.8.254 (192.168.8.254): 100 data bytes
108 bytes from 192.168.8.254: icmp_seq=0 ttl=255 time=0.0 ms
108 bytes from 192.168.8.254: icmp_seq=1 ttl=255 time=0.0 ms
108 bytes from 192.168.8.254: icmp_seq=2 ttl=255 time=0.0 ms
108 bytes from 192.168.8.254: icmp_seq=3 ttl=255 time=0.0 ms

--- 192.168.8.254 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

2-4 STATUS

2-4-1 Device Info

STATUS → Device Info



DEVICE INFO

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

WAN PORT INFORMATION

Factory Default MAC Address :	001CF0721BF8
Net Link :	Disconnected
IP Address :	
Subnet Mask :	
Default Gateway :	
DNS :	

LAN PORT INFORMATION

MAC Address :	001CF0721BF6
IP Address :	192.168.8.254
Subnet Mask :	255.255.255.0

DHCP SERVER

DHCP Server :	Enabled
IP Pool Range :	192.168.8.1 - 192.168.8.250
Lease Time :	1
DNS :	

HARDWARE

Hardware Platform :	DSLX
Hardware :	0.1
Driver :	0.8.3 29/Aug/2007 12:01:17

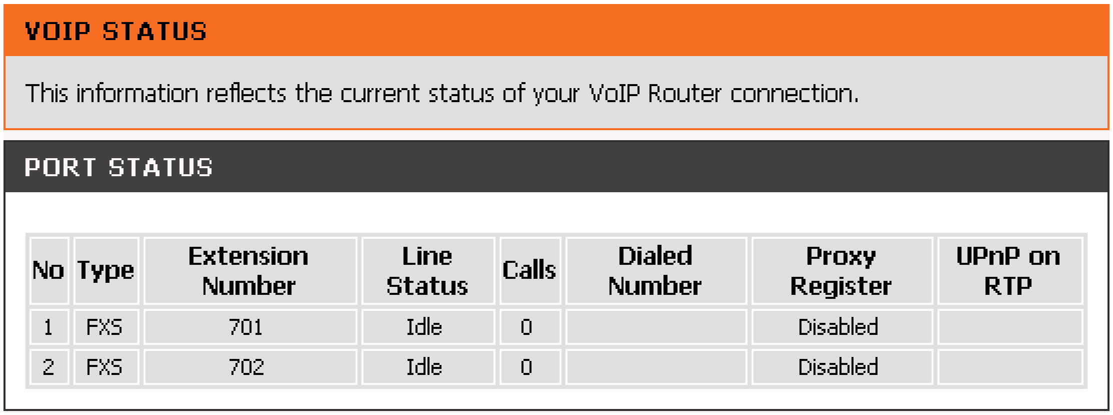
For WAN Port Information, it shows IP address, subnet mask, default gateway and DNS server. If you use PPPoE to obtain IP, you will know if the IP is obtained through this method. If IP address, subnet mask, default gateway is blank, it means that the VoIP Router does not obtain IP.

For LAN Port Information, it shows LAN port IP, subnet mask, and the status of DHCP server.

For Hardware, it shows the hardware platform and driver version.

2-4-2 VoIP Status

STATUS → VoIP Status



VOIP STATUS

This information reflects the current status of your VoIP Router connection.

PORT STATUS

No	Type	Extension Number	Line Status	Calls	Dialed Number	Proxy Register	UPnP on RTP
1	FXS	701	Idle	0		Disabled	
2	FXS	702	Idle	0		Disabled	

For Port Status, it includes if each port registers to Proxy successfully, the last dialed number, how many calls each port has made since the VoIP Router is start, etc.

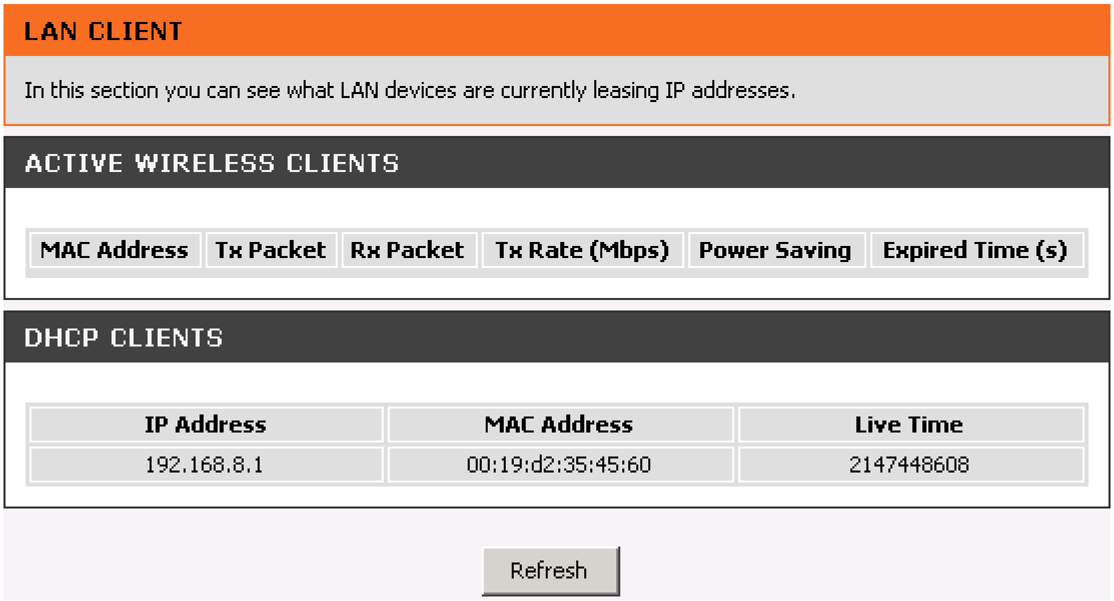
For Server Registration Status, it shows the registration status of DDNS, Phone Book Manager, STUN and UPnP.

2-4-3 LAN Client

The **Active Wireless Clients** table displayed the identification and transmission status of active wireless clients on wireless LAN interface.

The **DHCP Clients** table displayed LAN device that has already been assigned an address from DVG-G5402SP. You can check if the DHCP client has obtain an IP address.

STATUS → LAN Client



LAN CLIENT

In this section you can see what LAN devices are currently leasing IP addresses.

ACTIVE WIRELESS CLIENTS

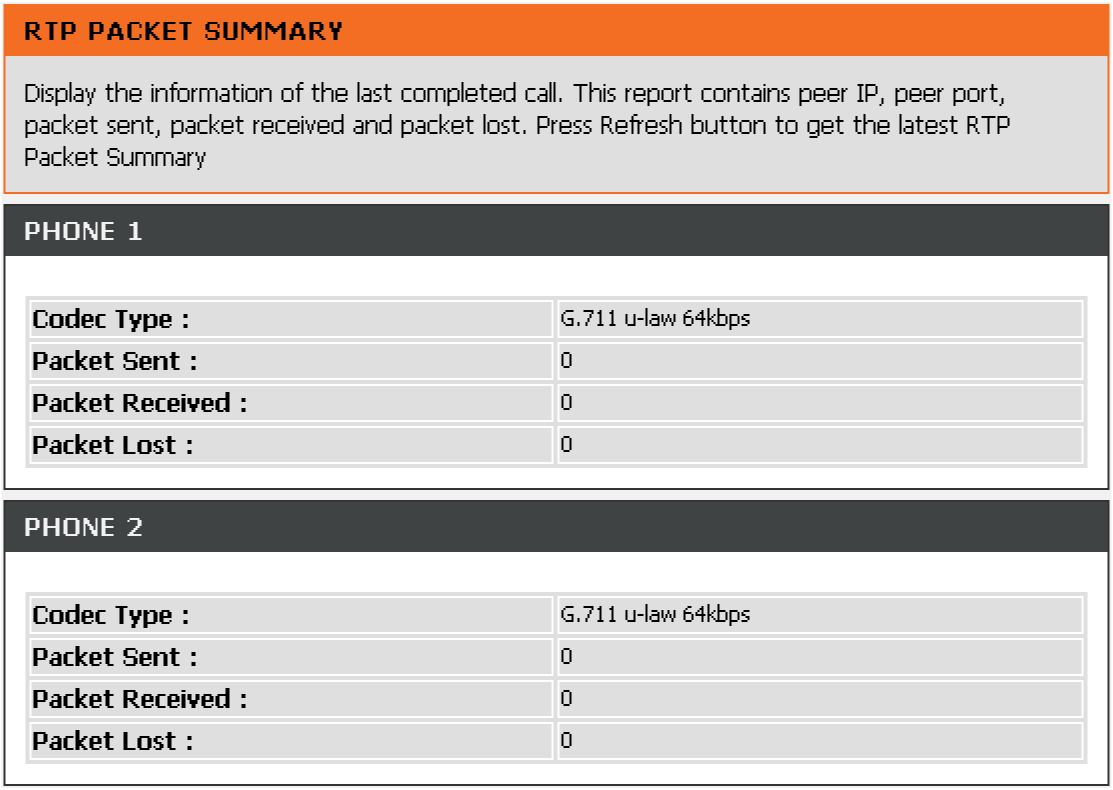
MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)

DHCP CLIENTS

IP Address	MAC Address	Live Time
192.168.8.1	00:19:d2:35:45:60	2147448608

2-4-4 Statistics

STATUS → Statistics



RTP PACKET SUMMARY

Display the information of the last completed call. This report contains peer IP, peer port, packet sent, packet received and packet lost. Press Refresh button to get the latest RTP Packet Summary

PHONE 1

Codec Type :	G.711 u-law 64kbps
Packet Sent :	0
Packet Received :	0
Packet Lost :	0

PHONE 2

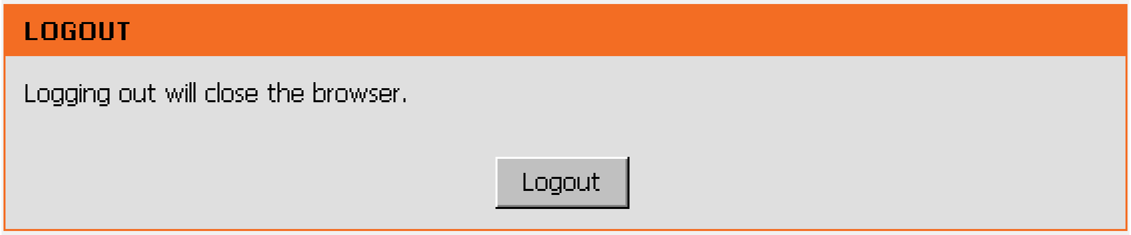
Codec Type :	G.711 u-law 64kbps
Packet Sent :	0
Packet Received :	0
Packet Lost :	0

Display the information of the last call made. Press **Refresh** button to get the latest RTP Packet Summary.

2-4-5 Logout

If setting or parameter has been changed, remember to save the changes before you logout the configuration menu.

Logout



LOGOUT

Logging out will close the browser.

Appendix

Product Features

WAN

- One 10/100Mbps auto-negotiation, auto-crossover RJ-45 Ethernet port
- Support static IP, PPPoE, BigPond Cable and DHCP address assignment and dynamic DNS (DDNS)
- QoS: IP TOS (Type of Services) and DiffServ (Differentiated Services) for both SIP signaling and RTP
- NAT Traversal : Port Forwarding, STUN, UPnP and Outbound Proxy
- NTP: (Network Time Protocol RFC 1305), Accepts up to 3 Time Server
- Time Zone Support
- MAC Address Clone
- RTP Packet Summary : packet sent, packet received, packet loss for voice quality analysis

LAN

- Four 10/100Mbps auto-negotiation, auto-crossover RJ 45 Ethernet ports
- Supports router and bridge mode (NAT mode and Non-NAT mode)
- DHCP server

Voice Features

- SIP (RFC3261) compatible
- Voice codecs : G.711 a /ulaw, G.726, G.729A, G.723.1
- CNG (Comfort Noise Generation)
- VAD (Voice Activity Detection)
- G.165/G.168 echo cancellation
- Adjustable Jitter Buffer and programmable Gain Control
- In-Band DTMF, Out-Of-Band DTMF relay (RFC2833, SIP INFO)
- Multiple SIP Proxy server entries with failover mechanism
- Polarity reversal detection (FXO/PSTN) and generation (FXS)
- T.30 (G.III) / Real time T.38 / Secured T.38 FAX relay
- DTMF, FSK (Bellcore & ETSI) Caller ID detection and generation.
- Support Caller ID Restriction (CLIR)
- Digit Map for dial plan
- Speed Dial
- Local phone book for peer-to-peer calling
- E.164 Numbering & ENUM support
- Hot-Line, Warm-Line support
- Single Number / Account (reprehensive number) for multiple ports
- Recordable greeting message
- Call features:
  - Call Hold, Call Waiting, Call Pickup
  - Call Forward - Unconditional, Busy, No Answer
  - Call Transfer - Unattended, Attended
  - Three Way Calling (Media Server required)
- Analogue interface
  - Connector : RJ-11
  - Signaling protocol : Loop Start

Configuration & Maintenance

- Configuration methods:
  - Web
  - IVR
  - Telnet
- Status reports:
  - Port status
  - Registration status
  - Ping tests
  - STUN/UPnP status
  - Hardware / software information
- Firmware Upgrade through TFTP, FTP and proprietary image server
- Configuration Backup/Restore
- Reset button (with restore factory default function)
- Front Panel LED : voice ports, WAN, LAN1~4, Run, Power, Alarm
- Optional Auto Provisioning Server (APS) for mass