

D-Link DVG-G5402SP

VoIP Wireless Router

User Manual



D-Link®

Building Networks for People



RECYCLABLE

2007/10/03

Ver. 1.00

© 2007 D-Link Corporation. All rights reserved.

Reproduction in any manner whatsoever without the written permission of D-Link Corporation is strictly forbidden.

Trademarks used in this text: *D-Link* and the *D-Link* logo are trademarks of D-Link Corporation/D-Link Systems Inc.; Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. D-Link Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

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	4
1-1 Product Overview	4
1-2 Hardware Description	5
2. Getting Started	7
3. VoIP Router Web Configuration (continued)	11
3-1 SETUP	14
3-1-1 Internet Setup	14
3-1-2 VoIP Setup	18
3-1-3 Wireless Setup	25
3-1-4 LAN Setup	29
3-1-5 Time and Date	32
3-2 ADVANCED	33
3-2-1 VoIP	33
3-2-2 Access Control	56
3-2-3 Firewall and DMZ	57
3-2-4 Advanced Wireless	62
3-2-5 Advanced Network	66
3-3 MAINTENANCE	71
3-3-1 Device Management	71
3-3-2 Backup and Restore	72
3-3-3 Firmware Update	74
3-3-4 Dynamic DNS	75
3-3-5 Log Settings	76
3-3-6 Diagnostics	77
3-3-7 Provision	78
3-3-8 CDR	80
3-4 STATUS	81
3-4-1 Device Info	81
3-4-2 VoIP Status	82
3-4-3 LAN Client	83
3-4-4 Statistics	84
3-4-5 Logout	84
4. Configuring the VoIP Router through IVR	85
4-1 IVR (Interactive Voice Response)	85
4-1-1 IVR Functions Table:	87
4-2 IP Configuration Settings—Set the IP Configuration of the WAN Port	88
4-2-1 PPPoE Character Conversion Table:	90
5. Dialing Principles	91
5-1 Dialing Options	91
5-2 Dialed Number Processing Flow	91
Appendix	93
Product Features	93

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.

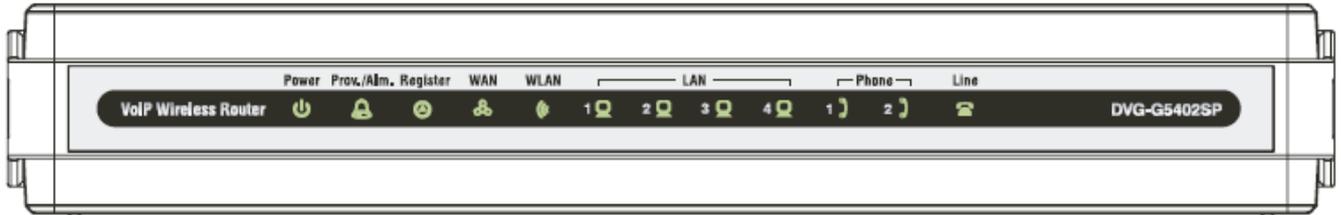
The DVG-G5402SP can be seamlessly integrated into an existing network by connecting to a phone set and fax machine. With only a broadband connection such as an ADSL bridge/router, a Cable Modem or a leased-line router, the VoIP Router allows you to use voice and fax services over IP in order to reduce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

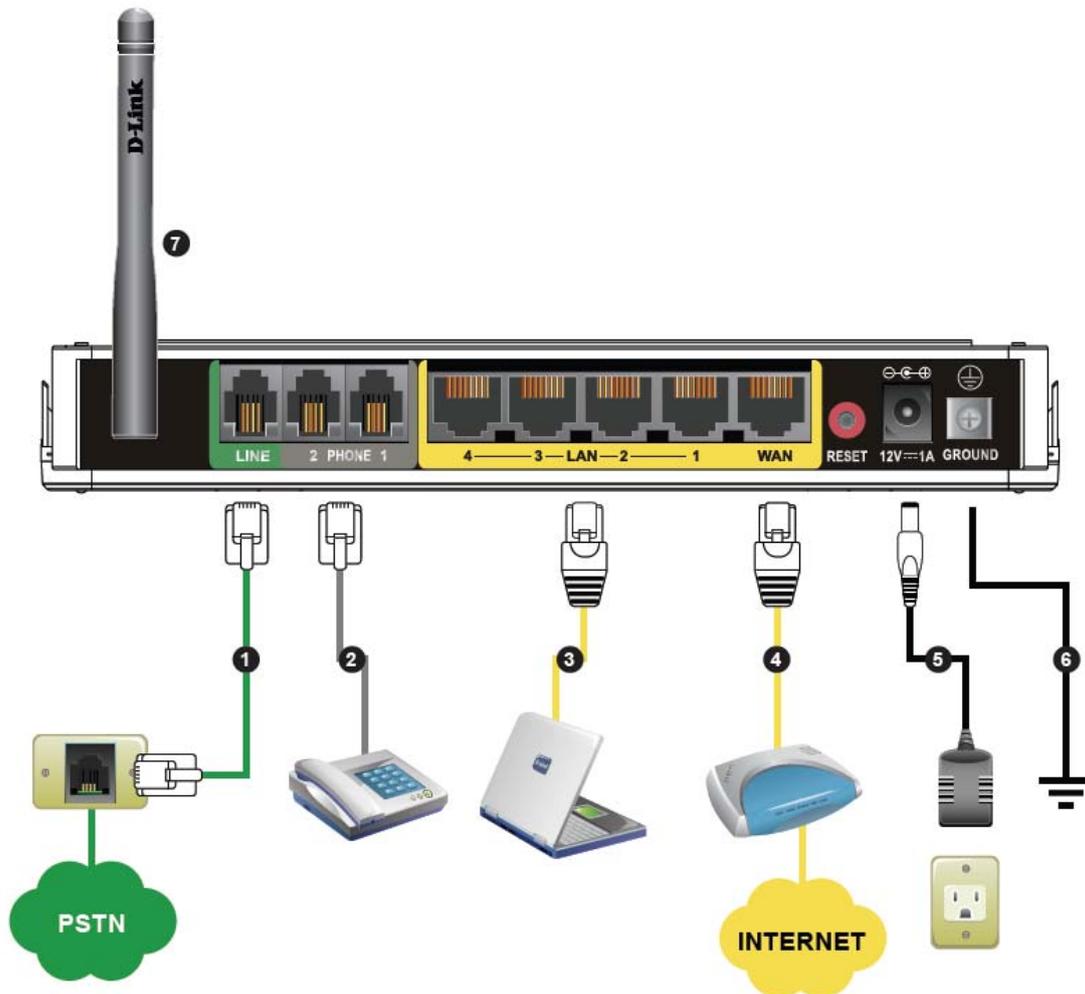
WLAN: A steady light indicates a wireless connection. A blinking light indicates that the VoIP Router is receiving/transmitting from/to the wireless network.

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.

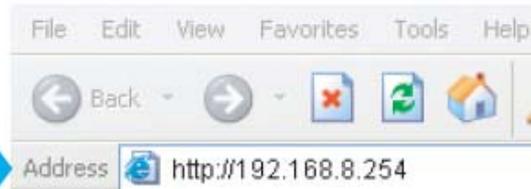
Use Reset Button to restore factory default settings:

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

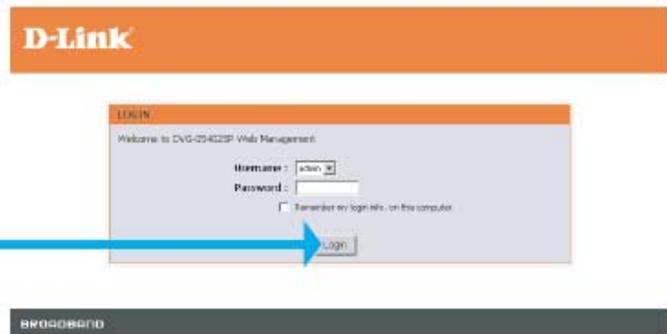
2. Getting Started

To access the web-based configuration utility, open a web browser such as Internet Explorer and enter the IP address of the DVG-G5402SP.

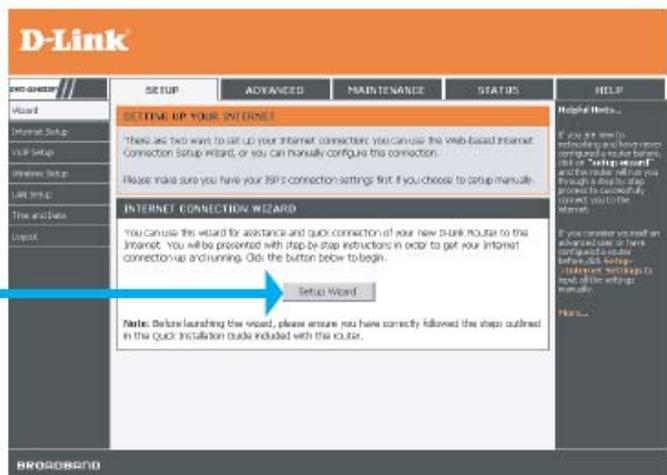
Open your Web browser and type <http://192.168.8.254> into the URL address box. Press the Enter or Return Key.



Click **Login** to enter Web Site. The factory default settings for Login ID is "admin" and without **Password**.



Click **Setup Wizard**.



Click **Next**.



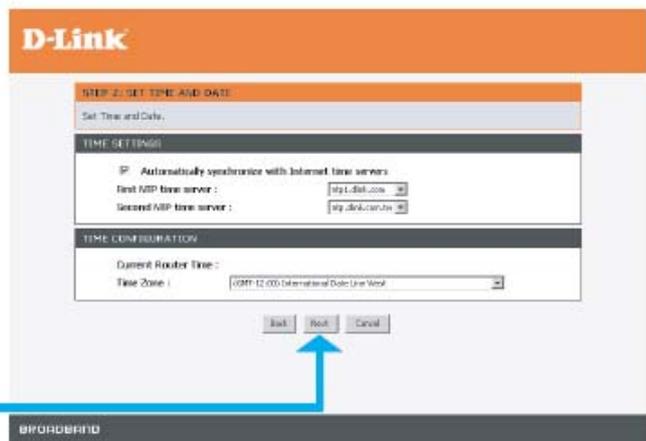
The username of **ADMIN** and **USER** have been defined and locked by default. It is highly recommended to create a login password to keep your router secure.

Click **Next**.



Enter a NTP server or use the default server.

Click **Next**.



Select your Internet connection type:
DHCP – Most Cable ISPs or if you are connecting the DVG-5402SP behind a router.
Static IP – Select if your ISP supplied you with your IP settings.
PPPoE – Most DSL ISPs.
PPTP – Select if required by your ISP.
BigPond – For Australia only.

Select **Manual** to manually enter IP address of DNS or select **Auto** if DNS is assigned by ISP.

Click **Next**.

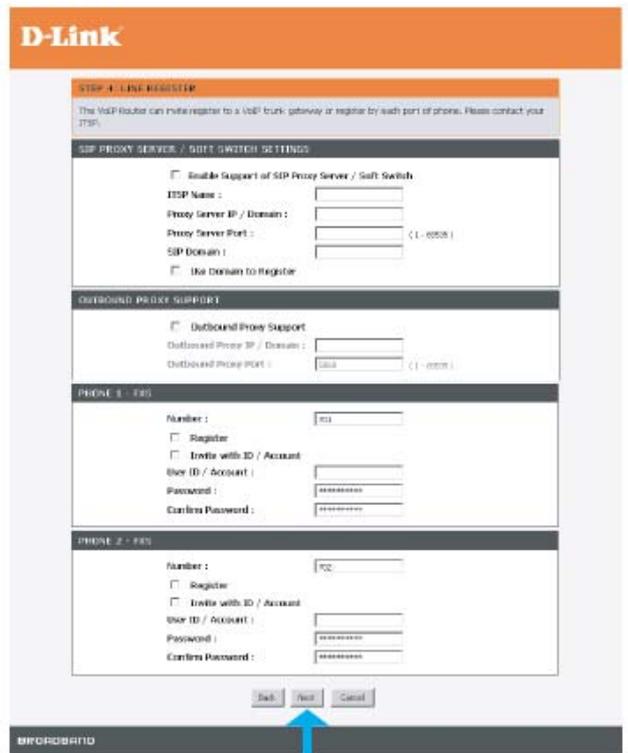


Register to the SIP Proxy Server by clicking **Enable support of SIP Proxy Server**. Enter **Proxy Server IP/Domain** and **Port**.

The **Outbound Proxy Support** is optional. To register, please click on the **Outbound Proxy Support** check box and enter **Outbound Proxy IP/Domain** and **Port** in it.

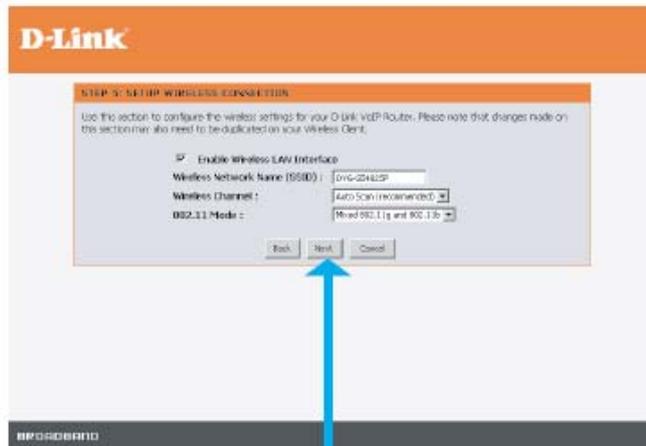
Registration by phone line: enter **Number**, **User ID/Account** and **Password** supplied by your ITSP. Click on the **Register** check box to register to Proxy Server.

Click **Next**.



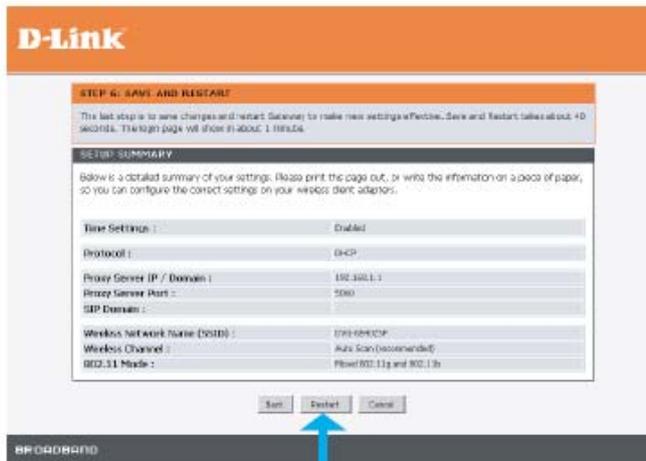
Click on the **Enable wireless LAN interface** check box to build a wireless network. Enter the SSID to name your wireless network. All devices must have the same SSID to communicate on the wireless network. Select a wireless channel. For best results, use 1, 6 or 11. Select the 802.11 Mode of your network which can work in different speed of wireless connection.

Click **Next**.



Setup is finished. Check the summary of your settings. To make new settings effective, you must click on the **Restart** button to reboot the DVG-G5402SP.

Click **Restart**.



3. 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.

<input checked="" type="radio"/> DHCP <input type="radio"/> Static IP <input type="radio"/> PPPoE <input type="radio"/> PPTP <input type="radio"/> BigPond Cable	
DHCP	
Hostname :	<input type="text"/>
MTU :	<input type="text" value="1500"/>
DNS	
Domain Name Server Assignment :	<input type="radio"/> Auto <input checked="" type="radio"/> Manual
Domain Name Server (Primary) IP :	<input type="text" value="168.95.1.1"/>
Domain Name Server (Secondary) IP :	<input type="text"/>
MAC	
Factory Default MAC Address :	00E04C8186D1 <input type="button" value="Restore"/>
Your MAC Address :	001122334455 <input type="button" value="Clone"/>
Current MAC Address :	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
New settings will take effect after Save & Restart .	

Situation 2: (example: VoIP Proxy Server)



Setup Hint:

1. Click "Edit" to start configuration.

2. Click "Apply" after settings.
3. Go to "MAINTAINACE"-> "Backup and Restore" save settings and reboot the system.

VOIP SETTINGS

The device can set up multiple SIP proxy servers for load balancing on the same ITSP to get the better response, and high availability.

PROXY SERVER

	Proxy Status	ITSP Name	Proxy Server IP	Proxy Server Port	
1	Disable		192.168.1.1	5060	
2	Disable		192.168.1.1	5060	Edit 
3	Disable		192.168.1.1	5060	

Situation 3: (example: Enable IP Filtering)

i 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

4

IP	TCP / UDP	Remark		
192.168.8.1	Both			

2

IP :

TCP / UDP :

Remark :

3

New settings will take effect after [Save & Restart](#).

3-1 SETUP

3-1-1 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)
4. PPTP
5. BigPond (for Australia only)

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, BigPond. If you are unsure of your connection method, please contact your Internet Service Provider.

- DHCP**
- Static IP**
- PPPoE**
- PPTP**
- BigPond Cable**

SETUP → Internet Setup

DHCP

Hostname :	
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 :	<input type="text"/>
PPPoE Password :	<input type="password" value="*****"/>
Confirm Password :	<input type="password" value="*****"/>
MTU :	<input type="text" value="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

PPTP	
IP Address :	<input type="text"/>
Subnet Mask :	<input type="text"/>
Default Gateway IP :	<input type="text"/> (Optional)
PPTP Server :	<input type="text"/>
PPTP ID :	<input type="text"/>
PPPoE Password :	<input type="password" value="*****"/>
Confirm Password :	<input type="password" value="*****"/>
MTU :	<input type="text" value="1452"/>

PPTP: Point-to-Point Tunneling Protocol (PPTP) is a WAN connection. Enter the **IP Address**, **Subnet mask**, **PPTP Server**, **PPTP ID** and **Password**.

SETUP → Internet Setup

BIGPOND CABLE	
User Name :	<input type="text"/>
BigPond Cable Password :	<input type="password" value="*****"/>
Confirm Password :	<input type="password" value="*****"/>
Login Server :	<input type="text"/>
MTU :	<input type="text" value="1500"/>

BigPond: Dynamic IP Address for BigPond is a WAN connection used in Australia. Enter the username and password for the BigPond account and the login server if required.

SETUP → Internet Setup

DNS	
Domain Name Server Assignment :	<input type="radio"/> Auto <input checked="" type="radio"/> Manual
Domain Name Server (Primary) IP :	<input type="text" value="168.95.1.1"/>
Domain Name Server (Secondary) IP :	<input type="text"/>

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.

SETUP → Internet Setup

MAC

Factory Default MAC Address :	00:17:9A:98:AF:6C	<input type="button" value="Restore"/>
Your MAC Address :	00:0A:79:60:17:28	<input type="button" value="Clone"/>
Current MAC Address :	<input style="width: 100px;" type="text"/>	(xx:xx:xx:xx:xx:xx)

Factory Default MAC Address: The original MAC address of the VoIP Router.

Your MAC Address: It is left blank as you log-in via the WAN port.

Current MAC Address: It shows the current MAC Address if you ever used the different MAC address from Factory Default MAC Address. You can click **Clone** to automatically copy the MAC address of the Ethernet Card installed in the computer used to configure the device.

Note: This is only necessary to fill the field if required by your ISP.

3-1-2 VoIP Setup

In this section, it supports registration to multiple Proxy Servers which is allowed to choose ITSP by user manually. If any registration problem occurs, please consult your VoIP Service Provider.

SETUP → VoIP Setup

Click Edit icon to modify the settings.

The same configurations and applications apply to three Proxy Servers. Select one of three Proxy Servers for SIP configuration.

VOIP SETTINGS

The device can set up multiple SIP proxy servers for load balancing on the same ITSP to get the better response, and high availability.

PROXY SERVER

	Proxy Status	ITSP Name	Proxy Server IP	Proxy Server Port	
1	Disable		192.168.1.1	5060	
2	Disable		192.168.1.1	5060	
3	Disable		192.168.1.1	5060	

SETUP → VoIP Setup

Enable Support of SIP Proxy Server / Soft Switch

Enable Support of SIP Proxy Server / Soft Switch

ITSP Name :

Enable Support of SIP Proxy Server / Soft Switch: Check the box to register the VoIP Router with SIP proxy server or soft switch.

ITSP Name: Enter the name of ITSP.

SETUP → VoIP Setup

FXS Representative Number registers to Proxy:

FXS REPRESENTATIVE NUMBER

Number :

Register

User ID / Account :

Password :

Confirm Password :

Number: Enter the representative number for Line 1 and Line 2. If the VoIP Router is configured to register with SIP proxy server, Line 1 and Line 2 are using this number to call through SIP proxy server. It is the Caller ID for the called party when you make a VoIP call. If you register the VoIP Router to a SIP proxy server, then it should be the number that provided by SIP proxy server.

Register: Check the box to register with SIP proxy server.

User ID/Account: User ID/Account are usually the same as Number from most SIP proxy servers.

Password: Enter password and re-enter to confirm.

Note: Please ensure if your VoIP Service Provider allows one account for multi-port using.

SETUP → VoIP Setup

Each line registers to Proxy independently:

PHONE 1 - FXS	
Number :	<input type="text" value="701"/>
<input type="checkbox"/> Register	
<input type="checkbox"/> Invite with ID / Account	
User ID / Account :	<input type="text"/>
Password :	<input type="text" value="*****"/>
Confirm Password :	<input type="text" value="*****"/>
PHONE 2 - FXS	
Number :	<input type="text" value="702"/>
<input type="checkbox"/> Register	
<input type="checkbox"/> Invite with ID / Account	
User ID / Account :	<input type="text"/>
Password :	<input type="text" value="*****"/>
Confirm Password :	<input type="text" value="*****"/>

Number: Enter the number, text or number and text in this field. It is the Caller ID for the called party when you make a VoIP call. If you register the VoIP Router to a SIP proxy server, then it should be the number that provided by SIP proxy server. Number and User ID/Account are usually the same from most SIP proxy servers. Each line has a number. And the number of each line is not reiteration.

Register: Check the box to register with SIP proxy server.

Invite with ID / Account: Check the box to call through SIP proxy server without registration. It is always ticked when Register is also ticked. Most VoIP Service Providers will interdict the connection without registration.

User ID/Account: User ID/Account are usually the same as Number from most SIP proxy servers.

Password: Enter password and re-enter to confirm.

SETUP → VoIP Setup

Proxy Server IP / Domain :	<input type="text" value="192.168.1.1"/>	
Proxy Server Port :	<input type="text" value="5060"/>	(1 - 65535)
Proxy Server Realm :	<input type="text"/>	
TTL (Registration interval) :	<input type="text" value="600"/>	(10 - 7200 s)
SIP Domain :	<input type="text"/>	
<input type="checkbox"/> Use Domain to Register		
Bind Proxy Interval for NAT :	<input type="text" value="0"/>	(0 - 180 s)
<input type="checkbox"/> Initial Unregister		

Proxy Server IP/Domain: Enter the IP address or URL (Uniform Resource Locator) of SIP proxy server or soft switch.

Proxy Server Port: Enter the SIP proxy server's listening port for the SIP in this field. Leave this field to the default if your VoIP Service Provider did not give you a server port number for SIP.

Proxy Server Realm: Enter the realm for SIP proxy server. It is used for authentication in a SIP server. In most cases, the VoIP Router can automatically detect your SIP server realm. So you can leave this option blank. However, if your SIP server requires you to use a specific realm you can manually enter it in.

TTL (Registration interval) [10-7200 s]: Enter the desired time interval at which the VoIP Router will report to your SIP proxy server.

SIP Domain: Enter the SIP domain provided by your VoIP Service Provider. (Note some SIP proxy servers might not require this.) If you enable "Uses Domain to Register", the VoIP Router will register to the SIP proxy server with the domain name you filled in. Otherwise, the VoIP Router will register to a SIP proxy server with the IP it resolves.

Use Domain to Register: Check the box to use Domain to register with SIP proxy server. The VoIP Router is registered to the SIP proxy server with IP address if un-ticked.

Note: Proxy Server Realm, SIP Domain and Use Domain to Register are the parameters provided by VoIP Service Provider. If you fail to make a call, please contact your VoIP Service Provider.

Bind Proxy Interval for NAT: Check the box to keep the binding exist by sending packets when the VoIP Router is behind a NAT and SIP proxy server is not able to keep the binding.

Initial Unregister: Check the box to send an unregistered message initially by the VoIP Router and then it will perform a general register process.

SETUP → VoIP Setup

Outbound Proxy Support

Outbound Proxy IP / Domain :

Outbound Proxy Port : (1 - 65535)

Outbound Proxy Support: Check the box to send all SIP packets to the destined outbound proxy server. An outbound proxy server handles SIP call signaling as a standard SIP proxy server would do. Further, it receives and transmits phone conversation traffic (media) between two communication parties. This option tells the VoIP Router to send and receive all SIP packets to the destined outbound proxy server rather than the remote VoIP device. This helps VoIP calls to pass through any NAT protected network without additional settings or techniques. Please make sure your VoIP Service Provider supports outbound proxy services before you enable it.

Outbound Proxy IP/Domain: Enter the outbound proxy's IP address or URL.

Outbound Proxy Port: Enter the outbound proxy's listening port.

SETUP → VoIP Setup

Enable P-Asserted

Privacy Type :

Enable P-Assert: Check the box to enable the caller ID protection.

Privacy Type: It is used to disguise the caller ID when queried via an ITSP/Third-Party Assertion. The Privacy Type includes 'user', 'header', 'session', 'none', 'critical', 'id' and 'history'.

SETUP → VoIP Setup

Enable P-Asserted
 Privacy Type :

NUMBER TRANSLATION

VoIP Dial-Out defined here overrides "Digit Map"

Copy From :

Scan Code	VoIP Dial-out
11	22

The rule of dialing of inviting to VoIP Service Providers may vary. That is, you have to configure different Digit Map for different ITSP. In this filed, you can configure individual Digit Map for each Proxy Server. The following examples introduce some cases. For general configuration, refer to **Digit Map** page.

Note: Press “Add” to add an entry. Don’t forget to press “Apply” which in the above of Number Translation.

For example (Example in Taiwan),

If Server 1 is local ITSP, you can refer to **Digit Map** page for general settings.

If Server 2 is global ITSP (VoIP STUN, free to dial to some cities free charge) you can set individual Digit Map in **Number Translation** field. Its dialing rule is Country code + Area Code + phone number. If you would like to make calls to Taipei through this ITST, you have to dial 8862xxxxxxx; if you would like to make calls to UK via this ITSP, the number should be 44xxxxxx. The settings for Server 2 appear like:

NUMBER TRANSLATION	
VoIP Dial-Out defined here overrides "Digit Map"	
Copy From : <input type="text" value="None"/>	
Scan Code	VoIP Dial-out
02%	8862%
00244%	44%

If Server 3 is ITSP in UK, you can set individual Digit Map in **Number Translation** field. As you make calls to UK through this ITSP, "Country code" should be removed and plus "0". The settings for Server 3 appear like:

NUMBER TRANSLATION	
VoIP Dial-Out defined here overrides "Digit Map"	
Copy From : <input type="text" value="None"/>	
Scan Code	VoIP Dial-out
00244%	0%

3-1-3 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.

3-1-3-1 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) :

Wireless Channel :

802.11 Mode :

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.

3-1-3-2 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 :

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

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

WEP	
<p>If you choose the WEP security option this device will ONLY operate in Legacy Wireless mode (802.11B/G).</p> <p>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.</p> <p>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.</p>	
WEP Key Length :	64 bit (length applies to all keys)
Default Tx Key :	1
WEP Key Format :	ASCII (5 characters)
WEP Key 1 :	<input type="text"/>
WEP Key 2 :	<input type="text"/>
WEP Key 3 :	<input type="text"/>
WEP Key 4 :	<input type="text"/>

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 :

WPA Cipher Suite : TKIP AES Both

WPA2 Cipher Suite : TKIP AES Both

PRE-SHARED KEY

Pre-Shared Key Format :

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 :

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.

3-1-4 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 :	<input checked="" type="radio"/> Router <input type="radio"/> Bridge
LAN Port Address :	<input type="text" value="192.168.8.254"/>
Subnet Mask :	<input type="text" value="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	
<input checked="" type="checkbox"/> Enable DHCP Server	
IP Pool Starting Address :	<input type="text" value="192.168.8.1"/>
IP Pool Ending Address :	<input type="text" value="192.168.8.250"/>
<input type="checkbox"/> IP Pool Uses Other Default Gateway	
IP Pool Default Gateway :	<input type="text" value="192.168.8.254"/>
IP Pool Subnet mask :	<input type="text" value="255.255.255.0"/>
Lease Time :	<input type="text" value="1"/> (1 - 9999 hours)
Domain Name Server Assignment :	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
Domain Name Server (Primary) IP :	<input type="text"/>
Domain Name Server (Secondary) IP :	<input type="text"/>

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.

3-1-5 Time and Date

SETUP → Time and Date

TIME

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

TIME SETTINGS

Automatically synchronize with Internet time servers

First NTP time server : ▼

Second NTP time server : ▼

TIME CONFIGURATION

Current Router Time :

Time Zone : ▼

Automatically synchronize with Internet time servers: The VoIP Router should automatically sync up with time servers.

First NTP time server: Select the desired domain name of a NTP server as first priority.

Second NTP time server: Select the domain name of a NTP server as second priority.

Current Router Time: It shows the current time of the VoIP Router.

Time Zone: Select your time zone from the drop-down menu.

3-2 ADVANCED

3-2-1 VoIP

3-2-1-1 Caller Filter

This function allows you to accept or reject any incoming call from the IP address listed in the filter rule. The call from the IP address of SIP proxy server is always accepted, despite Deny is selected or the IP address of SIP proxy server is not in the filter rule of Allow.

ADVANCED → VoIP → Caller Filter

CALLER FILTER

This function is used at allow or deny SIP Invite from the Proxy list ONLY.

Caller Filter :

Status	Filter IP Address	Subnet Mask		
Enable	192.168.8.21	255.255.255.0		

Caller Filter: It is to allow or deny the filter rule.

Status: It is to show the status of enable or disable.

Filter IP Address: Enter the start IP address which you would like to Allow or Deny.

Subnet mask: Enter the subnet mask you would like to Allow or Deny.

3-2-1-2 Caller ID

ADVANCED → VoIP → Caller ID

CALLER ID

In this section, it allows you to set Caller ID generation.. There are two type of FSK Caller ID. Choose the proper type for you.

FXS Caller ID Generation :

FSK Caller ID Type :

FXS Caller ID Generation: Select **DTMF** or **FSK** to enable the caller ID display function on FXS ports. When enabled, the caller's phone number will be displayed on your phone set when the call comes through.

FSK Caller ID Type: Either Bellcore or ETSI can be selected.

3-2-1-3 Calling Features

ADVANCED → VoIP → Calling Features

CALLING FEATURES

It provides Call Forward, Call Hold, Call Transfer and Call Waiting.

It also provides Three-Way Calling based on Nortel Soft Switch and works with the conference call supported by Voice Service Provider.

FXS REPRESENTATIVE NUMBER

Unconditional Forward :

Busy Forward :

LINE1 - FXS

Do Not Disturb

Unconditional Forward :

Busy Forward :

No Answer Forward : After(10 - 60) s

Call Hold

Call Transfer

Call Waiting

Three-Way Calling / Service ID :

Do Not Disturb: Check the box to reject (busy tone played) incoming calls.

Unconditional Forward: Check the box to forward incoming calls to the assigned “Forwarding Number” automatically. If configured forwarding to FXO it only makes FXO hook off, but not making FXO dial out.

Busy Forward: Check the box to forward incoming calls to the “Forward incoming Number” when the line is busy.

No Answer Forward: Check the box to forward incoming calls to the “Forward incoming Number” after ringing timeout (configurable from 10 to 60 seconds) expires.

Call Hold: Check the box to hold the call on the specific FXS port.

Note: Call Transfer or Call Waiting can only be activated when Call Hold is checked..

Call Transfer: Check the box to transfer the call to another destination (FXS port only).

Call Waiting: Check the box to accept incoming call while talking (FXS port only).

Calling Feature Instructions:

Call Hold: The call will be held after the FLASH button is pressed on the phone set. The VoIP Router will play a hold music (provided by your ITSP or VSP) to the remote end.

Call Transfer: The call will be held after FLASH button is pressed on local phone set (the VoIP Router plays on-hold music to the remote end). Meanwhile, the local user can dial out another number after the dial tone is heard. After the handset is on-hooked, the call originally on hold will then be transferred to the new number regardless the status of the new call. If wrong number is dialed for the new call, press the FLASH button will switch back to the call on hold. Also, if the local user doesn't hang up the phone after the new call is set up, press the FLASH button will switch between the original call and the new call. Please note that the PBX between phone sets and the VoIP Router must support FLASH features in order to use this function. If a phone set is connecting directly to the FXS port of the VoIP Router and the FLASH button does not function, please adjust the settings in "Flash Detect Time" from "Advanced Options" section.

Note: The availability of the above features also depends on your VoIP network. Please also check with your service provider for these services.

Examples of establishing a Three-Way call:

1. Phone1 dials to Phone2, Phone2 answers the call.
 2. Phone1 presses Flash then calls Phone3 (Phone2 is on hold) and Phone3 answers the call.
 3. Phone1 dials *61 and then presses Flash to start the conference call.
- Or**
4. Phone1 dials to Phone2, Phone2 answers the call.
 5. Phone3 dials to Phone1 (Call Waiting), Phone1 presses Flash to pick up the second call and talk to Phone3.
 6. Phone1 dials *61 and then presses Flash to start the conference call.

Note: The availability of a Three-Way call also depends on your VoIP network. Please also check with your service provider for these services.

3-2-1-4 Codec

ADVANCED → VoIP → Codec

CODEC

It can set the preferred codec, Jitter Buffer, Silence Detection/Suppression and Echo Cancellation in this section.

Preferred Codec Type : G.729 8kbps ▼

Jitter Buffer : 120 (60 - 1200 ms)

Silence Detection / Suppression

Echo Cancellation

	Codec	Type	Packet Interval (ms)	Approximate Bandwidth Required (kbps)
<input checked="" type="checkbox"/>	G.711 u-law		20 ▼	85.6
<input checked="" type="checkbox"/>	G.711 a-law		20 ▼	85.6
<input checked="" type="checkbox"/>	G.723.1	G.723.1 6.3k ▼	30 ▼	20.8
<input checked="" type="checkbox"/>	G.726 32K		20 ▼	53.6
<input checked="" type="checkbox"/>	G.729		20 ▼	29.6

Preferred Codec Type: Select a preferred codec type for all calls. Since different voice codecs have different compression ratios, the sound quality and occupied bandwidths are also different. The factual codec may determine by the called party. It is recommended that you use the default provided (G.723.1) codec because it occupies less bandwidth and provides better sound quality.

Jitter Buffer: Enter the jitter of receiving packets.

Silence Detection / Suppression: Check the box to enable the silence packets and send less voice data (package) during the silent period while talking.

Echo Canceling: Check the box to remove echo and improve voice quality during conversation.

Codec: Check the box to codec for the VoIP Router to support. All codecs are selected and supported by default. You can un-check the box that is not used.

Packet Interval: Select the frame size of voice package from different codec. It defines the time interval for the VoIP Router to send a RTP packet or voice packet to the receiving side. The smaller the value, the greater the bandwidth takes, and larger values might cause voice delay.

Approximate Bandwidth Required: It shows the bandwidth required from different codec and packet interval.

3-2-1-5 CPT/Cadence

ADVANCED → VoIP → CPT / Cadence

CPT # 1						Default
Tone Type	Low Frequency	High Frequency	T_ON_1	T_OFF_1	T_ON_2	T_OFF_2
Dial Tone	350	440	3000	0	0	0
Congestion Tone	480	620	250	250	0	0
Busy Tone	480	620	500	500	0	0
Ring-Back Tone	440	480	1000	2000	0	0

CPT # 1 Enable Setting 1: The CPT has a set of parameter table. Please adjust the CPT based on the local PSTN or PBX settings and requirements.

ADVANCED → VoIP → CPT / Cadence

FXS Ring Cadence Settings							Default
Range	ON_1 [250 - 8000 ms]	OFF_1 [250 - 8000 ms]	ON_2 [0, 250 - 8000 ms]	OFF_2 [0, 250 - 8000 ms]	ON_3 [0, 250 - 8000 ms]	OFF_3 [0, 250 - 8000 ms]	
1	1000	2000	0	0	0	0	

FXS Ring Cadence Settings: Specify the ring cadence for the FXS port. In this field, you specify the on and off pulses for the ring. The ring cadence that should be configured differs depending on local PSTN or PBX settings and requirements.

3-2-1-6 Digit Map

Digit Map supports multiple dial plans which help users to arrange least cost route. Each Proxy Server has individual dial plan which combines the original feature of Digit Map and Speed Dial. You can use “?” or “%” in the column of Scan Code and VoIP Dial-out. “?” represents a single digit, and “%” represents a wildcard. The function of the signs is to mapping the numbers between the number received from user and the replaced or modified number for actual dial out. With this function, users can easily add certain leading digits to replace a full set of numbers. There are 50 sets of leading digit entries to choose voice routing interface.

ADVANCED → VoIP → Digit Map

DIGIT MAP

There are 50 sets of leading digit entries to choose voice routing interface – Auto select VoIP or Deny.

Enable Pound Key ' #' Function

Default Call Route : VoIP ▾

Default VoIP Route Profile : 1 ▾

Enable Pound Key ' #' Function: Check the box to treat ‘ # ’ as a digit and send out with other numbers when dialing. If you un-check the box and ‘ # ’ is pressed after dialing, it will speed up the phone number detection of the VoIP Router.

Default Call Route: Select **VoIP** or **Deny** as the default call route for the calls.

Default VoIP Route Profile: Enter the Profile ID (ranging from 1-10) for the Default VoIP routing.

ADVANCED → VoIP → Digit Map

Scan Code	VoIP Dial-out	User Dial Length	Route	VoIP Route Profile			
<div style="border: 1px solid gray; padding: 5px; display: inline-block; margin: 10px auto;">Add</div>							

Scan Code: Enter the digits for the VoIP Router to scan while user is dialing.

VoIP Dial-out: Enter the actual dialing number rule for the VoIP Router to call through the Internet.

User Dial Length: Enter the total number of digits that user dialed.

Route: Select **VoIP** or **Deny** for this entry.

VoIP Route Profile: Choose the proper Profile ID and click the **Config** button to set the priority of VoIP Route Profile.

ADVANCED → VoIP → Digit Map

	Description	1	2	3	4	
1	MobilePhone	Server 1	None	None	None	
2	LongDistance	Server 2	Server 1	None	None	
3	InternationalCall	Server 3	Server 2	Server 1	None	

For example, Assume

Server 1 is local ITSP

- As you make Mobile call, it will try local ITSP as first priority.

Server 2 is VoIP STUN (ITSP, free to dial to some cities free charge)

- As you make long distance calls, it will try free ITSP at first. If fail, it will go through local ITSP (Server 1).

Server 3 is ITSP in UK

- As you dial to UK call, UK ITSP is first priority.

Methods of Digit Map:

Method 1- Single mapping: Fill a short code into the Scan Code column, and enter the desired phone number into the VoIP Dial-out column.

For example,

Scan Code: 09

VoIP Dial-out: 0911888997

User Dial Length: 2

Route: VoIP

VoIP Route Profile: Route # 1

Scan Code	VoIP Dial-out	User Dial Length	Route	VoIP Route Profile		
09	0911888997	2	VoIP	1		

Pick up the handset and dial 09, the VoIP Router will dial 0911888997 and follow Route # 1.

Method 2- Multi mapping: Fill the prefix code into the Scan Code column and the format to transfer into the VoIP Dial-out column.

For example,

Scan Code: 2???

VoIP Dial-out: 35106???

User Dial Length: 4

Route: VoIP

VoIP Route Profile: Route # 2

Scan Code	VoIP Dial-out	User Dial Length	Route	VoIP Route Profile		
09	0911888997	2	VoIP	1		
2???	35106???	4	VoIP	2		

Pick up the handset and dial 2301. The VoIP Router will dial 35106301 and follow Route # 2.

For example,
 Scan Code: 0%
 VoIP Dial-out: 1805%
 User Dial Length: Disable
 Route: VoIP
 VoIP Route Profile: Route # 3

Scan Code	VoIP Dial-out	User Dial Length	Route	VoIP Route Profile		
09	0911888997	2	VoIP	1		
2???	35106???	4	VoIP	2		
0%	1805%	Disable	VoIP	3		

Pick up the handset and dial 0423456789. The VoIP Router will dial 1805423456789 and go through Internet first and follow Route # 3.

Method 3- Substitution: It helps you dial to destination that you can not dial by phone. Destination like: test@1.1.1.1. Fill in the number into the **Scan Code** column and enter the desired name into the **VoIP Dial-out** column.

For example,
 Scan Code: 11
 VoIP Dial-out: test
 User Dial Length: 2
 Route: VoIP
 VoIP Route Profile: Route # 1.

Scan Code	VoIP Dial-out	User Dial Length	Route	VoIP Route Profile		
11	test	2	VoIP	1		

Pick up the handset and dial 11. The VoIP Router will dial "test" and go through Internet and follow Route # 1.

3-2-1-7 DTMF & PULSE

ADVANCED → VoIP → DTMF & PULSE

DTMF & PULSE	
It can help to solve the dialing number form these parameters.	
Dial Wait Timeout :	<input type="text" value="10"/> (1 - 60 s)
Inter Digits Timeout :	<input type="text" value="4"/> (1 - 60 s)
Minimum DTMF ON Length :	<input type="text" value="80"/> (40 - 500 ms)
Minimum DTMF OFF Length :	<input type="text" value="80"/> (40 - 500 ms)
DTMF Detection Sensitivity :	<input type="text" value="3"/> ▼
<input checked="" type="checkbox"/> Enable Out-of-Band DTMF	
Out-of-Band DTMF :	<input checked="" type="radio"/> RFC 2833 <input type="radio"/> SIP Info
Enable Hook Flash Event :	<input type="text" value="Disable"/> ▼
Payload Type :	<input type="text" value="101"/> (96 - 127)
Volume :	<input type="text" value="0 dB"/> ▼

Dial Wait Timeout: Enter the timeout duration after the user picks up the phone set.

Inter Digits Timeout: Enter the timeout duration between the intervals of each key pressed. When exceeding the set timeout duration without entering further digits, the numbers entered will be dialed out.

Minimum DTMF ON Length (Dial on)/ Minimum DTMF OFF Length (Dial off - between tones): This variable is to set the length of DTMF playback.

DTMF Detection Sensitivity: This variable is to set the sensitivity of the telephone keys for the VoIP Router to detect the DTMF.

Enable Out-of-Band DTMF: This variable is to set the method of DTMF transmission. RFC2833 or SIP Info.

Note: Out-of-Band DTMF transport method varies from VoIP networks, please contact your VoIP provider for the preferred method.

Enable Hook Flash Event: Select **Auto**, **RFC2833**, or **SIP info** for the signaling method of Hook Flash Event.

Payload Type: payload type of RFC2833.

Volume: Select the volume of RFC 2833 from the drop-down menu.

3-2-1-8 Fax

ADVANCED → VoIP → FAX

FAX	
The function is auto detect FAX by T.30 Fax, T.38 Fax, T.30/Modem or T.30 Only. Choose the type of FAX protocol and set the related settings.	
FAX / MODEM	
Line1 :	T.30 Fax <input type="button" value="v"/>
Line2 :	T.30 Fax <input type="button" value="v"/>

Disable - Select it if you are not sending fax, but it is still accepted fax by the VoIP Router.

T.38 Fax - Select it if you are using T.38 as the protocol for fax transmission. T.38 is used for reliable and efficient facsimile transmission over network. It transmits and receives FAX waveform (relaying) over the codec negotiated during call setup this bandwidth consumed is lowered. T.38 protocol also supports redundancy to get better FAX quality.

T.30 Fax - Select it if you are using T.30 as the protocol for fax transmission. It transmit FAX signal as voice thus uncompressed G.711 would be the choice. (G.726 also works but not recommended). Due to this nature, T.30 always requires a SDP change (change of codec within a session, SIP Re-Invite required) after FAX tone detected by the callee. It will consume more network resources and will affect transmission quality. The VoIP Router is still able to change the protocol from T.38 to T.30 if the called party uses T.38 for fax transmission.

T.30 Fax/Modem - Select it if you use it as the protocol for transmission of fax/modem over IP network.

T.30 Only - Select it if you are using G.711 a-law or G.711 u-law for fax transmission. The VoIP Router won't accept T.38 for fax transmission.

T.38 Native - Select it if you are only using T.38 for fax transmission.

Note: When a fax tone is detected from the call, the VoIP Router will automatically switch from voice mode to fax mode. Hence, the fax settings will be temporarily applied to a specific port which detects the fax tones, instead of its default voice settings.

ADVANCED → VoIP → FAX

FAX T.38	
<input checked="" type="checkbox"/> Enable High Quality	

FAX T.30	
FAX Codec :	G.711 u-law 64kbps ▼
FAX Jitter Buffer :	200 (60 - 1200 ms)

Enable High Quality: Check the box to increase approximately two times the bandwidth in order to compensate possible loss of packet during transmission and offers a better and reliable fax quality.

FAX Codec: Select **G.711 a-law**, **G.711 u-law**, or **G.726** for T.30 from the drop-down menu.

FAX Jitter Buffer: Enter the buffer or jitter when receiving packets.

Note: When you send a fax over an IP network, the IP network needs to support fax over IP functionality (either T.38 or T.30). Please consult your VoIP Service Provider for this setting.

3-2-1-9 Hot Line

ADVANCED → VoIP → Hot Line

HOT LINE	
Hot Line No.: Enter the hotline number for an automatic dialing function.	
Warm Line: When the Warm Line function is in use, user can dial a number. Otherwise the system will divert incoming calls from an outside line to the Hot Line Number after a set wait time.	
PHONE 1	
<input type="checkbox"/> Hot Line	
Hot Line No.:	<input type="text"/>
Warm Line (Hot Line Delay):	<input type="text" value="0"/> (0 - 60 s)
<input type="checkbox"/> VoIP Call Allow PSTN In	
PHONE 2	
<input type="checkbox"/> Hot Line	
Hot Line No.:	<input type="text"/>
Warm Line (Hot Line Delay):	<input type="text" value="0"/> (0 - 60 s)

Hot Line: Check to direct the call automatically to a pre-configured destination without any action when the FXS is off-hook. (ie. as the user picks up the phone). When the FXS is under Hot Line mode, no other phone numbers can be dialed.

Hot Line No.: Enter the number for pre-defined destination.

Warm Line: Enter the time for the call to start with a pause, so the user can dial another number. The call will be automatically directed to the pre-configured destination within timeout period.

VoIP Call Allow PSTN In: it is used only on Phone 1. Check the box to allow an incoming waiting call from PSTN while VoIP call is in use. To enable this feature, following settings need to be done first:

1. Tick **VoIP Call Allow PSTN In** to allow a waiting call from PSTN.
2. Tick **Call Hold** to hold the VoIP call when pressing the FLASH button on the phone set. (Calling Feature → Call Hold).

3-2-1-10 Line

ADVANCED → VoIP → Line

LINE

The function of Line setting is adjusting listening volume, speaking volume and tone volume.

LINE1 - FXS

Enable

Listening Volume : (3dB per step)

Speaking Volume : (3dB per step)

Tone Volume :

Min. FXS Hook Flash Time : (50 - 950 ms)

Flash Time : (50 - 950 ms)

Enable Polarity Reversal

FXS Chip Option 1

Enable: Tick the check box to enable a line. If some lines are not used, disable them (Pause Function) to avoid unnecessary waiting when an incoming call is diverting to the line.

Listening Volume: Use the drop-down menu to adjust the hearing (listening) volume.

Speaking Volume: Use the drop-down menu to adjust the speaking volume.

Tone Volume: Use the drop-down menu to adjust the tone volume. It will apply to all tones generated by the VoIP Router including Dial Tone, Ring Back Tone and Busy Tone.

Min. FXS Hook Flash Time: Enter the minimum flash time for FXS detecting. When the flash signal generated by the phone set is shorter than Min. FXS Hook Flash Time, FXS port will be on-hook.

Flash Time: Enter the maximum flash time for FXS detecting. When the flash signal generated by the phone set is longer than the Flash Time, FXS port will be on-hook.

Enable Polarity Reversal: Check the box to activate the generation of polarity reversal from FXS.

FXS Chip Option 1: Check the box to avoid mis-detecting the loop state of a subscriber line or PBX user loop from FXS interface. In some cases, the off-hook voltage might cause the FXS interface mis-detect the idle and the active state, in order to avoid this situation, un-check this feature.

ADVANCED → VoIP → Line

LINE3 - PSTN	
Flash Time :	<input type="text" value="600"/> (50 - 950 ms)
PSTN Ring OFF Length :	<input type="text" value="4000"/> (1000 - 20000 ms)
CO Line Type :	<input type="text" value="PSTN (48V)"/> ▼

Flash Time: Enter the time for PSTN to detect if the voltage keeps the on-hook status.

PSTN Ring OFF Length: Enter the ring length detected if the remote party is on-hook from PSTN by PSTN port. If the ring length from PSTN is longer than this setting, the PSTN will be on-hook, and it will stop the ringing from FXS.

CO Line Type: Select **PSTN (48V)** or **PABX (24V)** for the CO line type connected to PSTN port.

ADVANCED → VoIP → Line

Ring (Early Media) Time Limit :	<input type="text" value="90"/>	(10 - 600 s)
<input type="checkbox"/> Enable End of Digit Tone		
Force Calling Thru PSTN Code :	<input type="text"/>	
<input type="checkbox"/> Early Media Treatment		
Loop Current Drop Trigger Time :	<input type="text" value="0"/>	(0 = disable, 3 - 30 s)
Loop Current Drop Duration :	<input type="text" value="2"/>	(1 - 5 s)
<input type="checkbox"/> Enable ROH		
VoIP Centrex Extension Digit Count :	<input type="text" value="0"/>	(0 = disable, 1 - 30)
VoIP Centrex Digit :	<input type="text" value="5"/>	

Ring (Early Media) Time Limit[10 - 600secs]: Enter the timeout to cancel a call if no one answers the phone.

Enable End of Digit Tone: Check the box to activate the function of playing a “Beep-Beep” tone to notify the user that the call is in progress.

Force Calling Thru PSTN code: Enter the code to get a PSTN line before dialing out. For example: If you specify code “33” in this option and would like dial “23456789” via a PSTN line: Dial “33” and you will hear dial tone from the PSTN line, now you’re able to dial “23456789” via PSTN line.

Early Media Treatment: Check the box to send the one-way RTP immediately when a connection with a VoIP service provider has been set up.

Loop Current Drop Trigger Time: Enter the time to avoid the line being engaged when FXS port is connected to PBX. It stops the loop current from FXS port when FXS port is playing busy tone. The setting “0” zero is to disable this function.

Loop Current Drop Duration: Enter the drop duration for loop current.

Enable ROH: Check the box to play Receiver Off-Hook tone in order to notify user to hang up the phone set if FXS is off-hook for more than 20 seconds.

VoIP Centrex Extension Count: This feature is to enable and set the digit count of VoIP Centrex. The setting “0” zero is to disable this function.

VoIP Centrex Digit: Enter the digit for VoIP call. If you dial VoIP Centrex Digit first, the dialing plan is according to the Digit Map; otherwise the VoIP Router will send the number which digit count is the same as VoIP Centrex Extension Digit Count.

ADVANCED → VoIP → Line

TERMINATION IMPEDANCE	
Termination Impedance :	Taiwan 600 Ohm 

FXS Impedance: Select different impedance from the drop-down menu.

ADVANCED → VoIP → Line

VOICE MENU OPTIONS	
Silence Detection Threshold :	<input type="text" value="0"/> (0=disable, 1 - 60 db)
Drop Silent Call Timeout :	<input type="text" value="120"/> (0=disable, 1 - 3600 s)

This feature is a call drop standard for a VoIP Router to determine whether or not to hang up the phone. The VoIP Router will disconnect the call automatically to avoid keeping the line engaged if the detected volume is below the **Silence Detection Threshold** or the time exceeds the **Drop Silent Call Timeout**.

Silence Detection Threshold: Enter the threshold (dB) to detect if there is voice coming from RJ-11 interface.

Drop Silent Call Timeout: Enter the duration (second) for detecting if there are RTP packets receiving from RJ-45 interface.

Note: Improper values for above settings might cause unexpected automatic disconnection of a call. Default values are recommended.

ADVANCED → VoIP → Line

<input checked="" type="checkbox"/> Enable IVR Option
<input checked="" type="checkbox"/> Enable Call Feature Code

Enable IVR Option: Check the box to enable IVR function.

Enable Call Feature Code: Check the box to enable the advanced function for Call Features, such as Call Pickup, Automatic Redial and Unattended transfer.

3-2-1-11 Phone Book

Phone Book: It is used for peer-to-peer communication. Some peer information needs to be added to this section prior to making peer-to-peer calls. You need to enter the phone number and the IP address of the remote peer.

ADVANCED → VoIP → Phone Book

PHONE BOOK

It has 100 phone numbers to restore into a phone book and provides an IP address query when calling to other gateway(s).

Gateway Name	Gateway Number	IP / Domain Name	Port		
					

Gateway Name :

Gateway Number :

IP / Domain Name :

Port :

Gateway Name: Enter the alias of the remote peer.

Gateway Number: Enter the phone number of the remote peer.

IP / Domain Name: Enter the IP address or URL (Uniform Resource Locator) of the remote peer.

Port: Enter the listen port of the remote peer.

3-2-1-12 SIP Advanced

ADVANCED → VoIP → SIP Advanced

SIP ADVANCED

There are many parameters that need to contact with VSP (Voice Service Provider) before setting up.

Listen Port UDP : (1 - 65535)

RTP Starting Port UDP : (1 - 65500)

Listen Port UDP: Enter the VoIP Router's listening port in this field. Leave it as default settings, unless it conflicts with ports used by other device in your network.

RTP Starting Port UDP: Enter the starting port number or transmitting voice data among VoIP devices. Each line requires 2 ports.

For example, if the starting port is 9000, then Line 1 will take up ports 9000 and 9001, and Line 2 will take up ports 9002 and 9003, and so forth.

ADVANCED → VoIP → SIP Advanced

E.164

International Call Prefix Digit :

Country Code :

Long Distance Call Prefix Digit :

Area Code :

E.164 Numbering (To Invite Proxy)

ENUM Header Exception :

International Call Prefix Digit: Enter the International call prefix.

Country Code: Select the desired country code from the drop-down menu or enter the country code if **Other** is selected.

Long Distance Call Prefix Digit: Enter the long-distance prefix digit for making a long-distance call.

Area Code: Enter the area code.

E.164 Numbering(To Invite Proxy): This variable is followed the E.164 rule, but it depends on the SIP proxy server. Click the check box to send the number following the E.164 rule by the VoIP Router.

ENUM Header Exception: Enter the prefix number that the VoIP Router sends the number without followed the E.164 rule.

Note: E.164 Numbering depends on the proxy. If you fail to make a call, please contact your VoIP Service Providers.

ADVANCED → VoIP → SIP Advanced

SESSION TIMER	
Session Expiration :	<input type="text" value="0"/> (0 = disable, 10 - 1800 s)
Session Refresh Request :	<input checked="" type="radio"/> UPDATE <input type="radio"/> re-INVITE
Session Refresher :	<input checked="" type="radio"/> UAS <input type="radio"/> UAC

Session Expiration: This field will set the time that the VoIP Router will allow a SIP session to remain die (without traffic) before dropping it.

Session Refresh Request: Select **UPDATE** or **re-INVITE** to send refresh requests to the Server.

Session Refresher: This determines which side of an expired call session will initiate the session refresh. uac – specifies that the Caller side will initiate the session refresh. uas – specifies that the Call receiver (the “Callee”) will initiate the session refresh.

ADVANCED → VoIP → SIP Advanced

SIP TIMEOUT ADJUSTMENT	
SIP Message Resend Timer Base :	<input type="text" value="0.5"/> s
Max. Response Time for Invite :	<input type="text" value="4"/> (1 - 32)

SIP Message Resend Timer Base: Select the resend timer base from the drop-down menu if response is not received within the base time. The sequence of sending is like "base time" * 2, and send again at "base time" *2 *2. The maximum resend time is four seconds. Resend action will stop when the total resend time has reached 20 seconds.

Max. Response Time for Invite: Enter the maximum response time for INVITE packet. When the destination does not reply within the set time, the call is failed.

ADVANCED → VoIP → SIP Advanced

<input type="checkbox"/> VoIP Failure Announcement

VoIP failure announcement: Check the box to play a voice announcement if the VoIP Router fails to register to the SIP proxy server while FXS is off-hook.

ADVANCED → VoIP → SIP Advanced

<input type="checkbox"/>	Anonymous Caller ID (CLIR)
<input type="checkbox"/>	VoIP Call Out Notification
<input checked="" type="checkbox"/>	Enable Built-in Call Hold Music
<input checked="" type="checkbox"/>	Enable Non-SIP Inbox Call
<input checked="" type="checkbox"/>	Delay PSTN Hangup Detection
<input checked="" type="checkbox"/>	Invite URL Need 'User=Phone'
<input type="checkbox"/>	Reliability of Provisional Responses
<input type="checkbox"/>	Compact Form
SIP Caller ID Obtaining :	
	Remote-Party-Id Display Name <input type="button" value="v"/>
<input type="checkbox"/>	Put Caller ID in URI
<input type="checkbox"/>	INVITE With Remote-Party-ID Header
<input type="checkbox"/>	Support URI Percent-Encoding (RFC 3986)

Anonymous Caller ID (CLIR): Check the box to lock the delivery of the Caller ID to the called party.

VoIP Call Out Notification: Check the box to enable the function of playing a tone to notify user that the call is through VoIP.

Enable Built-in Call Hold Music: Check the box to enable the function of playing music when receiving Call Hold request.

Enable Non-SIP Inbox Call: Check the box to make local calls. Local Call here means the call does not go through the Internet and if the dialed number is the extension of other line. You can un-check it to configure as all calls go through the Internet.

Delay PSTN Hangup Detection: Check the box to delay the detection of dully PSTN line on-hook status from PSTN port. You can un-check it to change the sensitivity of detection from PSTN port to detect the PSTN line on-hook status.

Invite URL need 'user=phone': Check the box to add 'user=phone' as a hint that the part left to the '@' sign is actually a phone number.

Reliability of Provisional Responses: Check the box to send a PRACK request during the progress of the request processing. Reliability of Provisional Responses is to ACK at every SIP packet. With this method, SIP packet will act like TCP, ie. every packet sent will receive an ACK to make sure that packet sent has been received by other peer.

Compact Form: Check the box to represent common header field names in an abbreviated form. This may be useful when SIP message is too large to be carried on and recognized by the user agent.

SIP CallerId Obtaining: Select the part of the SIP packet from the VoIP Router to obtain Caller ID. There are several places where the Caller ID is located.

Remote-Party-Id Display Name - It is located at SIP → Remote-Party-ID → Before [<sip:]

Remote-Party-Id User Name - It is located at SIP → Remote-Party-ID → After [<sip:], Before [@]

From-Header Display Name - The standard way is in SIP → Message Header → From → SIP Display info.

From-Header User Name - It is located at SIP → Message Header → From → SIP from address before [@].

Put Caller ID In URI: This feature is to put Caller ID in URL. The Caller ID is located in SIP → Message Header → After [From:], Before [<sip:] by default settings. It will be located in SIP → Message Header → After [<sip:], Before [@] if ticked.

INVITE With Remote-Party-ID Header: Check the box to comprise the information of Remote-Party-ID in the message header of INVITE. Different format of INVITE header might cause the call not to be connected. Please consult with your VoIP Service Provider before enabling it.

Support URI Percent-Encoding(RFC 3986): Check the box to encode/decode the letters of the basic Latin alphabet, digits, and a few special characters which follow RFC 3986.

3-2-2 Access Control

3-2-2-1 MAC Filtering

Use MAC Filters to deny computers within the local area network from accessing the Internet. You can either manually add a MAC address that are connected to the VoIP Router.

ADVANCED → Access Control → MAC Filtering

MAC FILTERING

The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to DENY network/Internet access.

Enable MAC Filtering

MAC	Remark
<input type="button" value="Add"/>	

MAC :
Remark :

Enable MAC Filtering: Check the box to deny from accessing Internet.

MAC: Enter the MAC of the computer in the LAN (Local Area Network) to be used in the MAC filter table.

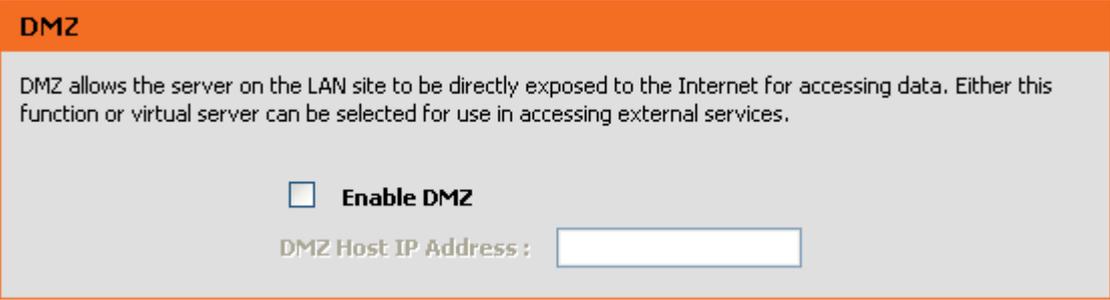
Remark: Enter comments.

3-2-3 Firewall and DMZ

3-2-3-1 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



The screenshot shows a web interface for configuring DMZ. At the top, there is an orange header with the text "DMZ". Below the header, there is a grey box containing the following text: "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." Below this text, there is a checkbox labeled "Enable DMZ". Below the checkbox, there is a label "DMZ Host IP Address:" followed by a text input field.

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.

3-2-3-2 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

<input checked="" type="checkbox"/> SYN	<input type="text" value="50"/>	(Packets/Second) (50 - 500)
<input checked="" type="checkbox"/> FIN	<input type="text" value="50"/>	(Packets/Second) (50 - 500)
<input type="checkbox"/> UDP	<input type="text" value="150"/>	(Packets/Second)
<input checked="" type="checkbox"/> ICMP	<input type="text" value="50"/>	(Packets/Second) (50 - 500)

PER-SOURCE IP FLOOD

<input checked="" type="checkbox"/> SYN	<input type="text" value="30"/>	(Packets/Second) (30 - 300)
<input checked="" type="checkbox"/> FIN	<input type="text" value="30"/>	(Packets/Second) (30 - 300)
<input type="checkbox"/> UDP	<input type="text" value="150"/>	(Packets/Second)
<input checked="" type="checkbox"/> ICMP	<input type="text" value="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.

3-2-3-3 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
<input type="button" value="Add"/>		

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 field.

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

Remark: Enter comments.

3-2-3-4 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
<input type="button" value="Add"/>		
Port Range : <input style="width: 40px;" type="text"/> - <input style="width: 40px;" type="text"/>	TCP / UDP : <input style="width: 40px;" type="text" value="Both"/>	Remark : <input style="width: 100%;" type="text"/>

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.

3-2-3-5 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 port on your router for redirection to an internal LAN IP Address and 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
<input type="button" value="Add"/>				
WAN Port Range :	<input style="width: 40px;" type="text"/> - <input style="width: 40px;" type="text"/>	TCP / UDP :	<input style="width: 40px;" type="text"/>	LAN Host IP Address :
Server Port Range :	<input style="width: 40px;" type="text"/> - <input style="width: 40px;" type="text"/>	Remark :	<input style="width: 100%;" type="text"/>	

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.

3-2-4 Advanced Wireless

3-2-4-1 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 type :	Auto	▼
Fragmentation :	2346	(256 - 2346)
RTS Threshold :	2347	(0 - 2347)
Beacon Interval :	100	(20 - 1024 ms)
Data Rate :	Auto	▼
Preamble Type :	Long Preamble	▼
<input checked="" type="checkbox"/> Broadcast SSID		
<input checked="" type="checkbox"/> IAPP		
<input checked="" type="checkbox"/> 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.

3-2-4-2 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 :

MAC	Comment
<input type="button" value="Add"/>	

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.

3-2-5 Advanced Network

3-2-5-1 QoS

WAN QoS

ADVANCED → Advanced Network → QoS

QoS

Choose WAN or LAN to configure network traffic bandwidth.

Enable WAN QoS

Enable LAN QoS

WAN QoS

Downstream Bandwidth : kbps

Upstream Bandwidth : kbps

ToS / DiffServ Settings :

ToS IP Precedence

DiffServ (DSCP)

TOS IP PRECEDENCE

Signaling Precedence :

Voice Data Precedence :

Enable WAN QoS: Check the box to guaranty the voice quality. Voice packets have the highest priority in IP networks, and the data transmission is distributed to less bandwidth.

Downstream Bandwidth - Select the downstream bandwidth that is the same as the actual bandwidth subscribed from the drop-down menu.

Upstream Bandwidth - Select the upstream bandwidth that is the same as the actual bandwidth subscribed from the drop-down menu.

ToS IP Precedence: Select the precedence for signaling (data) and voice (voice data).

DiffServ (DSCP): Select the number of signaling (data) and voice (voice data) values.

Note: For the VoIP Router, ToS IP Precedence and DiffServ are the same function. You only select one for priority marking.

LAN QoS

ADVANCED → Advanced Network → QoS

LAN QoS				
Port	Priority	Flow Control	Incoming Rate Limit	Outgoing Rate Limit
LAN Port 1	LOW <input type="button" value="v"/>	<input checked="" type="checkbox"/>	Full <input type="button" value="v"/>	Full <input type="button" value="v"/>
LAN Port 2	LOW <input type="button" value="v"/>	<input checked="" type="checkbox"/>	Full <input type="button" value="v"/>	Full <input type="button" value="v"/>
LAN Port 3	LOW <input type="button" value="v"/>	<input checked="" type="checkbox"/>	Full <input type="button" value="v"/>	Full <input type="button" value="v"/>
LAN Port 4	LOW <input type="button" value="v"/>	<input checked="" type="checkbox"/>	Full <input type="button" value="v"/>	Full <input type="button" value="v"/>

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.

3-2-5-2 NAT Traversal

If your VoIP Router is set up behind an Internet sharing device, you can select either the NAT or STUN protocol.

ADVANCED → Advanced Network → NAT Traversal

NAT TRAVERSAL

If the gateway is set up behind an Internet sharing device, you can select either the NAT or STUN protocol.

NAT PUBLIC IP

Enable
 NAT IP / Domain :

STUN CLIENT

Enable
 STUN Server IP / Domain :
 STUN Server Port : (1 - 65535)

Enable NAT Public IP: Check the box to use the IP address of the Internet sharing device if the VoIP Router is set up behind an Internet sharing device. Also the VoIP Router will use the IP address of the Internet sharing device as the public IP when it connects to Internet. Furthermore, some of the Internet sharing device's type is symmetric NAT. You need to set Virtual Server or Port Mapping (Forwarding) from the Internet sharing device for the listen port and communication ports (RTP ports) of the VoIP Router.

NAT IP/Domain: Enter the real public IP address of the IP sharing device or the router; or enter a true URL (Uniform Resource Locator) when DDNS is used. Please refer to the DDNS settings.

Note: If you are setting a public IP in this field, it has to be a static public IP, otherwise VoIP communication may not be established properly. Please contact your ISP to check if your Internet connection has static public IP addresses.

Enable STUN Client: Check the box to use the STUN protocol prevents problems from setting the IP sharing function. (Some NATs do not support this protocol.)

Note: You can use the "Status → STUN Inquiry" page to detect the NAT type of your Internet sharing device. If the NAT type is "Symmetric NAT," then the VoIP Router is not able to traverse the NAT. It is not a flaw of the VoIP Router design, but rather a limitation of the STUN protocol.

STUN Server IP/Domain and Port: Enter the IP address and listen port of the STUN server. You can set two STUN server IPs separated by a semicolon.

3-2-5-3 STUN Inquiry

Use "STUN Inquiry" to detect your IP sharing device's NAT type and communication between a STUN server and client.

ADVANCED → Advanced Network → STUN Inquiry

STUN INQUIRY

Use STUN Inquiry to detect your IP sharing device's NAT type and communication between a STUN server and client.

NAT Type :	Unknown
STUN Server IP / Domain :	<input type="text"/>
STUN Server Port :	<input type="text" value="3478"/> (1 - 65535)

NAT Type: It shows the NAT type of your router.

STUN Server IP/Domain: Enter the IP address or URL of the STUN server for query.

STUN Server Port: Enter the STUN Server's listening port

3-2-5-4 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	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input style="width: 100%;" type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input style="width: 100%;" type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input style="width: 100%;" type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input style="width: 100%;" type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input style="width: 100%;" type="text"/>

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.

3-2-5-5 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.

3-3 MAINTENANCE

3-3-1 Device Management

MAINTENANCE → Device Management

ADMIN	
New Password :	<input type="password" value="*****"/>
Confirm Password :	<input type="password" value="*****"/>

USER	
New Password :	<input type="password" value="*****"/>
Confirm Password :	<input type="password" value="*****"/>

Note: There are two operating levels when entering the Web UI. Logging-in as the ADMIN allows you to change all settings. A Web UI USER only has access to some settings.

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

MAINTENANCE → Device Management

Port of Web Access from WAN :	<input type="text" value="8080"/>
Web Idle Time Out :	<input type="text" value="180"/> (30 - 300 s)
<input checked="" type="checkbox"/> Enable Web UI	
<input checked="" type="checkbox"/> Enable Telnet Service	

Port of Web Access from WAN: Enter the port number when accessing the web-based configuration utility from the WAN port.

Web Idle Time Out: Enter the range of effective time when log-in the web interface. The user will be disconnected from the web page to allow others to log-in.

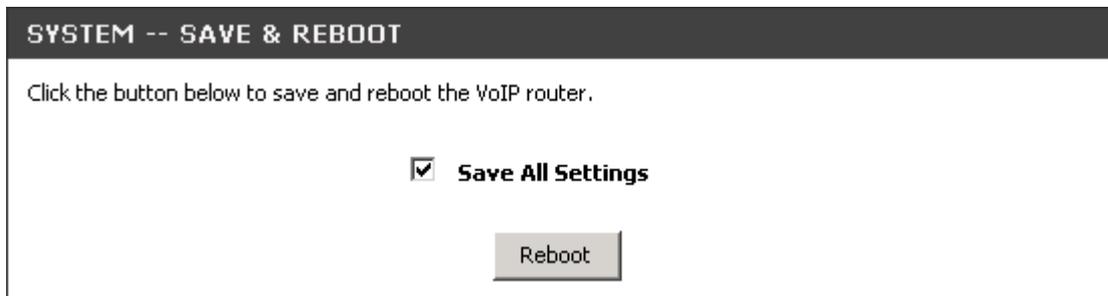
Enable Web UI: Check the box to enable WEB access from WAN or LAN.

Enable Telnet Service: Check the box to enable Telnet access from WAN or LAN.

3-3-2 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

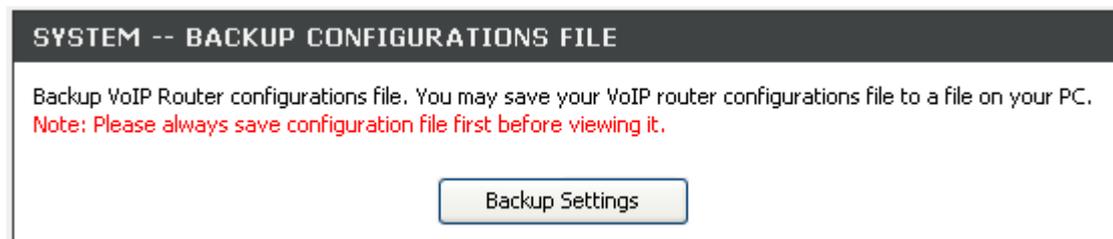
Reboot

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.

Backup Configurations File

MAINTENANCE → Backup and Restore



SYSTEM -- BACKUP CONFIGURATIONS FILE

Backup VoIP Router configurations file. You may save your VoIP router configurations file to a file on your PC.

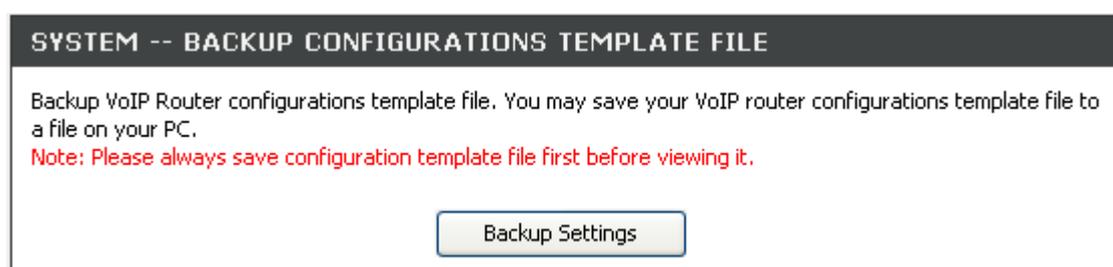
Note: Please always save configuration file first before viewing it.

Backup Settings

The current system settings can be saved as a file onto the local hard drive. Click the **Backup Settings** button to save your current settings to a file.

Backup Configurations Template File

MAINTENANCE → Backup and Restore



SYSTEM -- BACKUP CONFIGURATIONS TEMPLATE FILE

Backup VoIP Router configurations template file. You may save your VoIP router configurations template file to a file on your PC.

Note: Please always save configuration template file first before viewing it.

Backup Settings

Click the **Backup Settings** button to save your current settings to a template file for editing.

Update Settings

MAINTENANCE → Backup and Restore

SYSTEM -- UPDATE SETTINGS

Update VoIP Router settings. You may update your router settings using your saved files.

Settings File Name :

To restore a system settings file, click on **Browse** to search the local hard drive for the file to be used. Once you locate the file, click **Upload Settings** to overwrite the current settings with the settings saved to the file.

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.

3-3-3 Firmware Update

The VoIP Router supports a software upgrade function from a remote server. Please consult your VoIP Service Provider for information about the following details.

MAINTENANCE → Firmware Update

FIRMWARE UPDATE

The Firmware Upgrade section can be used to update to the latest firmware code to improve functionality and performance.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot. Please DO NOT power off your device before the update is complete.

Current Firmware Version :	1.02.37.42	
Upgrade Server :	<input type="text" value="TFTP"/>	
Server IP Address :	<input type="text"/>	
Server Port :	<input type="text" value="69"/>	(1 - 65535)
User Name :	<input type="text"/>	
Password :	<input type="text"/>	
Directory :	<input type="text"/>	

Upgrade Server: Select the upgrade type: **TFTP**, **FTP**, or **HTTP**.

Server IP Address: Enter the server's IP address.

Server Port: Enter the server's port.

User Name/ Password: Enter the account information for accessing the server if needed.

Directory: Enter the location of the firmware file.

3-3-4 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.whateveryounameis.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 : <<

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.

3-3-5 Log Settings

MAINTENANCE → Log Settings

SYSTEM LOG

The System Log options allow you to send log information to a SysLog Server.

Enable

Server Address :

Port : (1 - 65535)

Enable: Check the box to send event notification messages across IP networks to the Server.

Server Address: Enter the System Log Server's IP address.

Port: Enter the System Log Server's listening port. Leave this field to the default if your VoIP Service Provider did not provide you a server port number for System Log Server.

3-3-6 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 :

Number of Ping : (1 - 100)

Ping Packet Size : (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
```

3-3-7 Provision

Provisioning is a function that automatically updates your VoIP Router's configuration by using a TFTP, FTP, or HTTP server located on the Internet. If you have access to such service, you will need to know the URL or IP address of the Provisioning Server.

Note: Fill in the parameters needed by your VoIP Service Provider. Please check with your VoIP Service Provider about the availability of these services.

MAINTENANCE → Provision

PROVISION

Provision setting is for the device that can be auto upgrade the firmware and configuration.

Enable Auto Provisioning

Provision Server Address :

Port : (1 - 65535)

Packet Format : ▼

Verify Servers Certificate

Connect Provision Server During Start Up

Connect Provision Server Periodically

Auto Provision Interval : (60 - 604800 s)

Random Offset : (0 - 1800 s)

Provision Retry Times : (0 = always, 0 - 99)

Retry Interval: (30 - 120 s)

Suspend Call Service

Enable Auto Provisioning: Check the box to start provisioning.

Provision Server Address: Enter the Provisioning Server's IP address or URL required by your VoIP Service Provider.

Port: Enter the Provisioning Server's listening port.

Packet Format: Use the drop-down menu to choose the packet transmitting format required by your VoIP Service Provider.

Verify Servers Certificate: It is used for Provision Server certification while HTTPS packet format is in use.

Connect Provision Server During Start Up: Check the box to connect to Provisioning Server when the VoIP Router is powered on or rebooted.

Connect Provision Server Periodically: Check the box to connect to Provisioning Server periodically.

Auto Provision Interval: Enter the time for auto provisioning.

Random Offset: Enter the offset of the time for auto provisioning.

Provision Retry Times: Enter the retry time if a provisioning attempt fails.

Retry Interval: Enter the interval for retrying.

Suspend Service: Check the box to stop VoIP call service.

Note: Contact your server provider if necessary.

MAINTENANCE → Provision



The screenshot shows a configuration panel with a dark header bar. Below the header, there is a checkbox labeled "Binding Server for Trigger". Underneath this checkbox, there are two rows of input fields. The first row is labeled "Binding Port :" and contains a text box with the value "10104" and a range indicator "(1 - 65535)". The second row is labeled "Binding Interval :" and contains a text box with the value "10" and a range indicator "(1 - 65535 s)".

Binding Server for Trigger: Check the box to trigger a connection between Provisioning Server and the VoIP Router. Provisioning Server will bind a port for the VoIP Router to send provision request.

Binding Port: Enter the port number of Provisioning Server is used for binding.

Binding Interval: Enter the interval at which the VoIP Router will keep the binding.

3-3-8 CDR

The user can set up a CDR Server to record call details for every phone call with TCP protocol. The present CDR provides the call event such as HOOK ON, HOOK OFF, DIALED NUMBER, DATE...recording in a text file and which can be imported to prepare an analysis report.

MAINTENANCE → CDR

CDR

The user can set up a CDR Server to record call details for every phone call with TCP protocol. The present CDR provides the call event such as HOOK ON, HOOK OFF, DIALED NUMBER, DATE...recording in a text file and which can be imported to prepare an analysis report.

Send record to CDR Server

CDR Server IP / Domain :

Port :

Support RADIUS

RADIUS Accounting Port :

RADIUS Server Secret :

RADIUS User ID :

RADIUS Password :

Send record to CDR Server: Tick the check box to enable the call detail recording.

CDR Server IP / Domain: Enter the IP address of the CDR server.

Port: Enter the listen port of the CDR server.

Support RADIUS: Tick the checkbox to enable RADIUS as database and enter the information of RADIUS needed. It includes RADIUS Accounting Port, RADIUS Server Secret, RADIUS User ID and RADIUS Password.

3-4 STATUS

3-4-1 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.

3-4-2 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	
SERVER REGISTRATION STATUS							
DDNS Registration :				Disabled (00:17:04)			
Phone Book Manager Registration :				Disabled (00:17:04)			
STUN Registration :				Disabled (00:17:04)			
UPnP Negotiation :				Disabled (00:17:04)			
SIP Proxy Hunting Number Registration :				FXS Disabled (00:17:04)			

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.

3-4-3 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

3-4-4 Statistics

STATUS → Statistics

RTP PACKET SUMMARY

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

PHONE 1

Talk Information :	G.711 u-law 64kbps
Packet Sent :	0
Packet Received :	0
Packet Lost :	N/A
The Last Packet's Source IP :	
The Last Packet's Source Port :	0

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

3-4-5 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.

Logout

4. Configuring the VoIP Router through IVR

VoIP transmits voice data (packets) via the Internet, hence the condition and status of the network environment is relatively important to the telecommunications quality. If any one of the parties involved in VoIP communications has insufficient bandwidth or frequent packet loss, the telecommunication quality will be poor. Therefore, excellent telecommunication can only happen when the VoIP Routers are connected to the Internet and when the network environment is stable.

Preparation

1. Connect the power supply, telephone set, telephone cable, and network cable properly.
2. If a static IP is provided, confirm the correct IP settings of the WAN Port (IP address, Subnet Mask, and Default gateway). Please contact your local Internet Service Provider (ISP) if you have any question.
3. If you are using ADSL (PPPoE) for your network connection, confirm the account number and password.
4. If you intend to operate the VoIP Router under NAT, the IP range of VoIP Router WAN Port and LAN Port IP Address should not be the same in order to avoid phone failures.

Basic Setup

The VoIP Router provides two setup modes:

1. Telephone IVR Configuration Mode
2. Browser Configuration Mode

IVR configuration provides basic query and setup functions, while browser configuration provides full setup functions.

4-1 IVR (Interactive Voice Response)

The VoIP Router provides convenient IVR functions. Users are able to get query and setup the VoIP Router with a phone-set and function-codes without turning on the PC.

Note: When finishing the setup, make sure the new settings are saved. This will enable the new settings to take effect after the system is restarted.

Instructions

FXS Port: Connect to telephones. To access IVR mode, passwords should be entered, “* * password #”. Alphabets to digits conversion information is provided in the PPPoE Character Conversion Table. (Refer to Page 71) When correct IVR passwords are entered and accepted, an indication tone can be heard indicates the system is in IVR setup mode. Enter function codes to check or configure the VoIP Router. (Please refer to page 68 for function codes).

Example: If your password is “1234”, enter * (star) * (star) 1 2 3 4 # (pound), and now you are entering IVR setup mode. Next, enter a function code to check or configure the VoIP Router. If your password is “admin”, enter * (star) * (star) * (star) 41 44 53 49 54 # (pound). Please refer to the IVR Functions Table (page 68) for available functions and codes.

Once the setting or query has been completed, you can hear a dial tone. Use the same procedure to make a second query or setting. To exit IVR mode, simply hang up the phone.

Example: enter “***#” (you are now in IVR mode) → enter **101** (to query the current IP address) → the system responds with an IP address. You can continue with more settings or queries: enter **111** (to set

a new IP address) →enter 192*168*1*2 (new IP address).

Save Settings

When all setting procedures are completed, dial 509 (Save Settings) from phone keypad. Wait for about three seconds, you should hear a voice prompt "1 (one)." You can now hang up the phone and please reboot the VoIP Router to enable the new settings.

To inquire about the current VoIP Router WAN Port IP address setting

After completing all your settings, dial 101 from the keypad, then you can hear the system play back the current WAN Port IP address. If the system does not play back the IP address after dialing 101, this indicates that the VoIP Router currently is not connected to the Internet. Please check and make sure the cable connections, account numbers, and passwords are correct.

4-1-1 IVR Functions Table:

Function Code	Description	Example / Notes
111/101	WAN Port IP address Set/Query	Dial function code 114 and then dial 1 for a Static IP connection then setup the IP address.
112/102	WAN Port Subnet Mask Set/Query	
113/103	WAN Port Default Gateway Set/Query	
114/104	Current Network IP Access Set/Query (1: Static IP, 2: DHCP, 3: PPPoE)	
115/105	DNS IP address Set/Query	
116/106	Phone Book manager IP address Set/Query	
117/107	Set/Query whether or not to use a Public Telephone Book (0: Disable 1: Enable)	
199/099	Set/Query whether or not this VoIP Router acts as the Phone Book manager (0: Disable 1: Enable)	
066	Querying the connection to Phone Book manager	
118	Restart	
121	Setup PPPoE Account	Dial function code 114 and then dial 3 for a PPPoE connection.
122	Set PPPoE Password	
123	Set NAT IP address	
124	Uses NAT (0: Disable 1: Enable)	
311/301	LAN Port IP Set/Query	
312/302	LAN Port Subnet Mask Set/Query	
109	Restore factory default IP address configuration	A static IP address for WAN Port IP : 192.168.1.2 Mask : 255.255.255.0 Gateway : 192.168.1.254
409	Restore factory default settings	
509	Save settings	
900	Set the IVR and the language used on the Web GUI (1: English, 2: Traditional Chinese, 3: Simplified Chinese)	
209	Software Upgrade	

4-2 IP Configuration Settings—Set the IP Configuration of the WAN Port

Static IP Settings

Note: Complete static IP settings should include a static IP (option 1 under [114](#)), IP address ([111](#)), Subnet Mask ([112](#)), and Default Gateway ([113](#)). Please contact your Internet Service Provider (ISP) if you have any question.

Function	Command
Select a Static IP	<ul style="list-style-type: none"> After entering IVR mode, dial 114. When voice prompt plays "Enter value", dial 1 (to select static IP)
IP address Settings	<ul style="list-style-type: none"> After entering IVR mode, dial 111. When voice prompt plays "Enter value", enter your IP address followed by "#". <p>Example: If the IP address is 192.168.1.200, dial 192*168*1*200#.</p>
Subnet Mask Settings	<ul style="list-style-type: none"> After entering IVR mode, dial 112. When voice prompt plays "Enter value", enter your subnet mask followed by "#". <p>Example: If the subnet mask value is 255.255.255.0, dial 255*255*255*0#.</p>
Default Gateway Settings	<ul style="list-style-type: none"> After entering IVR mode, dial 113. When voice prompt plays "Enter value", enter your default gateway's IP address followed by "#". <p>Example: If the default gateway is 192.168.1.254, dial 192*168*1*254#.</p>
Save Settings and Restart	<ul style="list-style-type: none"> To save settings, dial 509 (Save Settings). The system will save the current settings. Please restart the system. Wait for about 40 seconds for the system to restart, and then enter 101 to check whether the IP address was retained. If the system does not play back the IP address after dialing 101, this indicates that the VoIP Router currently is not connected to the Internet. Please check and make sure the cable connections, account numbers, and passwords are correct.

Dynamic IP (DHCP) Settings

After entering IVR mode, dial [114](#).

When voice prompt plays "Enter value", dial 2 (to select DHCP).

Saving settings –press [509](#) (Save Settings). Please restart the system. After the system is restarted, press [101](#) to check whether or not the IP address was retained.

Note: If the system does not play back the IP address, this indicates that the VoIP Router failed to communicate with a DHCP server. Please check with your DHCP server or ISP.

ADSL PPPoE Settings

Note: Complete PPPoE settings should include: Select PPPoE (option 3 of [114](#)), PPPoE account ([121](#)) and PPPoE password ([122](#)).

Please contact your local Internet Service Provider (ISP) if you have any questions.

Select a PPPoE

After entering IVR mode, dial 114.

When voice prompt plays "Enter value," dial 3 (to select PPPoE).

PPPoE Account Settings

After entering IVR mode, dial 121.

When voice prompt plays "Enter value", enter the account number followed by "#".

Example: If the account is "87654321@hinet.net," please enter 08 07 06 05 04 03 02 01 71 48 49 5445 6072544560#.

Note: It is necessary to enter two digits for each alphabet/number; for example, you must enter "01" for "1" and "11" for "A". Using the web Interface to configure your PPPoE account details is recommended. Refer to the PPPoE Character Conversion Table on the next page for key mappings if you choose to use IVR setup.

PPPoE Password Setting

After entering IVR mode, dial 122.

When voice prompt plays "Enter value," enter the new password followed by "#".

Example: If the password is "3t2ixiae", please enter "03 60 02 49 64 49 41 45#".

Save Settings and Restart

To save settings, dial 509 (Save Settings). The system will save the settings. Please restart the system. Wait for about 40 seconds for the system to restart, then enter 101 to check whether the IP address was retained. If the system does not play back the IP address after dialing 101, this indicates that the VoIP Router currently is not connected to the Internet. Please check and make sure the cable connections, account numbers, and passwords are correct.

4-2-1 PPPoE Character Conversion Table:

The table below provides a list of PPPoE conversion codes. The first row (high-lighted) of each pair of the column lists the numbers, alphabets or symbols and the second row (high-lighted) of each pair of the column ("Input Key") represents the codes to be entered for the corresponding numbers, alphabets or symbols. For example, to enter "D-Link" according to the table below, enter: 148322495451

Numbers	Input Key	Upper Case Letters	Input Key	Lower Case Letters	Input Key	Symbols	Input Key
0	00	A	11	a	41	@	71
1	01	B	12	b	42	•	72
2	02	C	13	c	43	!	73
3	03	D	14	d	44	"	74
4	04	E	15	e	45	\$	75
5	05	F	16	f	46	%	76
6	06	G	17	g	47	&	77
7	07	H	18	h	48	'	78
8	08	I	19	i	49	(79
9	09	J	20	j	50)	80
		K	21	k	51	+	81
		L	22	l	52	,	82
		M	23	m	53	-	83
		N	24	n	54	/	84
		O	25	o	55	:	85
		P	26	p	56	;	86
		Q	27	q	57	<	87
		R	28	r	58	=	88
		S	29	s	59	>	89
		T	30	t	60	?	90
		U	31	u	61	[91
		V	32	v	62	\	92
		W	33	w	63]	93
		X	34	x	64	^	94
		Y	35	y	65	_	95
		Z	36	z	66	{	96
							97
						}	98

5. Dialing Principles

5-1 Dialing Options

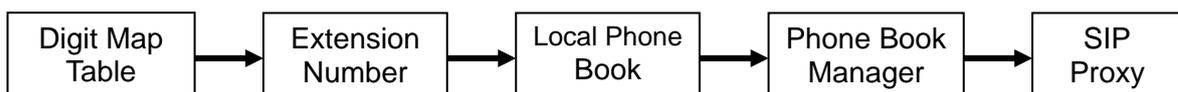
Dial the phone number which you want to call and press # to call out immediately. Note that if the “# (pound)” not dialed, the number will be called out after 4 seconds by default. The period between number dialed and call out is named “Inter Digits Timeout”. (Configurable from “DTMF and PULSE”, default=4 seconds, see page 43).

If the phone number matches the setting of the Digit Map, the phone number will be dialed out through the assigned interface automatically.

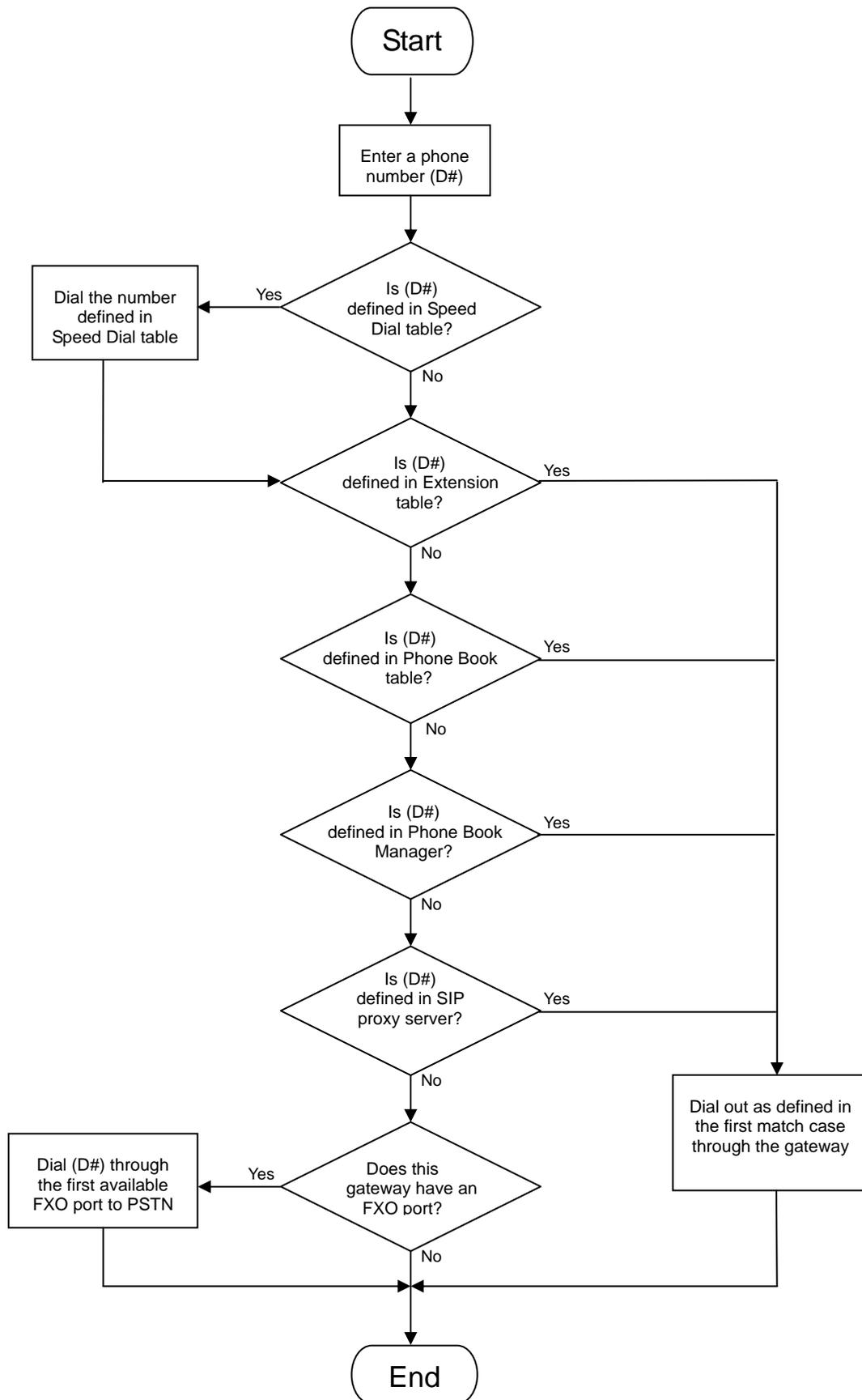
The phone number should contain at least 2 digits (not including * and #).

5-2 Dialed Number Processing Flow

To achieve maximum flexibility, the number dialed will be looked up in several tables defined by the VoIP Router. If no match is found from Digit Map Table, it will then look up the number from another table and to the registered SIP Proxy Server. The number look up flow is shown below:



A complete flow chart is shown on the next page.



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.111) / 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