



**DVG-N5412SP  
VoIP Wireless Router**

**User's Manual**

Version 1.1  
(Feb. 2012)

© 2011 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 Funkstörungen 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 caso, 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

<b>1. Introduction</b> .....	<b>4</b>
1-1 Product Overview .....	4
1-2 Hardware Description .....	5
<b>2. Getting Started</b> .....	<b>8</b>
<b>3. VoIP Router Web Configuration</b> .....	<b>16</b>
3-1 SETUP .....	16
3-1-1 Internet Setup.....	16
3-1-2 VoIP Setup .....	22
3-1-3 Wireless Setup .....	28
3-1-4 LAN Setup .....	39
3-1-5 USB Settings.....	42
3-1-6 Time and Date .....	43
3-2 ADVANCED .....	44
3-2-1 VoIP .....	44
3-2-2 Access Control .....	73
3-2-3 Firewall and DMZ .....	74
3-2-4 Advanced Wireless.....	79
3-2-5 Advanced Network .....	81
3-2-6 SNMP .....	86
3-3 MAINTENANCE.....	88
3-3-1 Device Management .....	88
3-3-2 Backup and Restore.....	89
3-3-3 Firmware Update.....	91
3-3-4 Dynamic DNS.....	92
3-3-5 Log Settings .....	93
3-3-6 Diagnostics.....	94
3-3-7 TR069.....	97
3-3-8 CDR.....	99
3-4 STATUS.....	100
3-4-1 Device Info .....	100
3-4-2 VoIP Status.....	101
3-4-3 LAN Client .....	102
3-4-4 Statistics .....	103
3-4-5 Routing Table .....	103
3-4-6 Logout .....	104
<b>4. Configuring the VoIP Router through IVR</b> .....	<b>105</b>
4-1 IVR (Interactive Voice Response) .....	105
4-1-1 IVR Functions Table: .....	107
4-2 IP Configuration Settings—Set the IP Configuration of the WAN Port.....	108
4-2-1 PPPoE Character Conversion Table:.....	110
<b>5. Dialing Principles</b> .....	<b>111</b>
5-1 Dialing Options .....	111
5-2 Number Translation .....	111
5-3 Routing .....	112
<b>6. Troubleshooting</b> .....	<b>114</b>
<b>Appendix</b> .....	<b>116</b>
Product Features .....	116

# 1. Introduction

---

## 1-1 Product Overview

The DVG-N5412SP 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-N5412SP 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-N5412SP is also an 802.11b/g/n 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-N5412SP 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, G.723.1 or iLBC 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 DVG-N5412SP can not register with SIP Server or can not get the IP address. A blinking light also indicates the DVG-N5412SP is attempting to connect with the Provisioning server. Once the service connects, the LED will turn off. The LED will light solid red if the self-test or boot-up fails.

**Reg.:** The Register LED will turn on and continuously working when DVG-N5412SP is connected to a VoIP service provider. The LED will flash if not connected to a service provider.

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

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

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

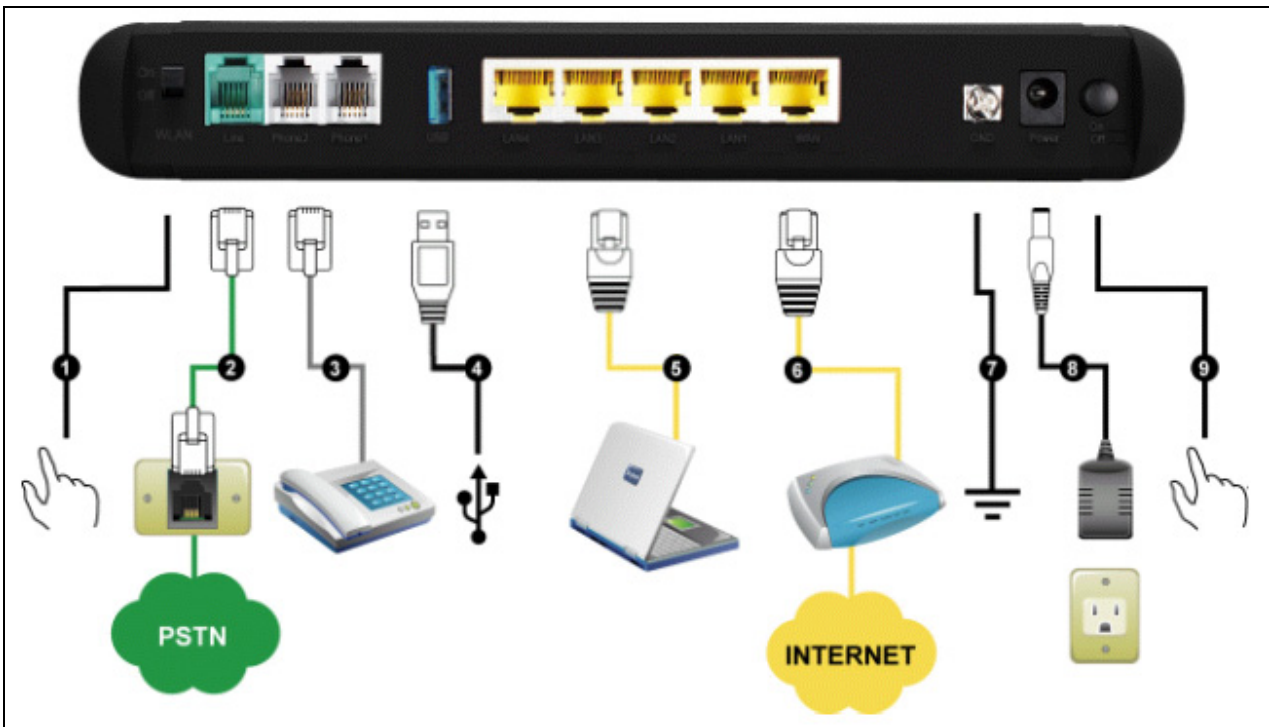
**USB:** This indicates that DVG-N5412SP detects a supported 3G modem dungle or a USB device.

**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.

**WPS:** Flashing in blue as DVG-N5412SP processing WPS-PBC wireless connecting progress.

Rear Panel



1. **WiFi Switch:** Turn on/off wireless LAN.
2. **Line:** Connect to your original telephone line on the wall jack with RJ-11 cable.
3. **Phone Port (1-2):** Connect to your phones using standard phone cabling (RJ-11).
4. **USB:** Connect to a 3G USB dongle or a printer.
5. **LAN:** Connect to your Ethernet enabled computers using Ethernet cabling.
6. **WAN:** Connect to your broadband modem using an Ethernet cable.
7. **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.
8. **Power Receptor:** Receptor for the provided power adapter.
9. **Power Switch:** Press down to turn-on DVG-N5412SP.

**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). (3) Stacking is forbidden. Doing so may damage your VoIP Router.



**WPS:** WPS button for wireless WPS-PBC setup method.

**Antenna:** Connect to a wireless network.

**Reset button:** Use to restore factory default settings.

**Use Reset Button to restore factory default settings:**

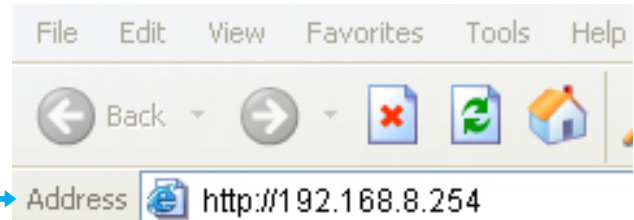
1. Press and hold the reset button for 5 seconds.
2. As Alarm indicator is blinking, please release the reset button. Factory settings will be restored.

## 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-N5412SP from WAN port.

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



**LOGIN**

Welcome to DVG-N5412SP Web Management

**Username :**

**Password :**

Remember my login info. on this computer

Click **Login** to enter Web Site.



**SETTING UP YOUR INTERNET**


There are two ways to set up your Internet connection: you can use the Web-based Internet Connection Setup Wizard, or you can manually configure the connection.

Please make sure you have your ISP's connection settings first if you choose to setup manually.

**INTERNET CONNECTION WIZARD**

You can use this wizard for assistance and quick connection of your new D-Link Router to the Internet. You will be presented with step-by-step instructions in order to get your Internet connection up and running. Click the button below to begin.

Click **Setup Wizard**.



Setup Wizard

**Note:** Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the router.

**WELCOME TO D-LINK SETUP WIZARD**

This wizard will guide you through a step-by-step process to configure your new D-Link router and connect to the Internet.

- **Step 1** : Change Device Login Password
- **Step 2** : Set Time and Date
- **Step 3** : Setup Internet Connection
- **Step 4** : Line Register
- **Step 5** : Setup Wireless Connection
- **Step 6** : Setup Wireless Security
- **Step 7** : Save and Restart

Click **Next**.



Next

Cancel

**STEP 1: CHANGE DEVICE LOGIN PASSWORD**

The factory default password of this router is admin. To help secure your network, D-Link recommends that you should choose a new password. If you do not wish to choose a new password now, just click Skip to continue. Click Next to proceed to next step.

**ADMIN**

New Password :

Confirm Password :

**USER**

New Password :

Confirm Password :

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 VoIP Router secure.

Click **Next**.

**STEP 2: SET TIME AND DATE**

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.

**TIME SETTINGS**

**Automatically synchronize with Internet time servers**

**First NTP time server :** ntp1.dlink.com

**Second NTP time server :** ntp.dlink.com.tw

**TIME CONFIGURATION**

**Current Router Time :** 2008/12/18 17:23:46

**Time Zone :** (GMT-12:00) International Date Line West

**Enable Daylight Saving**

**Daylight Saving Offset:** 0:00

**Daylight Saving Dates:**

	Month	Week	Day	Time
Start	Jan	1st	Sun	12 am
End	Jan	1st	Sun	12 am

Back Next Cancel

Enter a NTP server or use the default server. Select your time zone from the drop-down menu. Enable Daylight Saving for your local time if required.

Click **Next**.

**STEP 3: SETUP INTERNET CONNECTION**

Use this section to configure your Internet Connection type. If you are unsure of your connection method, please contact your Internet Service Provider.

**DHCP**  
 **Static IP**  
 **PPPoE**  
 **PPTP**  
 **3G USB Adapter**

Advanced Configuration

**WAN 1 SETTINGS**

**Hostname :**   
**Vendor Class ID :**   
**MTU :**   
**WAN 1 Domain Name Server :**   
**Domain Name Server ( Primary ) IP :**   
**Domain Name Server ( Secondary ) IP :**

**WAN LINK SPEED**

**WAN Link Speed :**

**VOIP**

**Connection :**

**MAC**

**Factory Default MAC Address :** 00:0B:2C:11:22:33   
**Your MAC Address :** 00:0A:79:60:17:28   
**Current MAC Address :**  (xx:xx:xx:xx:xx:xx)

Select your Internet connection type:

**DHCP** – Most Cable ISPs or if you are connecting the DVG-N5412SP 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.

**WAN1 Domain Name Server** – Select **Manual** to manually enter IP address of DNS or select **Auto** if DNS is assigned by ISP.

Click **Next**.

**STEP 4: LINE REGISTER**

The VoIP Router can invite register to a VoIP trunk gateway or register by each port of phone. Please contact your ITSP.

**SOFT SWITCH SETTING**

Enable Support of SIP Proxy Server / Soft Switch  
ITSP Name :

**PHONE 1 - FXS**

Number :   
 Register  
 Invite with ID / Account  
User ID / Account :   
Password :   
Confirm Password :

**PHONE 2 - FXS**

Number :   
 Register  
 Invite with ID / Account  
User ID / Account :   
Password :   
Confirm Password :

**SIP PROXY SERVER**

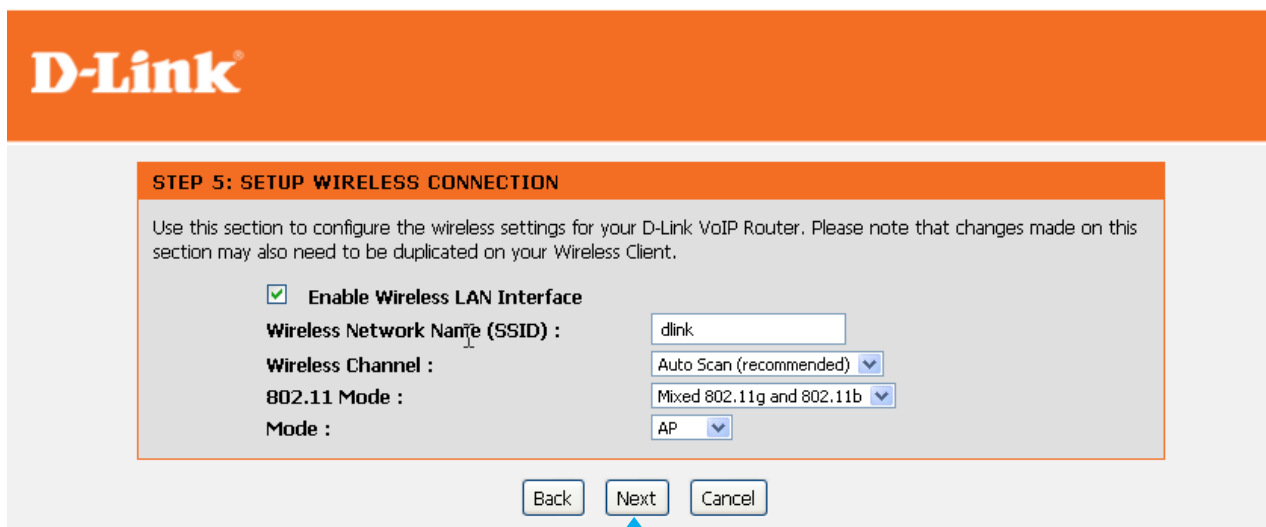
Proxy Server IP / Domain :   
Proxy Server Port :  (1-65535)  
Proxy Server Realm :   
TTL (Registration interval) :  (10-7200s)  
SIP Domain :   
 Use Domain to Register

**OUTBOUND PROXY SUPPORT**

Outbound Proxy Support  
Outbound Proxy IP / Domain :   
Outbound Proxy Port :  (1 - 65535)

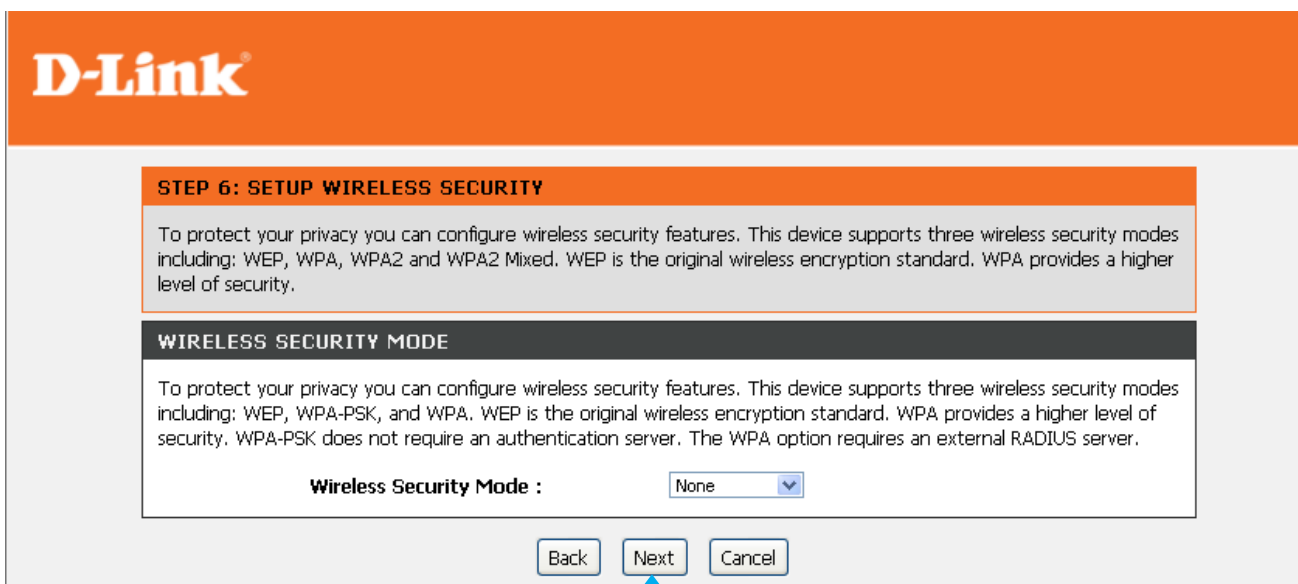
Register to the SIP Proxy Server by clicking **Enable support of SIP Proxy Server**. Enter **Proxy Server IP/Domain** and **Port**. **Outbound Proxy Support** is optional. To register, please click on the **Outbound Proxy Support** box and enter **Outbound Proxy IP/Domain** and **Port** in it. Registration by phone line: Enter **Number**, **User ID/Account** and **Password** supplied by your ITSP. Check on the **Register** 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 clear wireless channel. Select the 802.11 Mode of your network which can work in different speed of wireless connection.

Click **Next**.



Select **Security Mode** for your wireless network.

Click **Next**.



**STEP 7: SAVE AND RESTART**

The last step is to save changes and restart Gateway to make new settings effective. Save and Restart takes about 40 seconds. The login page will show in about 1 minute.

**SETUP SUMMARY**

Below is a detailed summary of your settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

<b>Time Settings :</b>	Enable
<b>Protocol :</b>	DHCP
<b>Proxy Server IP / Domain :</b>	192.168.1.1
<b>Proxy Server Port :</b>	5060
<b>SIP Domain :</b>	
<b>Phone 1 - FXS Number :</b>	701
<b>Phone 2 - FXS Number :</b>	702
<b>Wireless Network Name (SSID) :</b>	dlink
<b>Wireless Channel :</b>	Auto Scan (recommended)
<b>802.11 Mode :</b>	Mixed 802.11g and 802.11b
<b>Wireless Security Mode :</b>	None

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-N5412SP.

Click **Restart**.

# 3. VoIP Router Web Configuration

## 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. 3G USB Adapter

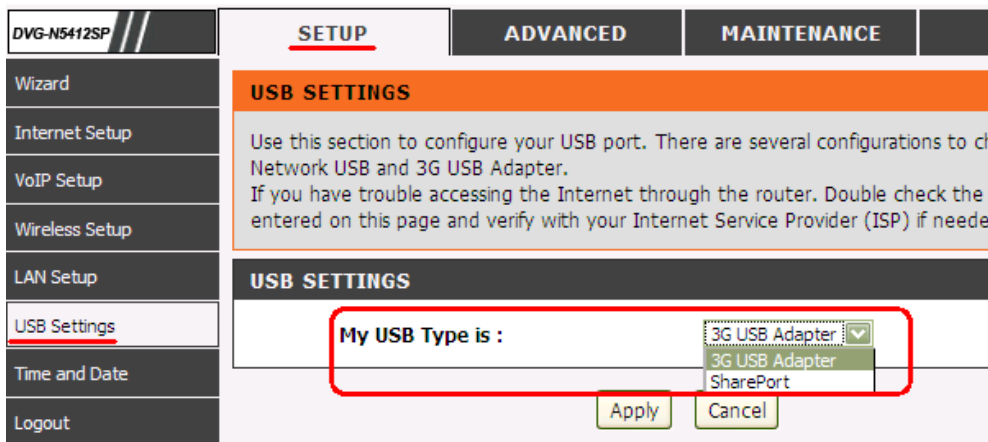
Methods for using DHCP and PPPoE for obtaining an IP address may vary. If you are not familiar with creating a network connection, please contact your local ISP.

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 **Backup and Restore** from the left menu. Tick **Save Settings** and **Restart**, and 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.

**Note:** 3G USB Adapter mode can't execute with "Share port" at the same time. If you would like USB port connected with a 3G USB dungle, please change USB type to be "3G USB Adapter".





SETUP → Internet Setup

**WAN**

Use this section to configure your Internet Connection type. If you are unsure of your connection method, please contact your Internet Service Provider.

**DHCP**  
 **Static IP**  
 **PPPoE**  
 **PPTP**  
 **3G USB Adapter**

SETUP → Internet Setup

**WAN 1 SETTINGS**

**Hostname :**   
**Vendor Class ID :**   
**MTU :**   
**WAN 1 Domain Name Server :**   
**Domain Name Server ( Primary ) IP :**   
**Domain Name Server ( Secondary ) IP :**

**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

**WAN 1 SETTINGS**

**IP address :**   
**Subnet mask :**   
**Default Gateway IP :**   
**MTU :**   
**Domain Name Server ( Primary ) IP :**   
**Domain Name Server ( Secondary ) IP :**

**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

WAN 1 SETTINGS	
PPPoE Account :	<input type="text"/>
PPPoE Password :	<input type="password"/>
Confirm Password :	<input type="password"/>
PPPoE Service Name :	<input type="text"/> ( Optional )
MTU :	<input type="text" value="1492"/>
WAN 1 Domain Name Server :	<input type="text" value="Manual"/> ▼
Domain Name Server ( Primary ) IP :	<input type="text" value="168.95.1.1"/>
Domain Name Server ( Secondary ) IP :	<input type="text"/>

**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

WAN 1 SETTINGS	
PPTP Server :	<input type="text"/>
PPTP ID :	<input type="text"/>
PPTP Password :	<input type="password"/>
Confirm Password :	<input type="password"/>
MTU :	<input type="text" value="1452"/>
WAN 1 Domain Name Server :	<input type="text" value="Manual"/> ▼
Domain Name Server ( Primary ) IP :	<input type="text" value="168.95.1.1"/>
Domain Name Server ( Secondary ) IP :	<input type="text"/>
Second Access IP Type :	<input type="text" value="Dynamic IP"/> ▼
Hostname :	<input type="text"/>
Vendor Class ID :	<input type="text"/>

**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

WAN 1 SETTINGS	
Country	-- None --
ISP	-- None --
Username :	<input type="text"/>
Password :	<input type="text"/>
Dial Number :	<input type="text"/>
Authentication Protocol :	Auto(PAP+CHAP)
APN :	<input type="text"/>
MTU :	1492

**3G USB Adapter:** 3G/3.5G WISP. Enter Username, Password, Dial Number and APN to connect to Internet via 3G/3.5G WISP. Users could also select a configured WISP from the list and DVG-N5412SP will fill necessary parameter automatically.

SETUP → Internet Setup

WAN LINK SPEED	
WAN Link Speed :	Auto

**WAN Link Speed:** Select WAN port link speed.

SETUP → Internet Setup

VOIP	
Connection :	WAN1

**VoIP Connection Interface:** Select a WAN interface for DVG-N5412SP VoIP traffic.

SETUP → Internet Setup

MAC		
Factory Default MAC Address :	00:17:9A:98:AF:6C	Restore
Your MAC Address :	00:0A:79:60:17:28	Clone
Current MAC Address :	<input 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.

SETUP → Internet Setup

**WAN**

Use this section to configure your Internet Connection type. If you are unsure of your connection method, please contact your Internet Service Provider.

- DHCP**
- Static IP**
- PPPoE**
- PPTP**
- 3G USB Adapter**

Advanced Configuration

Click "Advanced Configuration" for 802.11q/p VLAN tag or dual WAN access configuration.

WAN SETTINGS				
	Enable	Type	<input type="checkbox"/> Enable VLAN Tagging	
			VLAN ID	Priority
WAN 1	Default Route	DHCP	1	0
WAN 2	<input type="checkbox"/>	DHCP	3	7

VLAN is optional. It works with the Router or Switch that supports VLAN tag. By adding VLAN tag in packets may improve efficiency of voice traffic performance and security.

**Enable VLAN Tagging:** It is to tag the packets for VLAN Router or Switch identifying.

**VLAN ID:** It is to assign uniquely a user-defined ID to each packet.

**Priority:** It is the proprietary to VLAN Router or Switch.

**Note:** Please do not change anything here unless requested 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

<b>Enable Support of SIP Proxy Server / Soft Switch</b>	
<input type="checkbox"/>	<b>Enable Support of SIP Proxy Server / Soft Switch</b>
<b>ITSP Name :</b>	<input type="text"/>

**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:**

<b>FXS REPRESENTATIVE NUMBER</b>	
<b>Number :</b>	<input type="text" value="21234567"/>
<input checked="" type="checkbox"/> <b>Register</b>	
<b>User ID / Account :</b>	<input type="text"/>
<b>Password :</b>	<input type="password" value="....."/>
<b>Confirm Password :</b>	<input type="password" value="....."/>

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

SIP PROXY SERVER	
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"/> (10-7200s)
SIP Domain :	<input type="text"/>
<input type="checkbox"/> Use Domain to Register	
Bind Proxy Interval for NAT :	<input type="text" value="0"/> (0-1800s)
<input type="checkbox"/> Initial Unregister	
<input type="checkbox"/> Unregister All Contacts	
<input type="checkbox"/> Keep SIP Auth	
<input type="checkbox"/> Support Message Waiting Indication (MWI)	
MWI Subscribe Interval :	<input type="text" value="7200"/> (0=disable, 60-86400s)

**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.

**Unregister All Contacts:** DVG-N5412SP will fill "\*" (a star) in Contact field in un-register request to release all registered accounts in this DVG-N5412SP.

**Keep SIP Auth:** DVG-N5412SP keeps the last register SIP MD5 authentication information and re-use it for next register request.

**Support Message Waiting Indication (MWI):** It is used to enable/disable Message Waiting Indication. It is available only when Voice Mail Service is available from the VoIP Service Provider.

**MWI Subscribe Interval:** It is used to set the subscribe time for the VoIP Router to check the voice mail.

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

**NUMBER TRANSLATION**

VoIP Dial-Out defined here overrides "Digit Map"

Copy From :

Scan Code	VoIP Dial-out

The rule of dialing of inviting to VoIP Service Providers may vary. That is, you have to configure different Digit Map for different VoIP Service Providers. In this filed, you can configure individual dialing plan for each VoIP Service Provider. 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 VoIP Service Provider you can refer to **Digit Map** page for general settings.

If Server 2 is global VoIP Service Provider (VoIP STUN, free to dial to some cities free charge) you can set individual dialing plan for VoIP STUN in **Number Translation** field. **Scan Code** can be your dialing custom, and **VoIP Dial-out** is the number on the basis of the dialing rule needed by VoIP STUN. Its dialing rule is Country code + Area Code + phone number. When you make calls to Taipei through VoIP STUN, you don't change the dialing custom, just dial 02xxxxxxx, and the system will change the number from 02xxxxxxx to 8862xxxxxxx. The same rule is for #2. When you make calls to UK via VoIP STUN, you'll dial 00244xxxxx, and the system will change it to 44xxxxx.

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 a VoIP Service Provider in UK, you can set individual dialing plan in **Number Translation** field. As you make calls to UK through this VoIP Service Provider, "Country code" should be removed and plus "0" by the system. 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 :**

**Mode :**

**Network Type :**

**Channel Width :**

**Broadcast SSID**

**Enable WMM**

**Enable Universal Repeater Mode  
(Acting as AP and client simultaneously)**

**SSID of Extended Interface :**

**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.

**802.11n only** - Allow all 802.11n compliant wireless devices to associate with the wireless AP.

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

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

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

**Access Mode:** DVG-N5412SP has ability to serve as two operating modes in wireless network separately.

**AP:** As a wireless AP that allows wireless-equipped stations to communicate with a wired network and the other wireless network for Internet access and resources sharing.

**Client:** As a wireless client, you are allowed to access Internet via an Access Point in infrastructure mode or build a group of wireless network for files and printer sharing in ad-hoc Mode. **Under Wireless Client Mode, Bridge Mode is not available for the VoIP Router**

**Network Type:** Select network type for Access Client Mode.

**Infrastructure:** Connect to another wireless AP or WISP.

**Ad hoc:** Connect to another wireless Ad hoc device. Usually it is used for peer-to-peer connect mode.

**Channel Width:** Wireless channel width for 802.11n. Select 40 MH for higher speed.

**Broadcast SSID:** Broad AP's SSID for convent usage. To hid SSID for more security.

**Enable WMM:** Wi-Fi Multimedia. It provides higher priority for multimedia stream to get better quality.

**Enable Universal Repeat Mode:** Set DVG-N5412SP to be wireless repeat mode. Please fill the same SSID as the root AP in "SSID of Extended Interface".

SETUP -> Wireless Setup -> Wireless Basic

MULTIPLE AP					
Enable	802.11 Mode	SSID	Broadcast SSID	Enable WMM	Access
<input type="checkbox"/>	ngb ▾	SSID-1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN+WAN ▾
<input type="checkbox"/>	ngb ▾	SSID-2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN+WAN ▾
<input type="checkbox"/>	ngb ▾	SSID-3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN+WAN ▾
<input type="checkbox"/>	ngb ▾	SSID-4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN+WAN ▾

**Multiple AP:** It is used for different level of clients. Such as different departments or guests. And you could assign different password for each SSID.

### 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**

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA, WPA2 and WPA2 Mixed. WEP is the original wireless encryption standard. WPA provides a higher level of security.

Select SSID :

**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.

Wireless Security Mode :

**Select SSID:** Select an SSID to configure wireless security mechanism.

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

### 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 :**

**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.



SETUP -> Wireless Setup -> Site Survey

WIRELESS SITE SURVEY						
SSID	BSSID	Channel	Type	Encrypt	Signal	Select
802.11-SSID	00:00:00:15:7a:34	1 (B+G)	AP	no	58	<input checked="" type="radio"/>
802.11	00:00:00:12:c5:a0	9 (B+G)	AP	WPA-PSK	18	<input type="radio"/>
802.11-AirStation	00:00:00:bc:95:e6	11 (B+G)	AP	WEP	13	<input type="radio"/>
802.11a	00:00:00:cb:fa:73	1 (B+G)	AP	WPA2-PSK	12	<input type="radio"/>

**Site Survey**

When wireless client mode is enabled, click the Refresh button to display any Access Point on your wireless network so that a wireless client can obtain SSID, BSSID, Channel, Type, Encryption, and Signal through scanning using this Site Survey tools.

**Example:**

1. Select the Wireless AP and click Accept bottom.

WIRELESS SITE SURVEY						
SSID	BSSID	Channel	Type	Encrypt	Signal	Select
802.11-SSID	00:00:00:15:7a:34	1 (B+G)	AP	no	58	<input checked="" type="radio"/>
802.11	00:00:00:12:c5:a0	9 (B+G)	AP	WPA-PSK	18	<input type="radio"/>
802.11-AirStation	00:00:00:bc:95:e6	11 (B+G)	AP	WEP	13	<input type="radio"/>
802.11a	00:00:00:cb:fa:73	1 (B+G)	AP	WPA2-PSK	12	<input type="radio"/>

2. Enter the password of the Wireless AP and click Apply bottom.

**PRE-SHARED KEY**

Pre-Shared Key Format :

Pre-Shared Key :

3. Save the configuration and restart DVG-N5412SP.

**SYSTEM -- SAVE AND REBOOT**

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

**Save All Settings**

### 3-1-3-3 WPS

SETUP -> Wireless Setup -> WPS

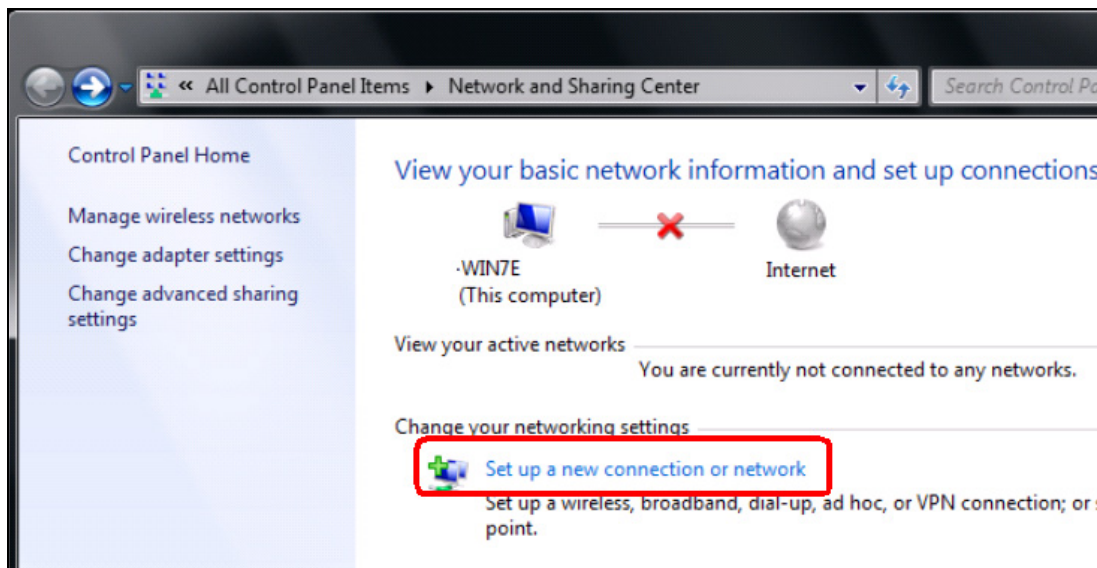


It allows users establish wireless connect between DVG-N5412SP and computers via WPS(Wireless Protect Setup) method.

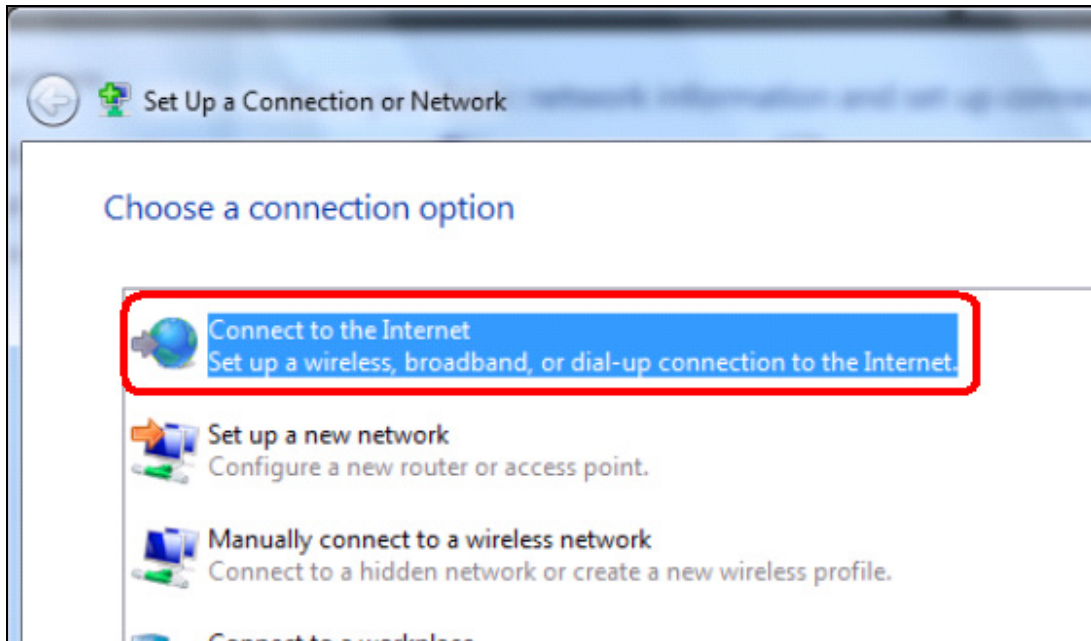
#### Example for setting Wireseess profile via WPS method on Windows 7.

Enter [Network and Sharing Center]

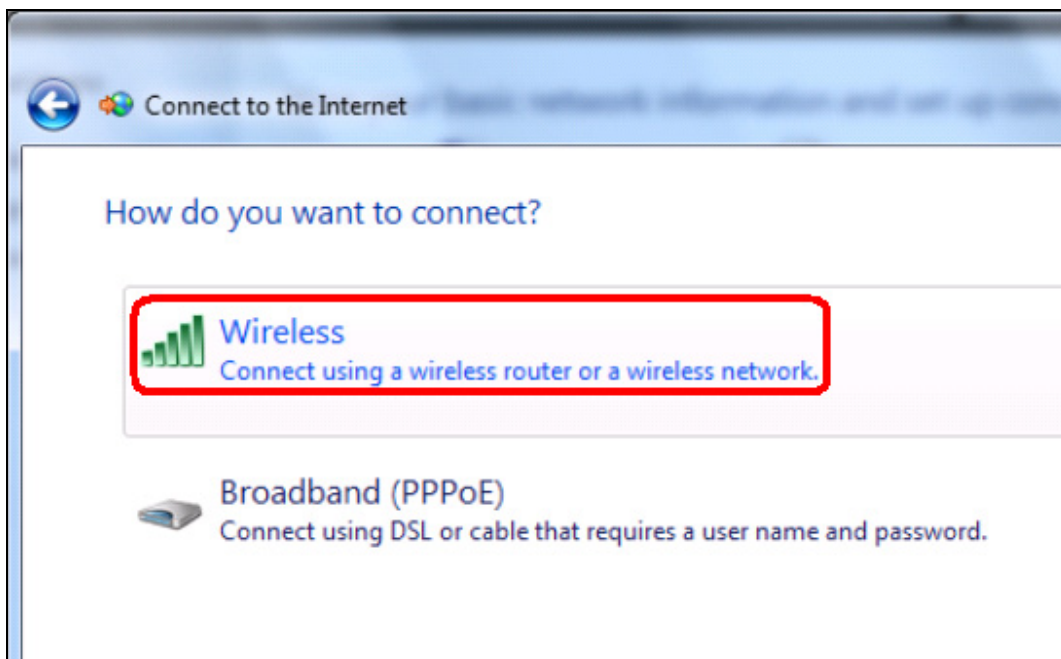
Click [Set up a new connection or network]



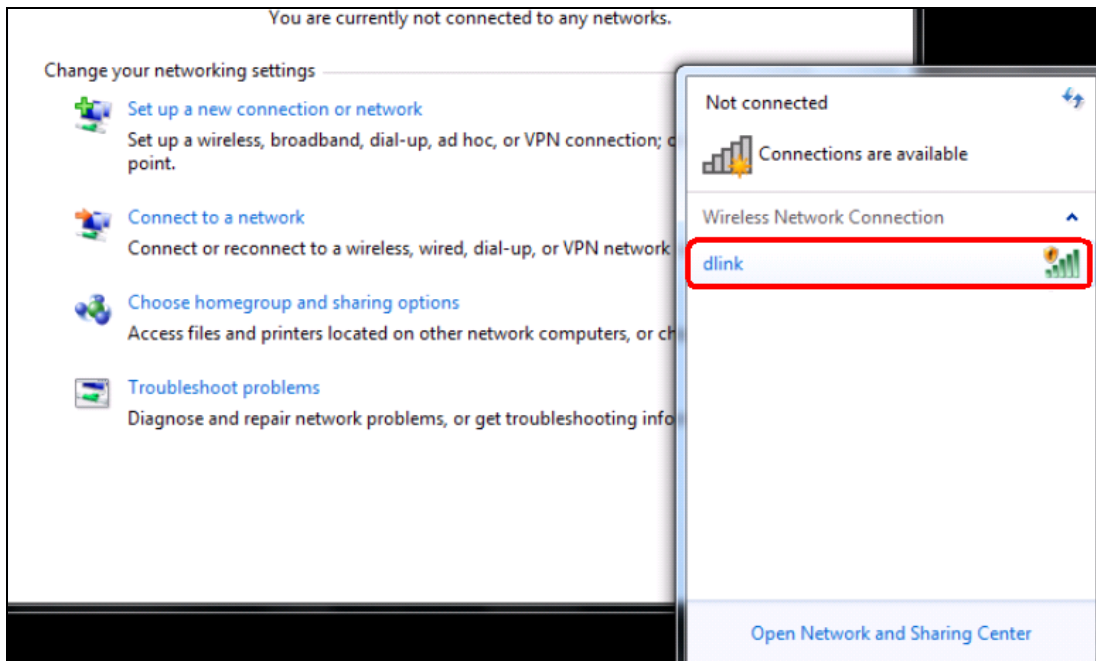
Click [Connect to the Internet]



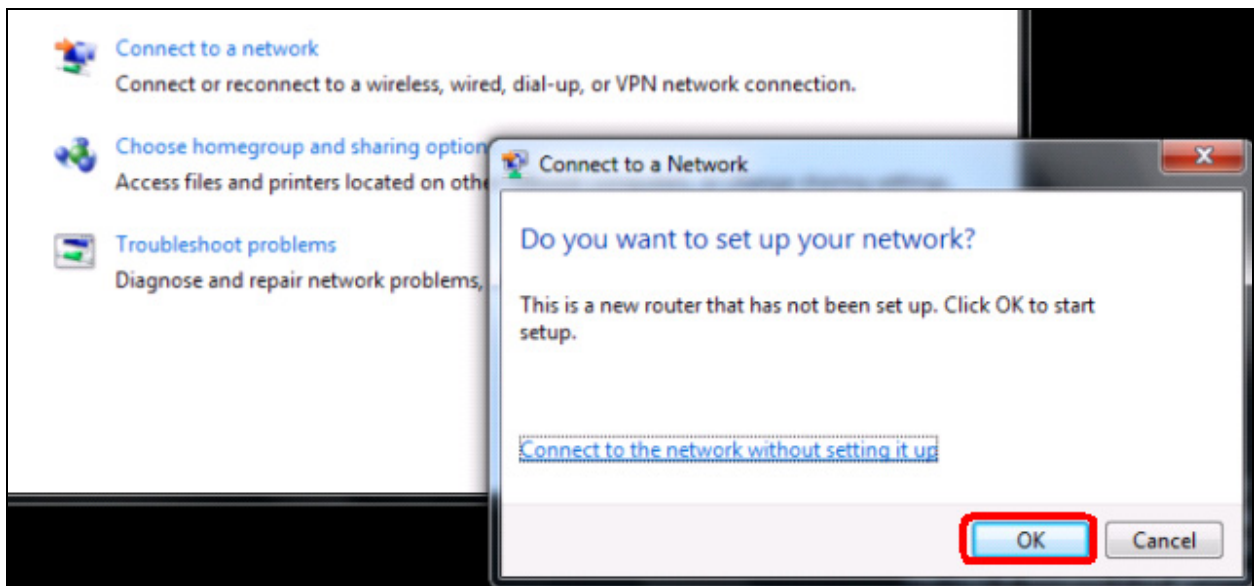
Click [Wireless]



Select a Wireless AP.

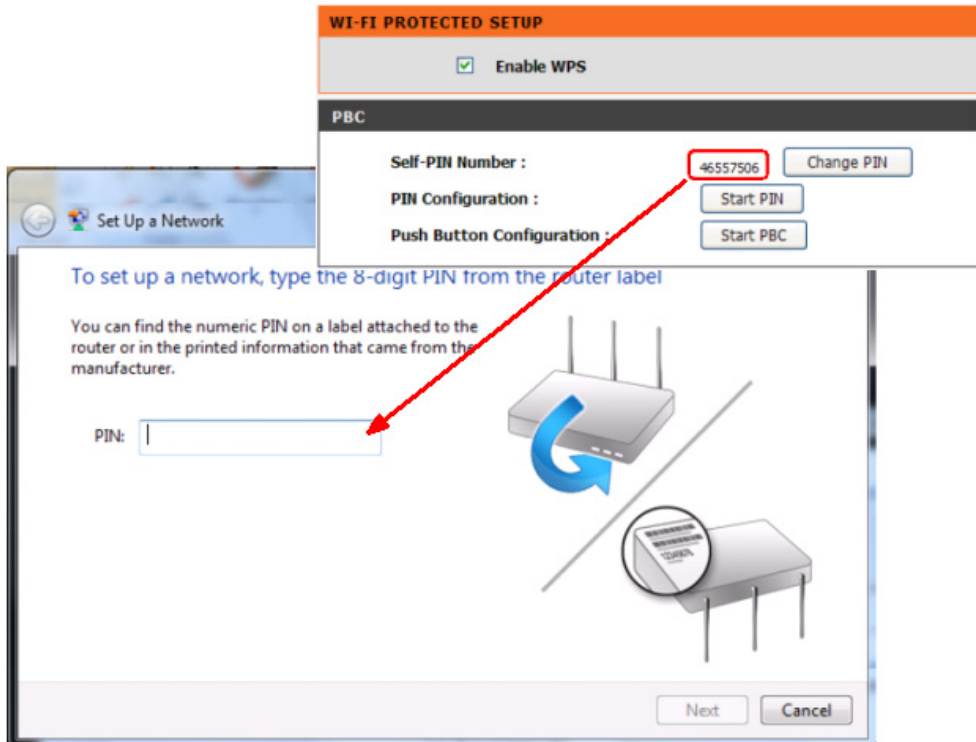


Click [OK] to start setup.

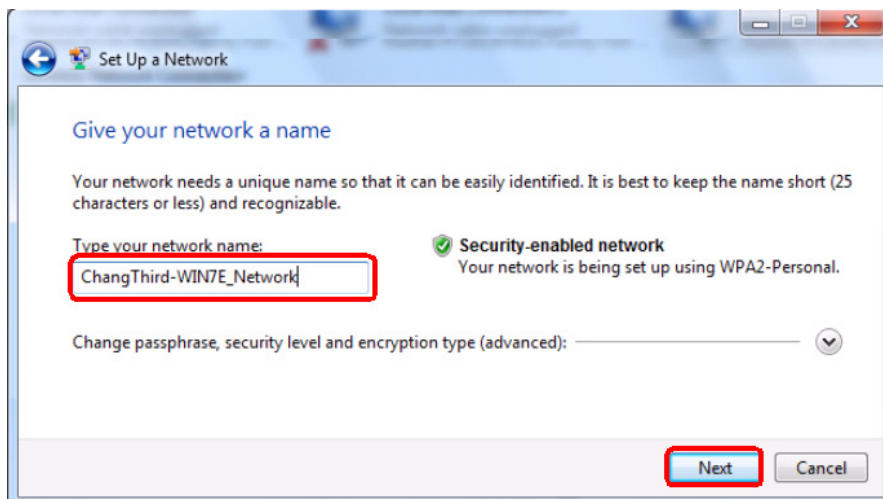


Enter the 8-digit PIN from DVG-N5412SP label then click Next.

**Note:** If you have ever click “Change PIN” button on the WEB UI of DVG-N5412SP, please enter the PIN number displayed on WEB GUI.



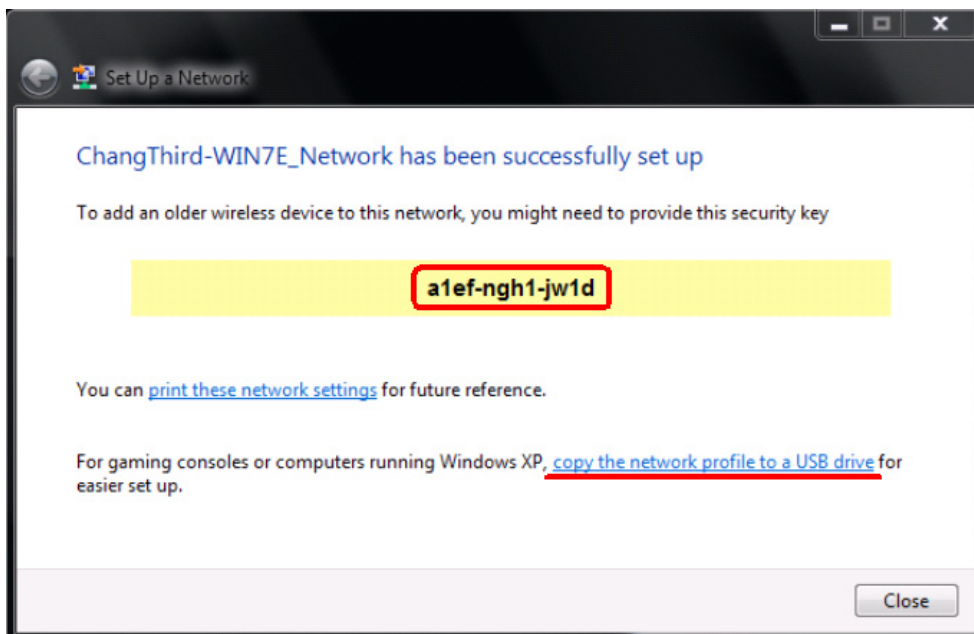
Type network name(SSID) then click Next.



Wait for Windows 7 setting up wireless network.



Configuration finished, you could connect to DVG-N5412SP at present. You could also print security key of save this profile for another computer to add this wireless network manually.



**Note:** DVG-N5412SP supports WPS work with WindowsR Vista and Windows 7 only.

### 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.

<b>LAN Port Address :</b>	<input type="text" value="192.168.8.254"/>
<b>Subnet mask :</b>	<input type="text" value="255.255.255.0"/>

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

**Subnet Make:** Enter the subnet mask for DHCP clients.

SETUP → LAN Setup

DHCP SERVER

**Enable DHCP Server**

**IP Pool Starting Address :**

**IP Pool Ending Address :**

**IP Pool Uses Other Default Gateway**

**IP Pool Default Gateway :**

**IP Pool Subnet mask :**

**Lease Time :**  ( 1 - 9999 hours)

**Domain Name Server Assignment :**  Auto  Manual

**Domain Name Server (Primary) IP :**

**Domain Name Server (Secondary) IP :**

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

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

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

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

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

**IP Pool Subnet mask:** Enter the new subnet mask.

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

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

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



SETUP → LAN Setup

LAN PORT CONTROL					
Port	Enable Port	Incoming Rate Limit	Outgoing Rate Limit	NAT/Bridge	VLAN ID
LAN Port 1	<input checked="" type="checkbox"/>	Full	Full	NAT	0
LAN Port 2	<input checked="" type="checkbox"/>	Full	Full	NAT	0
LAN Port 3	<input checked="" type="checkbox"/>	Full	Full	NAT	0
LAN Port 4	<input checked="" type="checkbox"/>	Full	Full	NAT	0

**Enable Port:** It is to active/des-active LAN port physical connection.

**Incoming Rate Limit:** Set the incoming (from LAN to WAN) rate limit of a specific LAN port (can not exceed the real downstream bandwidth).

**Outgoing Rate Limit:** Set the outgoing (from WAN to LAN) rate limit of a specific LAN port (can not exceed the real upstream bandwidth).

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

**Note:** If you set a LAN port to be bridge mode that the LAN port will be bundled with WAN. If you would like to connect to DVG-N5412SP at the bridged LAN port you must enter WAN port IP.

**VLAN ID:** Assign a VLAN ID for DVG-N5412SP to transit traffic through-out at WAN port for WAN-LAN bridge mode. The packets are un-tagged at LAN port and added tag at WAN port.

**Note:** It is not allowed to change VLAN ID for NAT mode LAN ports. The VLAN ID of NAT LAN ports are bundled with WAN 1 which assigned at Internet Setting page. The packets are un-tagged at LAN port and added tag at WAN port.

### 3-1-5 USB Settings

SETUP → USB Settings

**USB SETTINGS**

Use this section to configure your USB port. There are several configurations to choose from: Network USB and 3G USB Adapter.  
If you have trouble accessing the Internet through the router. Double check the settings you entered on this page and verify with your Internet Service Provider (ISP) if needed.

**USB SETTINGS**

**My USB Type is :**

**USB Type:** Select a USB device type.

**3G USB Adapter:** It allows you plug in a 3G dungle dial to WISP for Internet access.

**Share Port:** Connect USB device such as a printer, scanner or MFP(Multifunction Printer) to DVG and share it at Local Area Network. Please refer to **Share Port User Manual** for USB Share Port application.

**Note:** USB Share port is optional for particular area and users may need to pay additional royalty to get this feature.

### 3-1-6 Time and Date

SETUP → Time and Date

**TIME AND DATE**

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.

**TIME SERVER**

**Automatically synchronize with Internet time servers**

**First NTP time server :**

**Second NTP time server :**

**TIME CONFIGURATION**

**Current Router Time :** 2000/ 1/ 1 08:13:57

**Time Zone :**

**Enable Daylight Saving**

**Daylight Saving Offset :**

	Month	Week	Day	Time
<b>Daylight Saving Dates :</b> Start	<input type="text" value="Jan"/>	<input type="text" value="1st"/>	<input type="text" value="Sun"/>	<input type="text" value="12 am"/>
End	<input type="text" value="Jan"/>	<input type="text" value="1st"/>	<input type="text" value="Sun"/>	<input type="text" value="12 am"/>

**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.

**Enable Daylight Saving:** To enable/disable daylight saving time.

**Daylight Saving Offset:** Set the current time zone offset for your location.

**Daylight Saving Dates:** Set the start and end dates for daylight saving time.

## 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 :** Allow ▼

Apply
Cancel

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 :**

**Send Caller ID After The First Ring**

**FSK Caller ID Type :**

**FXS Caller ID Generation:** Select **DTMF**, **FSK** or **FSK+Type II** Caller ID to enable the caller ID display function on FXS port. When enabled, the caller's phone number will be displayed on your phone set when the call comes through. FSK+Type II Caller ID is used for displaying the caller ID when receiving call waiting calls.

**Note:** Make sure that your phone set supports Type II Caller ID before you select it.

**Send Caller ID After The First Ring:** Check the box to send the caller ID after the first ring by FXS port; otherwise, the caller ID is sent before the first ring.

**FSK Caller ID Type:** Either Bellcore, ETSI or NTT 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	
<input type="checkbox"/> Unconditional Forward :	<input type="text"/>
<input type="checkbox"/> Busy Forward :	<input type="text"/>
LINE1 - FXS	
<input type="checkbox"/> Do Not Disturb	
<input type="checkbox"/> Unconditional Forward :	<input type="text"/>
<input type="checkbox"/> Busy Forward :	<input type="text"/>
<input type="checkbox"/> No Answer Forward :	After( 10 - 60 ) <input type="text" value="20"/> s <input type="text"/>
<input type="checkbox"/> Call Hold	
<input checked="" type="checkbox"/> Call Transfer	
<input checked="" type="checkbox"/> Call Waiting	
<input checked="" type="checkbox"/> Three-Way Calling / Service ID :	<input type="text"/>
<input checked="" type="checkbox"/> Local Mixer	

**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.

**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.

**Call Waiting:** Check the box to accept incoming call while talking.

**Three-Way Calling / Service ID:** It is used for Nortel Style 3-Way conference. Please enter correct service ID assigned on the SoftSwitch or IPPBX.

**Local Mixer:** Enable 3-Way conference mixer on DVG. This option is conflict to “**Three-Way Calling / Service ID**”, don't enable these two options simultaneously.

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

ADVANCED → VoIP → Calling Features

CALL FEATURE CODE		
<input checked="" type="checkbox"/> <b>Enable Call Feature Code</b>		
	Enable	Disable
Unconditional Forward (FXS Representative Number)	<input type="text" value="*78"/>	<input type="text" value="#78"/>
Do Not Disturb	<input type="text" value="*74"/>	<input type="text" value="#74"/>
Unconditional Forward	<input type="text" value="*77"/>	<input type="text" value="#77"/>
Busy Forward	<input type="text" value="*76"/>	<input type="text" value="#76"/>
No Answer Forward	<input type="text" value="*75"/>	<input type="text" value="#75"/>
Call Hold	<input type="text" value="*70"/>	<input type="text" value="#70"/>
Call Transfer	<input type="text" value="*71"/>	<input type="text" value="#71"/>
Call Waiting	<input type="text" value="*72"/>	<input type="text" value="#72"/>
Local Mixer	<input type="text" value="*73"/>	<input type="text" value="#73"/>
Call Pickup	<input type="text" value="*40"/>	
Call Back on Busy	<input type="text" value="*41"/>	<input type="text" value="#41"/>
Blind Transfer	<input type="text" value="*50"/>	

**Enable Call Feature Code:** Check the box to enable/disable some call feature codes through a phone set.

**Call pickup:** Allow one to pick up someone else's telephone call.

**Call Back on Busy:** Your phone will ring back the last number that called you.

**Blink Transfer:** Blind Transfer involves passing a call without notifying the recipient.

**Call Feature Code Instructions (example):**

1. If you would like to enable **DND** function of FXS, pick up the phone connected to FXS and dial “\*74#”.
2. If you would like to enable **Unconditional Forward** of FXS and assign the number, pick up the phone and dial “\*77 0912345678#”. 0912345678 is the number which the incoming call is forwarded to.
3. If you would disable **Unconditional Forward** of FXS, pick up the phone and dial “#77#”.

**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 Service Provider. 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 presses Flash to start the conference call.

**Or**

4. Phone1 dials to Phone2, Phone2 answers the call.
5. Phone1 presses Flash then calls Phone3 (Phone2 is on hold) and Phone3 answers the call.
6. Phone1 presses Flash and dial 3 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 SETTINGS**

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

**Jitter Buffer :**  (60 - 1200ms)

**Silence Detection / Suppression**

**Echo Cancellation**

Enable	Codec	Codec Priority	Type	Packet Interval (ms)	Approximate Bandwidth Required (kbps)
<input checked="" type="checkbox"/>	G.711 u-law	<input type="text" value="4"/>		<input type="text" value="20"/>	85.6
<input checked="" type="checkbox"/>	G.711 a-law	<input type="text" value="5"/>		<input type="text" value="20"/>	85.6
<input checked="" type="checkbox"/>	G.723.1	<input type="text" value="2"/>	<input type="text" value="G.723.16.3k"/>	<input type="text" value="30"/>	20.8
<input checked="" type="checkbox"/>	G.726 32K	<input type="text" value="3"/>	<input type="text" value="98"/>	<input type="text" value="20"/>	53.6
<input type="checkbox"/>	G.729	<input type="text" value="1"/>		<input type="text" value="20"/>	29.6
<input type="checkbox"/>	iLBC	<input type="text" value="6"/>	<input type="text" value="99"/>	<input type="text" value="30"/>	27.7

**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.

**RTCP-XR:** Enable RTCP-XR(RFC-3611) to report network quality.

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

**Codec Priority:** The priority of code for communication.

**Type:** To set dynamic payload types of codec.

**Packet Interval:** Select the frame size of voice package from different codec. It defines the time interval for the VoIP Gateway 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:** Define the call process tones for the DVG-N5412SP generates.

ADVANCED → VoIP → CPT / Cadence

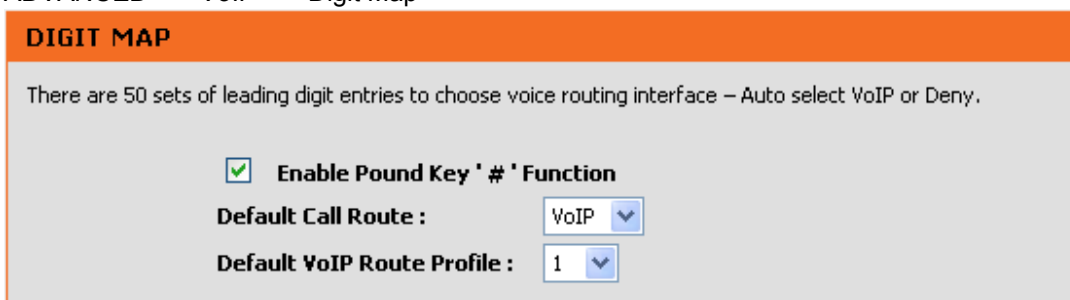
FXS Ring Cadence Settings						Default
Range	ON_1 [250 - 8000 ms]	OFF_1 [250 - 8000 ms]	ON_2 [0, 250 - 8000 ms]	OFF_2 [0, 250 - 8000 ms]	ON_3 [0, 250 - 8000 ms]	OFF_3 [0, 250 - 8000 ms]
1	1000	2000	0	0	0	0

**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

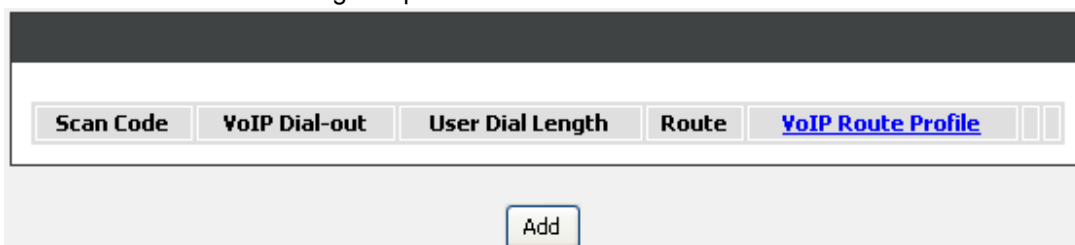


**Enable Pound Key '#' Function:** Check the box to treat '#' as a digit and send out with other numbers when dialing. If you un-check the box and '#' is pressed after dialing, it will speed up the phone number detection of the VoIP Router.

**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:** 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 **VoIP Route Profile** to set the priority of VoIP Route Profile.

ADVANCED → VoIP → Digit Map → VoIP Route Profile

VOIP ROUTE PROFILE

Please select your VoIP priority route by phone book or Proxy server.

	Description	1	2	3	4	
1	LocalServer	Server 1	None	None	None	
2	LongDistance	Server 2	Server 1	None	None	
3	InternationalCall	Server 3	Server 2	Server 1	None	
4	VoIPSTUN	Server 2	None	None	None	
5	UKServer	Server 3	None	None	None	
6		None	None	None	None	
7		None	None	None	None	
8		None	None	None	None	
9		None	None	None	None	
10		None	None	None	None	

There are 10 VoIP route profiles. Each VoIP route profile provides four routes to select. **Server 1, Server 2, Server 3, Phone Book** and **None** can be selected for each route.

**Example of VoIP Route Profile:**

Assume that VoIP TA is registered to three servers.

Server 1 is local VoIP Service Provider.











Server 2 is VoIP STUN (free to dial to some cities without charge).

Server 3 is VSP in UK.



**Example 1 – Single VoIP route,**

The number translation of each server is blank.

The VoIP route profile appears like:

	Description	1	2	3	4	
1	LocalServer	Server 1	None	None	None	
2		None	None	None	None	
3		None	None	None	None	
4		None	None	None	None	
5		None	None	None	None	
6		None	None	None	None	
7		None	None	None	None	
8		None	None	None	None	
9		None	None	None	None	
10		None	None	None	None	

Digit Map Table appears like:

Scan Code	VoIP Dial-out	PSTN Dial-out	User Dial Length	Route	VoIP Route Profile		
09%			10	Auto (VoIP first)	1		

As you dial the phone numbers starting with 09, like 0912345678, the call will only go through Server 1 (local VSP). If Sever1 is failed, the call will be diverted to PSTN.

**Example 2 – Multiple Route,**

The number translation of Server 1 is blank, and the number translation of Server 2 appears like:

**NUMBER TRANSLATION**

VoIP Dial-Out defined here overrides "Digit Map"

Copy From : None

Scan Code	VoIP Dial-out
03%	00453%

The VoIP route profile appears like:

	Description	1	2	3	4	
1	LocalServer	Server 1	None	None	None	
2	LongDistance	Server 2	Server 1	None	None	
3		None	None	None	None	
4		None	None	None	None	
5		None	None	None	None	
6		None	None	None	None	
7		None	None	None	None	
8		None	None	None	None	
9		None	None	None	None	
10		None	None	None	None	

Digit Map Table appears like:

Scan Code	VoIP Dial-out	PSTN Dial-out	User Dial Length	Route	<a href="#">VoIP Route Profile</a>		
09%			10	Auto (VoIP first)	1		
03%			10	VoIP	2		

As you dial the phone numbers starting with 03, like 0312345678, the number will be changed to 0045312345678, followed the number translation of Server 2, and the call will go through Server 2 (free VSP) at first. If failed, the number will be back to 0312345678, and the route will be changed to Server1 (local VSP).

**Example 3 – Multiple Route,**

The number translation of Server 1 is blank, and the number translation of Server 2 appears like:

NUMBER TRANSLATION			
VoIP Dial-Out defined here overrides "Digit Map"			
Copy From : <input type="text" value="None"/>			
Scan Code	VoIP Dial-out		
03%	00453%		
002%	00%		
4%	0044%		

The number translation of Server 3 appears 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%		

The VoIP Route Profile appears like:

	Description	1	2	3	4	
1	LocalServer	Server 1	None	None	None	
2	LongDistance	Server 2	Server 1	None	None	
3	InternationalCall	Server 3	Server 2	Server 1	None	
4		None	None	None	None	
5		None	None	None	None	
6		None	None	None	None	
7		None	None	None	None	
8		None	None	None	None	
9		None	None	None	None	
10		None	None	None	None	

Digit Map Table appears like:

Scan Code	VoIP Dial-out	PSTN Dial-out	User Dial Length	Route	VoIP Route Profile		
09%			10	Auto (VoIP first)	1		
03%			10	VoIP	2		
00244%			14	VoIP	3		

As you dial the phone numbers starting with 00244, like 00244123456789, the number will be changed to 0123456789 followed the number translation of Server3, and the call will go through Server 3 (UK VSP) at the first. If the first route is failed, the number is changed to 0044123456789, and the route is changed to Server 2 (free VSP). If the second route is failed, the number is back to 00244123456789, and the route is changed to Server 1 (local VSP).

**Methods of Digit Map:**

The VoIP route profile appears like:

	Description	1	2	3	4	
1	LocalServer	Server 1	None	None	None	
2	LongDistance	Server 2	Server 1	None	None	
3	InternationalCall	Server 3	Server 2	Server 1	None	
4	VoIPSTUN	Server 2	None	None	None	
5	UKServer	Server 3	None	None	None	
6		None	None	None	None	
7		None	None	None	None	
8		None	None	None	None	
9		None	None	None	None	
10		None	None	None	None	

**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: 091



VoIP Dial-out: 0912345678

PSTN Dial-out: leave it as blank

User Dial Length: 2

Route: Auto

VoIP Route Profile: Route # 1

Scan Code	VoIP Dial-out	PSTN Dial-out	User Dial Length	Route	VoIP Route Profile		
091	0912345678		2	Auto (VoIP first)	1		

Pick up the handset and dial 091, and the system will do the things as follow:

1. Change the phone number to the global number. 091 is changed to 0912345678. Then, follow the VoIP Route Profile # 1.
2. If Server 1 is failed, because of Route is Auto, the call is diverted to PSTN.

**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: leave it as blank

PSTN Dial-out: 351006???

User Dial Length: 4

Route: PSTN

VoIP Route Profile: leave it as default

Scan Code	VoIP Dial-out	PSTN Dial-out	User Dial Length	Route	VoIP Route Profile		
091	0912345678		2	Auto (VoIP first)	1		
2???		351006???	4	PSTN	1		

Pick up the handset and dial 2301. The system will divert 351006301 to PSTN.

**For example,**

Scan Code: 4%







VoIP Dial-out: 00244%

PSTN Dial-out: leave it as blank

User Dial Length: 11

Route: Auto

VoIP Route Profile: Route # 3

Scan Code	VoIP Dial-out	PSTN Dial-out	User Dial Length	Route	VoIP Route Profile		
091	0912345678		2	Auto (VoIP first)	1		
2???		351006???	4	PSTN	1		
4%	00244%	180544%	11	Auto (VoIP first)	3		

Pick up the handset and dial 4323456789. The system will do the things as follow:

1. Change the phone number to the global number. 4323456789 is changed to 00244323456789. Then, follow the VoIP Route Profile # 3.
2. Translate the global number to the private number followed the number translation of Server 3. 00244323456789 will be translated to 0323456789.
3. If Server3 is failed, the system will use the global number, 00244323456789, to go through Server 2.
4. Translate the global number to the private number followed the number translation of Server 2. 00244323456789 is translated to 0044323456789.
5. If Server 2 is failed, the system will use the global number to go through Server 1.
6. If all VoIP routes are failed, the system will change the global number based on the rule of PSTN Dial-out. The number is changed from 00244323456789 to 180544323456789 and diverted to PSTN.

**Method 3- Substitution:** It helps you dial to destination that you can not dial by phone. Destination like: anny@sip.com.uk. Fill 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: AnnyKC

PSTN Dial-out: leave it as blank

User Dial Length: Disable

Route: VoIP

VoIP Route Profile: Route # 5

Scan Code	VoIP Dial-out	PSTN Dial-out	User Dial Length	Route	VoIP Route Profile		
091	0912345678		2	Auto (VoIP first)	1		
2???		351006???	4	PSTN	1		
4%	00244%	180544%	11	Auto (VoIP first)	3		
11	AnnyKC		Disable	VoIP	5		

Pick up the handset and dial 11. The system will do the things as follow:

1. Change the phone number to the global number. 11 is changed to “AnnyKC”.
2. It sends “AnnyKC” to Server3 followed the VoIP Route Profile # 5.

If the VoIP route is failed, the call is disconnected.

### 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"/> ▼
DTMF Detection Volume Sensitivity :	<input type="text" value="0"/> ▼
DTMF Output Volume :	<input type="text" value="0"/> ▼
<input checked="" type="checkbox"/> FXS Pulse Detection	
<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"/> ▼
RFC 2833	
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.

**DTMF Detection Volume Sensitivity:** Adjust DTMF detect threshold of DTMF volume

**DTMF Output Volume:** Adjust the Tx volume of FXS port for DTMF Caller ID or Out of Band DTMF.

**FXS Pulse Detection:** It allows FXS detect PULSE dial method sends from a phone set.

**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 ▼

**Line2 :** T.30 Fax ▼

Option	Fax Detection	Content of SDP of re-INVITE	re-INVITE with T.38 from remote party
Disable	No	N/A	Accept and change RTP to T.38
T.38 Fax	Yes	re-INVITE with T.38 and T.30	Accept and change RTP to T.38
T.30 Fax	Yes	re-INVITE with T.30	Accept and change RTP to T.38
T.30 Fax/Modem	Detect CED only	re-INVITE with T.30	Accept and change RTP to T.38
T.30 Only	No	N/A	Accept and change RTP to T.38
T.38 Native	Yes	re-INVITE with T.38	Accept and change RTP to T.38
T.30 V.152	Yes	N/A	Accept and change RTP to T.38

**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	
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	
Line 1 :	T.30 Fax
Line 2 :	T.30 Fax
FAX	
<input type="checkbox"/>	Switch FAX On CED Detection
<input type="checkbox"/>	Restrict T.38
FAX Detection Sensitivity	0
FAX T.38	
High Speed Redundancy :	1
Low Speed Redundancy :	1
FAX Max Rate :	14400
High Speed Packet Time :	40
FAX T.30	
FAX Codec :	G.711 u-law 64kbps
T.30 Bypass Payload Type :	96 (96-127)
FAX Jitter Buffer :	200 (60-1200 ms)

**Switch FAX On CED Detection:** DVG will send FAX Re-Invite immediately as it detect FAX CED tone, that will save handshaking time between FAX machines.

**Restrict T.38:** DVG will reject T.38 Re-Invite in case the FAX type contains without T.38.

**FAX Detection Sensitivity:** To set higher value to make DVG to be more sensitive.

**High Speed Redundancy:** Set redundancy packets for FAX image. It could repair FAX image for non-continuous packets lost. The higher redundancy the higher bandwidth required.

**Low Speed Redundancy:** Set redundancy packets for FAX handshaking signaling.

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

**T.30 Bypass Payload Type:** Fill correct payload type of T.30 bypass method.

**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**

**Hot Line**

Hot Line No. :

Warm Line (Hot Line Delay):  ( 0 - 60 s )

**VoIP Call Allow PSTN In**

**PHONE 2**

**Hot Line**

Hot Line No. :

Warm Line (Hot Line Delay):  ( 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 Phone 1 is in VoIP call. To answer the PSTN call waiting is to hang up the phone to disconnect VoIP call and then pick up the phone.

### 3-2-1-10 Line

ADVANCED → VoIP → Line

**LINE SETTINGS**

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

**LINE 1 - FXS**

**Enable**

**Listening Volume :**  (3dB per step)

**Speaking Volume :**  (3dB per step)

**Tone Volume :**

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

**Flash Time :**  (50-950ms)

**Polarity Reversal**

**FXS Chip Option 1**

**FXS Current**  (18-48mA)

**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.

**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.

**FXS Current:** Set the output D.C. current of FXS port.



ADVANCED → VoIP → Line

LINE3 - PSTN	
<input checked="" type="checkbox"/> Enable	
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)"/> ▼

**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.

**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"/> (10-600s)
<input type="checkbox"/> Enable End of Digit Tone	
Force Calling Thru PSTN Code :	<input type="text"/>
<input checked="" type="checkbox"/> Early Media Treatment	
Loop Current Drop Trigger Time :	<input type="text" value="0"/> (0=disable, 3-30s)
Loop Current Drop Duration :	<input type="text" value="2"/> (1-5s)
ROH Begin Time :	<input type="text" value="0"/> (0=disable, 1-999s)
ROH Duration :	<input type="text" value="60"/> s
FXS Ring Voltage :	<input type="text" value="0"/> (45-80)
FXS Onhook Voltage :	<input type="text" value="0"/> (24-57)
VoIP Centrex Extension Digit Count :	<input type="text" value="0"/> (0=disable, 1-30)
VoIP Centrex Digit :	<input type="text"/>
Metering Pulse Type	<input type="text" value="Disable"/> ▼
Metering Pulse Period	<input type="text" value="0"/> s

**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:** Fill prefix code to dial out through PSTN(Life Line) port.

**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.

**ROH Begin Time:** As users forget hang up phone set it makes FXS play loud Howler Tone to notify users put hand set correctly. If this timer is set to be 20 seconds, that FXS play busy tone for 20 seconds then play ROH.

**ROH Duration:** It is the maximum time for FXS play ROH, then FXS will stop play ROH and keep silence.

**FXS Ring Voltage:** It is to set the Ring Voltage of FXS.

**FXS Onhook Voltage:** It is to set the idle Voltage of FXS.

**VoIP Centrex Extension Digit 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 Gateway will send the number which digit count is the same as VoIP Centrex Extension Digit Count.

**Metering Pulse Type/ Metering Pulse Period:** It is used for telephony device which connected to FXS port for billing purpose. **DVG-N5412SP provide 12k Hz and 16k Hz metering capacity. The fully support for detail Metering Pulse Period is not free charge, please contact with your vendor.**

ADVANCED → VoIP → Line

TERMINATION IMPEDANCE	
<b>FXS Impedance :</b>	Taiwan 600 Ohm ▼

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

ADVANCED → VoIP → Line

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

VOICE MENU OPTIONS	
<input checked="" type="checkbox"/>	<b>Enable IVR Option</b>

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

ADVANCED → VoIP → Line

FXS GROUP HUNTING / RING PRIORITY	
<b>Hunting / Ring :</b>	<input type="text" value="Hunting"/>
<b>Sequential Ring Time :</b>	<input type="text" value="6"/> ( 1 - 100 s )

**Hunting/Ring:** It is used to set FXS group hunting mode. There are **Hunting**, **Simultaneous Ring** and **Sequential Ring**.

**Hunting:** When someone calls in by dialing FXS representative number, the system will always assign the call to the first line.

**Simultaneous Ring:** When someone calls in by dialing FXS representative number, all FXS ports will ring at the same time.

**Sequential Ring:** When someone calls in by dialing FXS representative number, the system will assign the call to each FXS ports in order according **Sequential Ring Time**. You can adjust **Sequential Ring Time** for the ring time of each port.



### 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 )

**SIP Transport Protocol :**  ▾

**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.

**SIP Transport Protocol:** DVG-N5412SP supports UDP, TCP and TLS for SIP signaling. Most of SIP Server support UDP, if you prefer TCP or TLS please make sure whether remote party supports TCP/TLS or not.

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	
<b>Session Expiration :</b>	<input type="text" value="0"/> ( 0 = disable, 10 - 1800 s )
<b>Session Refresh Request :</b>	<input checked="" type="radio"/> UPDATE <input type="radio"/> re-INVITE
<b>Session Refresher :</b>	<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	
<b>SIP Message Resend Timer Base :</b>	<input type="text" value="0.5"/> s
<b>Max. Response Time for Invite :</b>	<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"/> <b>VoIP Failure Announcement</b>
---

**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

SUPPLEMENTARY FEATURES	
<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"/>	Call On Hold Notification
<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="checkbox"/>	Put Caller ID In URI
<input type="checkbox"/>	INVITE With Remote-Party-ID Header
Callee Quick Media	
	Disable ▼
FXS Hunting For Unknown Number	
	Disable ▼
<input type="checkbox"/>	Support URI Percent-Encoding (RFC 3986)
<input checked="" type="checkbox"/>	Call Hold Compatible With RFC 2543

**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.

**Call On Hold Notification:** FXS will send alert to phone set as users hang up if there is a call still held in another line.

**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:** This option make sure DVG-N5412SP cold release the PSTN line calls after FXS hang-up.

**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 Caller ID Obtaining:** Select the part of the SIP packet from the VoIP Gateway 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 locates 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.

**Callee Quick Media:** DVG-N5412SP will send RTP to remote party immediately as user answer an inbound call.

**FXS Hunting For Unknown Number:** Select the response for an incoming call which the called number is not exist in on the DVG.

**Disable** – DVG responses 404 not found.

**Hunt and Transit Dial** – DVG sends alert to an available FXS port and dial the number to PBX as the FXS port picked up by PBX. It works with SoftSwitch or IPPBX to allow a remote client reach the PBX extension for one step dial. (For virtual extension)

**FXS Group Hunting/ Ring Type** -- DVG sends alert to an available FXS port for hunting group.

**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.

**Call Hold Compatible With RFC 2543:** It is used to set the procedure of Call Hold being compatible with RFC 2543.



### 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 configuration page with two main sections. The top section is titled "DMZ / ALG" and has an orange header. Below the header, there is a grey box containing the 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" which is currently unchecked. To the right of the checkbox is a text input field labeled "DMZ Host IP Address :". The bottom section is titled "ALG" and has a dark grey header. Below the header, there are two checkboxes: "SIP ALG" and "RTSP ALG", both of which are currently unchecked.

**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.

**SIP ALG:** Enable ALG for LAN port SIP UA.

**RTSP ALG:** Enable ALG for RTSP multimedia stream.

### 3-2-3-2 DoS Prevention

ADVANCED → Firewall and DMZ → DoS Prevention

**DOS PROTECTION SETTINGS**

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

**Enable DoS Protection**

**WHOLE SYSTEM FLOOD**

<input checked="" type="checkbox"/>	<b>SYN</b>	<input style="width: 40px;" type="text" value="50"/>	(Packets/Second) (50-500)
-------------------------------------	------------	--	---------------------------

- TCP Scan**
- Ping of Death**
- ICMP Smurf**
- IP Spoof**

**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.

### 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**

Apply Cancel

IP	TCP / UDP	Remark
----	-----------	--------

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 :**  -

**TCP / UDP :** Both

**Remark :**

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

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

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

**Remark:** Enter comments.

### 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"/>				
<b>WAN Port Range :</b>	<input style="width: 40px;" type="text"/> - <input style="width: 40px;" type="text"/>	<b>TCP / UDP :</b>	Both ▼	
<b>LAN Host IP Address :</b>	<input style="width: 100%;" type="text"/>			
<b>Server Port Range :</b>	<input style="width: 40px;" type="text"/> - <input style="width: 40px;" type="text"/>			
<b>Remark :</b>	<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 LAN side server port range.

**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 WIRELESS		
Allows you to configure advanced features of the wireless LAN interface.		
<b>Fragmentation :</b>	<input type="text" value="2346"/>	(256-2346)
<b>RTS Threshold :</b>	<input type="text" value="2347"/>	(0-2347)
<b>RF Output Power :</b>	<input type="text" value="100%"/>	

**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.

**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.

### 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

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 SETTINGS**

Choose WAN or LAN to configure

**Enable WAN QoS**

**WAN QOS**

**Downstream Bandwidth :** Full Rate 64 kbps

**Upstream Bandwidth :** Full Rate 64 kbps

**ToS / DiffServ Settings :**

ToS IP Precedence  
 DiffServ (DSCP)

**TOS IP PRECEDENCE**

**Signaling Precedence :** 3 (Flash)

**Voice Data Precedence :** 5 (CRITIC / ECP)

**Enable WAN QoS:** Check the box to guaranty the voice quality. The system reserves the bandwidth for voice packets, and the data transmission is distributed to less bandwidth.

**Downstream Bandwidth** - Select the downstream bandwidth that is less than the actual bandwidth subscribed from the drop-down menu.

**Upstream Bandwidth** - Select the upstream bandwidth that is less than the actual bandwidth subscribed from the drop-down menu.

**ToS IP Precedence:** Select the precedence for signaling (data) and voice (voice data) to tag voice packets.

**DiffServ (DSCP):** Select the number of signaling (data) and voice (voice data) values to tag voice packets.

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

### 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.

<b>NAT Type :</b>	Unknown
<b>STUN Server IP / Domain :</b>	<input type="text"/>
<b>STUN Server Port :</b>	<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="border: none; background-color: #f0f0f0; text-align: center;" type="text"/> ▼
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input style="border: none; background-color: #f0f0f0; text-align: center;" type="text"/> ▼
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input style="border: none; background-color: #f0f0f0; text-align: center;" type="text"/> ▼
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input style="border: none; background-color: #f0f0f0; text-align: center;" type="text"/> ▼
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input style="border: none; background-color: #f0f0f0; text-align: center;" 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 UPnP device on DVG.

### 3-2-5-6 RIP

ADVANCED → Advanced Network → RIP

RIP	
RIP	
Enable RIP	<input type="checkbox"/>
Send Version	1 & 2 ▼
Receive Version	1 & 2 ▼
Enable Authentication	<input type="checkbox"/>
Authentication Password	••••••••
Update Timer	30
Timeout Timer	180
Garbage Timer	120

**Enable RIP:** Check the box to enable RIP to build small-multi router network via RIP protocol. This function is useless for home network.

### 3-2-6 SNMP

ADVANCED → Advanced Network → SNMP

DVG-N5412SP supports SNMP V1, V2 and V3. Please enter required parameter for SNMP V3 on each SNMP setting pages.

**SNMP**

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

**Enable SNMP Agent**  
 **Enable Authenticate Traps**

Host IP Address	SNMP Version	Community String/SNMPv3 User Name
<input type="text"/>	v1	<input type="text"/>
<input type="text"/>	v1	<input type="text"/>
<input type="text"/>	v1	<input type="text"/>
<input type="text"/>	v1	<input type="text"/>
<input type="text"/>	v1	<input type="text"/>

If the MIB browser supports SNMP V1 and V2 only, please refer to following configuration:

**Example for SNMP V2 configuration:**

Some keys configured on MIB browser:

Get Community: **public**

Set Community: **private**

Trap Community: **public**

- Enable [Advanced-> SNMP Management-> SNMP-> Enable SNMP Agent]

**SNMP**

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

**Enable SNMP Agent**  
 **Enable Authenticate Traps**

Host IP Address	SNMP Version	Community String/SNMPv3 User Name
<input type="text"/>	v1	<input type="text"/>
<input type="text"/>	v1	<input type="text"/>
<input type="text"/>	v1	<input type="text"/>
<input type="text"/>	v1	<input type="text"/>
<input type="text"/>	v1	<input type="text"/>

- Set [Advanced-> SNMP Management-> SNMP View-> View Name] as "all".
- Set [Advanced-> SNMP Management-> SNMP View-> View Name] as ".1"

**SNMP VIEW**

View Name	Subtree OID	View Type
all	.1	Include
		Include
		Include
		Include
		Include
		Include

- Set [Advanced-> SNMP Management-> SNMP Community-> Community Name] for public and private.
- Select a configured View Name.

**SNMP COMMUNITY**

Community Name	View Name	Access Right
public	all	Read Only
private	all	Read Write
		Read Only
		Read Only
		Read Only

### 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="80"/>	
Web Idle Time Out :	<input type="text" value="180"/>	( 30 - 3600 s )
TFTP Source Port :	<input type="text" value="69"/>	( 1 - 65535 )
<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.

**TFTP Source Port:** Enter the port number for sending out sends TFTP sessions.

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

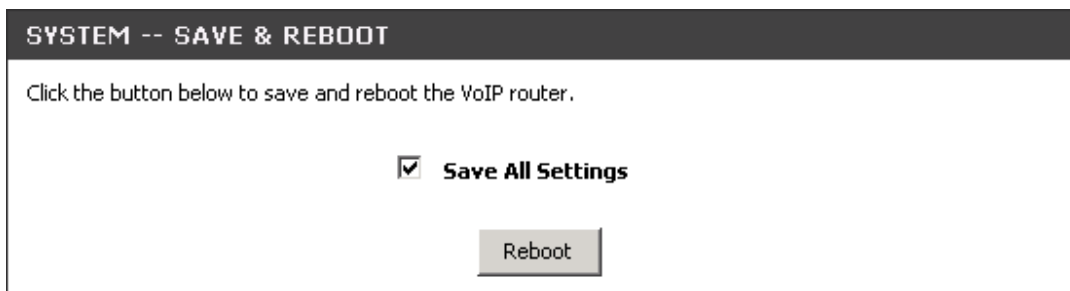
**Enable Telnet Service:** Check the box to enable Telnet access from WAN or LAN.



### 3-3-2 Backup and Restore

#### Save and Reboot

MAINTENANCE → Backup and Restore

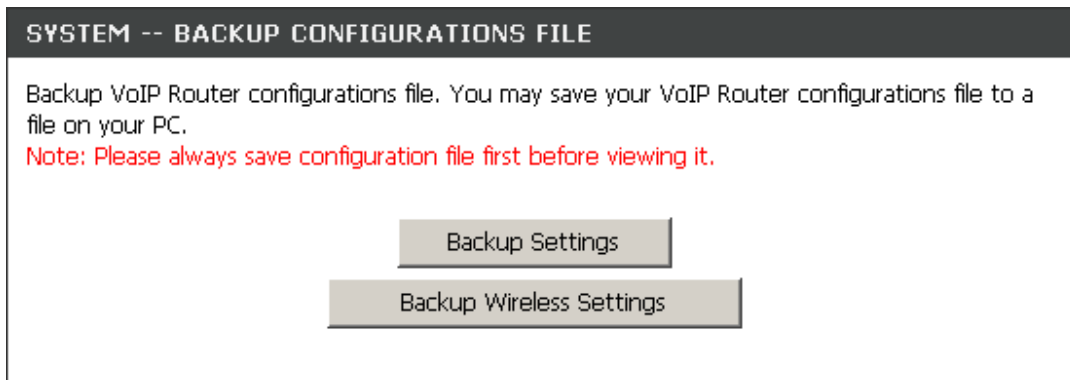


**Save All Settings:** Click the **Save All Settings** check box and reboot the system after completing changes. The new settings will take effect after the VoIP Router is restarted.

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

#### Backup Configurations File

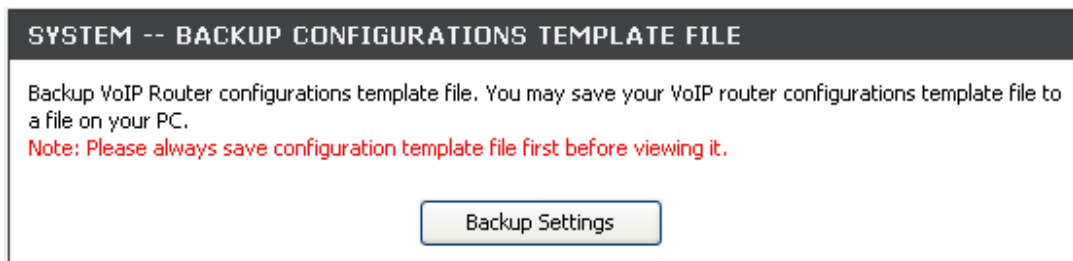
MAINTENANCE → Backup and Restore



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

### Backup Configurations Template File

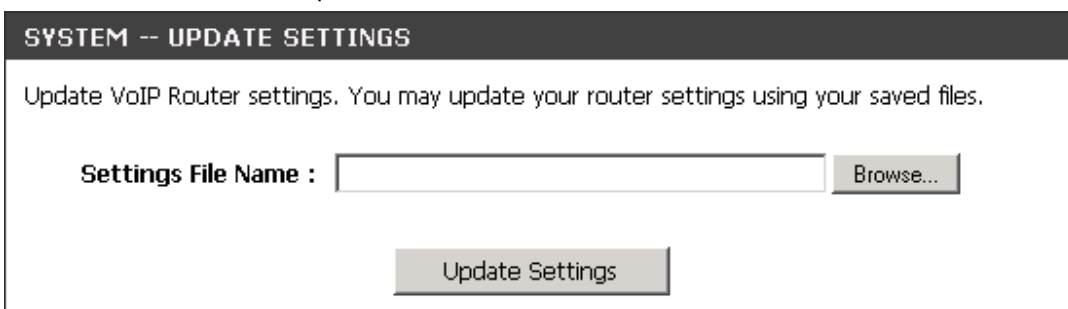
MAINTENANCE → Backup and Restore



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

### Update Settings

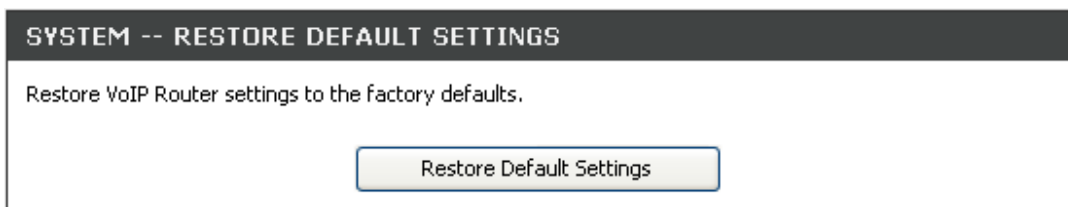
MAINTENANCE → Backup and Restore



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



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 :** GE\_1.03

**Upgrade Server :**

**Server IP Address :**

**Server Port :**  ( 1 - 65535 )

**User Name :**

**Password :**

**Directory :**

**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](http://www.DLinkDDNS.com).

**Enable Dynamic DNS**

**Server Address :**  << Select Dynamic DNS Server ▾

**Host Name :**

**Username or Key :**

**Password or Key :**

**Verify Password or Key :**

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

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

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

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

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

### 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

#### 3-3-6-1 Ping Test

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

The screenshot shows a web-based interface for a Ping Test. At the top, there is an orange header with the text "PING TEST". Below this, a grey box contains the instruction: "Ping Test sends 'ping' packets to test a computer on the Internet." There are three input fields: "Ping Destination" with the value "192.168.8.254", "Number of Ping" with the value "4" and a range "( 1 - 100 )", and "Ping Packet Size" with the value "100" and a range "( 56 - 5600 bytes )". Below the input fields are two buttons: "Test" and "Stop".

Below the configuration area is a dark grey header with the text "RESULT". Underneath is a scrollable text area containing the following output:

```
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
```

### 3-3-6-2 Outward Test

MAINTENANCE → Diagnostics → Outward Test

**OUTWARD TEST (GR-909)**

H.F. DC Voltage = Hazardous and foreign DC voltage  
 H.F. AC Voltage = Hazardous and foreign AC voltage

Line	Enable	Pass	Loop Open	H.F. DC Voltage	H.F. AC Voltage	Tip/Ring Short	Failed
1	<input type="checkbox"/> <span style="border: 1px solid #000; padding: 2px;">All</span>						
2	<input type="checkbox"/>						

**Enforced Test (Ignore Port State)**

Test
ACO
Stop

It allows operator to verify whether it is some problem on the cable between phone sets and DVG-N5412SP FXS ports.

**Enable:** Select the lines you want to test.

**Including Channel In Used:** Since the line test will interrupt a talking call, that DVG-N5412SP will ignore the in used line. If you would like to test all the lines you select even it is in used, please tick this item.

**Test:** Click start to test.

**ACO:** Clear alarm indication of the last test result.

### 3-3-6-3 FXS Inward Self Test

MAINTENANCE → Diagnostics → Inward Test

INWARD SELF TEST

FXS Inward Self Test

Line	Enable	Loopback - Codec	Loopback - Analogue	SLIC DC Power Voltage	Tip / Ring DC Feed	Ringer
1	<input type="checkbox"/> <span style="border: 1px solid black; padding: 2px;">All</span>					
2	<input type="checkbox"/>					

**Enforced Test (Ignore Port State)**

Test
ACO
Stop

It allows operator to verify if it is some problem on the FXS chip set.

**Enable:** Select the lines you want to test.

**Including Channel In Used:** Since the line test will interrupt a talking call, that DVG-N5412SP will ignore the in used line. If you would like to test all the lines you select even it is in used, please tick this item.

**Test:** Click start to test.

**ACO:** Clear alarm indication of the last test result.



### 3-3-7 TR069

TR069 allows operator to manage DVG-N5412SP with a TR069 standard protocol.

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

Advanced Settings → TR069

**TR-069**

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

**Enable TR069**

**TR069**

<b>User Name :</b>	<input style="width: 90%;" type="text"/>
<b>Password :</b>	<input style="width: 90%;" type="password"/>
<b>Confirm Password :</b>	<input style="width: 90%;" type="password"/>
<b>Auto Config. Server URL :</b>	<input style="width: 90%;" type="text"/>
<input checked="" type="checkbox"/> <b>Periodic Inform Enable</b>	
<b>Periodic Inform Interval :</b>	<input style="width: 80%;" type="text" value="10800"/> sec
<b>Random Offset :</b>	<input style="width: 80%;" type="text" value="600"/> (0 - 1800 s)
<b>Listen Port :</b>	<input style="width: 80%;" type="text" value="8001"/> (0 = disable, 1 - 65535)
<b>Connection Request Username :</b>	<input style="width: 90%;" type="text"/>
<b>Connection Request Password :</b>	<input style="width: 90%;" type="password"/>
<b>Confirm Password :</b>	<input style="width: 90%;" type="password"/>

**Enable TR069:** Check the box to start TR069 service

**Username:** Enter an available ACS user name.

**Password:** Enter the ACS password.

**Auto Config. Server URL:** Enter the Provisioning Server's URL required by your VoIP Service Provider.

**Periodic Info Enable:** It allows DVG connect to a TR069 server periodically according to following parameters.

**Periodic Info Interval:** Enter the time for auto provisioning.

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

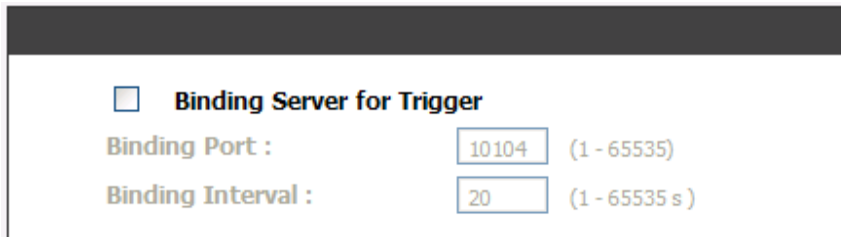
**Listen Port:** TR069 listen port for remote trigger.

**Connection Request Username:** Enter username for remote trigger.

**Connection Request Password:** Enter password for remote trigger.

**Note:** Contact your server provider if necessary.

MAINTENANCE → TR069



The screenshot shows a configuration panel with a dark header. Below the header, there is a section titled "Binding Server for Trigger" with an unchecked checkbox. Underneath, there are two rows of configuration options: "Binding Port :" with a text input field containing "10104" and a range "(1 - 65535)", and "Binding Interval :" with a text input field containing "20" and a range "(1 - 65535 s)".

**Binding Server for Trigger:** Check the box to trigger a connection between Provisioning Server and the VoIP Gateway. Provisioning Server will bind a port for the VoIP Gateway 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 Gateway 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 SETTINGS**

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 :

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.

**RADIUS:** 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.	
SYSTEM INFORMATION	
Model Name :	DVG-N5402SP
Time and Date :	2000/01/01 08:55:53
Firmware Version :	GE_1.00
WAN PORT INFORMATION	
Factory Default MAC Address :	001122334455
Net Link :	Disconnected
IP address :	192.168.100.1
Subnet mask :	255.255.255.0
Default Gateway :	192.168.100.254
Domain Name Server :	168.95.1.1
LAN PORT INFORMATION	
MAC Address :	001122334456
IP address :	192.168.8.254
Subnet mask :	255.255.255.0
WIRELESS LAN	
Wireless Radio :	Enable
Wireless Network Name (SSID) :	DVG
802.11 Mode :	Mixed 802.11n, 802.11g and 802.11b
Wireless Channel :	Auto Scan (recommended)
Wireless Security Mode :	WPA2 Mixed
DHCP SERVER	
DHCP Server :	Enabled
IP Pool Range :	192.168.8.1 - 192.168.8.250
Lease Time :	1 hour(s)
Domain Name Server :	168.95.1.1
HARDWARE	
Hardware :	B1
Driver :	1.2.2.86.135/263

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**

The information reflects the current status of your VoIP Router connection. Display the port status of each proxy server in the field of Extension Number, Proxy Register and FXS Representative Number.

**PORT STATUS**

No	Type	Extension Number	Line Status	Calls	Number	Proxy Register
1	FXS	S1 701 S2 2701	Idle	0		Disabled (01:00:11) Disabled (01:00:30)
2	FXS	S1 702 S2 2702	Idle	0		Disabled (01:00:11) Disabled (01:00:30)

**SERVER REGISTRATION STATUS**

<b>DDNS Registration :</b>	Disabled (01:00:11)
<b>STUN Registration :</b>	Disabled (01:00:11)
<b>SIP Proxy Hunting Number Registration :</b>	FXS: Server1 Disabled (01:00:11) Server2 Disabled (01:00:30)

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.

**Example:**

“S1 701” shows that the number of the first line which register to SIP Server 1 is 701.

“S2 2702” shows that the number of the second line which register to SIP Server 2 is 2701.

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

### 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-N5412SP. 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**

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

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

### 3-4-5 Routing Table

STATUS → Routing Table

**ROUTING TABLE**

This table is showing you the router forwards list. Routing Table enables you to view the information created by the router that displays the network interconnection topology.

Destination	Netmask	Gateway	Iface
61.221.24.0	255.255.255.224	0.0.0.0	eth0
192.168.8.0	255.255.255.0	0.0.0.0	eth1
default	0.0.0.0	61.221.24.1	eth0

The Routing Table stores the information for particular network destination around the VoIP Router. Press **Refresh** button to generate the details.

### 3-4-6 Logout

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

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 <b>114</b> 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	
118	Restart	
121	Setup PPPoE Account	Dial function code <b>114</b> and then dial 3 for a PPPoE connection.
122	Set PPPoE Password	
311/301	LAN Port IP Set/Query	
312/302	LAN Port Subnet Mask Set/Query	
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)	

## 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"> <li>After entering IVR mode, dial 114.</li> <li>When voice prompt plays “Enter value”, dial 1 (to select static IP)</li> </ul>
IP address Settings	<ul style="list-style-type: none"> <li>After entering IVR mode, dial 111. When voice prompt plays “Enter value”, enter your IP address followed by “#”.</li> </ul> <p><b>Example:</b> If the IP address is 192.168.1.200, dial 192*168*1*200#.</p>
Subnet Mask Settings	<ul style="list-style-type: none"> <li>After entering IVR mode, dial 112. When voice prompt plays “Enter value”, enter your subnet mask followed by “#”.</li> </ul> <p><b>Example:</b> 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"> <li>After entering IVR mode, dial 113. When voice prompt plays “Enter value”, enter your default gateway’s IP address followed by “#”.</li> </ul> <p><b>Example:</b> 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"> <li>To save settings, dial <a href="#">509</a> (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 <a href="#">101</a> to check whether the IP address was retained. If the system does not play back the IP address after dialing <a href="#">101</a>, 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.</li> </ul>

### 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 544560 72544560#.

**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

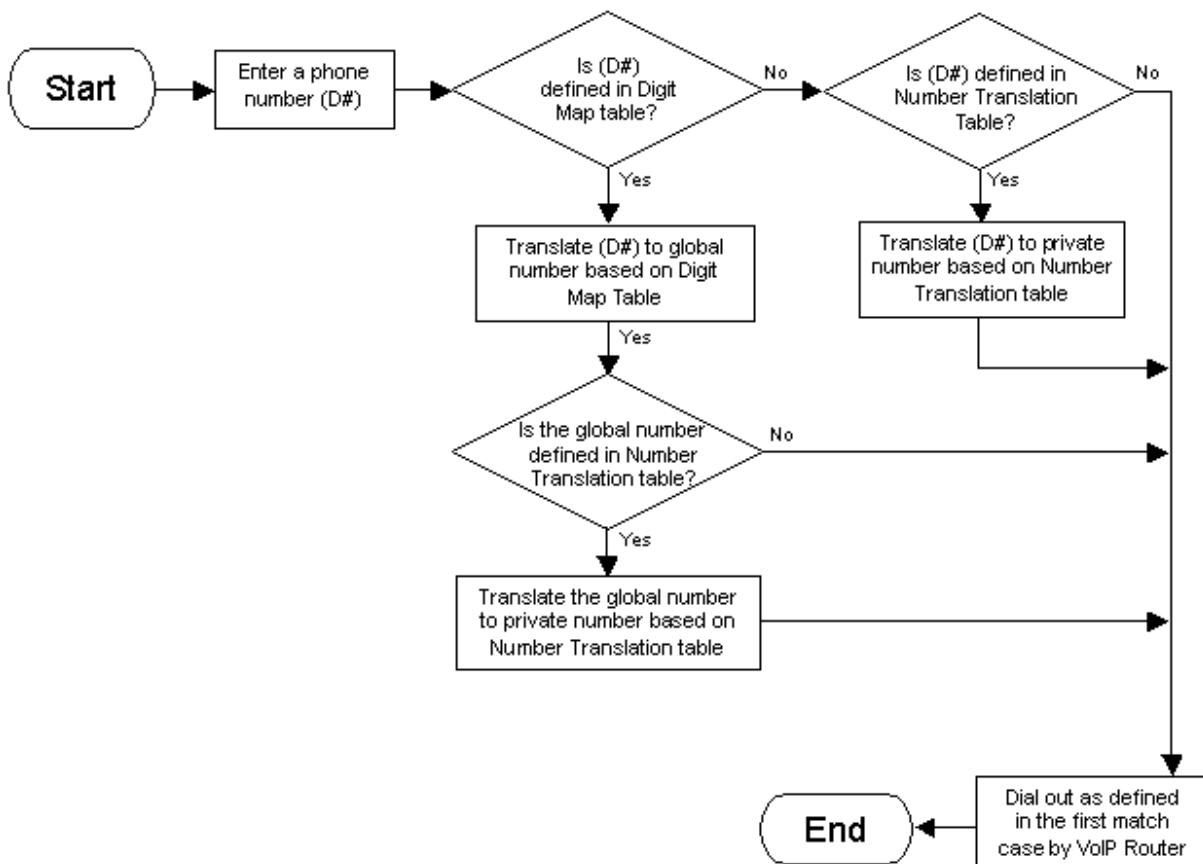
### 5-1 Dialing Options

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 50).

If the phone number matches the setting of the Digit Map, the phone number will be dialed out through the assigned VoIP Service Provider according to VoIP Route Profile automatically.

### 5-2 Number Translation

Phone number is dialed by user. The system will check if the phone number is matched Digit Map Table. If no matched is found from Digit Map Table, it will use the phone number to look up number translation of the server set in VoIP Routing Profile.

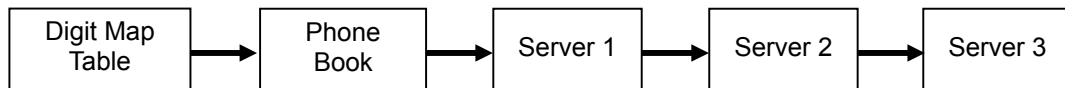


## 5-3 Routing

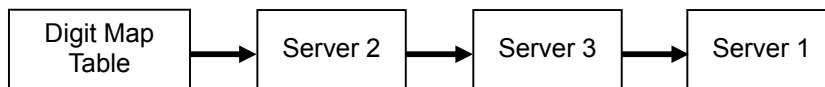
To achieve maximum flexibility, the number dialed will be looked up in several tables defined by VoIP Router. If no match is found from Digit Map Table, it will then look up the number from another table and to the registered VoIP Service Provider.

### Routing Processing Flow

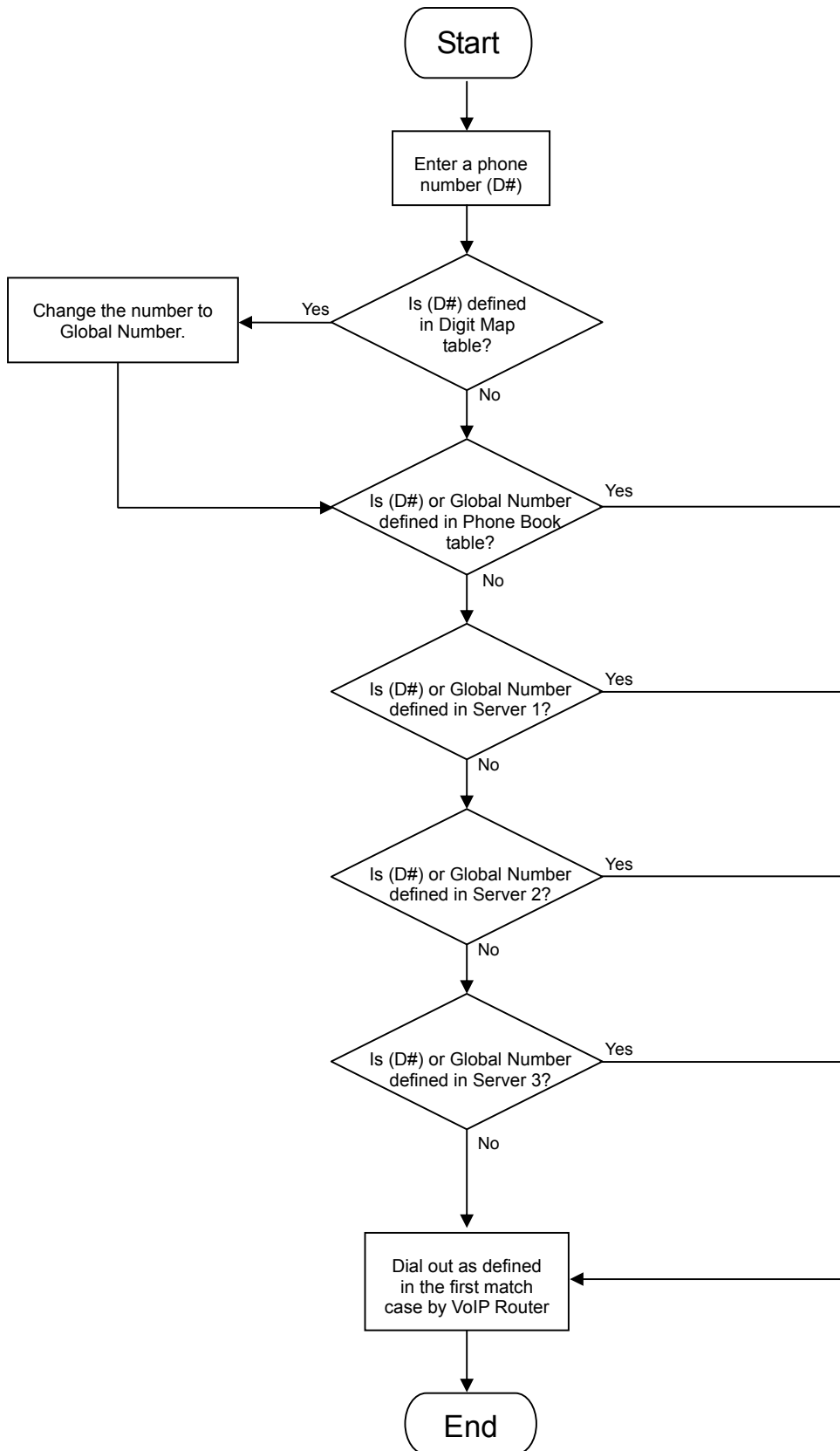
The routing after checking Digit Map Table may vary. The routing accords with VoIP Route Profile. By default, Phone Book is the first route of VoIP Route Profile. The second and third route is Server 1 and Server 2. Server 3 is the last route. Each server has a dialing plan, i.e. number translation, table, and the number will be translated according the dialing plan before dialing out. For default setting, the number look up flow appears like:



Assume that the route of Default Route Profile is Server 2 as the first route, Server 3 as the second route and Server 1 as the last route. The number look up flow appears like:







## 6. Troubleshooting

---

This chapter provides solutions to problems that can occur during the installation and operation of the DVG-N5412SP. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

### 1. Why can't I access the web-based configuration utility?

When entering the IP address of the D-Link router (192.168.8.254 for example), you are not connecting to a website on the Internet or have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:
  - Internet Explorer 6.0 or higher
  - Netscape 8 or higher
  - Mozilla 1.7.12 (5.0) or higher
  - Opera 8.5 or higher
  - Safari 1.2 or higher (with Java 1.3.1 or higher)
  - Camino 0.8.4 or higher
  - Firefox 1.5 or higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.
- Configure your Internet settings:
  - Go to **Start > Settings > Control Panel**. Double-click the **Internet Options** icon. From the **Security** tab, click the button to restore the settings to their defaults.
  - Click the **Connection** tab and set the dial-up option to **Never Dial a Connection**. Click the LAN Settings button. Make sure nothing is checked. Click **OK**.
  - Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.
  - Close your web browser (if open) and open it.
  -
- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for the web management.
- If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

### 2. What can I do if I forgot my password?

If you forgot your password, you must reset your router. Unfortunately this process will change all your settings back to the factory defaults.

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process.

Wait about 30 seconds to access the router. The default IP address is 192.168.8.254. When logging in, the username is **admin** and leave the password box empty.

### 3. Why can't I connect to certain sites or send and receive emails when connecting through my router?

If you are having a problem sending or receiving email, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

**Note: AOL DSL+ users must use MTU of 1400.**

To find the proper MTU Size, you'll have to do a special ping of the destination you're trying to go to. A destination could be another computer, or a URL.

- Click on Start and then click Run.
- Windows® 95, 98, and Me users type in command (Windows® NT, 2000, and XP users type in cmd) and press Enter (or click OK).
- Once the window opens, you'll need to do a special ping. Use the following syntax:  
ping [url] [-f] [-l] [MTU value]

Example: ping yahoo.com -f -l 1472

```
C:\>ping yahoo.com -f -l 1482
Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping yahoo.com -f -l 1472
Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:
Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 93ms, Maximum = 203ms, Average = 132ms

C:\>
```

# Appendix

---

## Product Features

### **WAN**

- One 10/100/1000Mbps auto-negotiation, auto-crossover RJ-45 Ethernet port
- Support static IP, PPPoE, 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 and Outbound Proxy
- NTP: (Network Time Protocol RFC 1305)
- Time Zone Support
- MAC Address Clone
- RTP Packet Summary : packet sent, packet received, packet loss for voice quality analysis

### **LAN**

- Four 10/100/1000Mbps 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 generation (FXS)
- T.30 (G.III) / Real time T.38 / Secured T.38 FAX relay
- DTMF, FSK (Bellcore & ETSI) Caller ID 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
- 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
  - Hardware / software information
- Firmware Upgrade through TFTP, FTP or HTTP server
- Configuration Backup/Restore
- Reset button (with restore factory default function)