## How to setup IPSec VPN connection between DIR-130 and DSL-G804V VPN Routers

This setup example uses the following network settings:



In our example the IPSec VPN tunnel is established between two LANs: 192.168.0.x and 192.168.1.x. **NOTE: It is essential to have private networks (LAN 1 and LAN 2) on different subnets.** 

# Configuration of DIR-130 router:

**Step 1:** Open your web browser and type in the IP address of the router (*192.168.0.1* by default). Enter the username (*admin* by default) and password (blank by default), and then click **OK**.

Step 2: Click on VPN SETTINGS and select IPSec from the ADD VPN PROFILE dropdown list and click Add.

Product Page: DIR-130					
D-Link	<i>è</i>				
and the second	and the second		المحصور المستحد المستحد	an an taon an an taon an taon an an taon an tao	
DIR-130	SETUP	ADVANCED	MAINTENANCE	STATUS	
Internet Network Settings VPN Settings	VPN SETTINGS Use this section to cre ADD VPN PROFILE IPSec - Internet Protoco	ate and configure your \ :  Security   - Add	/PN settings.		
	25 - VPN PROFILE Enable	:	Name	Туре	

Step 3: Configure the *IPSec VPN* as followed:

## **IPSEC SETTING**

- Enable: check box to enable
- Name: enter a name for the VPN
- Local Net/Mask: enter the local network and local subnet mask
- **Remote IP:** select Site to Site and enter the remote gateway (usually the WAN IP address of the remote site)
- Remote Local LAN Net /Mask: enter the remote network and remote subnet mask
  Authentication: enter a Pre-shared Key (Pre-shared key must be the same with the remote site)
- Local ID: leave as Default
- Remote ID: leave as Default
- PHASE 1
- Main Mode: selected
- NAT-T Enable: ticked (if required)
- Keep Alive / DPD: select Keep Alive
- DH Group: select 2-modp 1024-bit from the drop-down list
- •
- IKE PROPOSAL List
- Cipher #1: select 3DES; HASH: select SHA
- IKE Lifetime: leave as 28800 (default value should match with the remote site)
- •
- PHASE 2
- **PFS Enable**: ticked
- PFS DH Group: select 2-modp 1024-bit from the drop-down list
- •
- IPSec PROPOSAL List
- Cipher #1: select 3DES; HASH: select SHA1
- **IPSec Lifetime:** leave as **3600** (default value should match with the remote site)
- Click Save Settings at the top of the screen to save



## Configuration of the DSL-G804V router.

**Step 1:** Open your web browser and type in the IP address of the router (*192.168.1.1* by default). Enter the username (*admin* by default) and password (admin by default), and then click **OK** 

# Step 2: Go to Advanced > VPN and click on IPSec

- Connection Name Enter a name for the tunnel
- Local Network select "Subnet"
- **IP Address** enter the IP Address of the local network. Note that it should be Subnet ID, not a single IP address (e.g.192.168.1.0).
- Netmask enter the Subnet Mask of the local network
- Remote Secure Gateway IP enter the public IP address of the remote VPN router.
- Remote Network select "Subnet"
- **IP Address** enter the IP Address of the remote network. Note that it should be Subnet ID, not a single IP address (e.g.192.168.0.0).
- Netmask enter the Subnet Mask of the remote network
- Proposal select ESP
- Authentication Type select SHA1
- Encryption 3DES
- Perfect Forward Secrecy MODP 1024 (Group 2)
- **Pre-shared Key** enter the security key you want to use for your VPN connection. The same key will need to be specified in the VPN router on the other end (on remote network).
- Click on Advanced Options
- IKE Mode: select Main
- IKE Proposal
- HASH Function: select SHA1
- Encryption: select 3DES
- Local ID: leave as Default
- Remote ID: leave as Default
- SA Lifetime
- Phase 1 (IKE) : leave as 480 (default)
- Phase 2 (IPSec): leave as 60 (default)
- PING Keep Alive
- Keepalive: select None
- Click **Apply** when done and you should be back to the main **VPN->IPSec** page.
- Make sure that **Enable after "Apply**" is selected
- Click Apply button when done.

le		Wire	less ADSL \	PN Rou
	Home Advanc	ed Tools	Status	Help
	VPN © PPTP	IPSec	© L2TP	
	IPSec Enable after 'Apply' Connection Name	● Yes ● NO DIR-130		
	Local Network IP Address Netmask	Subnet		
	Remote Secure Gateway IP Remote Network	111.222.333.444 Subnet •		
	Netmask Proposal	255.255.255.0		
	Authentication Type Encryption Perfect Forward Secrecy	SHA1 ▼ 3DES ▼ MODP 1024 (Group 2	) +	
	Pre-shared Key Advanced Options	password123456		
			3 🔮 🔮 Back Apply	😕 🛟 Cancel Help

-

Building Networks for People		Wireless	ADSL VPN Router
	Home Advanced	Tools	Status Help
DSL-G804V	IPSec		
-Co-	IKE Mode	Main 🔻	
Virtual Server	IKE Proposal		
	Hash Function	SHA1 -	
Firewall	Encryption	3DES 💌	
	Diffie-Hellman Group	MODP 1024 (Group 2)	•
VPN			
	Local ID		_
DUNS	Туре	Default -	
Routing	Content		
Kooning	Demote ID		
Wireless		Defeut	
	Identifier		
ADSL	Identitier		
	SA Lifetime		
IP QoS	Phase 1 (IKE)	480	minutes
Time Slices	Phase 2 (IPSec)	60	minutes
	PING for keepalive		
Email	Keepalive	🖲 None 🛛 PING	© DPD
Device	PING to the IP	0.0.0.0	(0.0.0.0 means NEVER)
	Interval	10	seconds
IGMP		(0-3600, 0 means NEV	ER)
	Disconnection Time after no traffic	1200	seconds (180 at least)
VLAN Bridge	Reconnection Time	15	minutes (3 at least)
Logout			🍼 🛂 🔂 Apply Cancel Help

The tunnel should now appear in the list of **VPN/IPSec List** below:

	VPN/IPSec List					View IPSec Status	
Email	Name	Local Subnet	Remote Subnet	Remote Gateway	IPSec Proposal	Enable	
Device	🗹 DIR-130	192.168.1.0 /255.255.255.0	192.168.0.0 /255.255.255.0	111.222.333.444	AH:none ESP:sha1,3DES	Yes	
IGMP	1. <del></del>						_

## Step 3.

• Go to **Tools** > **System**. Click on the "**Save**" button. This will save the settings into the router's memory.

			Wireles	ss ADSL VF	PN Route
200407	Home	Advanced	Tools	Status	Help
10044	System Set	tings			
-	Save Settings T Backup Settin	o Local Hard Drive			
Admin	Load Settings F	rom Local Hard Drive			
& Time	Load				
stem	Save Config to	Device Memory			
	Please click 'Sa saving as confi	ive' to start saving config guration information is v	uration to device r vritten to device m	nemory. There will be emory.	a delay while
warre	Save				

### How to check VPN connection status on the DSL-G804V

- On the DSL-G804V click on Status > IPSec Status.
- Under VPN Tunnels > Status it should say Connected.



### How to check the VPN connection status on the DIR-130

- On the DIR-130, click on Status ->VPN
- The tunnel should be displayed for current VPN connection.

Product Page: DIR-130						
D-Link				Janala Sacara	Participant of the second s	
	Weighter an and the street	-	مىرىيىتىنى ئەھەرىيى			ana kana kana kana kana kana kana kana
DIR-130	SETU	P	ADVANCED	ŀ	1AINTENANCE	STATUS
Device Info	CONNECTE	ED VPN TU	NNEL LIST			
Log	The VPN List below displays current VPN information.					
Statistics						
Active Session						
LAN Clients	Туре	Local J	information	Remote	Information	Other
Routing	IPSec	192.16	8.0.0/24:0	192.168.	1.0/24:0	tunnel/151
VPN						

## If VPN Tunnel can not be established:

- Make sure that the modem in front of the DIR-130 is in bridge mode.
- Make sure that both networks are using different IP subnets.

• Check the Pre-shared keys, security algorithms and life times, make sure they match on both VPN routers.

• Restart both routers.

### Connecting to shared resources via VPN

- To connect to shared resources via VPN you can map remote computers' drives and folders by opening Windows
- Explorer and going to Tools > Map Network Drive (you need to specify the IP address of the computer on remote network and the name of the shared folder):

Map Network Drive				
	Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer. Specify the drive letter for the connection and the folder that you want to connect to:			
	<u>D</u> rive:	Z: 💌		
	Folder:	\\192.168.1.20\Shared Do 🖌 Browse		
		Example: \\server\share		
		Reconnect at logon		
		Connect using a <u>different user name</u> .		
		Sign up for online storage or connect to a network server.		
		< Back Finish Cancel		

- Alternatively you can do Search > Computers or People > Computer on Network > specify the IP address of the computer you are trying to connect to.
- If you do not see computers in My Network Places or My Network Neighbourhood you may need to enable NetBIOS over TCP/IP in Windows.
- Note that firewall/antivirus software installed on your local computer or remote computer may stop you from accessing remote network.