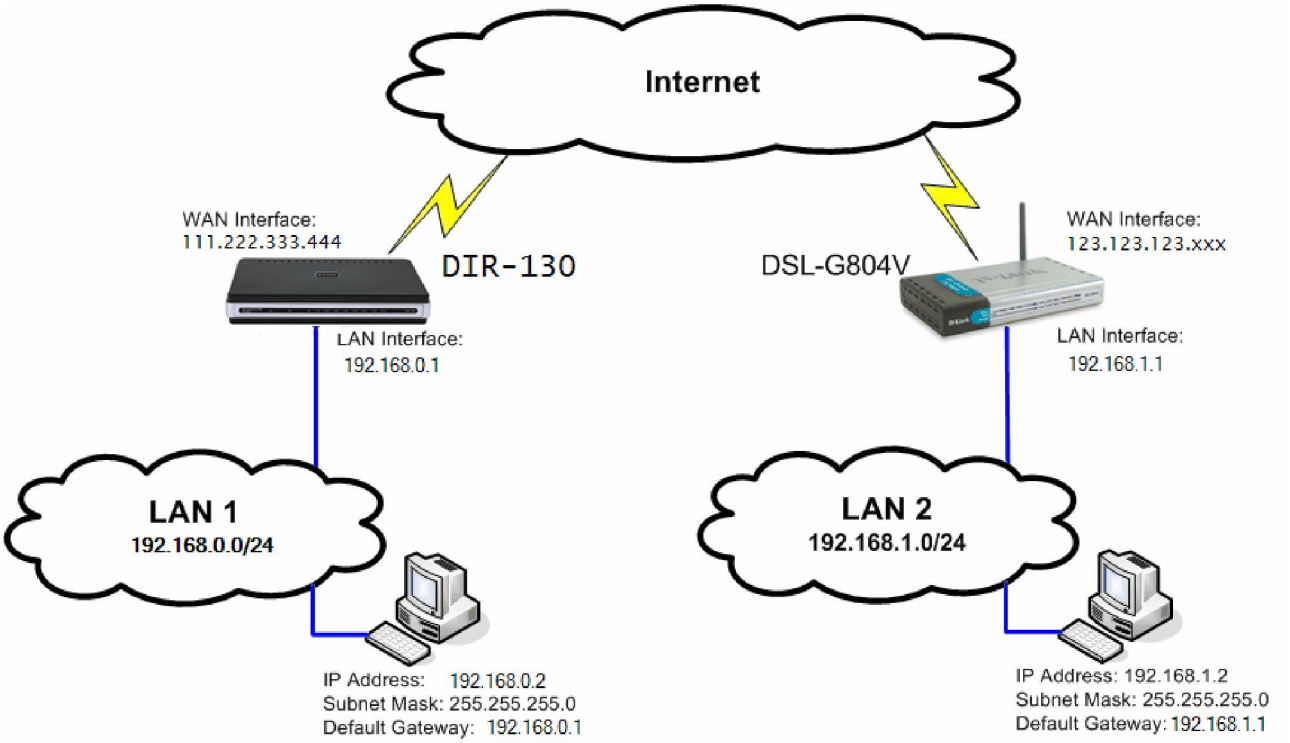
How to setup IPSec VPN connection between DIR-130 and DSL-G804V VPN Routers

This setup example uses the following network settings:

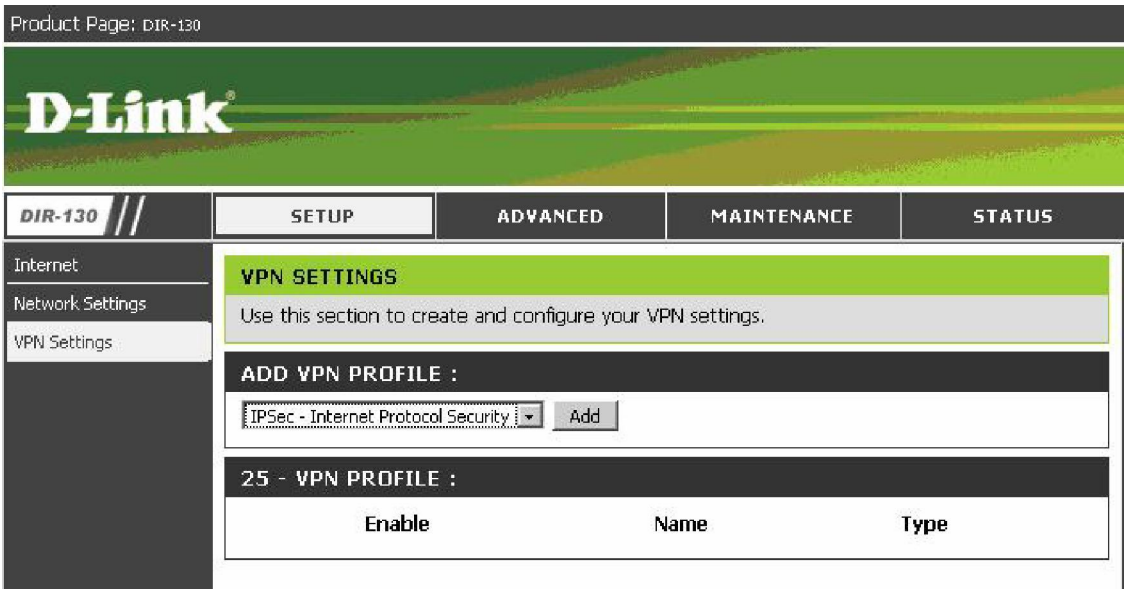


In our example the IPSec VPN tunnel is established between two LANs: 192.168.0.x and 192.168.1.x.
NOTE: It is essential to have private networks (LAN 1 and LAN 2) on different subnets.

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**.

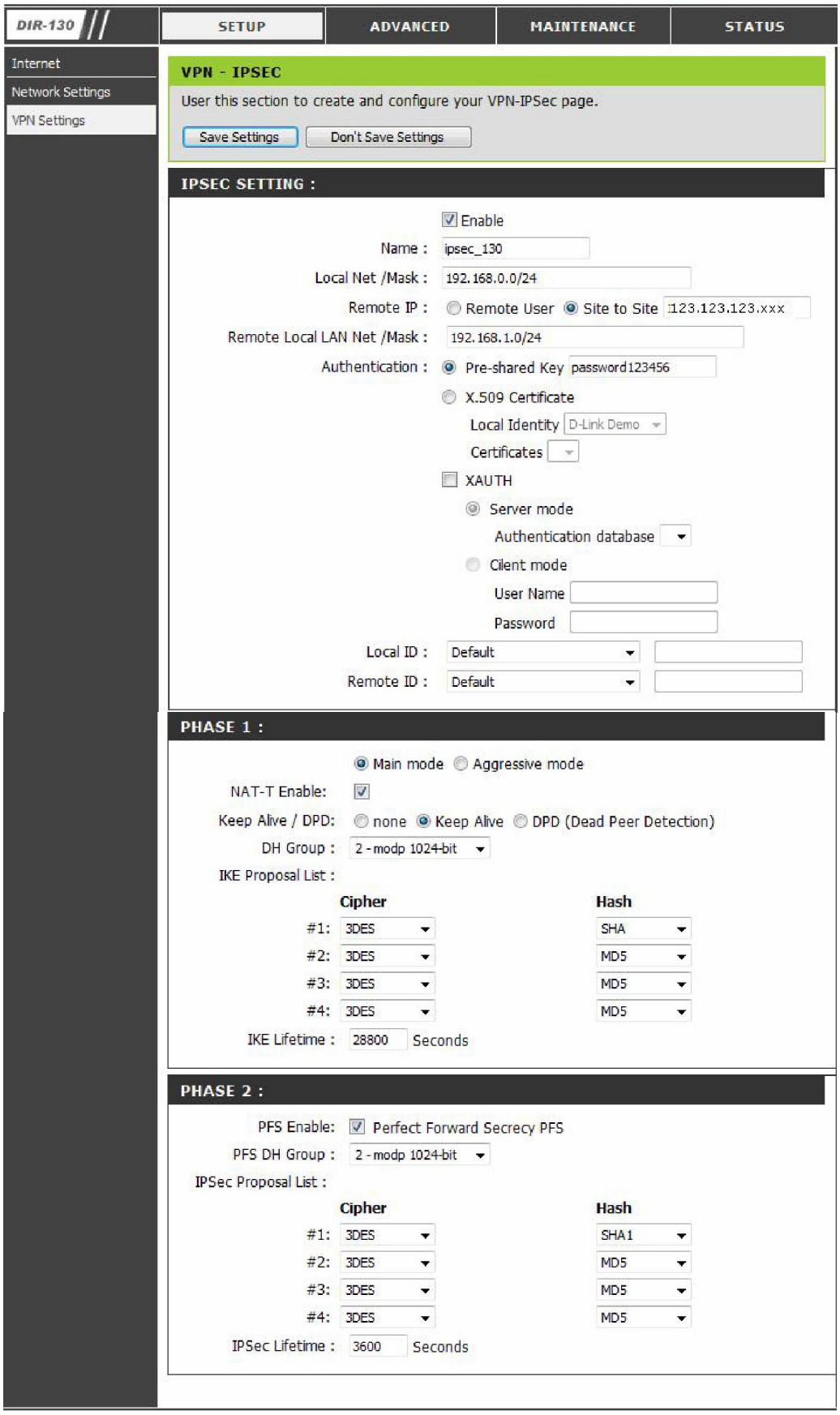


Step 3: Configure the *IPSec VPN* as followed:

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


DIR-130
SETUP
ADVANCED
MAINTENANCE
STATUS
Internet
Network Settings
VPN Settings
VPN - IPSEC
User this section to create and configure your VPN-IPSec page.
Save Settings
Don't Save Settings
IPSEC SETTING :
Enable
Name : ipsec_130
Local Net /Mask : 192.168.0.0/24
Remote IP : Remote User Site to Site 123.123.123.xxx
Remote Local LAN Net /Mask : 192.168.1.0/24
Authentication : Pre-shared Key password123456
X.509 Certificate
Local Identity D-Link Demo
Certificates
XAUTH
Server mode
Authentication database
Client mode
User Name
Password
Local ID : Default
Remote ID : Default
PHASE 1 :
Main mode Aggressive mode
NAT-T Enable:
Keep Alive / DPD: none Keep Alive DPD (Dead Peer Detection)
DH Group : 2 - modp 1024-bit
IKE Proposal List :
Cipher
Hash
#1: 3DES SHA
#2: 3DES MD5
#3: 3DES MD5
#4: 3DES MD5
IKE Lifetime : 28800 Seconds
PHASE 2 :
PFS Enable: Perfect Forward Secrecy PFS
PFS DH Group : 2 - modp 1024-bit
IPSec Proposal List :
Cipher
Hash
#1: 3DES SHA1
#2: 3DES MD5
#3: 3DES MD5
#4: 3DES MD5
IPSec Lifetime : 3600 Seconds

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).

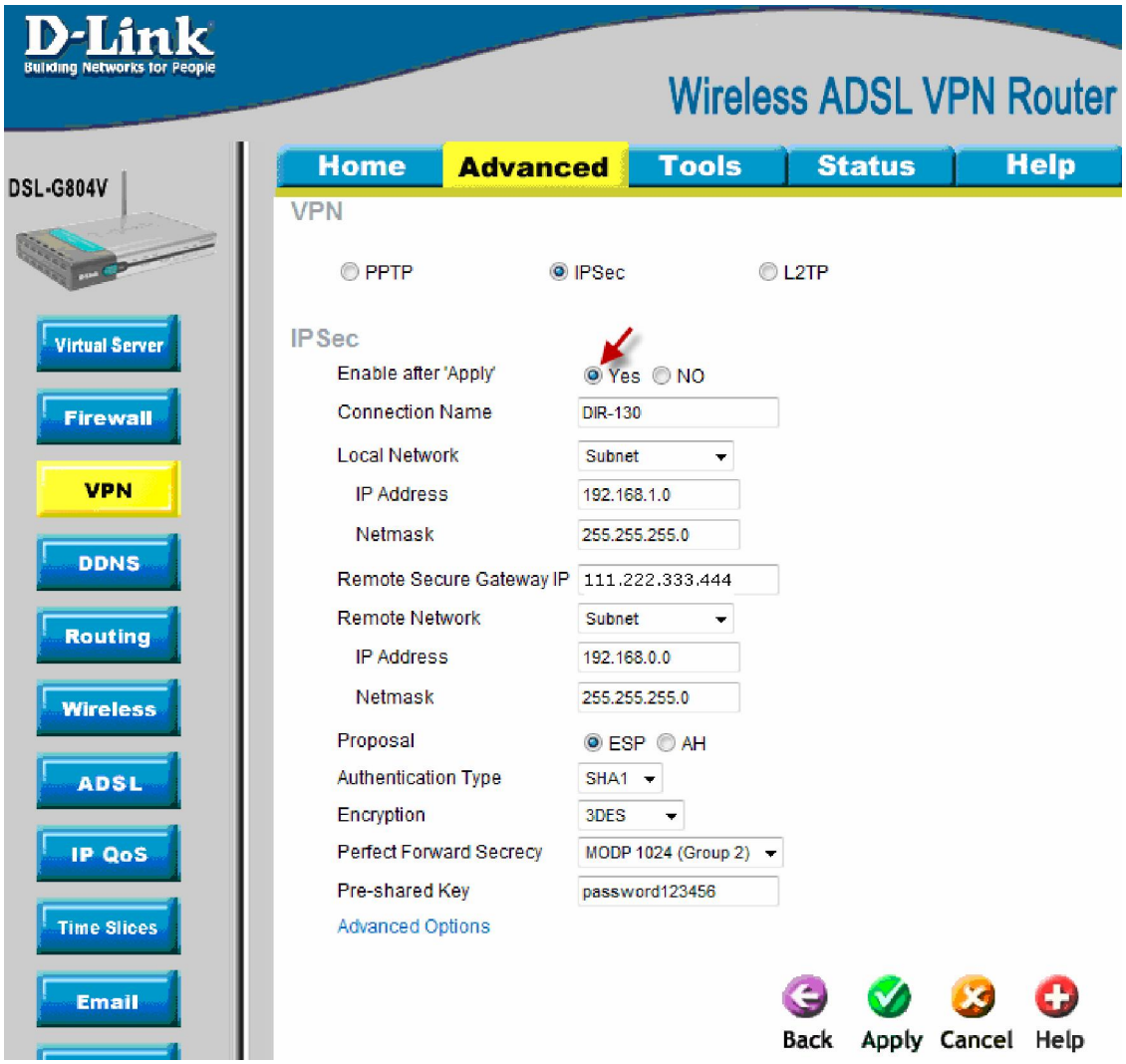
- Click on **Advanced Options**
- **IKE Mode**: select **Main**

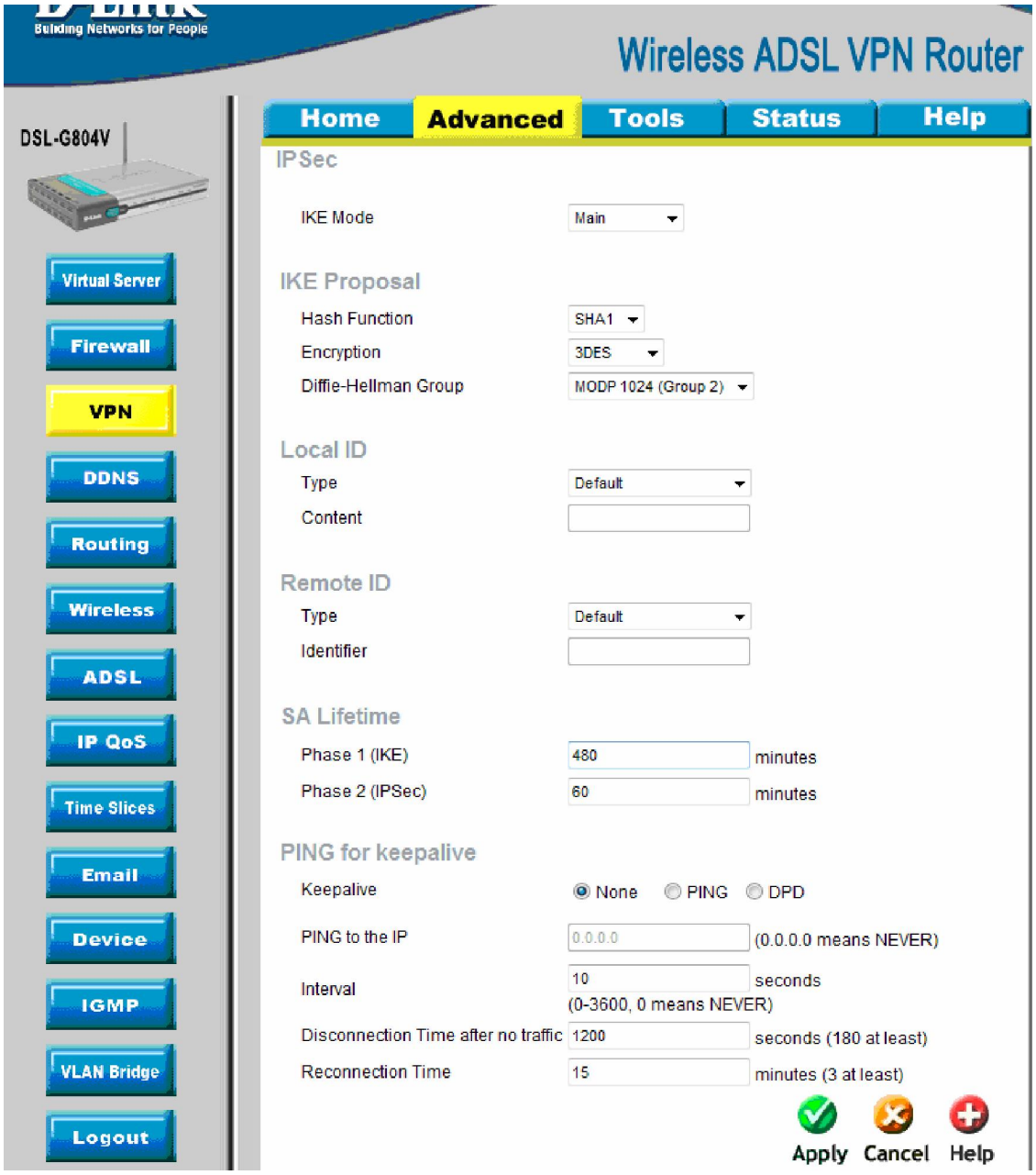
- **IKE Proposal**
- **HASH Function**: select **SHA1**
- **Encryption**: select **3DES**
- **Local ID**: leave as Default
- **Remote ID**: leave as Default

- **SA Lifetime**
- **Phase 1 (IKE)** : leave as 480 (default)
- **Phase 2 (IPSec):** leave as 60 (default)

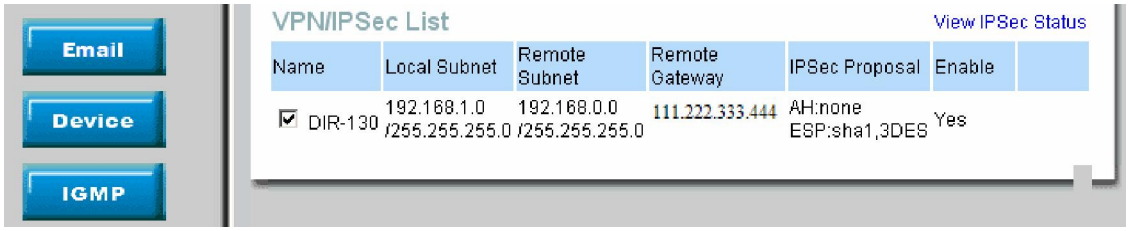
- **PING Keep Alive**
- **Keepalive**: select **None**

- 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.


D-Link
Building Networks for People
Wireless ADSL VPN Router
DSL-G804V
Home
Advanced
Tools
Status
Help
Virtual Server
Firewall
VPN
DDNS
Routing
Wireless
ADSL
IP QoS
Time Slices
Email
VPN
PPTP
IPSec
L2TP
IPSec
Enable after 'Apply'
Yes
NO
Connection Name
DIR-130
Local Network
Subnet
IP Address
192.168.1.0
Netmask
255.255.255.0
Remote Secure Gateway IP
111.222.333.444
Remote Network
Subnet
IP Address
192.168.0.0
Netmask
255.255.255.0
Proposal
ESP
AH
Authentication Type
SHA1
Encryption
3DES
Perfect Forward Secrecy
MODP 1024 (Group 2)
Pre-shared Key
password123456
Advanced Options
Back
Apply
Cancel
Help



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

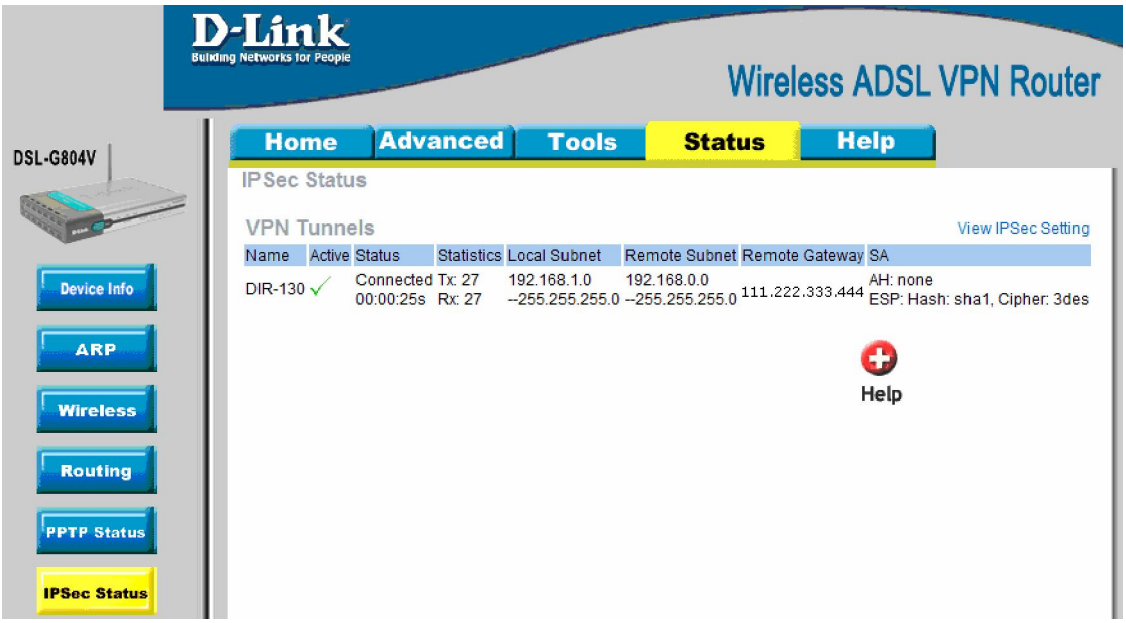


Step 3.

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

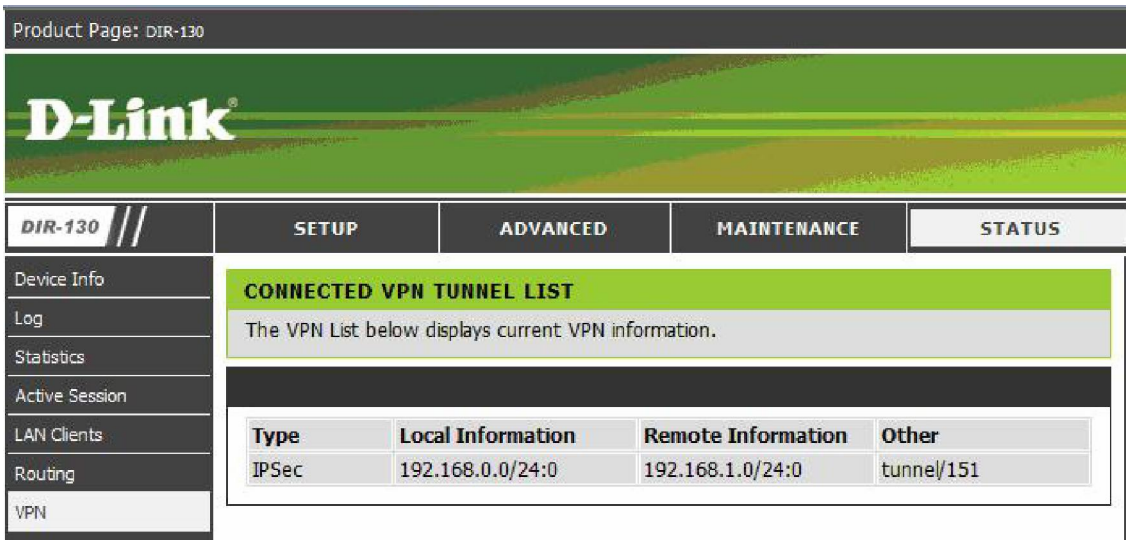
How to check VPN connection status on the DSL-G804V

- 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.

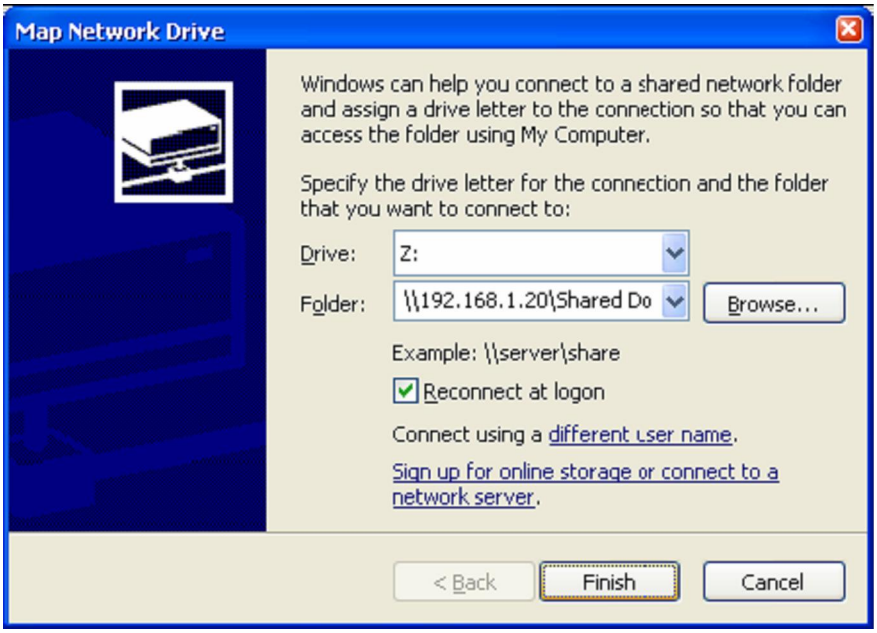


If VPN Tunnel can not be established:

• 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):



- 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.