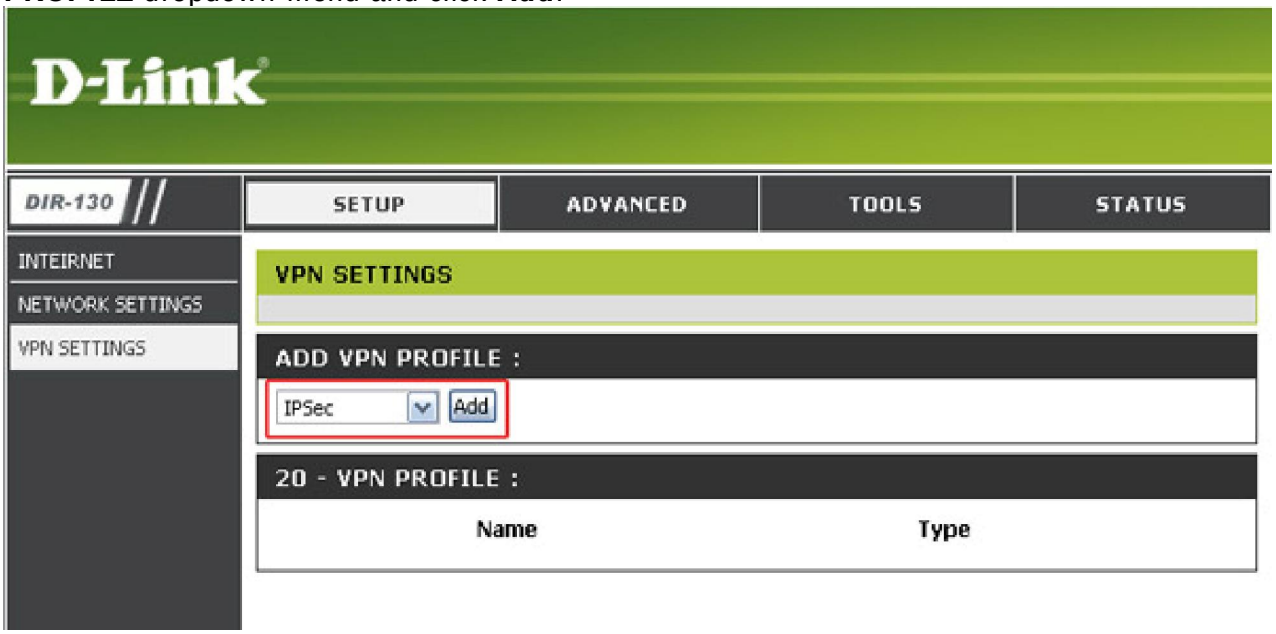
DS-60x VPN to DIR-130

Configuration of DIR-130

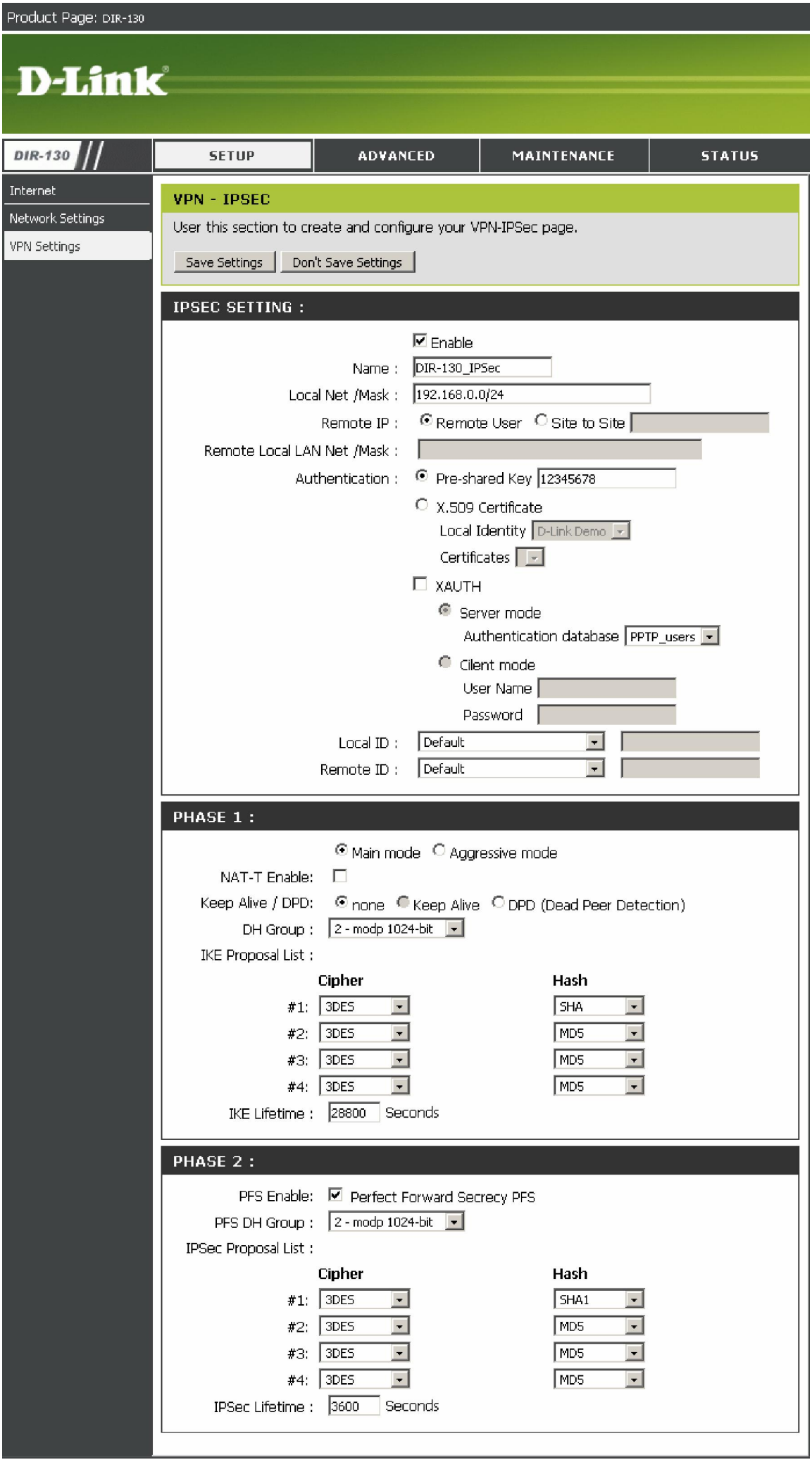
Step 1: Open your web browser and type in the IP address of the router (*192.168.0.1* by default). Enter the username (*admin* by default) and password (blank by default), and then click **OK**.

Step 2: Click on **SETUP** and select **VPN SETTINGS**. Choose **IPSec** from the **ADD VPN PROFILE** dropdown menu and click **Add**.

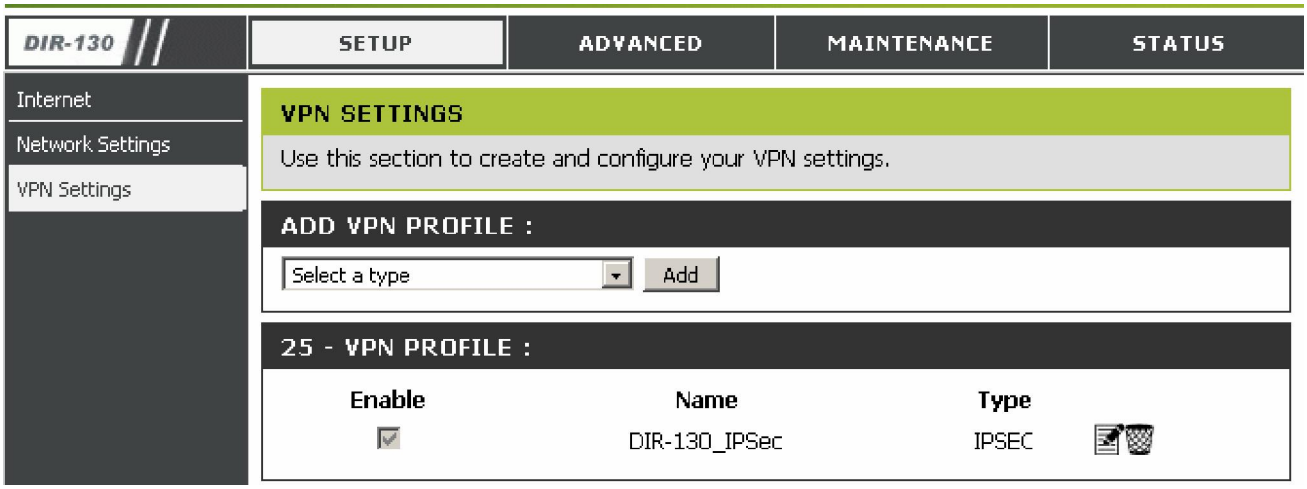


Step 3: Configure the *IPSec VPN* as followed:

- **Enable:** check box to enable
- **Name:** enter a name for the VPN
- **Local Net / Mask:** enter the local network and subnet mask
- **Remote IP:** select Remote User
- **Authentication:** enter your desired Pre-shared Key
- **Local ID:** leave as Default
- **Remote ID:** leave as Default
-
- **Phase 1 Main Mode:** selected
- **NAT-T Enable:** untick the box
- **Keep Alive / DPD:** select **none**
- **DH Group:** select **2-modp 1024-bit**
- **IKE Proposal List:**
- **Cipher #1:** select **3DES**
- **Hash: #1:** select **SHA**
- **IKE Lifetime:** enter **28800** (default)
-
- **Phase 2:**
- **PFS Enable:** tick the box (default)
- **PFS DH Group:** select **2-modp 1024-bit**
- **IPSec Proposal List:**
- **Cipher #1:** select **3DES**
- **Hash #1:** select **SHA1**
- **IPSec Lifetime:** enter **3600** (default)
- Click **Save Settings** then **Continue**

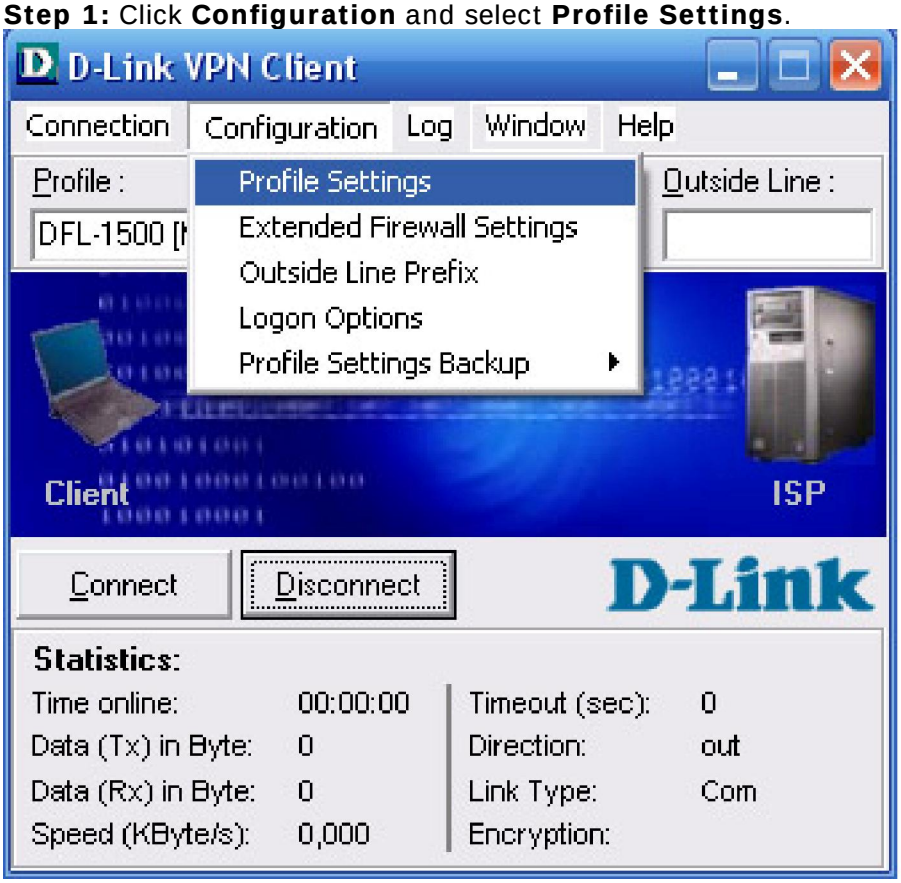

Product Page: DIR-130
D-Link
DIR-130
SETUP
ADVANCED
MAINTENANCE
STATUS
Internet
Network Settings
VPN Settings
VPN - IPSEC
User this section to create and configure your VPN-IPSec page.
Save Settings
Don't Save Settings
IPSEC SETTING :
Enable
Name : DIR-130_IPSec
Local Net /Mask : 192.168.0.0/24
Remote IP : Remote User Site to Site
Remote Local LAN Net /Mask :
Authentication : Pre-shared Key 12345678
X.509 Certificate
Local Identity D-Link Demo
Certificates
XAUTH
Server mode
Authentication database PPTP_users
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

The IPSec Tunnel should now appear in the **VPN PROFILE** list below.

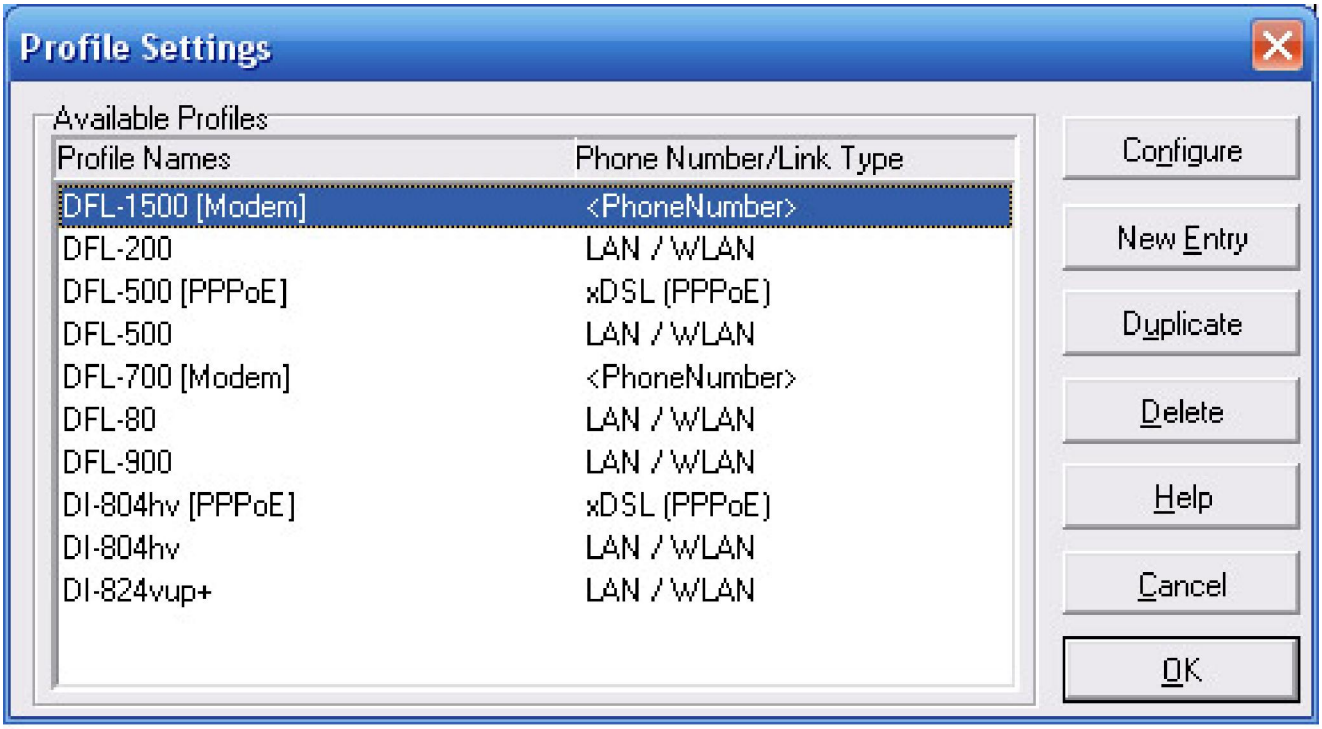


Configuration of DS-601/605 client VPN software

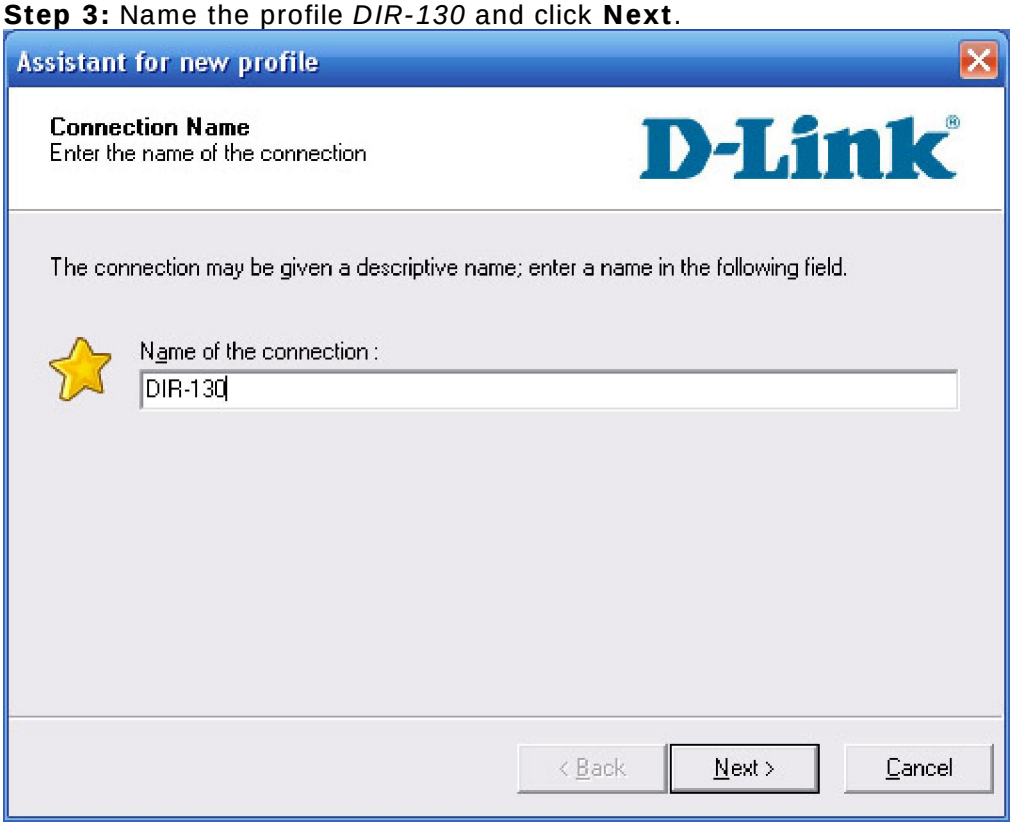
Step 1: Click **Configuration** and select **Profile Settings**.



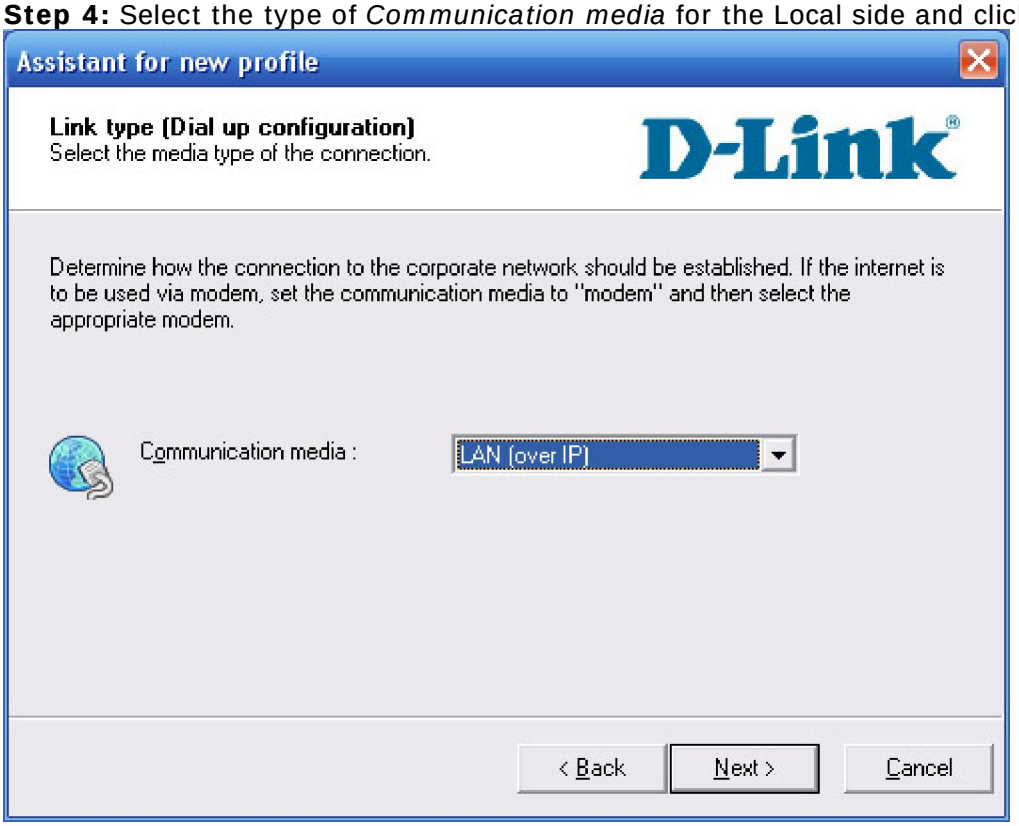
Step 2: Click **New Entry** to create a profile for the *DIR-130*.


Profile Settings
Available Profiles
Profile Names
Phone Number/Link Type
DFL-1500 [Modem]
<PhoneNumber>
DFL-200
LAN / WLAN
DFL-500 [PPPoE]
xDSL (PPPoE)
DFL-500
LAN / WLAN
DFL-700 [Modem]
<PhoneNumber>
DFL-80
LAN / WLAN
DFL-900
LAN / WLAN
DI-804hv [PPPoE]
xDSL (PPPoE)
DI-804hv
LAN / WLAN
DI-824vup+
LAN / WLAN
Configure
New Entry
Duplicate
Delete
Help
Cancel
OK

Step 3: Name the profile *DIR-130* and click **Next**.

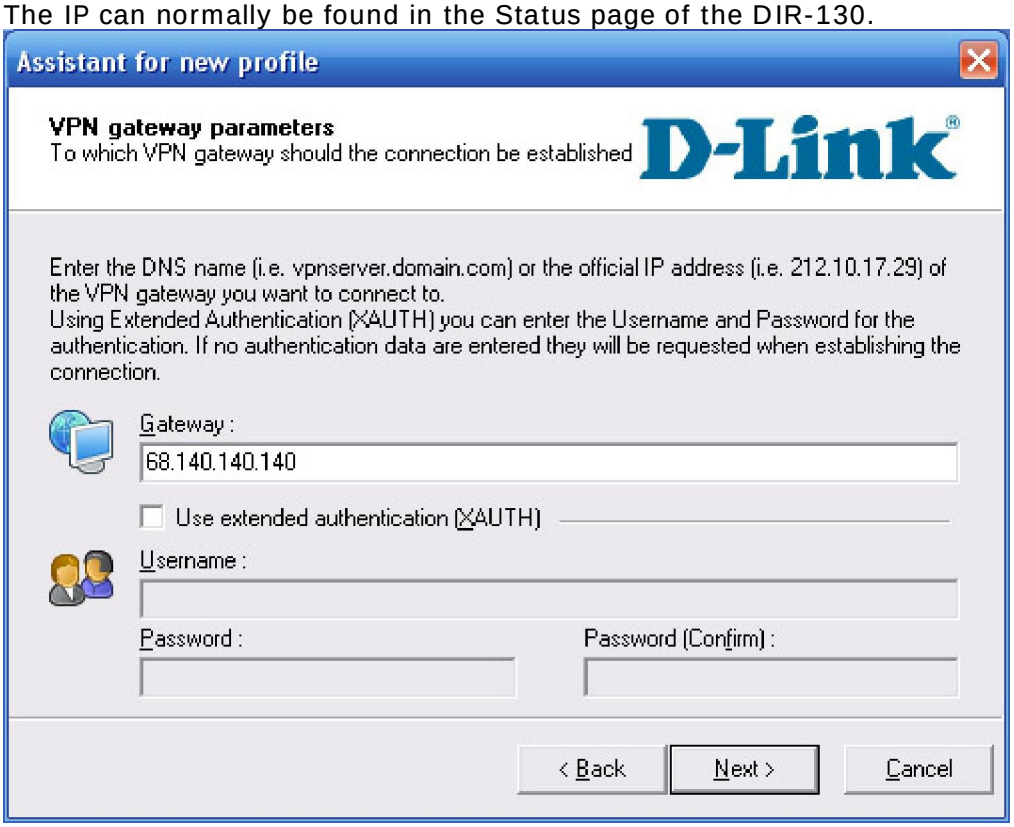


Step 4: Select the type of *Communication media* for the Local side and click **Next**.

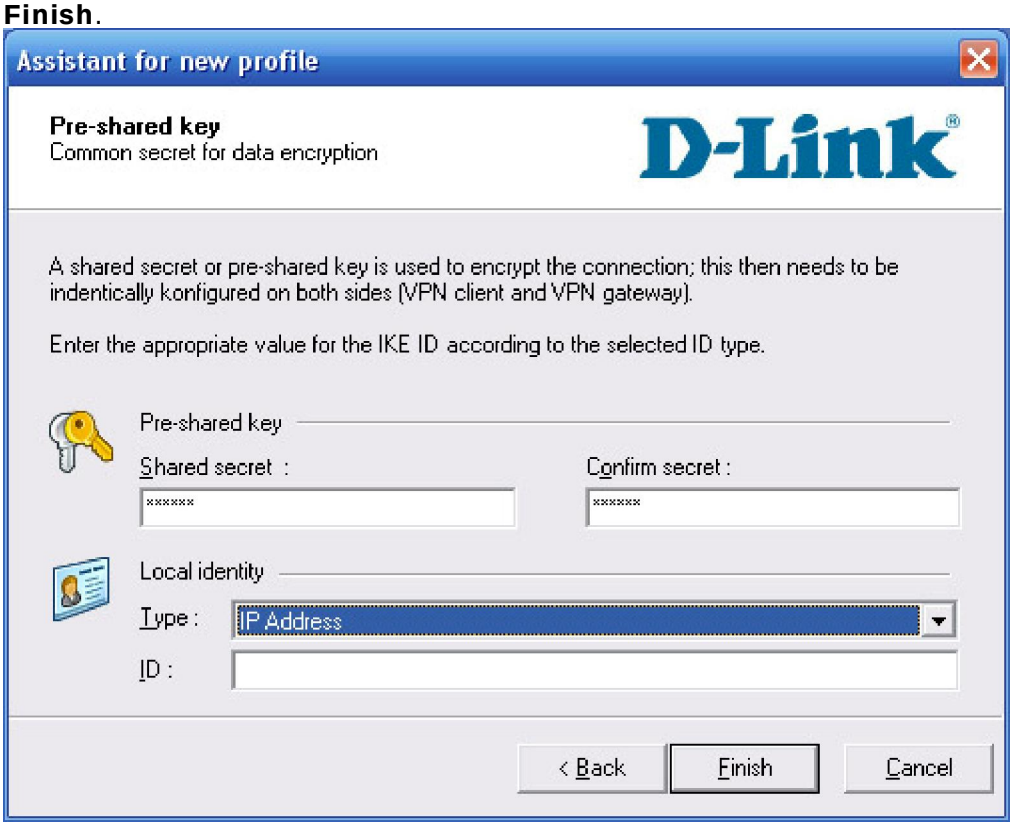


Step 5: Enter the *Remote Gateway* and click **Next**.

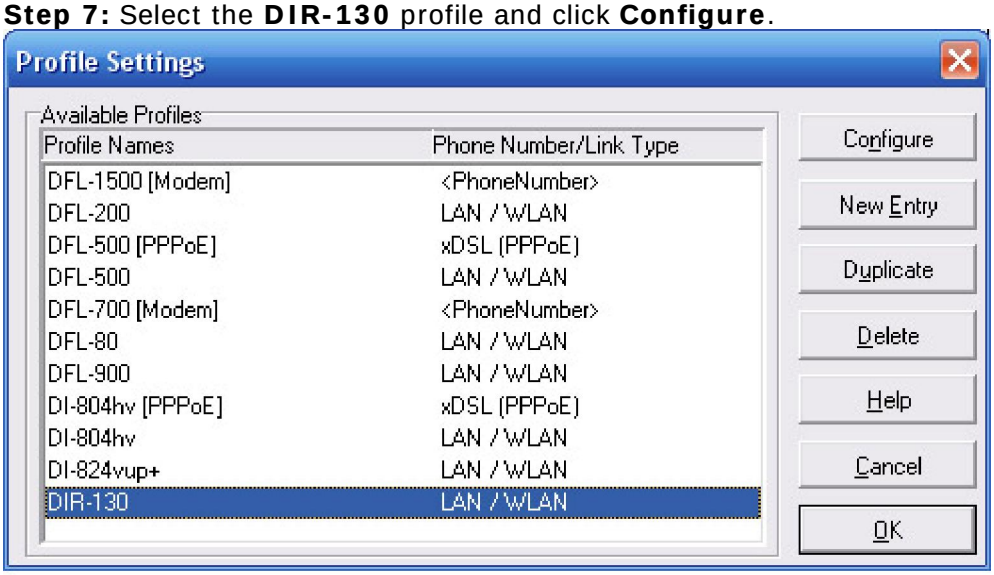
The IP can normally be found in the Status page of the DIR-130.



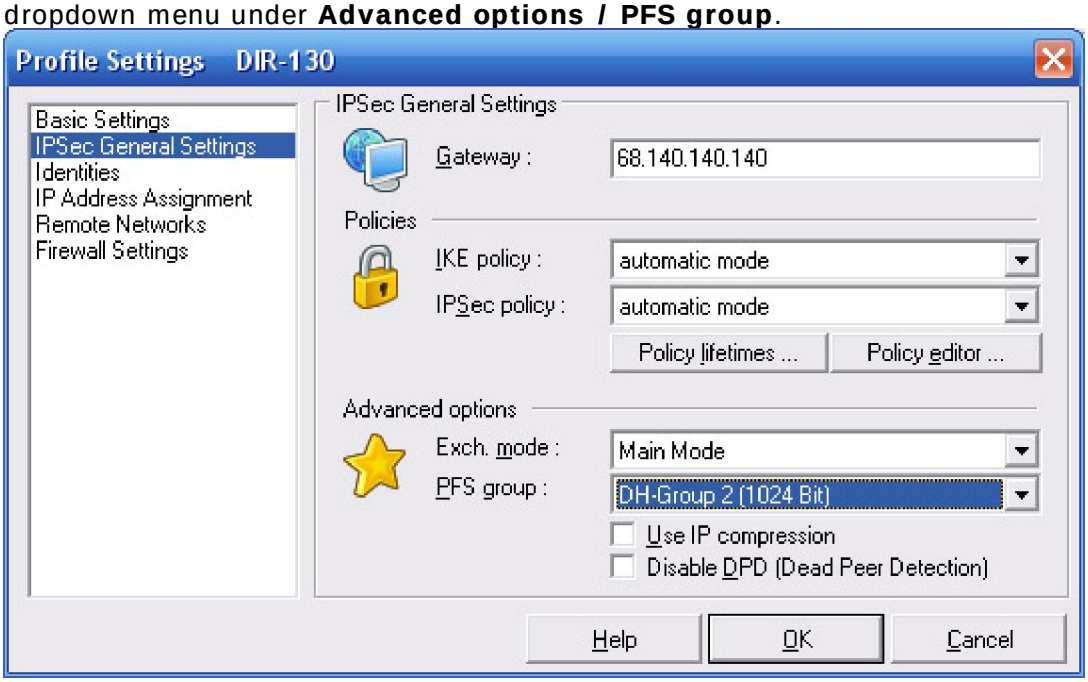
Step 6: Enter the *Pre-shared Key* in both the **Shared secret** and **Confirm secret** and click **Finish**.



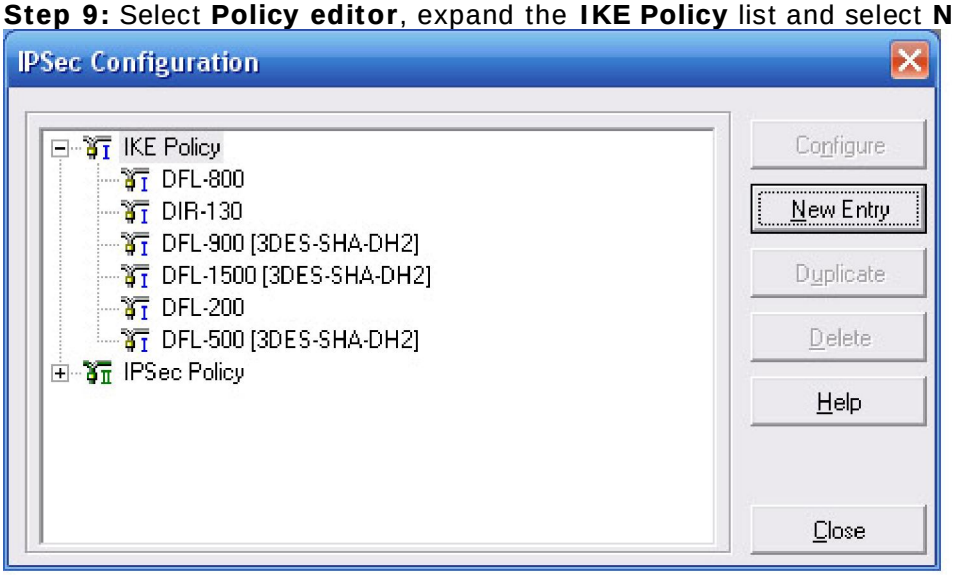
Step 7: Select the **DIR-130** profile and click **Configure**.



Step 8: Select **IPSec General Settings** and select **DH-Group 2 (1024 Bit)** from the dropdown menu under **Advanced options / PFS group**.



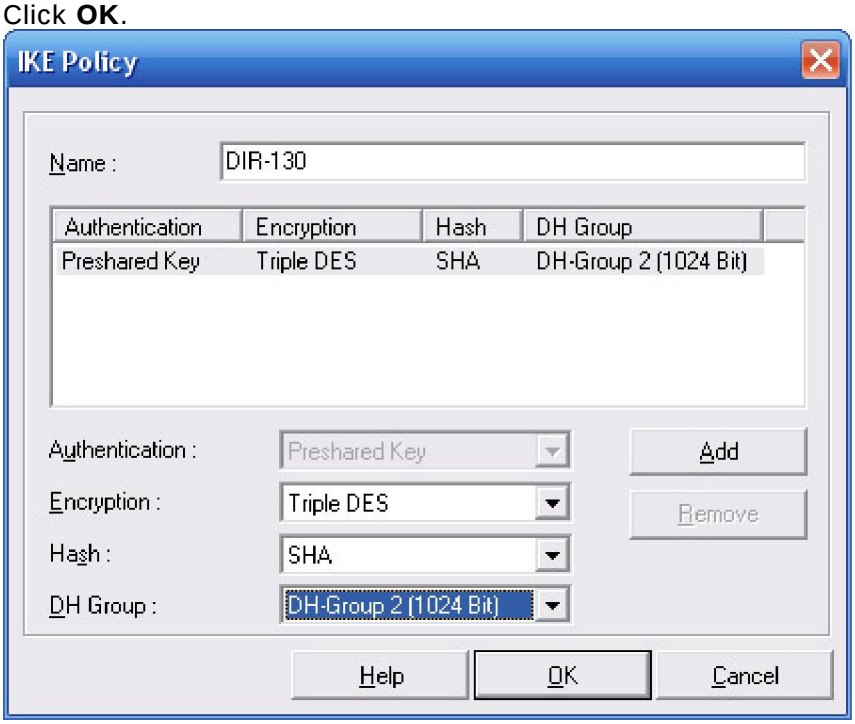
Step 9: Select **Policy editor**, expand the **IKE Policy** list and select **New Entry**.



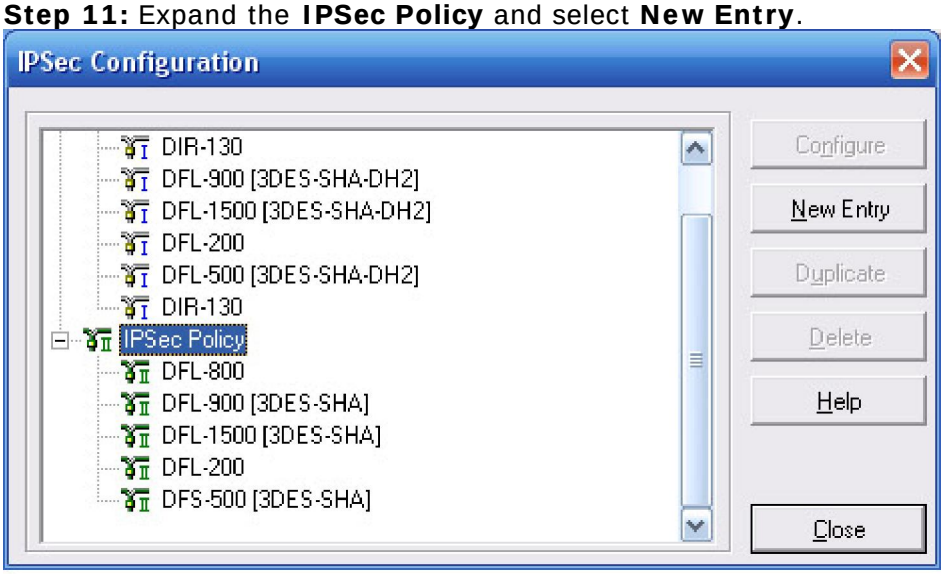
Step 10: Configure the *IKE Policy* as followed:

- **Name:** enter a name for the policy (*DIR-130* in this example)
- **Encryption:** *Triple DES*
- **Hash:** *SHA*
- **DH Group:** *DH-Group 2* (*1024 Bit*)

Click **OK**.



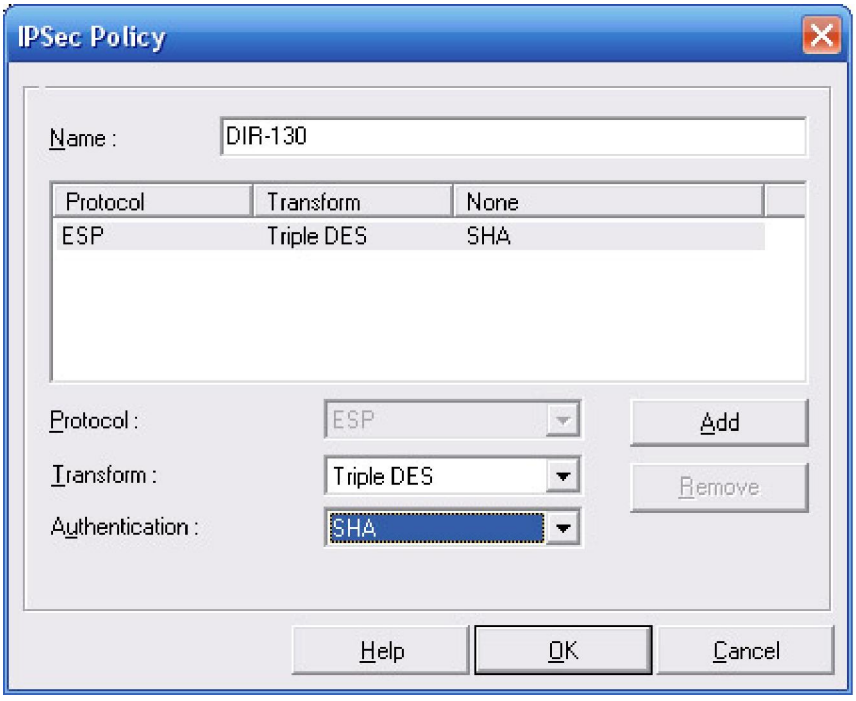
Step 11: Expand the **IPSec Policy** and select **New Entry**.



Step 12: Configure the *IPSec policy* as followed:

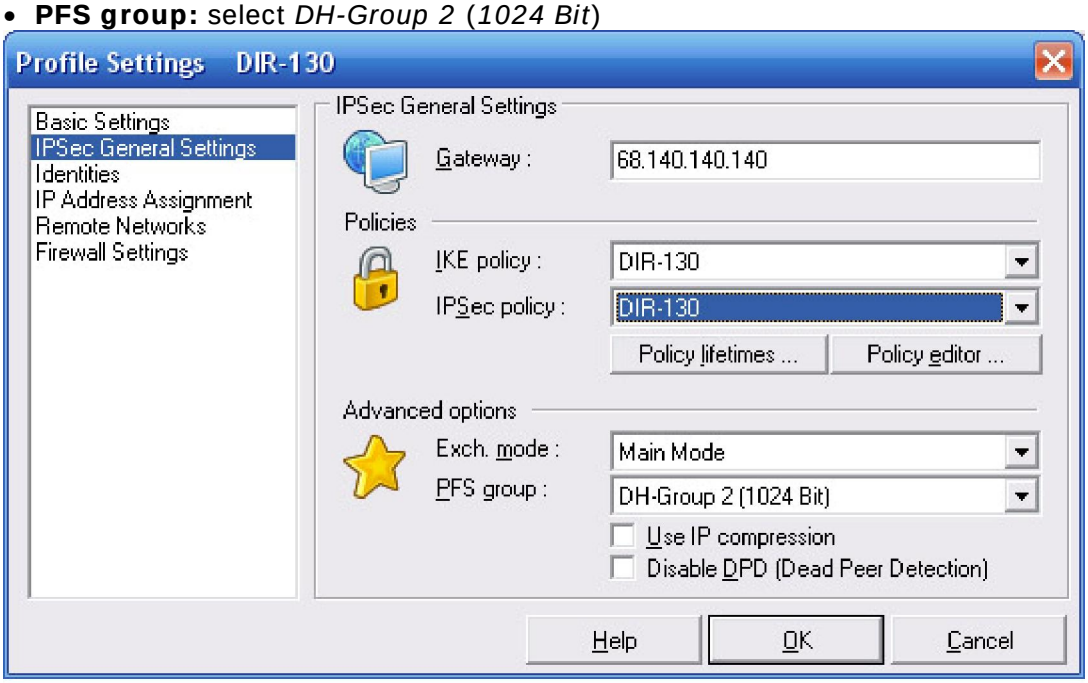
- **Name:** entry a name for the policy(*DIR-130* in this example)
- **Transform:** *Triple DES*
- **Authentication:** *SHA*

Click **OK** and **Close**.

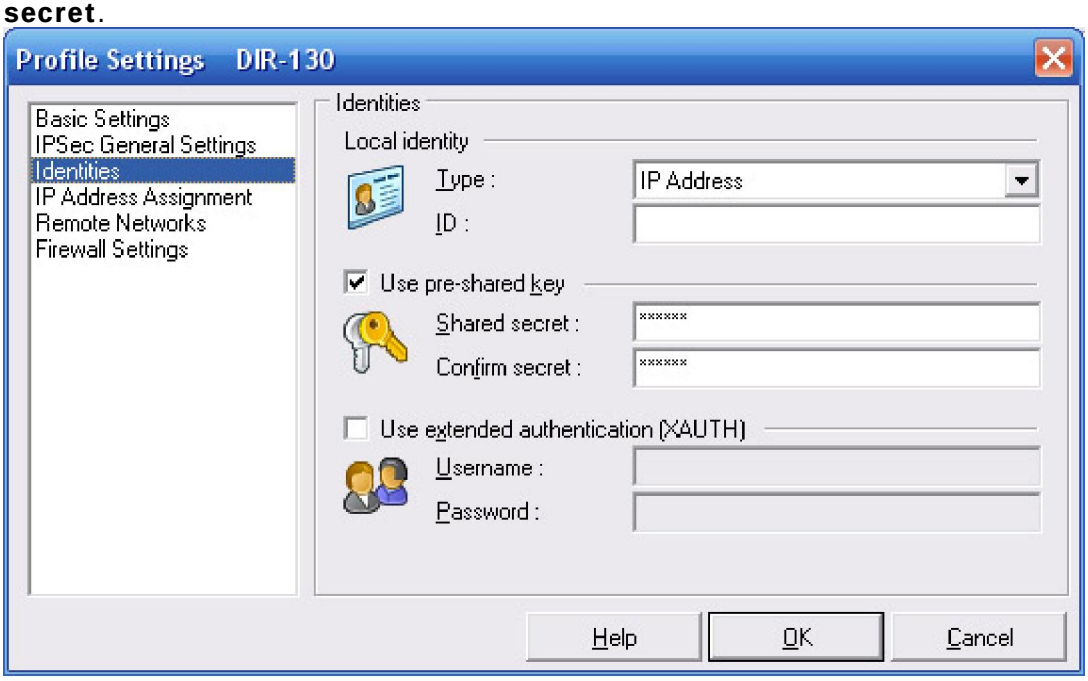


Step 13: The **IPSec General Settings** should be configured as followed:

- **Gateway: WAN IP** address of the remote router
- **IKE policy:** select *DIR-130* from the dropdown menu
- **IPSec policy:** select *DIR-130* from the dropdown menu
- **Exch. mode:** select *Main mode*
- **PFS group:** select *DH-Group 2* (*1024 Bit*)

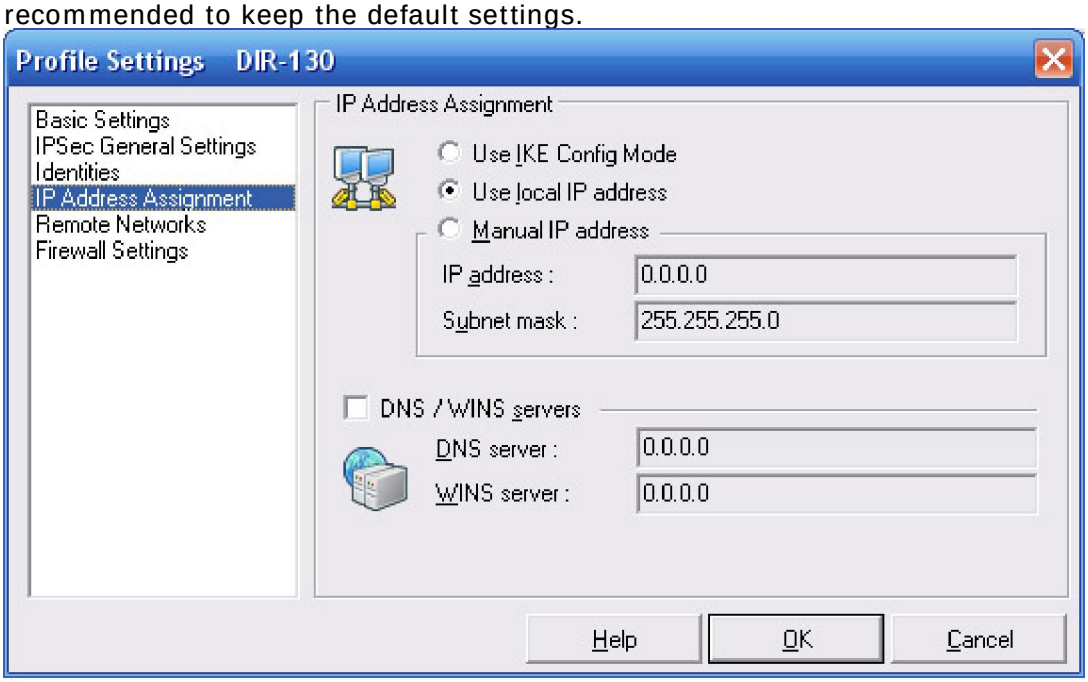


Step 14: Select **Identities** and enter the *pre-shared key* next to **Shared secret** and **Confirm secret**.



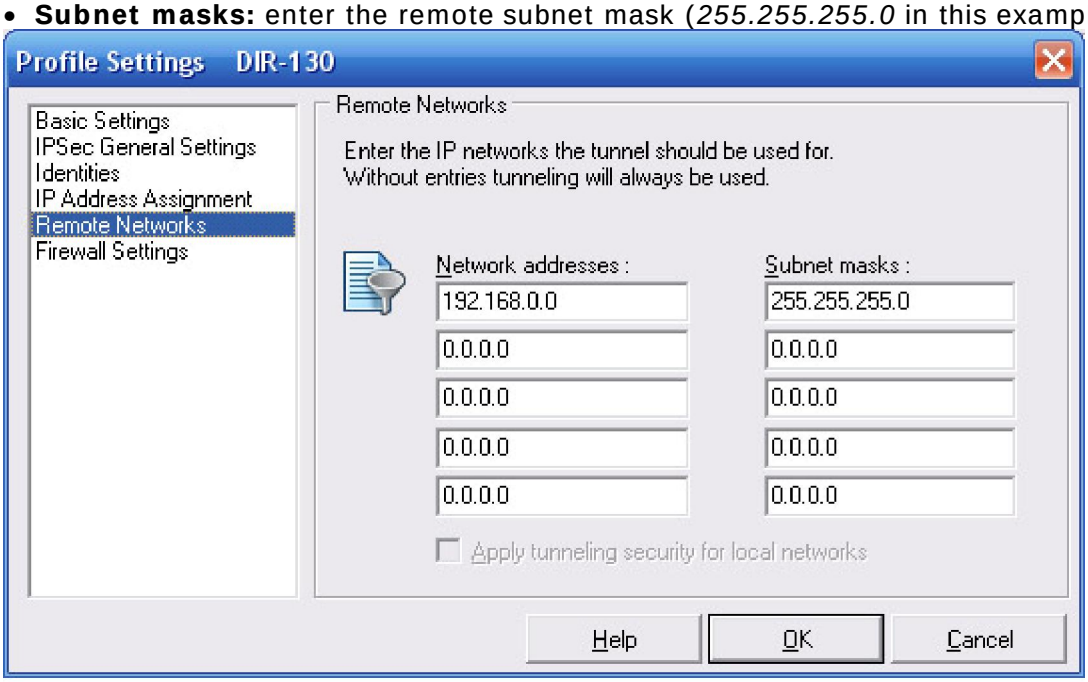
NOTE: *The Preshared Key must be identical to the one configured on the router.*

Step 15: Select **IP Address Assignment** and configure it according to your settings. It is recommended to keep the default settings.

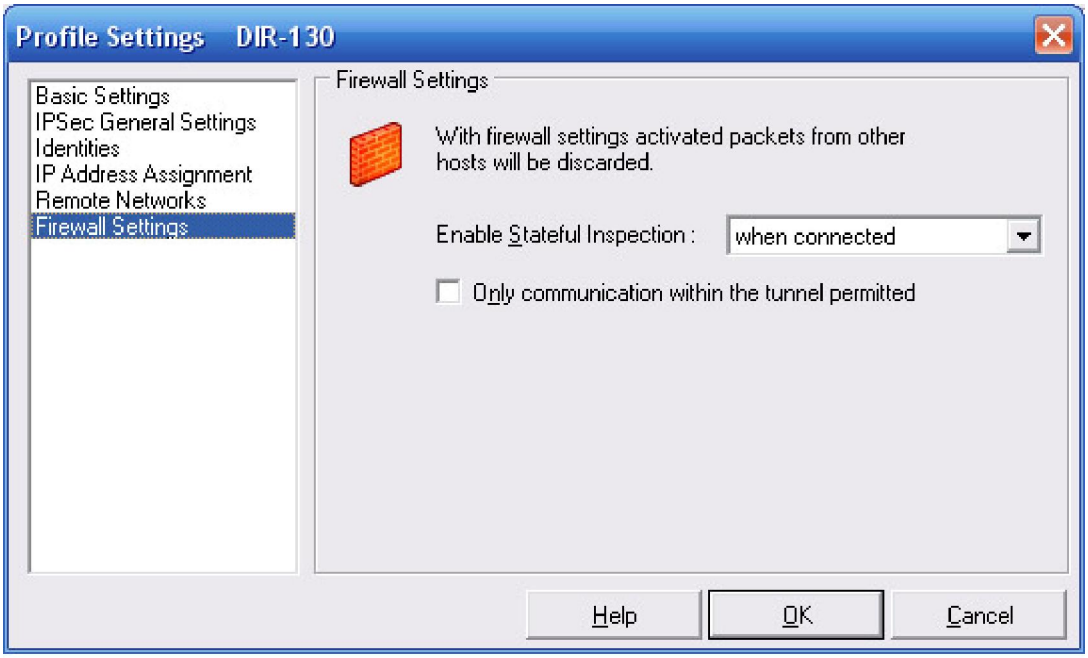


Step 16: Select **Remote Networks** and configure as followed:

- **Network addresses:** enter the remote network (*192.168.0.0* in this example)
- **Subnet masks:** enter the remote subnet mask (*255.255.255.0* in this example)



Step 17: Select **Firewall Settings** and set the *Enable Stateful Inspection* to **when connected**. Click **OK** to save the settings and then click **OK** again to go back to the connection screen.



Step 18: Click **Connect** to establish the VPN connection to the router.