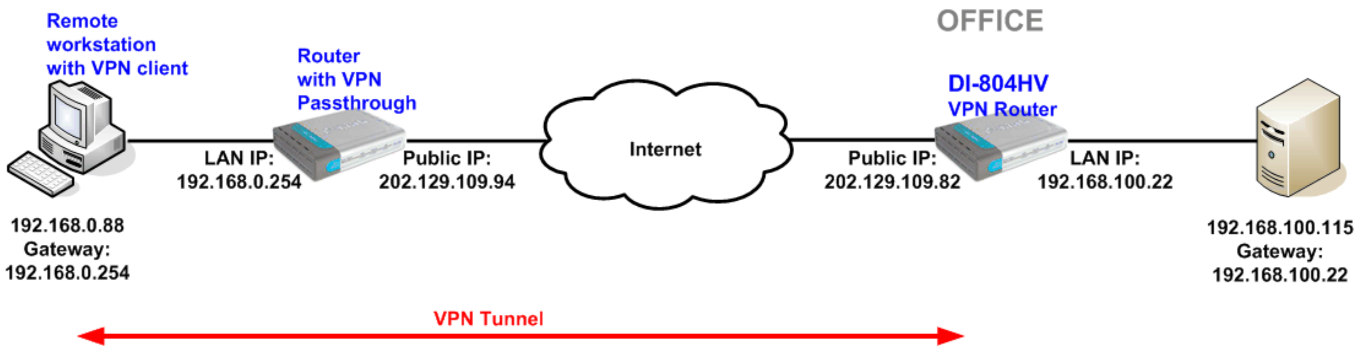
Setting up D-Link VPN Client to VPN Routers

Office Unit: DI-804HV (firmware 1.41)

LAN IP: 192.168.100.22   Subnet Mask: 255.255.255.0
WAN IP: 202.129.109.82 Subnet Mask: 255.255.255.224
Default Gateway: 202.129.109.65

Remote PC:

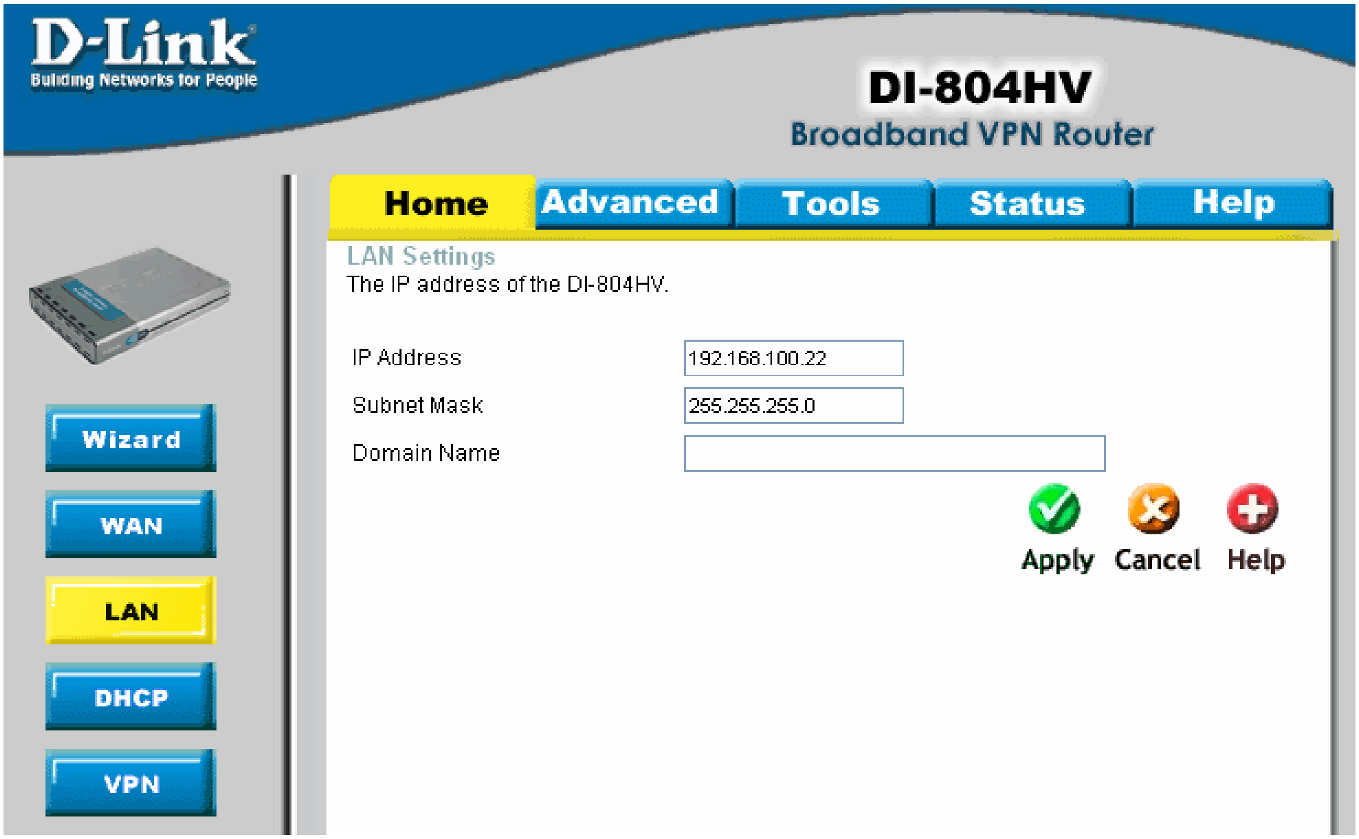
IP: 192.168.0.108 Subnet Mask: 225.255.255.0
Default Gateway: 192.168.0.254



Office DI-804HV Settings:

Log into the router’s WEB interface and go to Home > LAN. Change the IP address of the LAN port of the router to required IP.

> Once you have changed the LAN IP address on the router, make sure your PC has an IP address from the same subnet (192.168.100.x in this example), you may just need to renew IP on your PC or reboot.



LAN Settings

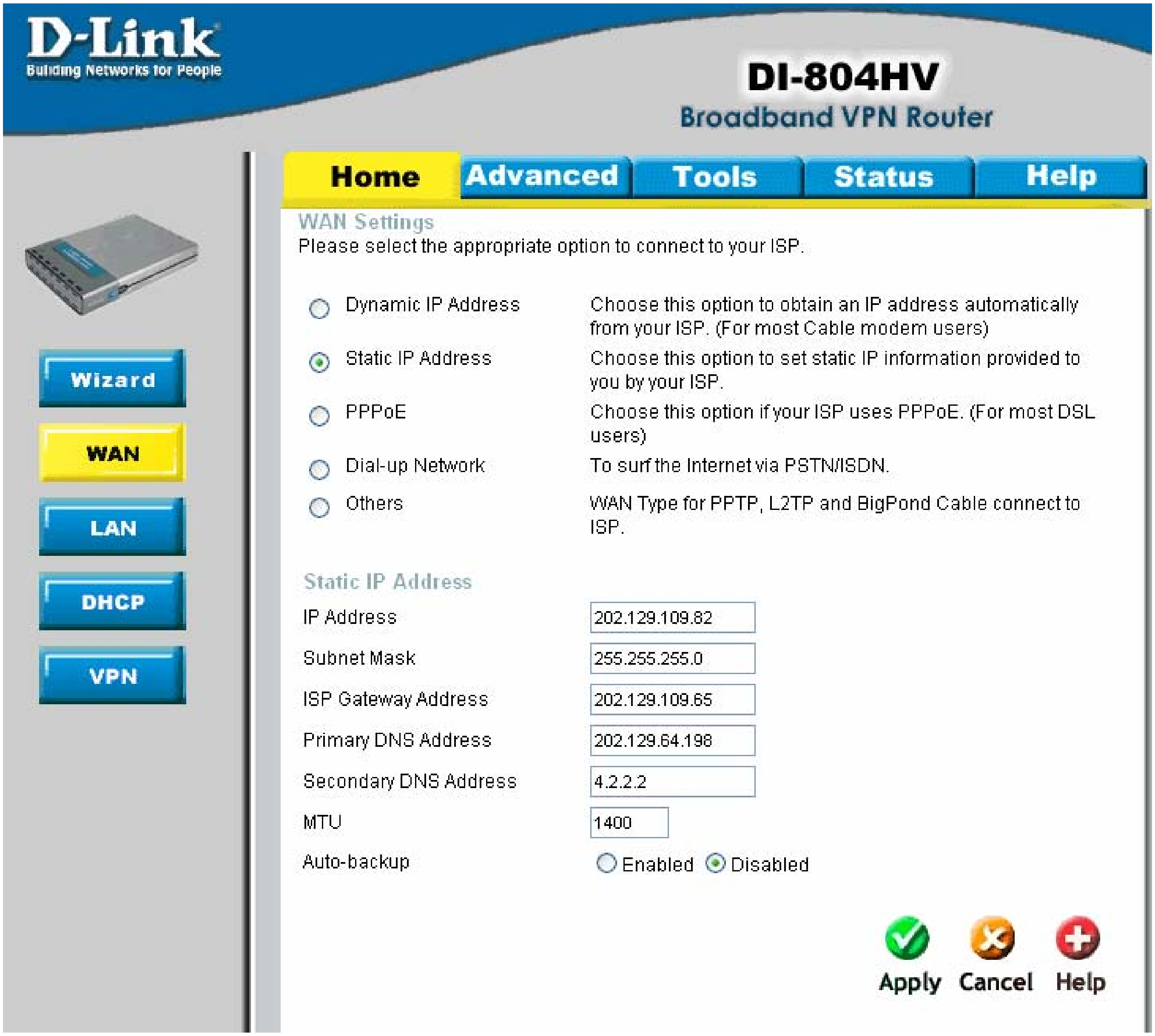
The IP address of the DI-804HV.

IP Address	192.168.100.22
Subnet Mask	255.255.255.0
Domain Name	

Next go to the Home > WAN page, choose the type of connection your ISP requires. In our example it is Static IP Address.

> You need to have a static IP address on the WAN port of at least one unit out of the two participating in VPN connection. Some PPPoE connections have a static IP as well (in most of such cases you do not have to specify the IP – your ISP will be providing you with the same IP every time you connect).

After setting up the WAN port click on Apply to save settings.



WAN Settings

Please select the appropriate option to connect to your ISP.

○	Dynamic IP Address	Choose this option to obtain an IP address automatically from your ISP. (For most Cable modem users)
●	Static IP Address	Choose this option to set static IP information provided to you by your ISP.
○	PPPoE	Choose this option if your ISP uses PPPoE. (For most DSL users)
○	Dial-up Network	To surf the Internet via PSTN/ISDN.
○	Others	WAN Type for PPTP, L2TP and BigPond Cable connect to ISP.

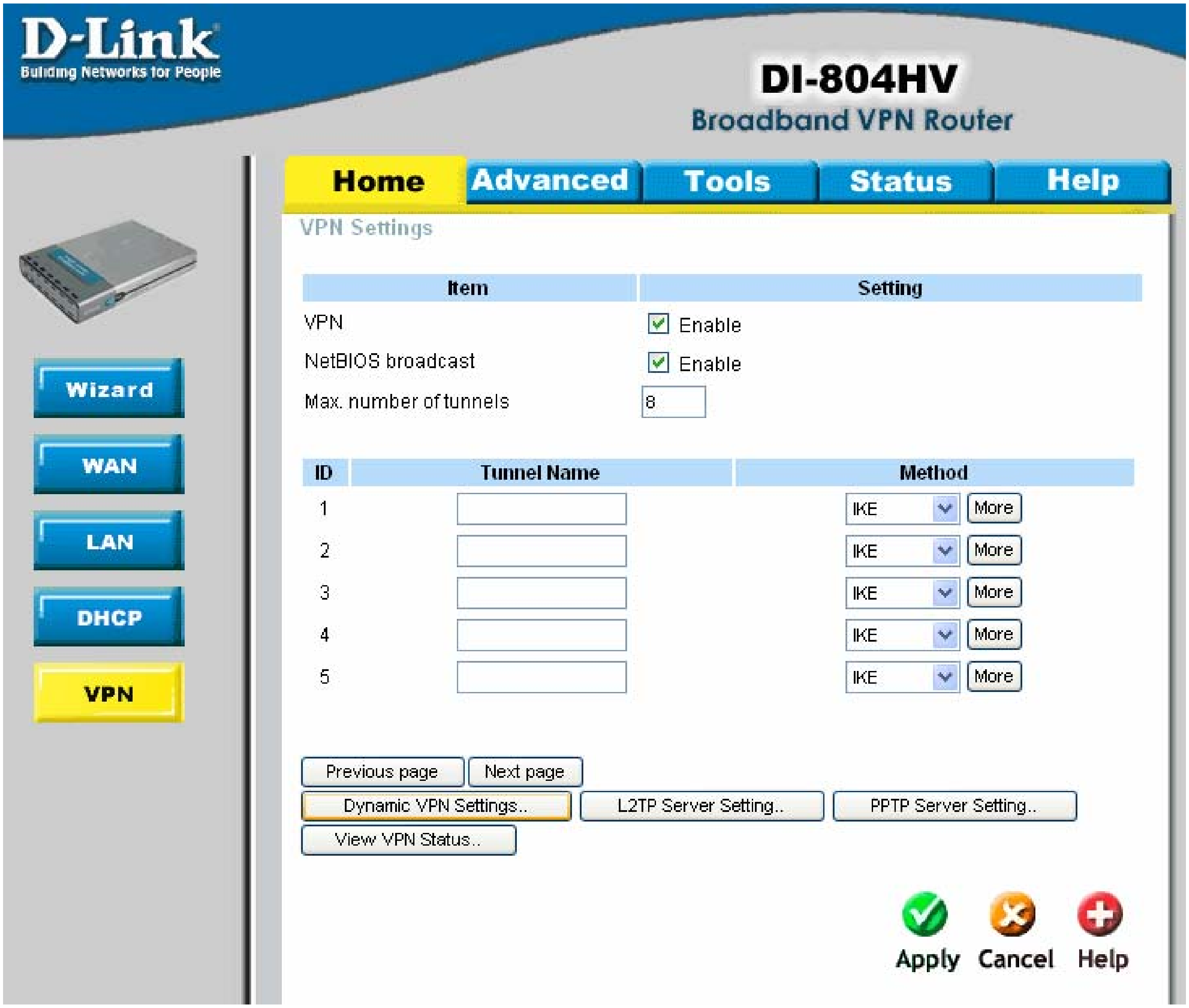
Static IP Address

IP Address	202.129.109.82
Subnet Mask	255.255.255.0
ISP Gateway Address	202.129.109.65
Primary DNS Address	202.129.64.198
Secondary DNS Address	4.2.2.2
MTU	1400
Auto-backup	○ Enabled ● Disabled

Next make sure you can access the Internet (that will confirm that you have set WAN settings correctly), then log back into the router and go into Home > VPN.

Make sure you have VPN Enable box ticked and tick NetBIOS Broadcast.

Click apply, once the page comes back click on Dynamic VPN Settings



VPN Settings

Item	Setting
VPN	☑ Enable
NetBIOS broadcast	☑ Enable
Max. number of tunnels	8

ID	Tunnel Name	Method
1		IKE
2		IKE
3		IKE
4		IKE
5		IKE

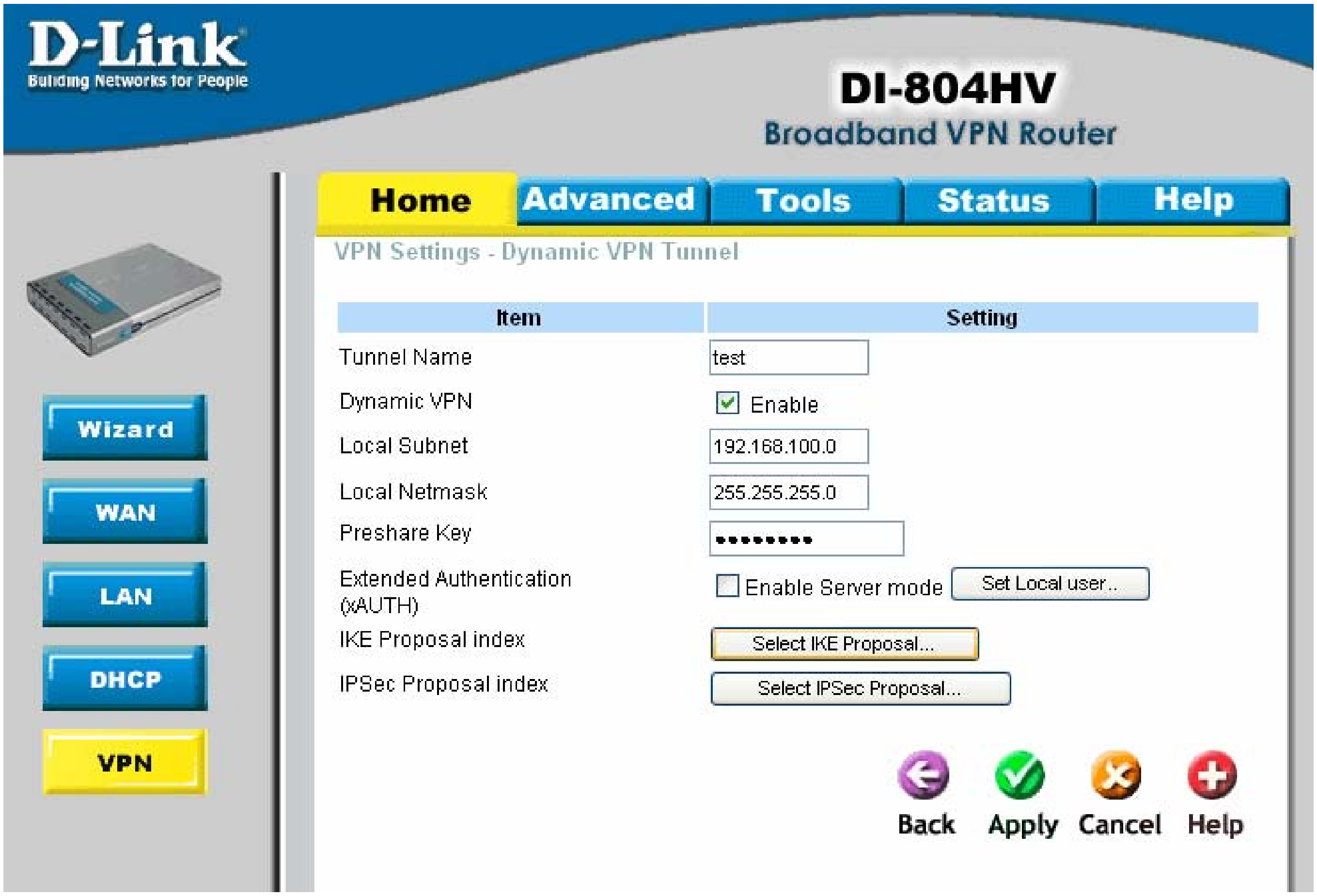
On the VPN Settings page enter the required information:

Tunnel name, select Dynamic VPN to enable Dynamic VPN

Local Subnet / Netmask are characteristics of the network where the Unit you are currently configuring is installed.

Preshare Key: this can be anything up to 31 characters long (write down this key as you will need it when configuring the remote VPN client).

Then click Apply, then click on “Select IKE Proposal…”



VPN Settings - Dynamic VPN Tunnel

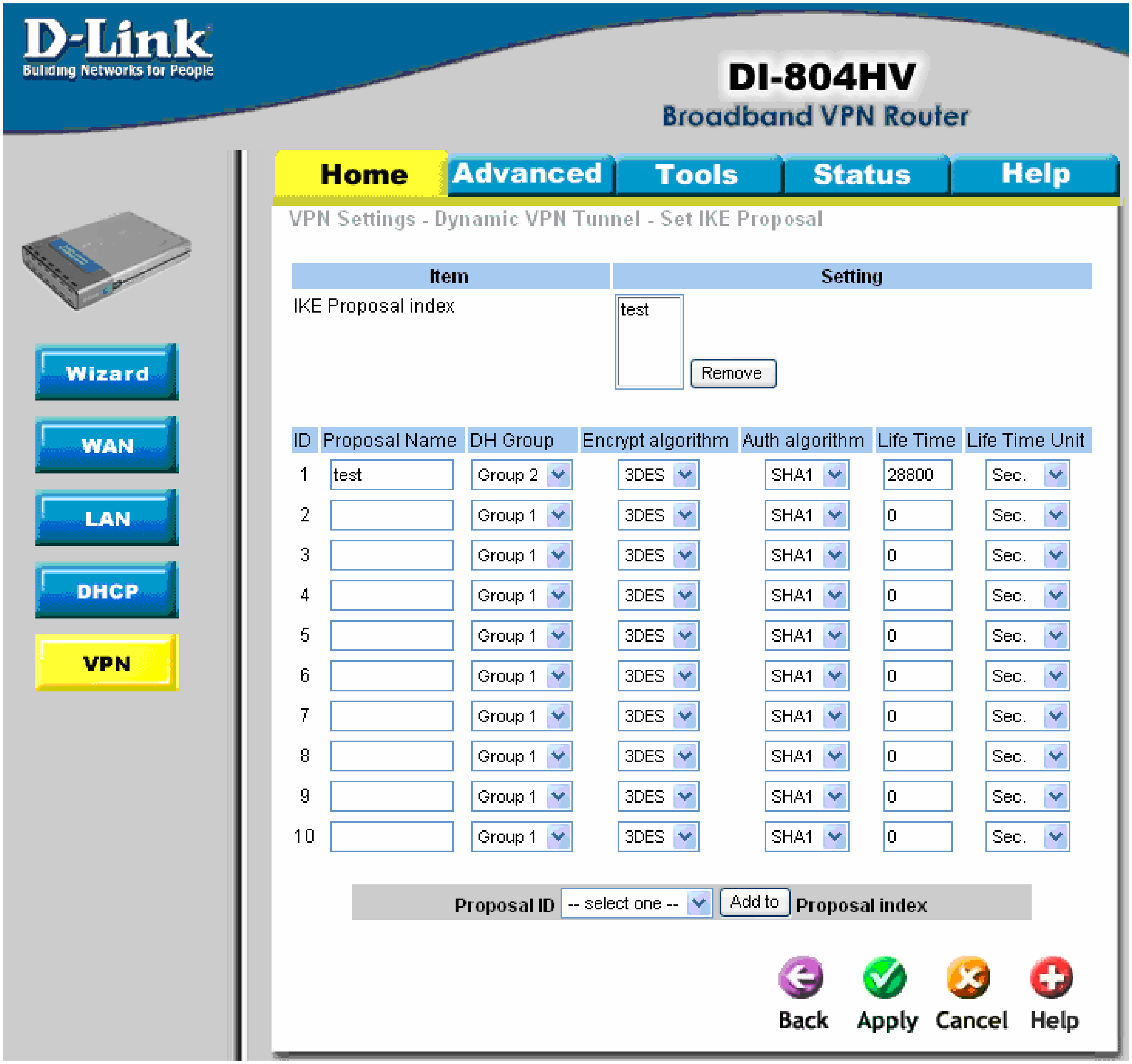
Item	Setting
Tunnel Name	test
Dynamic VPN	☑ Enable
Local Subnet	192.168.100.0
Local Netmask	255.255.255.0
Preshare Key	•••••••••
Extended Authentication (xAUTH)	☐ Enable Server mode [Set Local user..]
IKE Proposal index	[Select IKE Proposal...]
IPSec Proposal index	[Select IPSec Proposal...]

Below is the example how you can setup IKE Proposal.

We used the following settings:
ID 1, Name: test, Group 2, 3DES, SHA1, 28800, Sec

After you have entered in the information, you will need to click on the Proposal ID drop-down box and select ID 1, then click "Add to".

Click Apply, then click on Back.



VPN Settings - Dynamic VPN Tunnel - Set IKE Proposal

Item	Setting
IKE Proposal index	test Remove

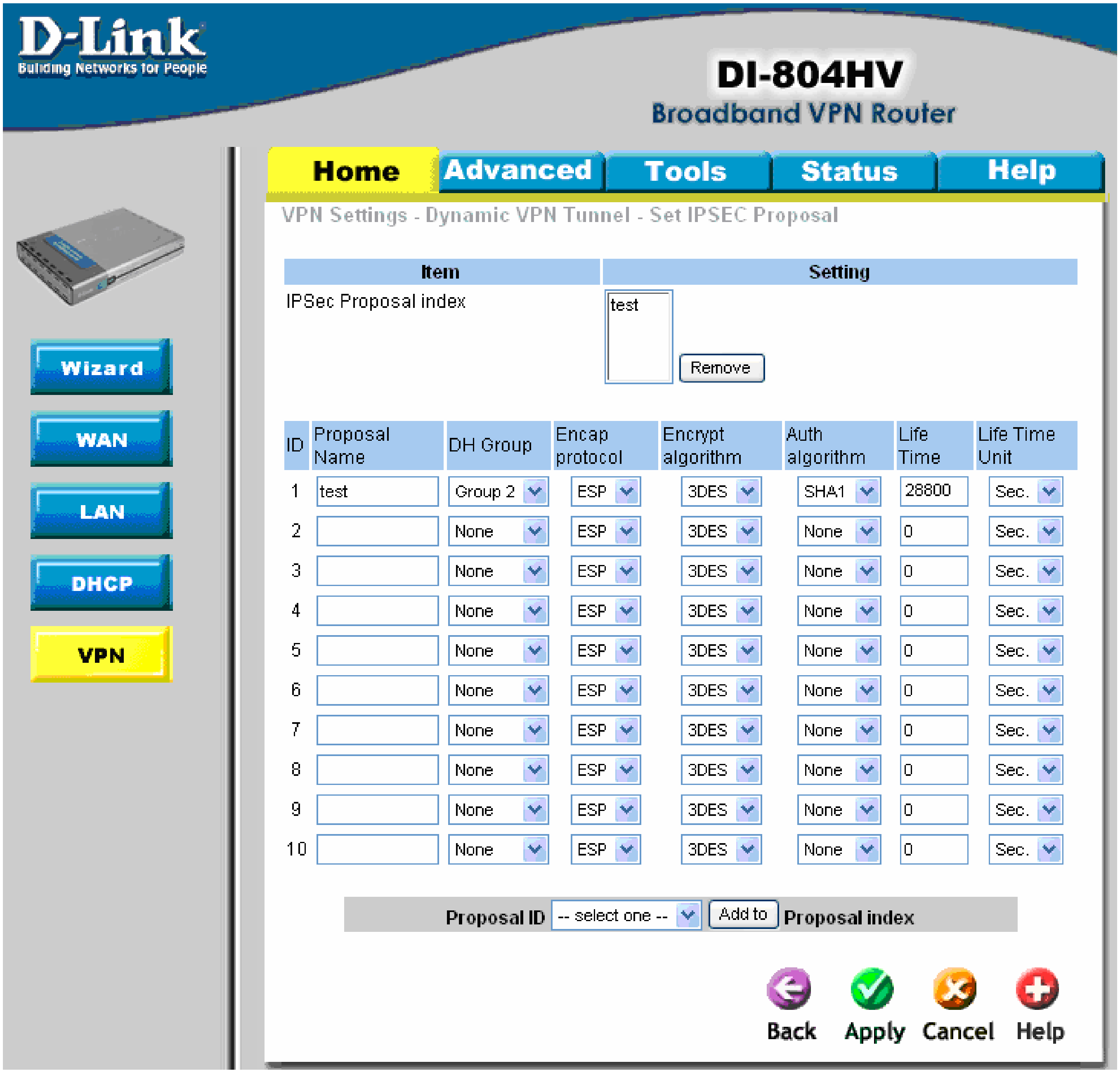
ID	Proposal Name	DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	test	Group 2	3DES	SHA1	28800	Sec.
2		Group 1	3DES	SHA1	0	Sec.
3		Group 1	3DES	SHA1	0	Sec.
4		Group 1	3DES	SHA1	0	Sec.
5		Group 1	3DES	SHA1	0	Sec.
6		Group 1	3DES	SHA1	0	Sec.
7		Group 1	3DES	SHA1	0	Sec.
8		Group 1	3DES	SHA1	0	Sec.
9		Group 1	3DES	SHA1	0	Sec.
10		Group 1	3DES	SHA1	0	Sec.

Proposal ID -- select one -- Add to Proposal index

Click on “IPSec Proposal” and you should see a page similar to the one below.
Configure it the same way as on the IKE Proposal page.

After you have entered in the information, you will need to click on the Proposal ID drop-down box and select ID 1, then click “Add to”.

Then click Apply.



VPN Settings - Dynamic VPN Tunnel - Set IPSEC Proposal

Item	Setting
IPSec Proposal index	test

ID	Proposal Name	DH Group	Encap protocol	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	test	Group 2	ESP	3DES	SHA1	28800	Sec.
2		None	ESP	3DES	None	0	Sec.
3		None	ESP	3DES	None	0	Sec.
4		None	ESP	3DES	None	0	Sec.
5		None	ESP	3DES	None	0	Sec.
6		None	ESP	3DES	None	0	Sec.
7		None	ESP	3DES	None	0	Sec.
8		None	ESP	3DES	None	0	Sec.
9		None	ESP	3DES	None	0	Sec.
10		None	ESP	3DES	None	0	Sec.

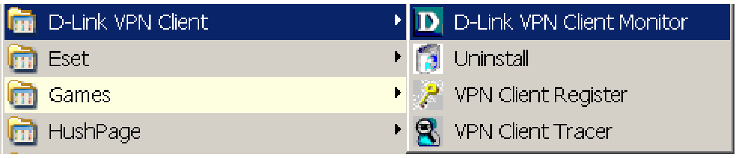
Proposal ID -- select one -- Add to Proposal index

This is all you need to do to configure the VPN router. Now you need to setup the Workstation (with the D-Link VPN client).

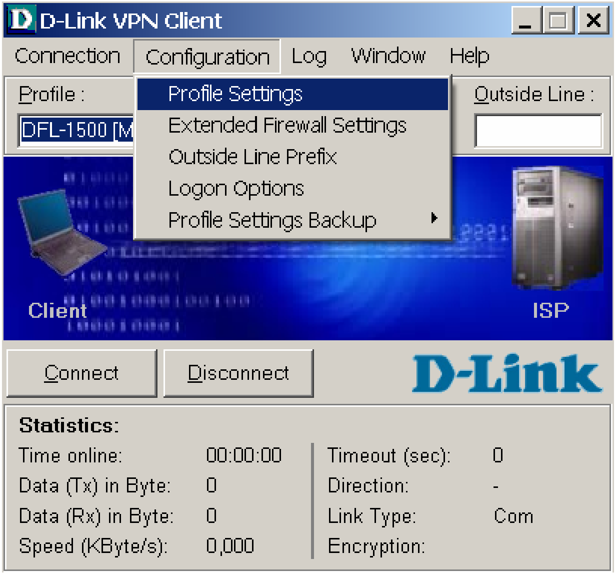
Configuring The Remote PC IPSec connection (D-Link DS-601 VPN Client Software)

First start the D-Link VPN software. You can find it under the Start button > Programs > D-Link VPN Client.

Click on D-Link VPN Client Monitor.



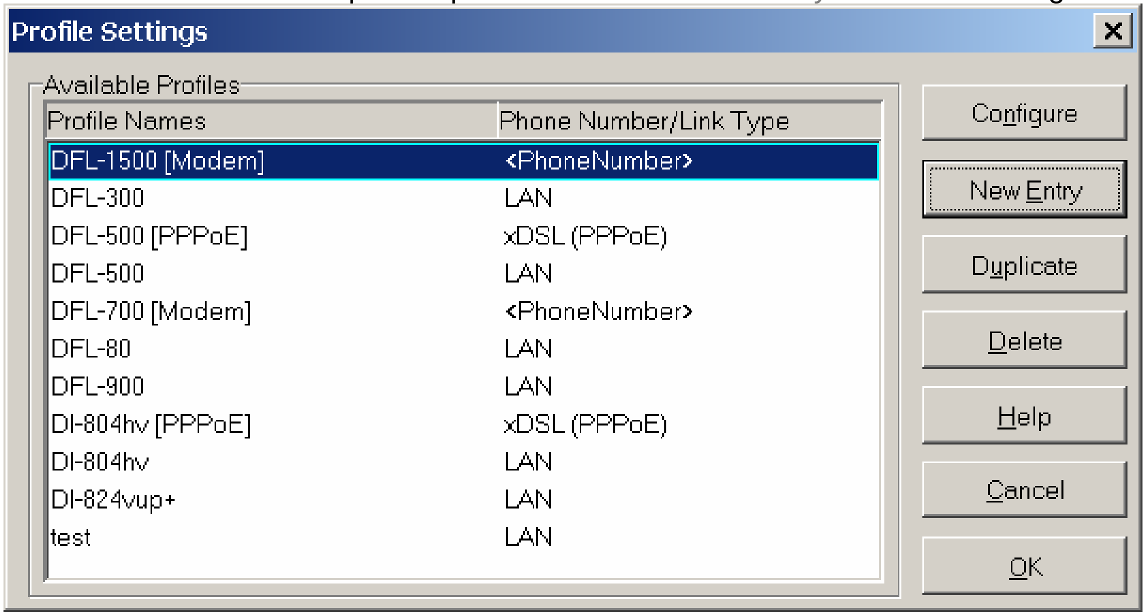
Once the software loads, click on Configuration > Profile Settings



Statistics:

Time online:	00:00:00	Timeout (sec):	0
Data (Tx) in Byte:	0	Direction:	-
Data (Rx) in Byte:	0	Link Type:	Com
Speed (KByte/s):	0,000	Encryption:	

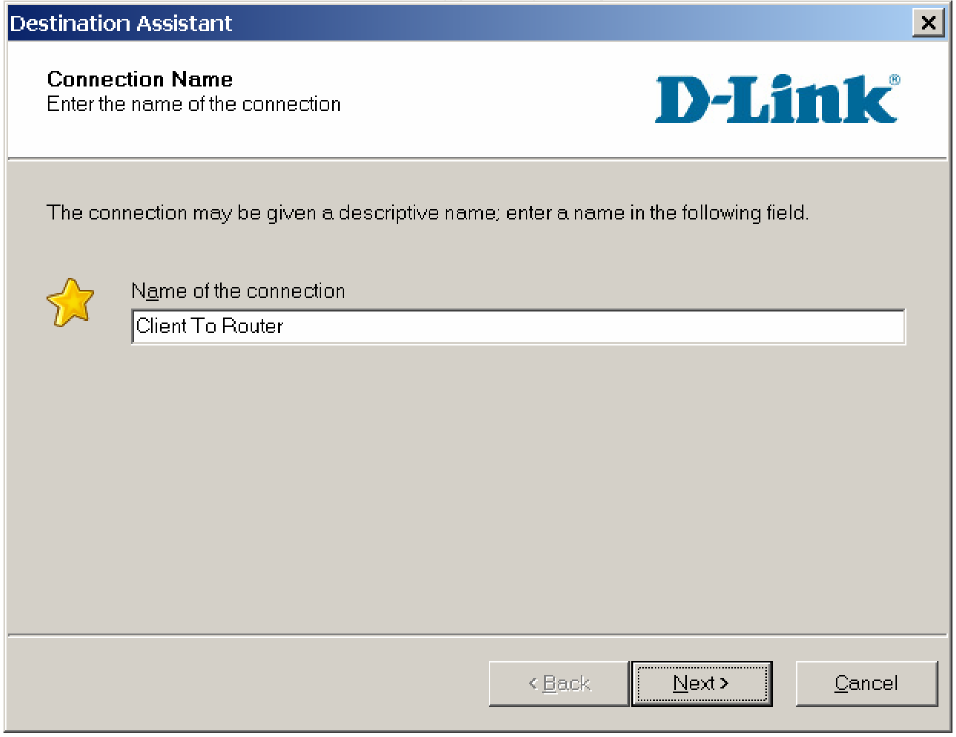
You should see the list of pre-set profiles. Click on "New Entry" button on the right hand side.



Profile Names	Phone Number/Link Type
DFL-1500 [Modem]	<PhoneNumber>
DFL-300	LAN
DFL-500 [PPPoE]	xDSL (PPPoE)
DFL-500	LAN
DFL-700 [Modem]	<PhoneNumber>
DFL-80	LAN
DFL-900	LAN
DI-804hv [PPPoE]	xDSL (PPPoE)
DI-804hv	LAN
DI-824vup+	LAN
test	LAN

It should bring up the wizard as shown below.

In the “Name of the connection” type in your profile name and click Next button.



Destination Assistant

Connection Name
Enter the name of the connection

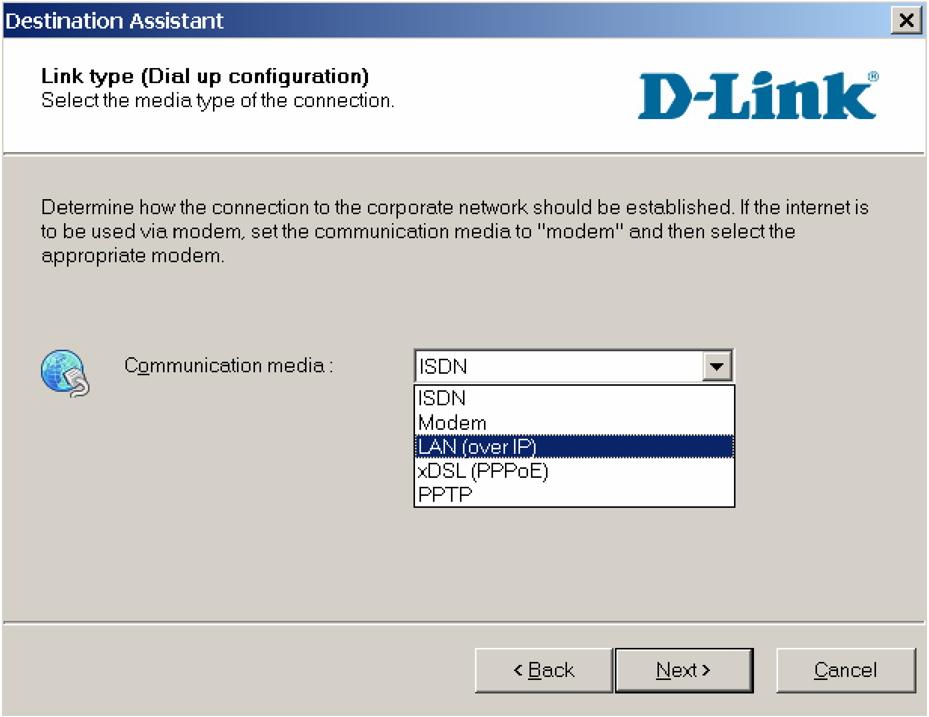
The connection may be given a descriptive name; enter a name in the following field.

Name of the connection: Client To Router

Next you need to select the type of Internet connection that you have.

Click Next after you have selected your connection type.

1) PC connected to a router or to a Telstra cable modem use “LAN (over IP)”.
2) PC connected to an ADSL modem use “LAN (over IP)”
3) PC uses a dial up connection use “Modem”
4) PC connected to ISDN use “ISDN”



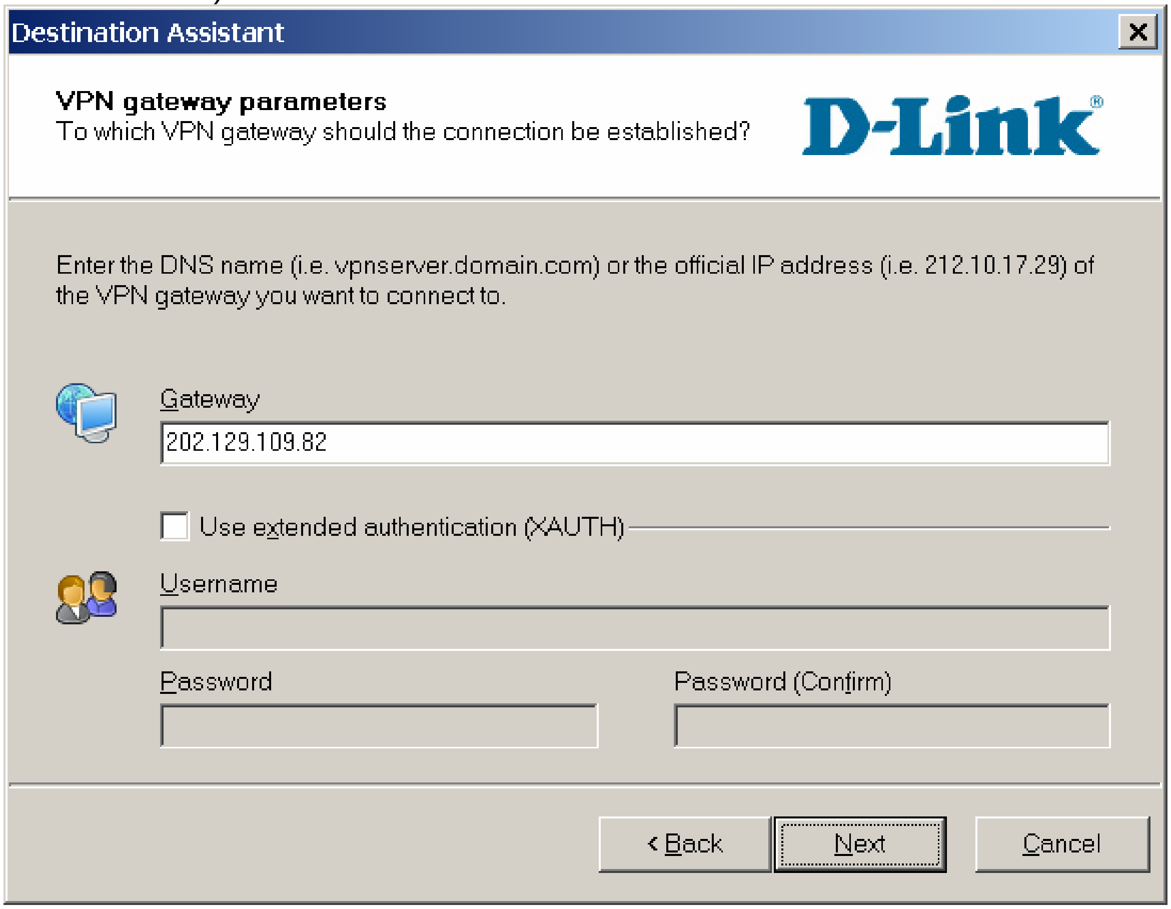
Destination Assistant

Link type (Dial up configuration)
Select the media type of the connection.

Determine how the connection to the corporate network should be established. If the internet is to be used via modem, set the communication media to "modem" and then select the appropriate modem.

Communication media : ISDN

Enter VPN Gateway address. This will be the public IP of the router in the Office (eg. 202.129.109.82). Click Next button.



Destination Assistant

VPN gateway parameters

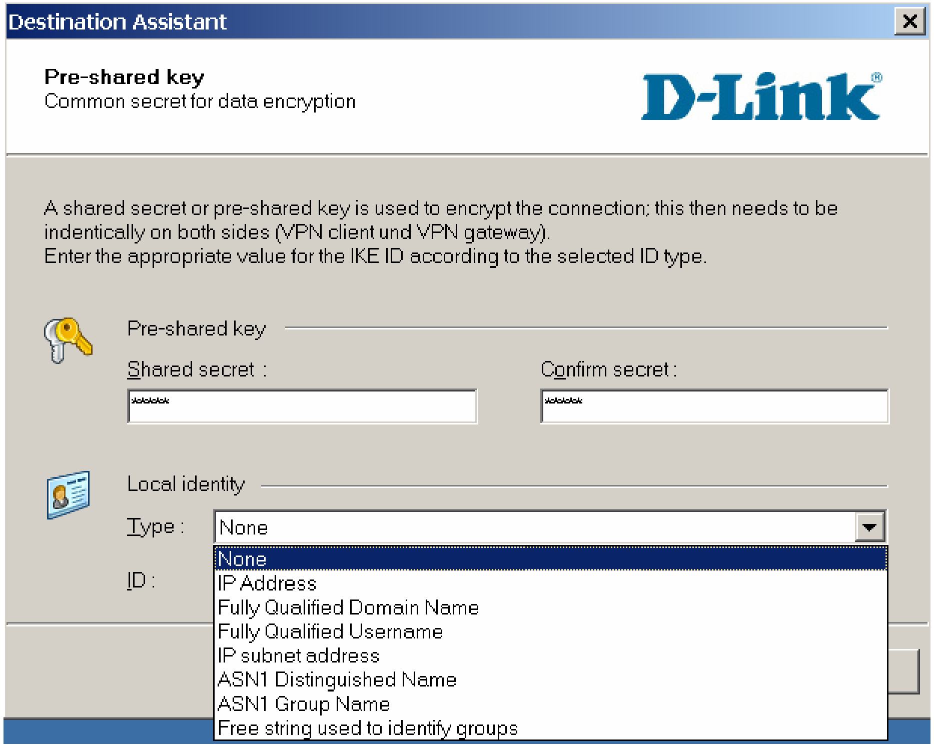
To which VPN gateway should the connection be established?

Enter the DNS name (i.e. vpnserver.domain.com) or the official IP address (i.e. 212.10.17.29) of the VPN gateway you want to connect to.

Gateway: 202.129.109.82

□ Use extended authentication (XAUTH)

Enter the same Pre-shared key that you have entered in the office VPN router in the Shared secret. Retype it in the Confirm secret.
Select “None” under the “Local identity” and click Finish button.



Destination Assistant

Pre-shared key

Common secret for data encryption

A shared secret or pre-shared key is used to encrypt the connection; this then needs to be indentically on both sides (VPN client und VPN gateway).
Enter the appropriate value for the IKE ID according to the selected ID type.

Pre-shared key

Shared secret : *****

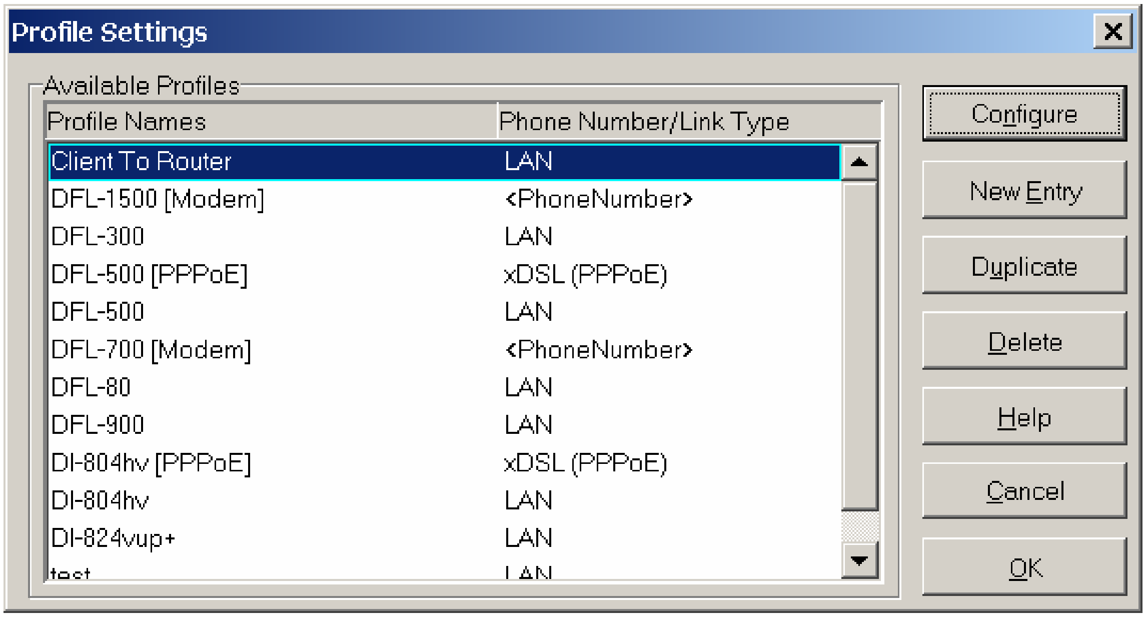
Confirm secret : *****

Local identity

Type : None

After finishing the wizard, you should see the new profile in the list.

Select the name of the profile you have just created. Then click on “Configuration” on the right hand side.

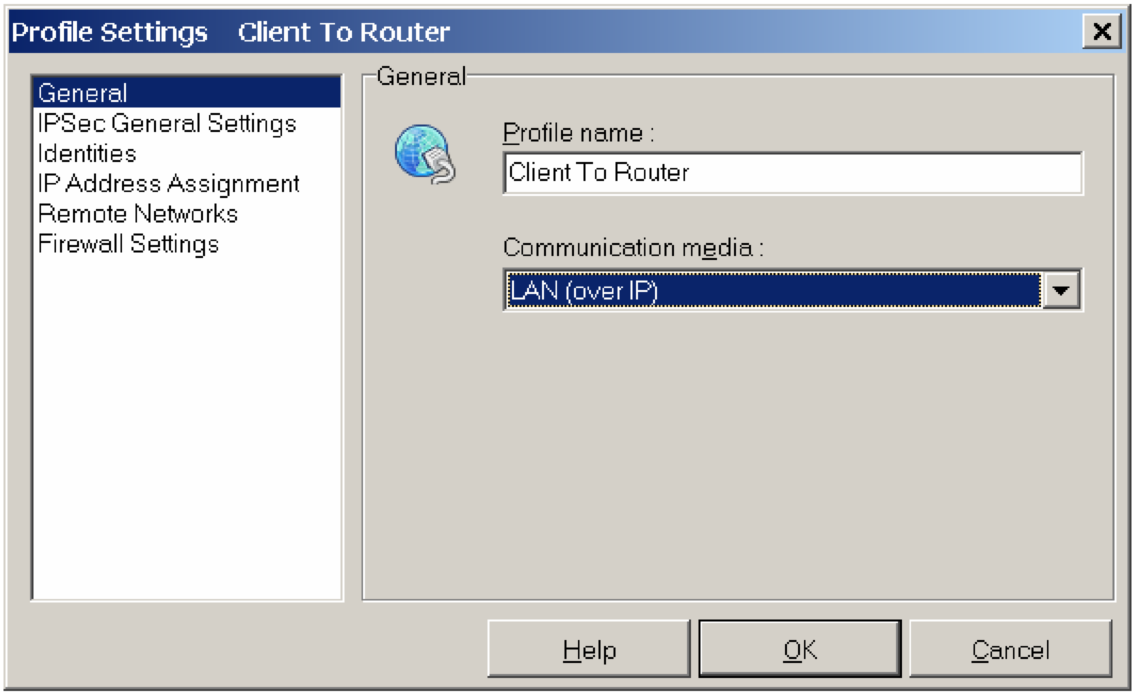


Profile Settings

Available Profiles

Profile Names	Phone Number/Link Type
Client To Router	LAN
DFL-1500 [Modem]	<PhoneNumber>
DFL-300	LAN
DFL-500 [PPPoE]	xDSL (PPPoE)
DFL-500	LAN
DFL-700 [Modem]	<PhoneNumber>
DFL-80	LAN
DFL-900	LAN
DI-804hv [PPPoE]	xDSL (PPPoE)
DI-804hv	LAN
DI-824vup+	LAN
test	LAN

Under the General options you can change the Profile name and the communication media type.



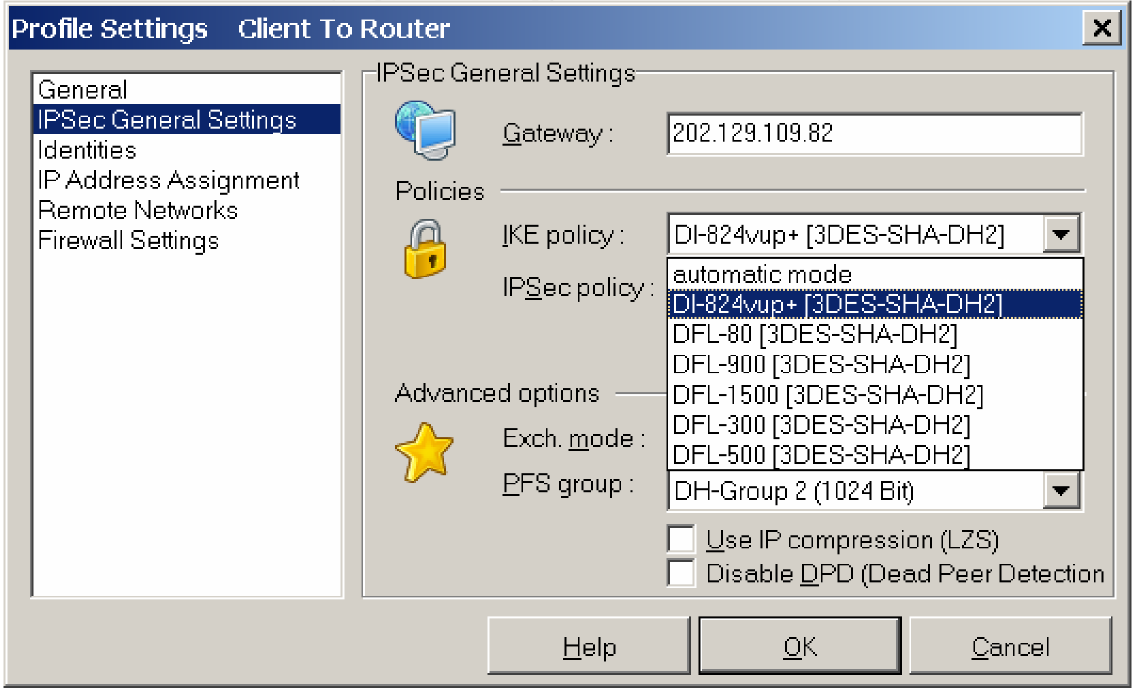
Profile Settings Client To Router

General

Profile name : Client To Router

Communication media : LAN (over IP)

Click on the “IPSec General Settings”.
You should see the below , Under Policies > IKE Policy, Select the pre-set profile called “DI-824vup+ [3DES-SHA-DH2]”
Also select the DI-824vup+ [3DES-SHA] profile for IPSec Policy.



Profile Settings Client To Router

IPSec General Settings

Gateway : 202.129.109.82

Policies

IKE policy : DI-824vup+ [3DES-SHA-DH2]

IPSec policy :

Advanced options

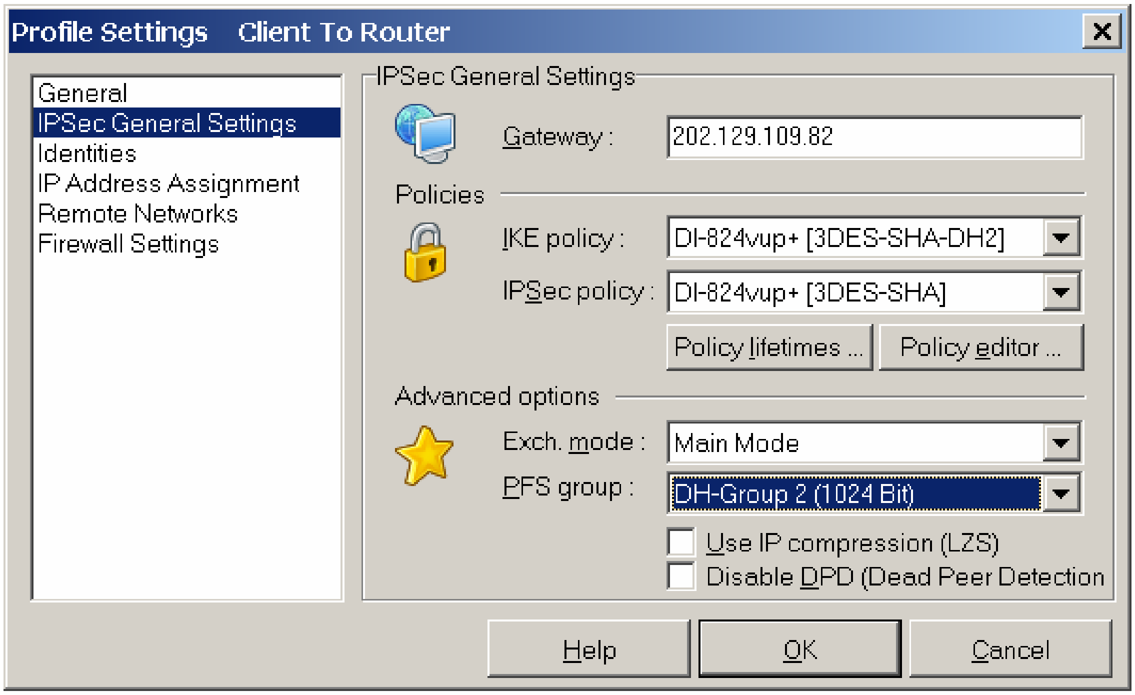
Exch. mode :

PFS group : DH-Group 2 (1024 Bit)

□ Use IP compression (LZS)

□ Disable DPD (Dead Peer Detection

Select the “Main Mode” option under Advanced options > Exch. mode.
And select DH-Group 2 under the PFS group.



Profile Settings Client To Router

IPSec General Settings

Gateway : 202.129.109.82

Policies

IKE policy : DI-824vup+ [3DES-SHA-DH2]

IPSec policy : DI-824vup+ [3DES-SHA]

Advanced options

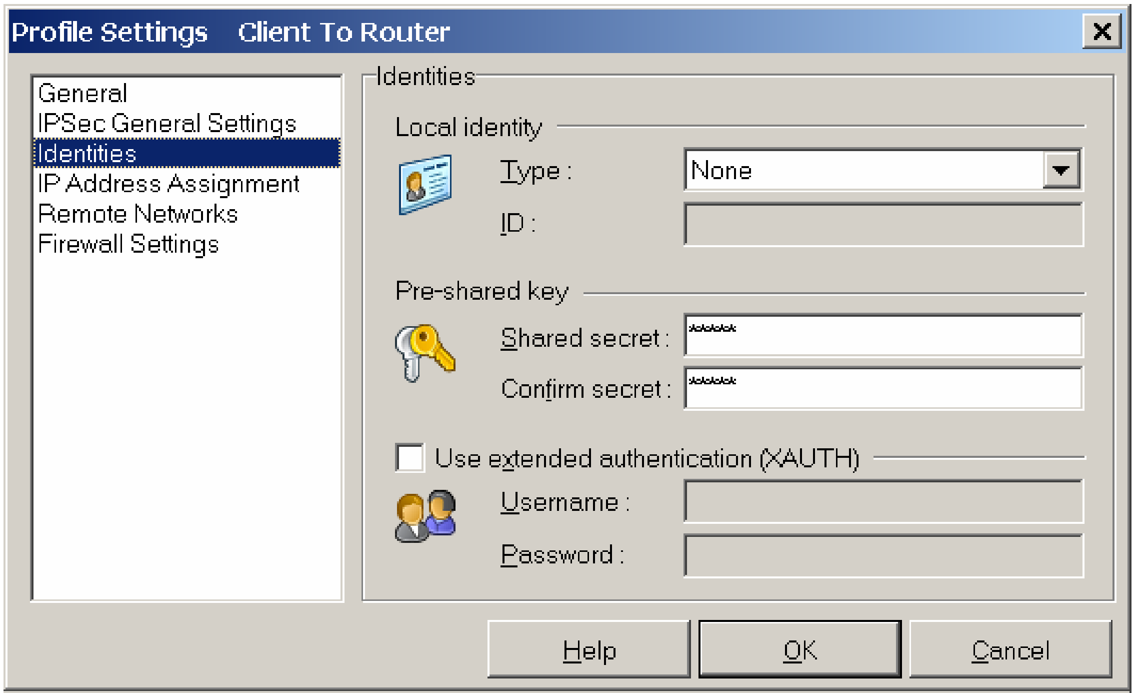
Exch. mode : Main Mode

PFS group : DH-Group 2 (1024 Bit)

□ Use IP compression (LZS)

□ Disable DPD (Dead Peer Detection

Under “Identities” and “IP Address Assignment” you do not need to change anything.



Identities

Local identity

Type : None

ID :

Pre-shared key

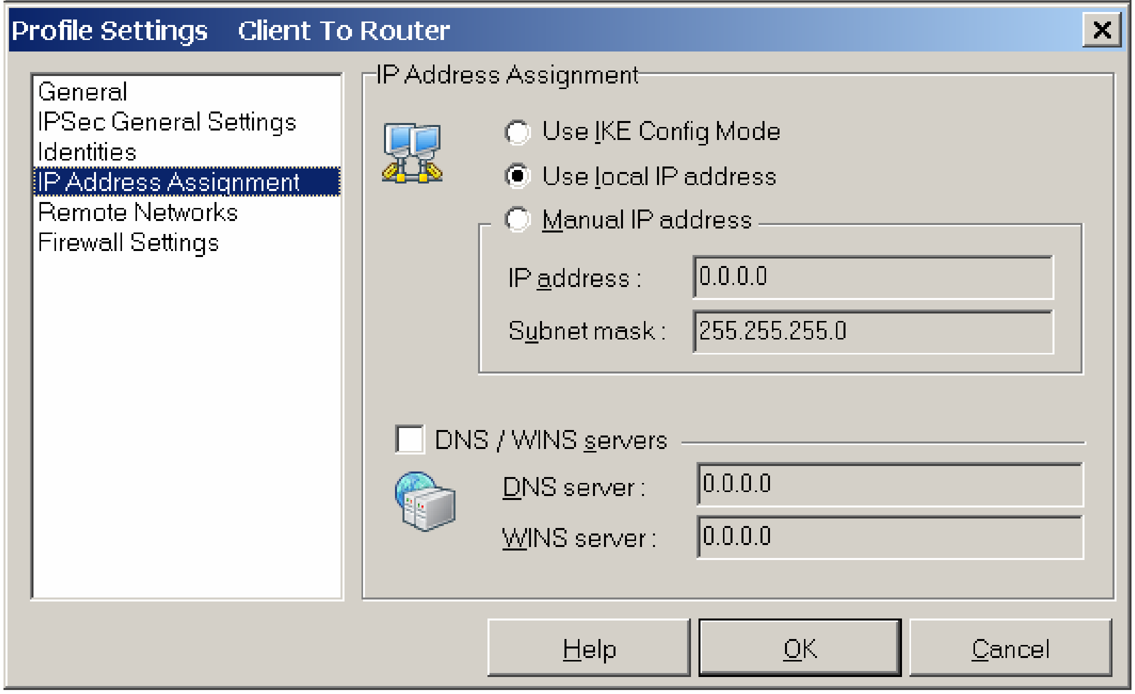
Shared secret : *****

Confirm secret : *****

□ Use extended authentication (XAUTH)

Username :

Password :



IP Address Assignment

○ Use IKE Config Mode

● Use local IP address

○ Manual IP address

IP address : 0.0.0.0

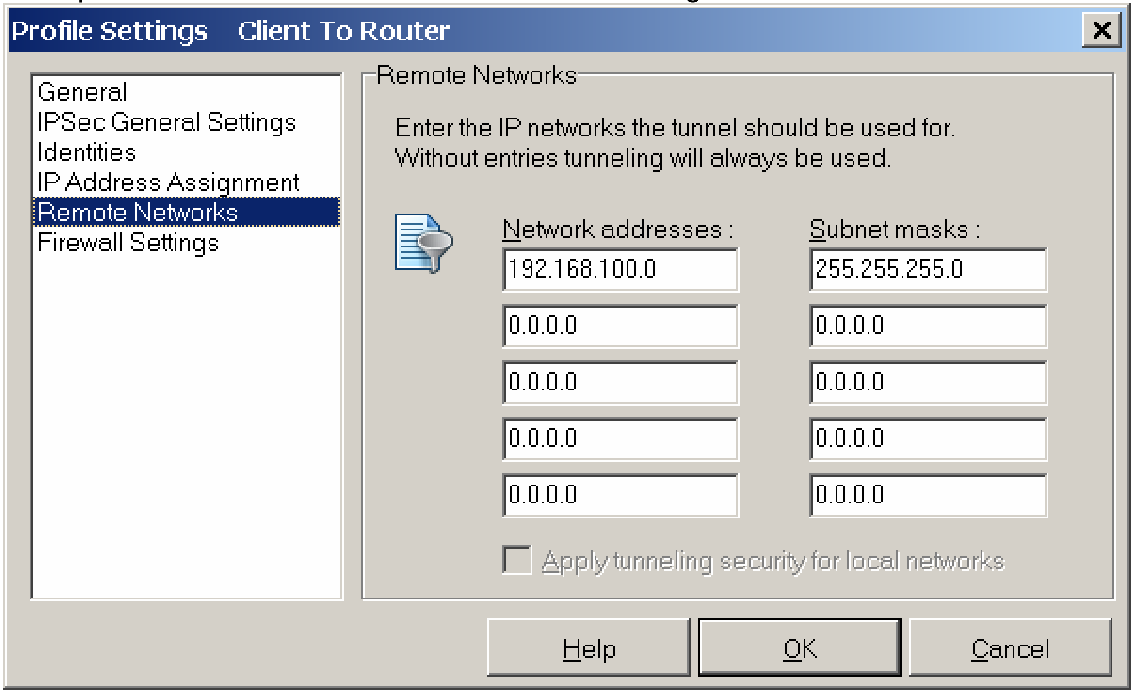
Subnet mask : 255.255.255.0

□ DNS / WINS servers

DNS server : 0.0.0.0

WINS server : 0.0.0.0

Under “Remote Networks” option you need to enter the remote LAN subnet and subnet mask. In our example the office network uses 192.168.100.x range of IP addresses, so we entered 192.168.100.0.



Profile Settings Client To Router

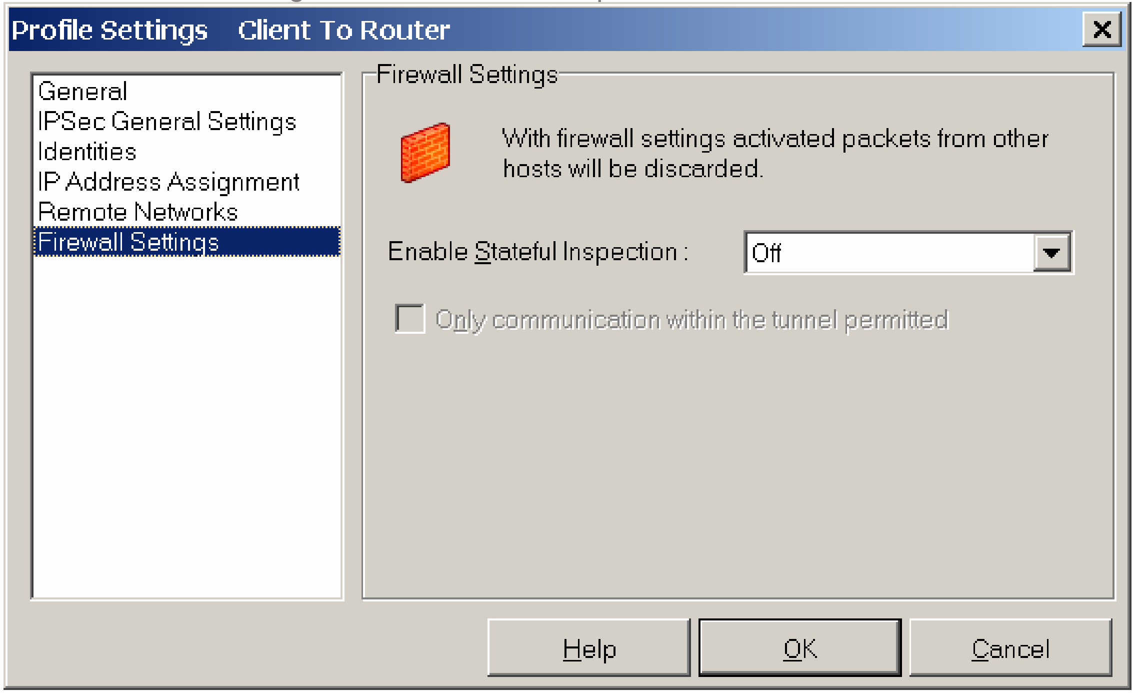
Remote Networks

Enter the IP networks the tunnel should be used for.
Without entries tunneling will always be used.

Network addresses :	Subnet masks :
192.168.100.0	255.255.255.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0

☐ Apply tunneling security for local networks

Under “Firewall settings”, set the Stateful Inspection as Off and click OK button.



Profile Settings Client To Router

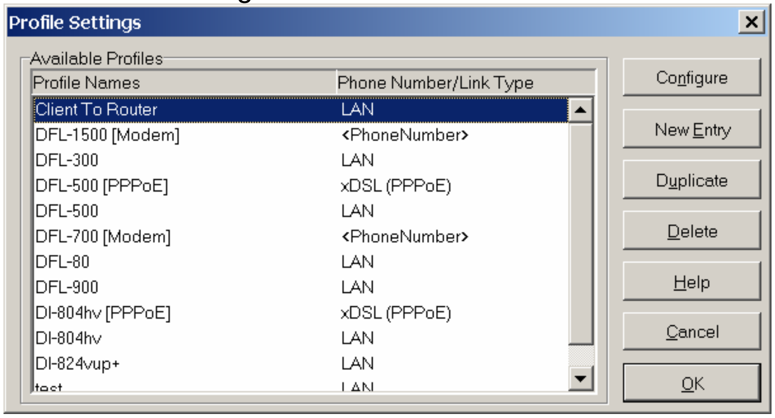
Firewall Settings

With firewall settings activated packets from other hosts will be discarded.

Enable Stateful Inspection : Off

☐ Only communication within the tunnel permitted

Then click “OK” again.

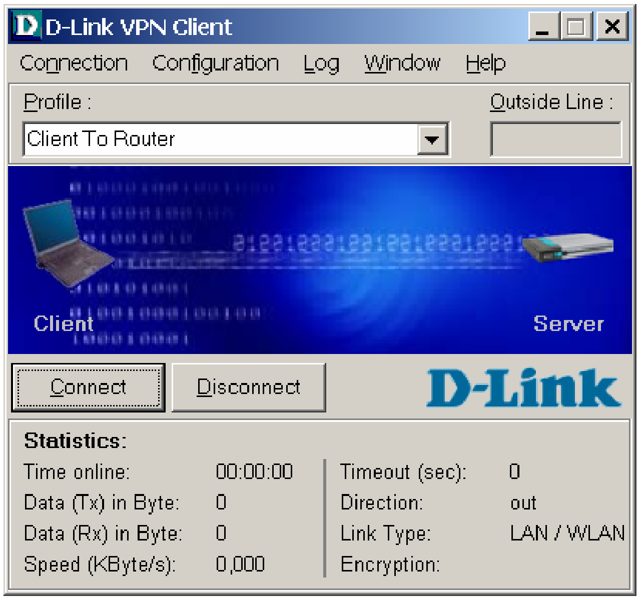


Profile Settings

Available Profiles

Profile Names	Phone Number/Link Type
Client To Router	LAN
DFL-1500 [Modem]	<PhoneNumber>
DFL-300	LAN
DFL-500 [PPPoE]	xDSL (PPPoE)
DFL-500	LAN
DFL-700 [Modem]	<PhoneNumber>
DFL-80	LAN
DFL-900	LAN
DI-804hv [PPPoE]	xDSL (PPPoE)
DI-804hv	LAN
DI-824vup+	LAN
test	LAN

Click the Connect button to establish the IPSec tunnel



D-Link VPN Client

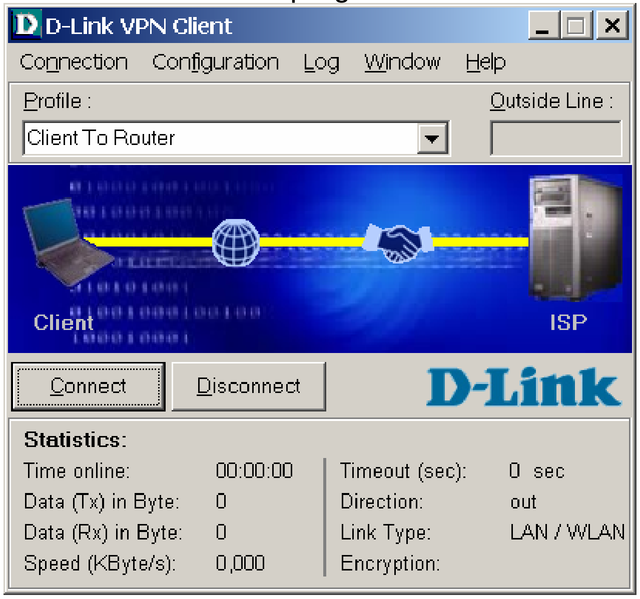
Profile : Client To Router

Outside Line :

Statistics:

Time online:	00:00:00	Timeout (sec):	0
Data (Tx) in Byte:	0	Direction:	out
Data (Rx) in Byte:	0	Link Type:	LAN / WLAN
Speed (KByte/s):	0,000	Encryption:	

VPN connection is in progress:



D-Link VPN Client

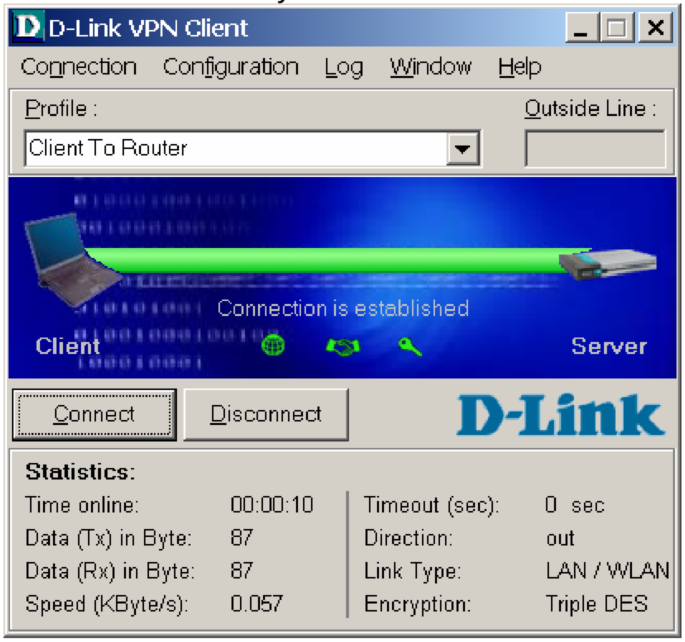
Profile : Client To Router

Outside Line :

Statistics:

Time online:	00:00:00	Timeout (sec):	0 sec
Data (Tx) in Byte:	0	Direction:	out
Data (Rx) in Byte:	0	Link Type:	LAN / WLAN
Speed (KByte/s):	0,000	Encryption:	

When its connected you should see the “Connection is established” message.



Profile : Client To Router

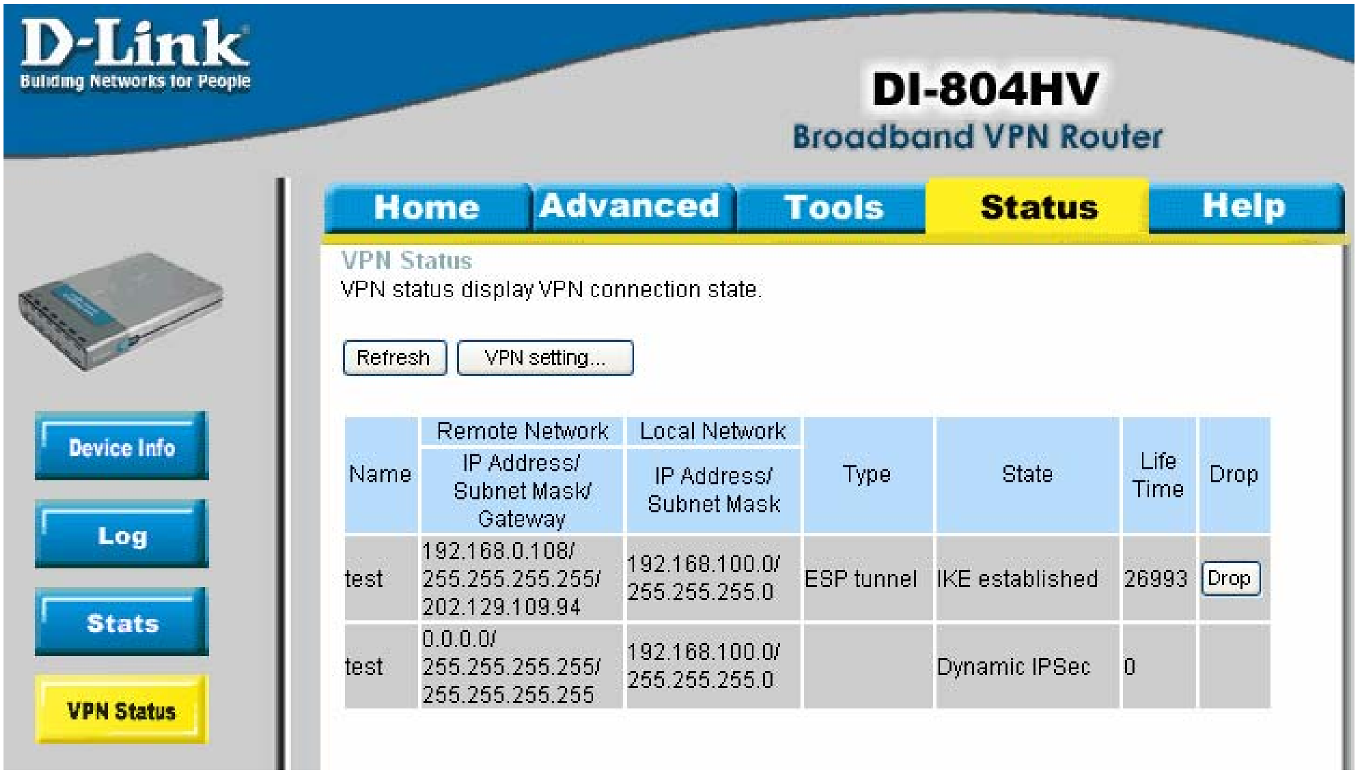
Outside Line :

Connection is established

Statistics:

Time online:	00:00:10	Timeout (sec):	0 sec
Data (Tx) in Byte:	87	Direction:	out
Data (Rx) in Byte:	87	Link Type:	LAN / WLAN
Speed (KByte/s):	0.057	Encryption:	Triple DES

If you login into the office router’s web configuration page and then go to Status > VPN Status, it should say “IKE established” in the State section.



VPN Status

VPN status display VPN connection state.

Name	Remote Network	Local Network	Type	State	Life Time	Drop
	IP Address/ Subnet Mask/ Gateway	IP Address/ Subnet Mask				
test	192.168.0.108/ 255.255.255.255/ 202.129.109.94	192.168.100.0/ 255.255.255.0	ESP tunnel	IKE established	26993	Drop
test	0.0.0.0/ 255.255.255.255/ 255.255.255.255	192.168.100.0/ 255.255.255.0		Dynamic IPSec	0	

Appendix 1.
How to test your VPN conection.

Make sure that computers on both locations can access the Internet.

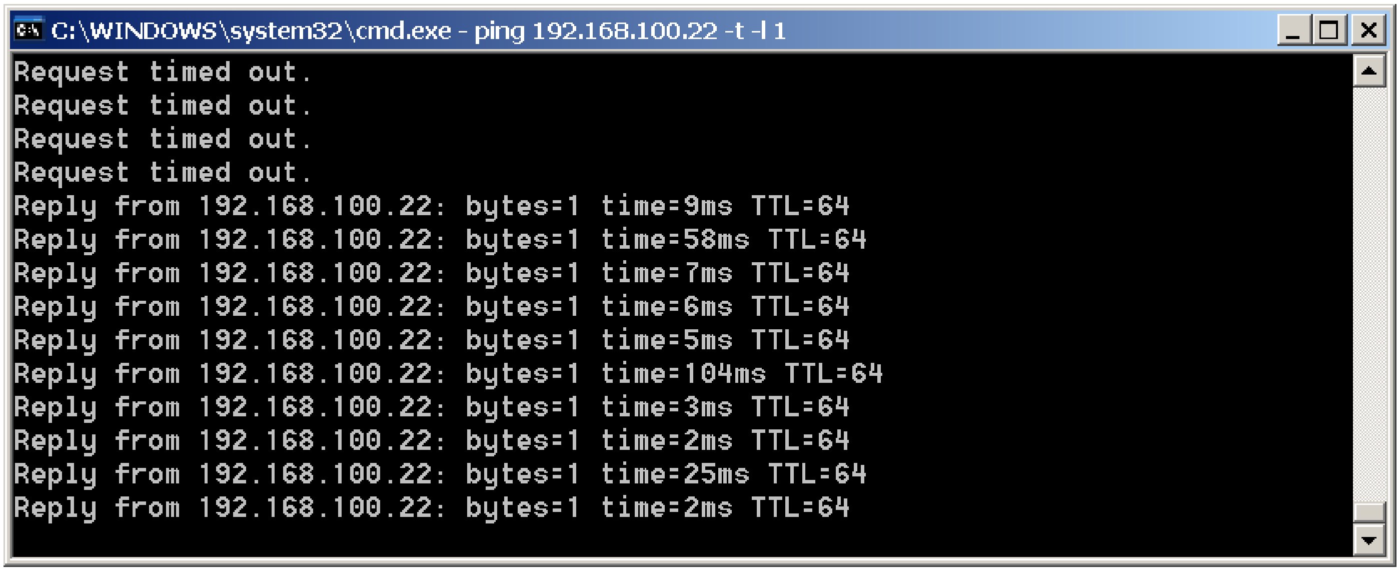
The make sure that you are on the PC which is running the D-Link VPN software.

The go to Start > Run, type *command* and click on OK.

If you type in the below then hit Enter.

ping 192.168.100.22 -t

You should see messages similar to the one below:

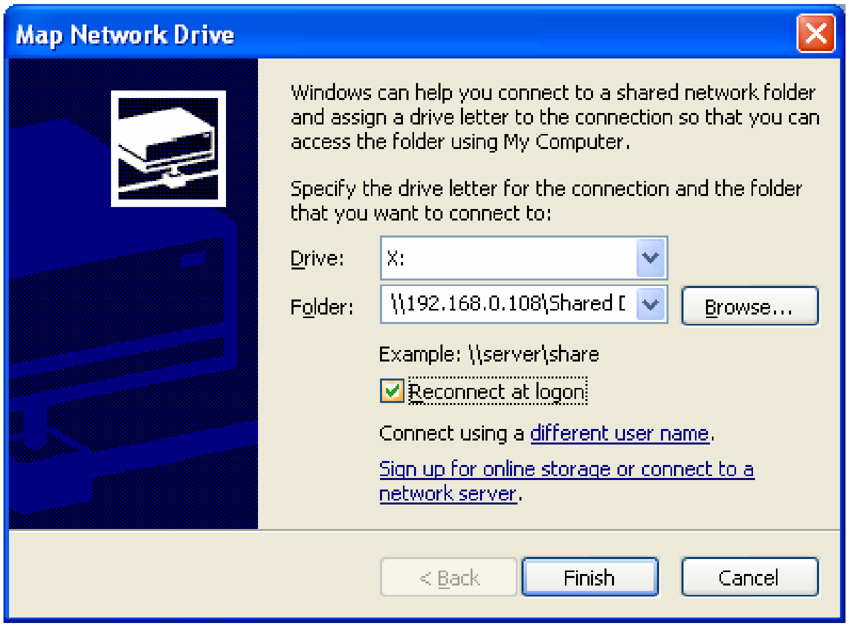


```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.100.22: bytes=1 time=9ms TTL=64
Reply from 192.168.100.22: bytes=1 time=58ms TTL=64
Reply from 192.168.100.22: bytes=1 time=7ms TTL=64
Reply from 192.168.100.22: bytes=1 time=6ms TTL=64
Reply from 192.168.100.22: bytes=1 time=5ms TTL=64
Reply from 192.168.100.22: bytes=1 time=104ms TTL=64
Reply from 192.168.100.22: bytes=1 time=3ms TTL=64
Reply from 192.168.100.22: bytes=1 time=2ms TTL=64
Reply from 192.168.100.22: bytes=1 time=25ms TTL=64
Reply from 192.168.100.22: bytes=1 time=2ms TTL=64
```

If you see a message saying Reply from… that means that VPN tunnel has been established successfully and you can communicate with remote network via VPN.

Appendix 2
Connecting to remote computers/drives via VPN

You can map remote computers’ drives 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):



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:

Drive: X:

Folder: \\192.168.0.108\Shared

Example: \\server\share

☑ Reconnect at logon

Connect using a different user name.

Sign up for online storage or connect to a network server.

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 Neighborhood you may need to enable NetBIOS over TCP/IP in Windows. Or use the methods described above.
Note that firewall/antivirus software installed on your or remote computer may stop you from accessing shared folders.

Appendix 3
Note to DSL-300, DSL-300+, DSL-302G modems users and DSL-500, DSL-504, DSL-604+ users.

If you are using **DSL-300** to connect your DI-804HV to the Internet please avoid using **192.168.1.x** addresses on your networks as it is the temporary subnet used by the modem.

If you are using **DSL-300+** to connect your DI-804HV to the Internet please avoid using **192.168.0.x** addresses on your networks as it is the temporary subnet used by the modem. Also note that DSL-300+ links to the MAC address of the device connected to it directly. So if you configured the modem while it was connected to your PC directly or to another router, you will need to reconfigure it while it is connected to your DI-804HV. Here are the steps:

1. Connect the DSL-300+ modem to the WAN port of your DI-804HV.
2. Set WAN port on DI-804HV to “Dynamic IP” and set LAN port to subnet different from 192.168.0.x (e.g. 192.168.3.1)
3. Renew IP address on your computer so it will be on 192.168.3.x subnet and log into the DSL-300+ using your Internet browser: http://192.168.0.1
4. In the DSL-300+ interface select Account Management. Put a tick next to your account and click on Delete.
5. Select Account Configuration and reconfigure the modem according to your ISP requirements. Click on OK to save settings.

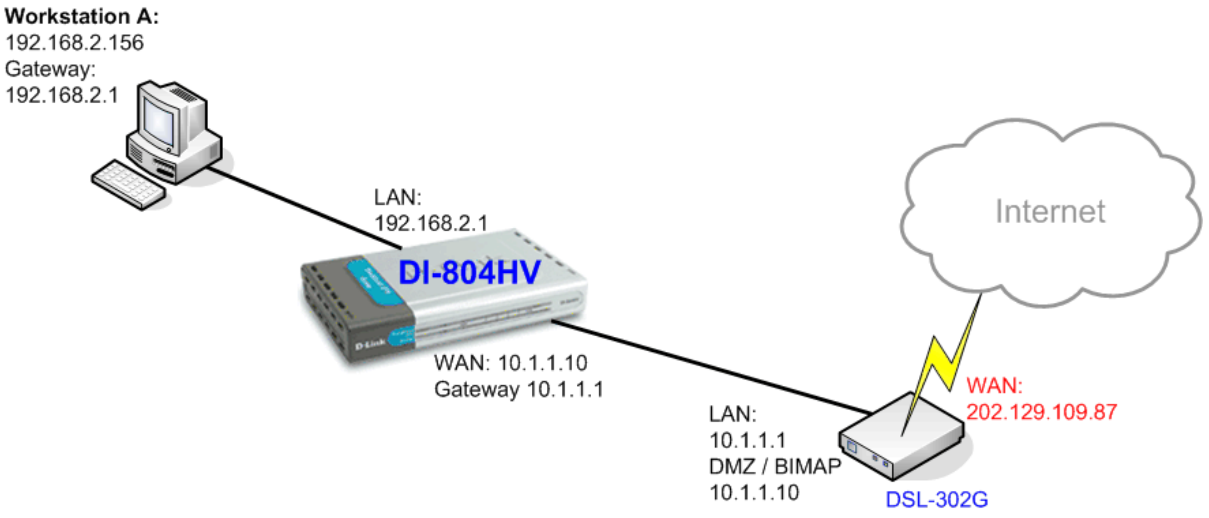
If you are using **DSL-500, DSL-504, DSL-604+** router to connect your DI-804HV to the Internet please avoid using **192.168.0.x** addresses on your networks as it is the default LAN subnet used by the routers. You may change it to a different subnet (e.g. 192.168.33.1) if you wish, under Configuration > Ethernet IP.

Note that you need to enable VPN pass-through on the router. Or go to NAT Configuration and enable DMZ: specify the IP address of the WAN port of DI-804HV there.

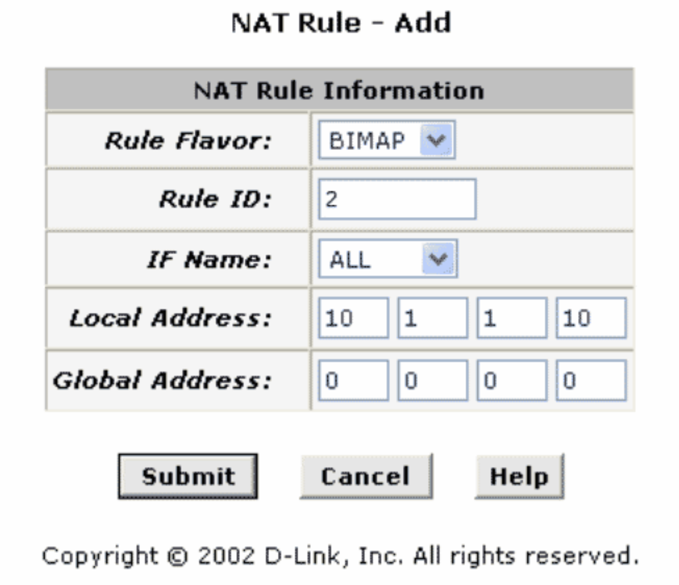
DI-804HV WAN port should be set with static IP from the same subnet as DSL-xxx LAN port. Default Gateway should be set as DSL-xxx LAN port IP address.

Please keep in mind that with DSL-xxx routers with NAT enabled your public IP address will be located on the WAN port of DSL-xxx router. WAN port of DI-804HV will have private IP address. When setting up Remote Gateway in VPN you will need to use public IP’s on DSL-xxx routers’ WAN ports, e.g. 202.129.109.87 (see example with DSL-302G below).

With **DSL-302G** the setup is similar. This modem uses **10.1.1.1** address on LAN.



In order to enable VPN traffic pass-through in this modem you need to do the following:
Log into the modem's WEB interface and select WAN > NAT. Under NAT Options select NAT Rule Entry. Click on Add button.
Under Rule Flavor select BIMAP. Set Rule ID as next number in the rules table (in our case it is 2). IF Name = ALL. Local Address will be the IP on the WAN port of your DI-804HV which is connected to this modem. Global address leave as 0.0.0.0:



NAT Rule - Add

NAT Rule Information	
Rule Flavor:	BIMAP
Rule ID:	2
IF Name:	ALL
Local Address:	10 . 1 . 1 . 10
Global Address:	0 . 0 . 0 . 0

Then click on Submit to apply the settings.

When setting up Remote Gateway in VPN you will need to use public IP on DSL-302G's WAN port.

D-Link Australia & NZ Technical Support Team can be contacted on 1300 766868 (AU), 0800 900 900 (NZ)
or support@dlink.com.au

~ End of Document ~