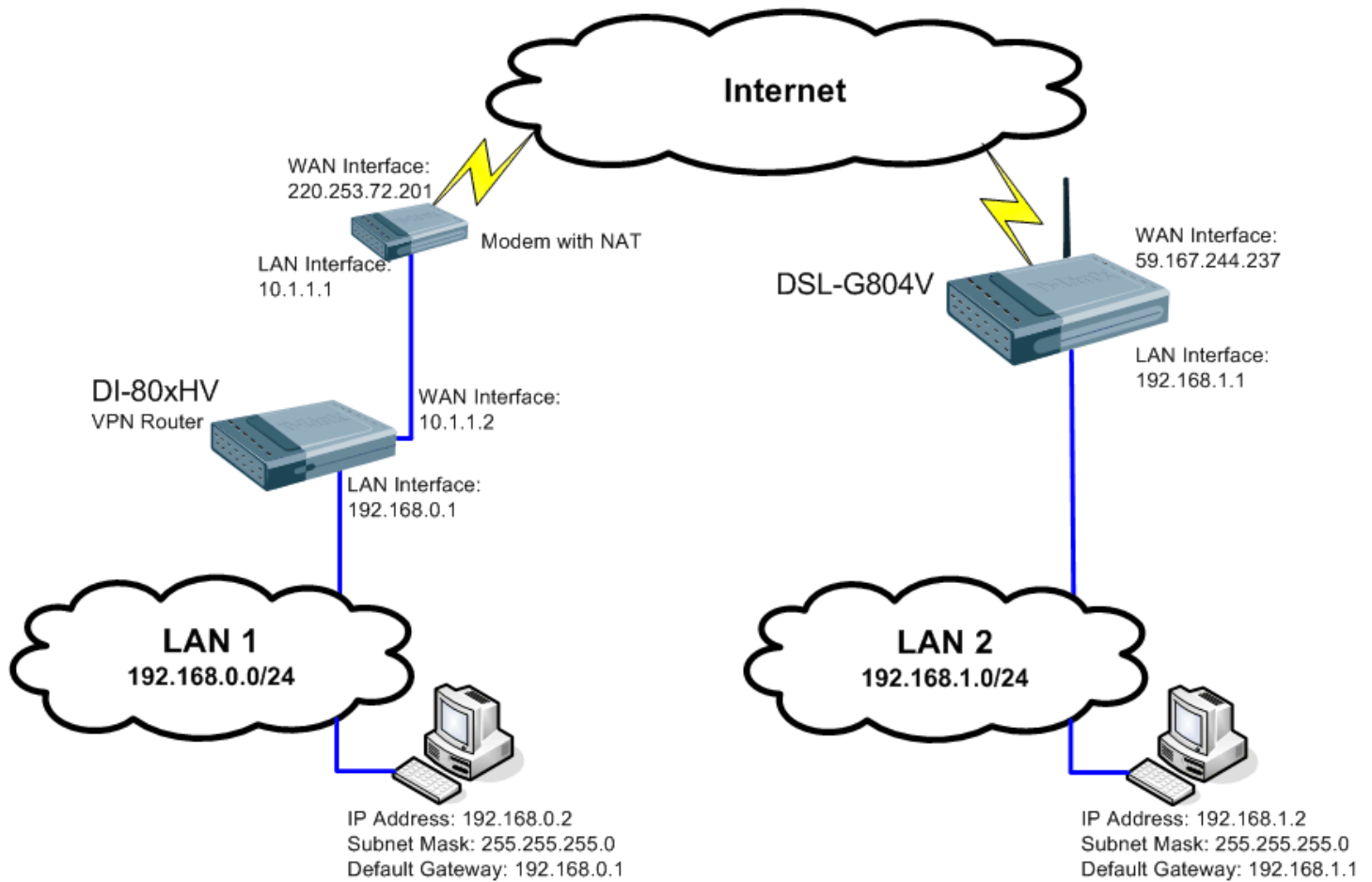


How to setup IPSec VPN connection between DSL-G804V and DI-80xHV

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 the DSL-G804V router on LAN 2

Step 1. Log into the DSL-G804V configuration page, then go to Advanced > VPN and click on IPsec.

Step 2. Set "Enable after Apply" to "Yes".

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 site.

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 768 (Group 1)

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).

The screenshot shows the D-Link DSL-G804V configuration interface. The top navigation bar includes Home, Advanced (selected), Tools, Status, and Help. The left sidebar lists various configuration options: Virtual Server, Firewall, VPN (highlighted), DDNS, Routing, Wireless, ADSL, IP QoS, Time Slices, Email, and Device. The main content area is titled 'VPN' and shows three radio buttons: PPTP, IPsec (selected), and L2TP. Under the 'IPsec' section, the 'Enable after Apply' checkbox is checked. The 'Connection Name' is 'test'. The 'Local Network' is set to 'Subnet' with an IP Address of 192.168.1.0 and a Netmask of 255.255.255.0. The 'Remote Secure Gateway IP' is 220.253.72.201. The 'Remote Network' is set to 'Subnet' with an IP Address of 192.168.0.0 and a Netmask of 255.255.255.0. The 'Proposal' is ESP, 'Authentication Type' is SHA1, 'Encryption' is 3DES, and 'Perfect Forward Secrecy' is MODP 768 (Group 1). The 'Pre-shared Key' is 'test'. At the bottom right, there are four buttons: Back, Apply, Cancel, and Help.

Click on the "Apply" button when done.

Step 3. If the remote VPN router is behind a modem with NAT (like the DI-804HV on LAN1 in our example), click on **“Advanced Options”**.

Specify Local ID:

Type – IPv4 Address

Content – the public IP on local site.

Specify Remote ID:

Type – IPv4 Address

Content – the IP address on the WAN port of the remote VPN router.

Local ID	
Type	IPv4 Address
Content	220.253.72.201
Remote ID	
Type	IPv4 Address
Identifier	10.1.1.2

Click on the “Apply” button when done.

Step 4. Go to Tools > System. Click on the “Save” button. This will save the settings into the router's memory.

D-Link
Building Networks for People

Wireless ADSL VPN Router

DSL-G804V

Admin
Date & Time
System
Firmware
Remote Access
Logout

Home **Advanced** **Tools** **Status** **Help**

System Settings

Save Settings To Local Hard Drive

Load Settings From Local Hard Drive

Save Config to Device Memory
Please click 'Save' to start saving configuration to device memory. There will be a delay while saving as configuration information is written to device memory.

Reboot Device
After restarting, please wait for a few seconds for system to come up. If you would like to reset all configuration to factory default settings, please select the "Factory Default Settings" option.
Restart Router with ☒ Current Settings ☐ Factory Default Settings


Help

Configuration of the DI-804HV VPN router on LAN 1

Step 1. Log into the VPN router by opening Internet Explorer and typing the LAN address of the router. In our example we are using the default 192.168.0.1. Enter Username and Password which you specified during the initial setup of the router.

Step 2. Go to Home > VPN. Make sure you have VPN Enable box ticked. Type in a name for the Tunnel Name. Then click on "More" button to the right of the ID "1".

D-Link
Building Networks for People

DI-804HV
Broadband VPN Router

Home Advanced Tools Status Help

VPN Settings

Item	Setting
VPN	☒ Enable
NetBIOS broadcast	☐ Enable
Max. number of tunnels	1

ID	Tunnel Name	Method
1	test	IKE ☒ More
2		IKE ☐ More
3		IKE ☐ More
4		IKE ☐ More
5		IKE ☐ More

Previous page Next page

Dynamic VPN Settings.. L2TP Server Setting.. PPTP Server Setting.. View VPN Status..

☒ ☐ ☐

Apply **Cancel** **Help**

Step 3. On the Tunnel 1 page enter the required information:

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

Remote Subnet/Netmask are for the network located on the other end of the VPN connection.

Remote Gateway: the public IP address of the remote site (the address Internet Provider assigns).

Preshare Key: this is the same key that you used when configuring the VPN tunnel settings on the remote router.

IPSec NAT Traversal – Enable this option if you have a modem with NAT enabled (like in our example).

Auto-reconnect – Enable.

If you have a modem with NAT enabled (like in our example) specify the Remote ID and Local ID.

Remote ID:

Type – IP Address

Value – the IP address on the WAN port of the remote VPN router.

Local ID:

Type – IP Address

Value – the IP address on the WAN port of this router.

Click on Apply.

D-Link
Building Networks for People

DI-804HV
Broadband VPN Router

Home Advanced Tools Status Help

VPN Settings - Tunnel 1

Item	Setting
Tunnel Name	test
Aggressive Mode	☐ Enable
Local Subnet	192.168.0.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.1.0
Remote Netmask	255.255.255.0
Remote Gateway	59.167.244.237
IKE Keep Alive (Ping IP Address)	192.168.1.1
Preshare Key	*****
Extended Authentication (xAUTH)	☐ Enable ☐ Server mode Set Local user... ☐ Client mode
	User Name
	Password
IPSec NAT Traversal	☒ Enable
Auto-reconnect	☒ Enable
Remote ID	Type IP Address Value 59.167.244.237
Local ID	Type IP Address Value 10.1.1.2
IKE Proposal Index	Select IKE Proposal...
IPSec Proposal Index	Select IPsec Proposal...

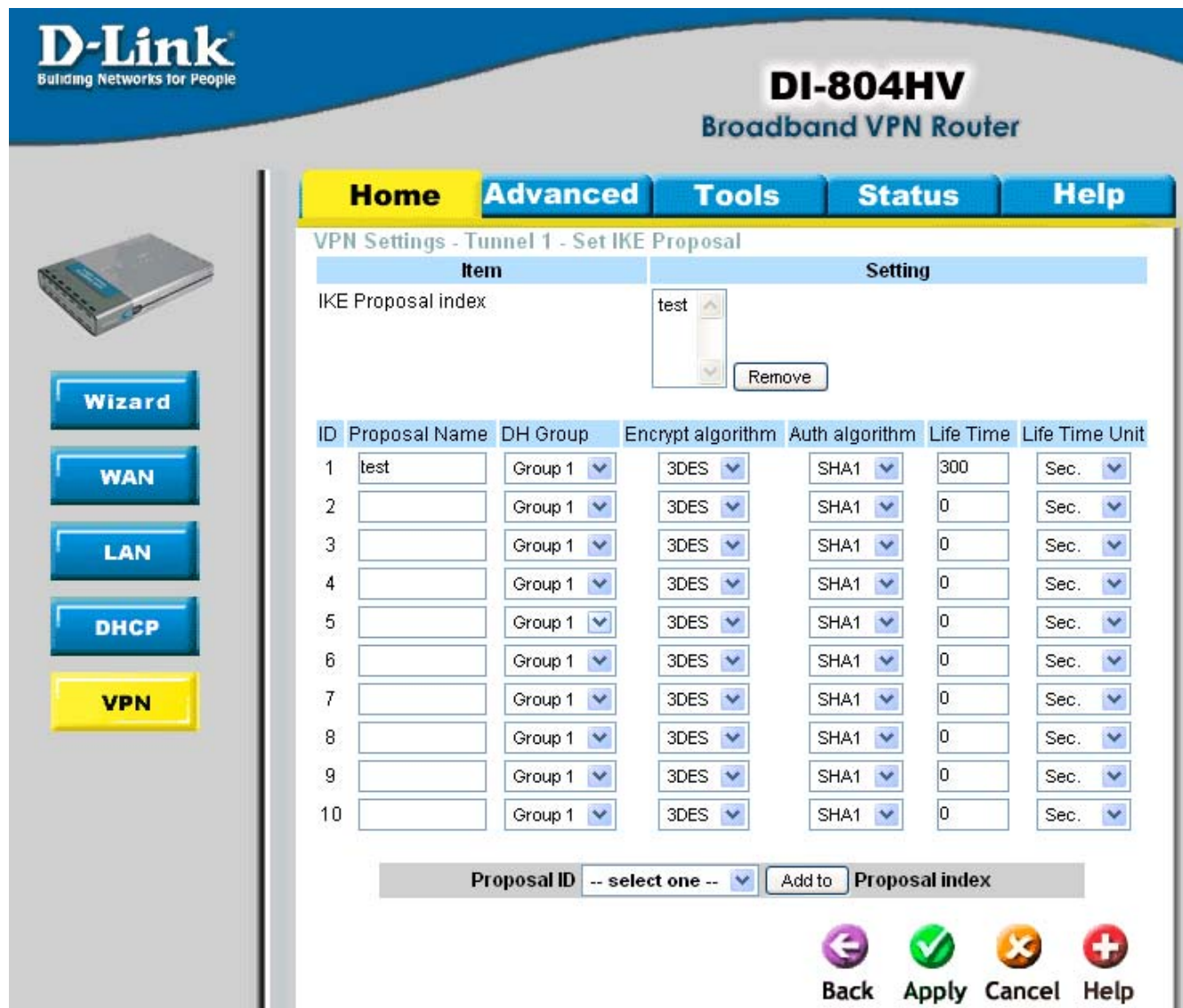
Back Apply Cancel Help

Step 4. Click on “Select IKE Proposal”.

Set ID 1 with a proposal name and the following settings: Group 1, 3DES, SHA1, 300, Sec.

Once the settings have been changed click on the drop down box for “Proposal ID” and select “1”. Then click on the Add to button. This should move the Proposal name to the IKE Proposal Index at the top of the page.

NOTE: If you need to change the setting you do not need to click the Add to button the second time.



D-Link
Building Networks for People

DI-804HV
Broadband VPN Router

Home Advanced Tools Status Help

VPN Settings - Tunnel 1 - Set IKE Proposal

IKE Proposal index: test [Remove]

ID	Proposal Name	DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	test	Group 1	3DES	SHA1	300	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

Back Apply Cancel Help

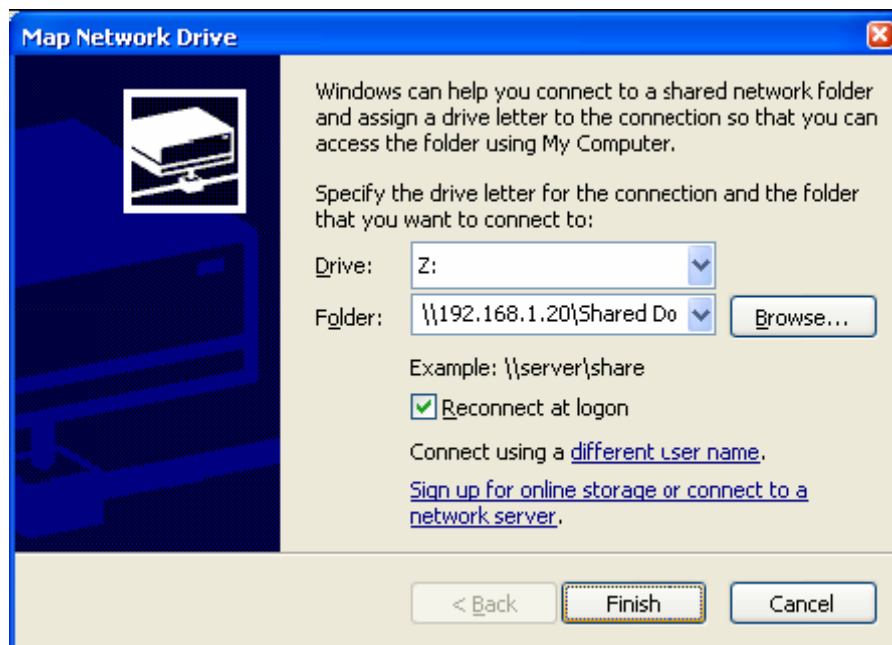
Click Apply, then click on Back.

Step 5. Click on “IPSec Proposal”. Configure it the same way as on the IKE Proposal page, then click Apply.

The router setup is now complete.

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 or remote computer may stop you from accessing remote network.