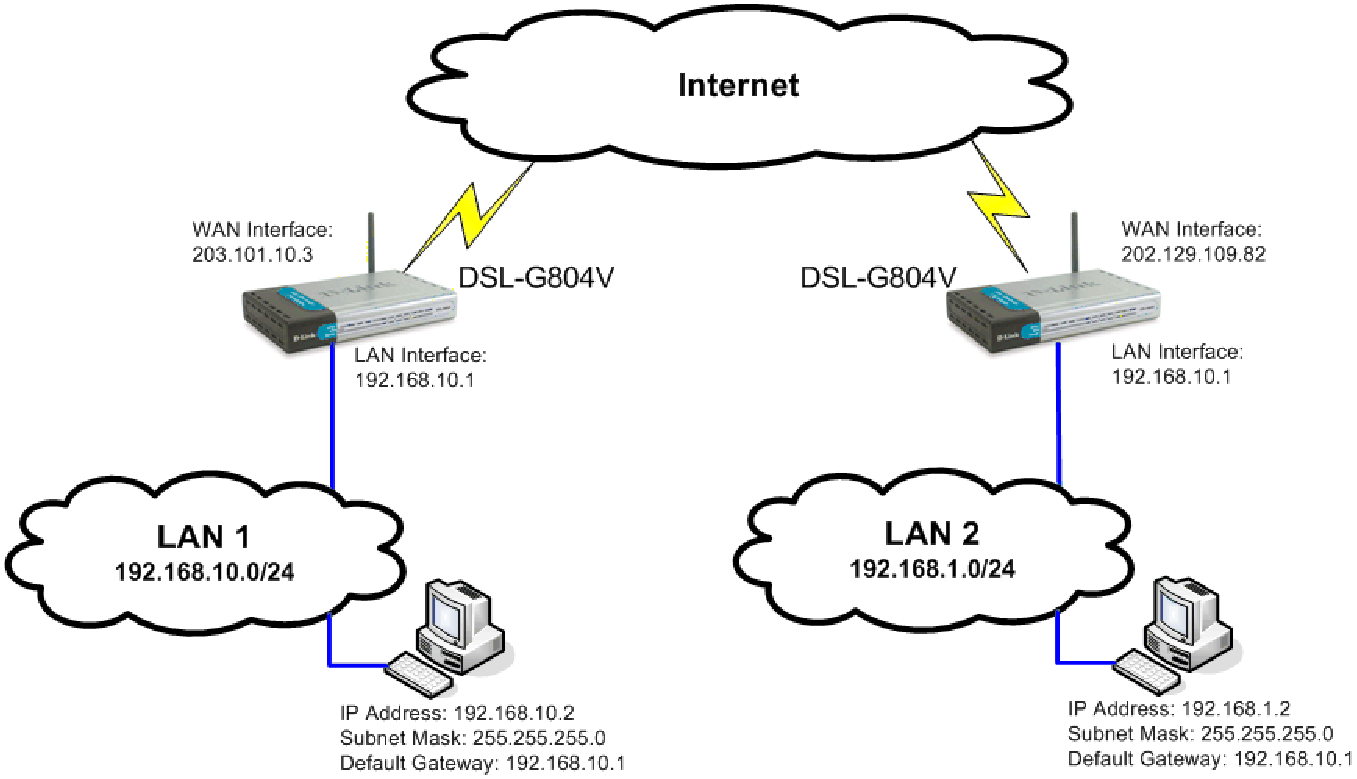
How to setup IPSec VPN connection between two DSL-G804V VPN Routers

This setup example uses the following network settings:



In our example the IPSec VPN tunnel is established between two LANs: 192.168.10.x and 192.168.1.x.
NOTE: It is essential to have private networks (LAN 1 and LAN 2) on different subnets.

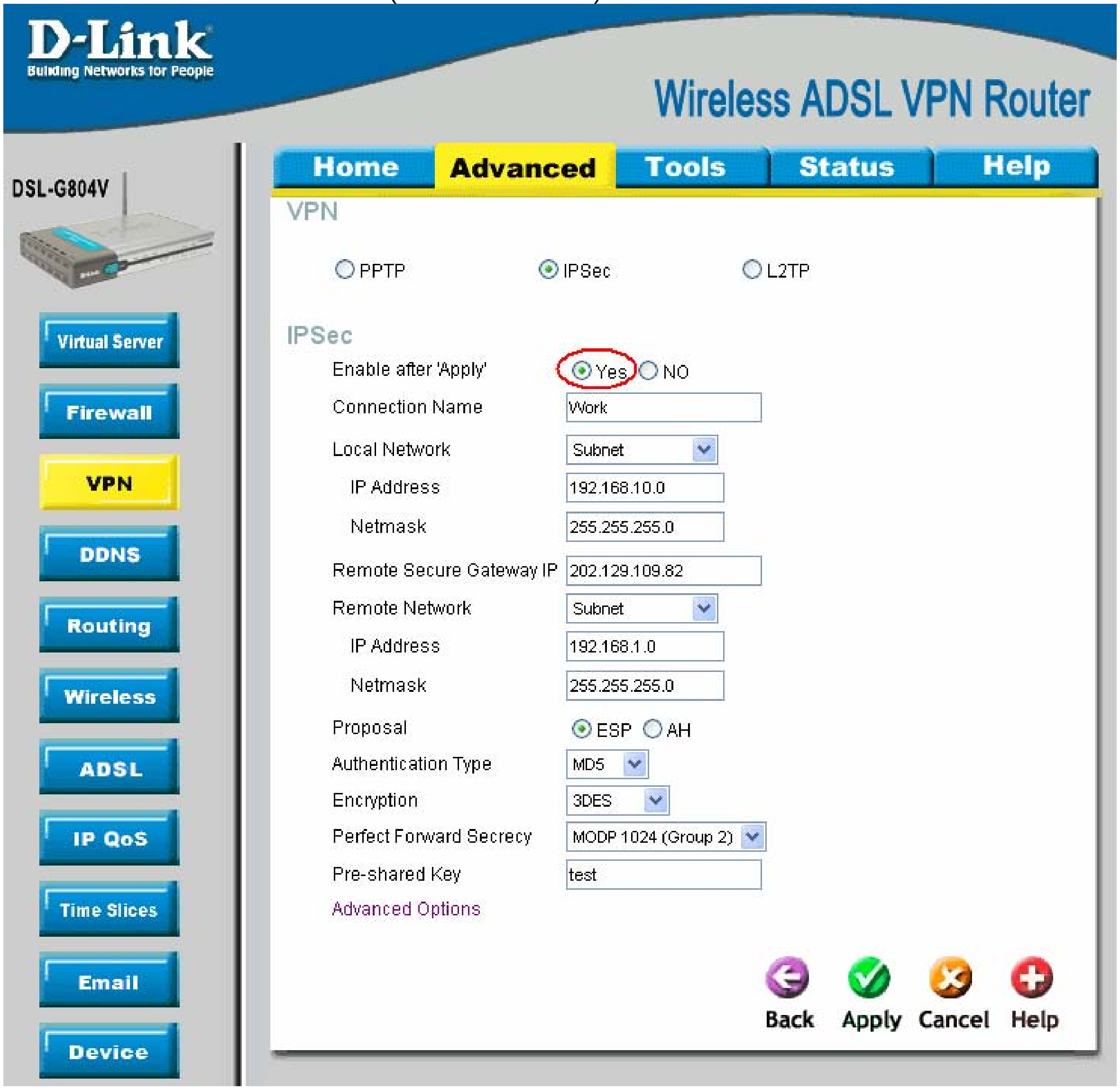
Configuration of the DSL-G804V router on LAN 1

Step 1. Log into the DSL-G804V located on LAN 1. 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. 192.168.10.0).
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. 192.168.1.0).
Netmask - enter the Subnet Mask of the remote network.

Proposal - select ESP.
Authentication Type - select MD5
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).



VPN

○ PPTP ● IPSec ○ L2TP

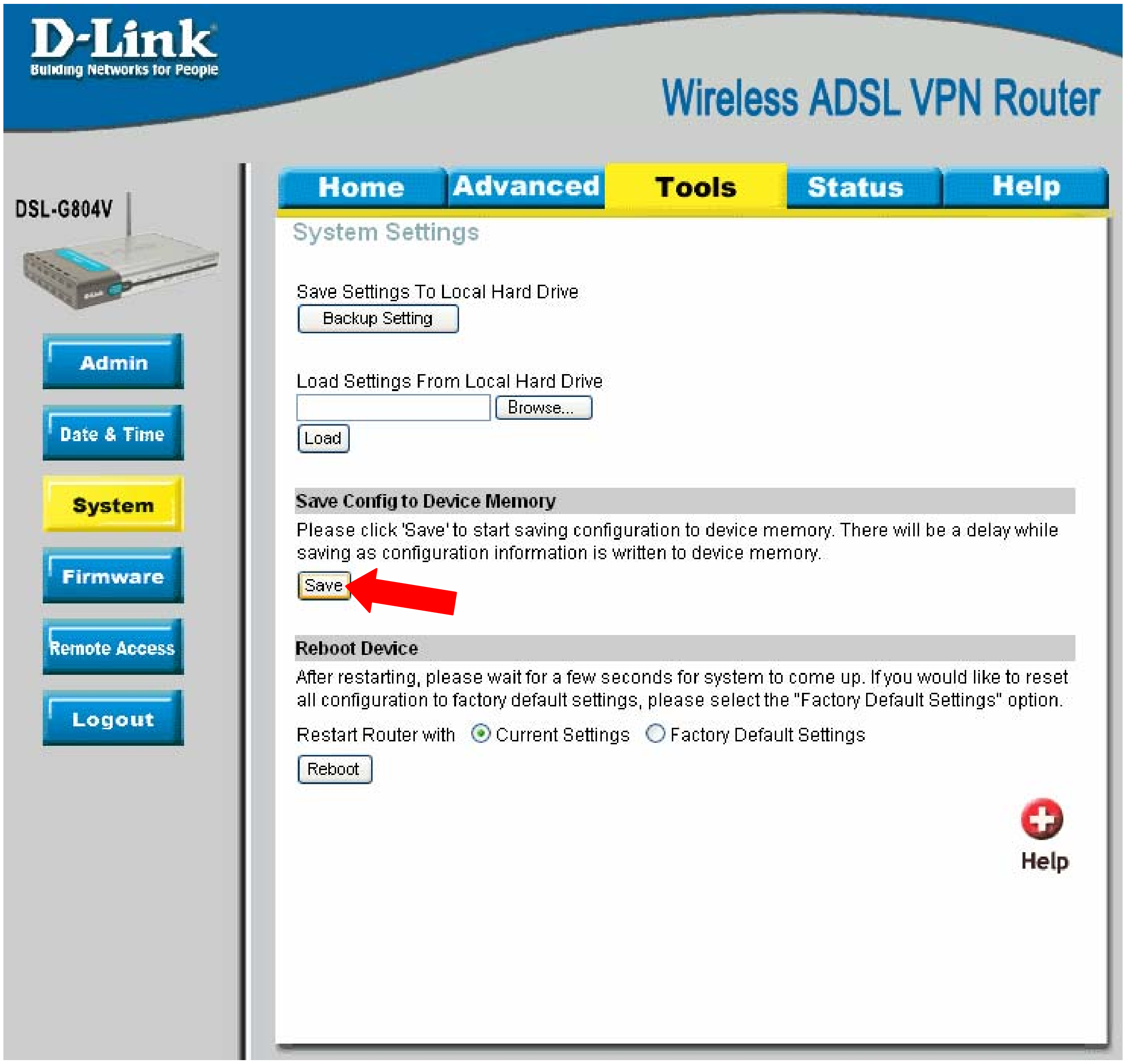
IPSec

Enable after 'Apply'	● Yes ○ NO
Connection Name	Work
Local Network	Subnet
IP Address	192.168.10.0
Netmask	255.255.255.0
Remote Secure Gateway IP	202.129.109.82
Remote Network	Subnet
IP Address	192.168.1.0
Netmask	255.255.255.0
Proposal	● ESP ○ AH
Authentication Type	MD5
Encryption	3DES
Perfect Forward Secrecy	MODP 1024 (Group 2)
Pre-shared Key	test

Advanced Options

Click on the "Apply" button when done.

Step 3. Go to Tools > System. Click on the “Save” button. This will save the settings into the router’s memory.



System Settings

Save Settings To Local Hard Drive

Backup Setting

Load Settings From Local Hard Drive

Browse...

Load

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.

Save

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

Reboot

Configuration of the DSL-G804V router on LAN 2

The steps to configure the second DSL-G804V will be almost identical to the steps for the VPN router on the LAN 1. The only exception is the Local Network, Remote Network and the Remote Secure Gateway IP settings. Note that the subnets on each LAN connecting through VPN should be different.

Step 1. Log into the DSL-G804V located on LAN 2. 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.

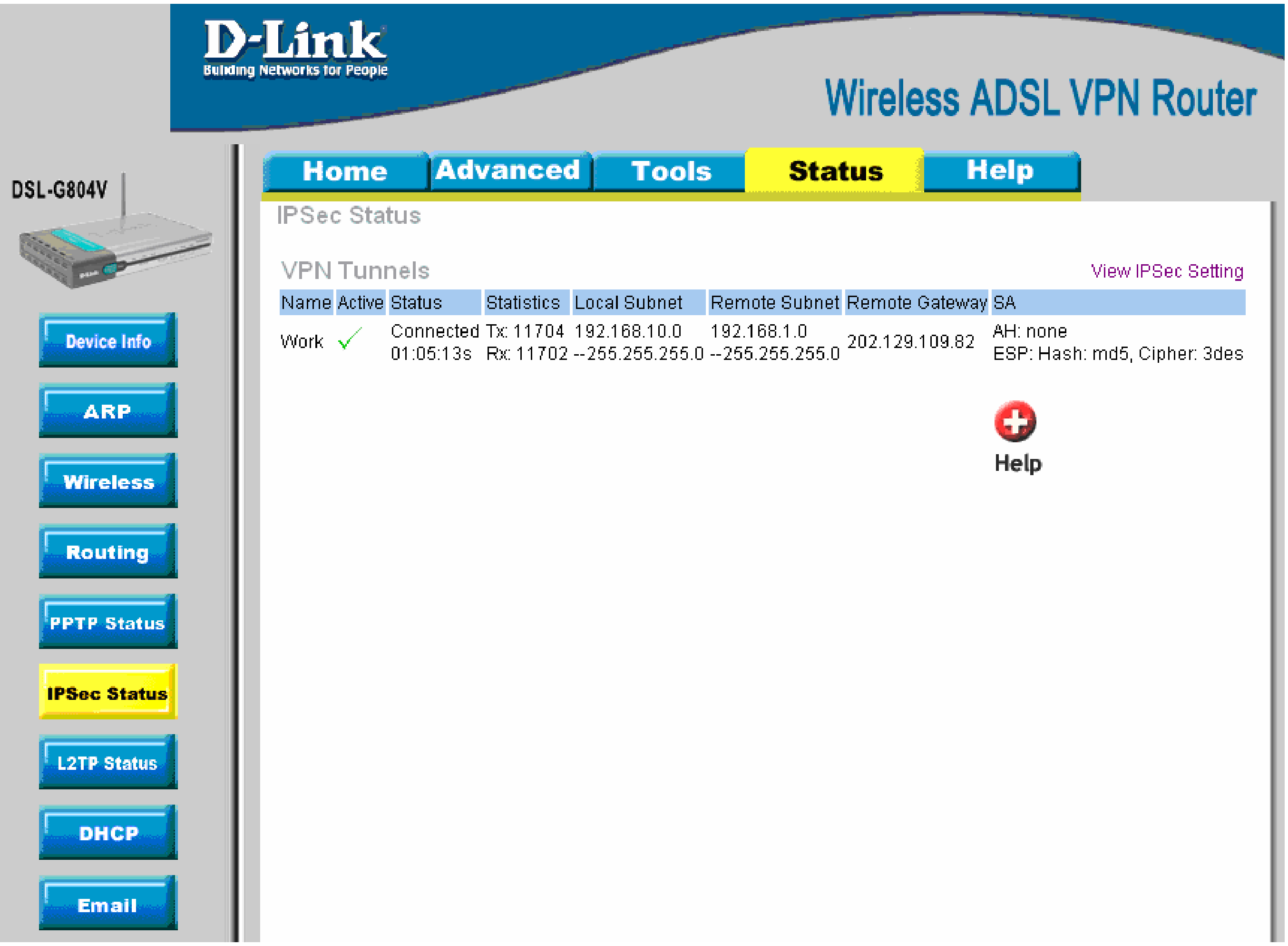
Remote Secure Gateway IP - enter the public IP address of the remote VPN router.
Remote Network - select “Subnet”.
IP Address - enter the IP Address of the remote network. Note that it should be Subnet ID, not a single IP address (e.g. 192.168.10.0).
Netmask - enter the Subnet Mask of the remote network.

Proposal - select ESP.
Authentication Type - select MD5
Encryption - 3DES
Perfect Forward Secrecy - MODP 1024 (Group 2)
Pre-shared Key - enter the same security key you have specified when setting up the VPN router on remote network.

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.



IPSec Status

VPN Tunnels

View IPSec Setting

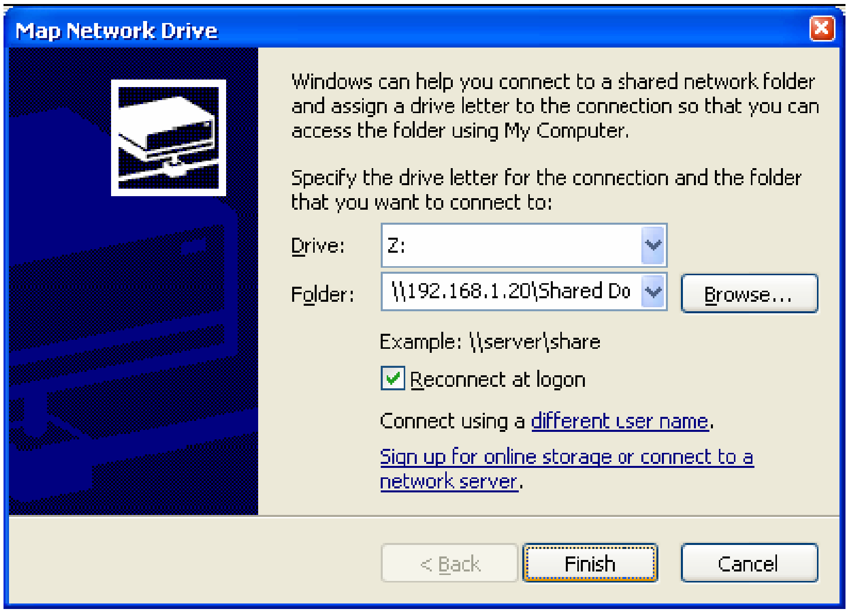
Name	Active	Status	Statistics	Local Subnet	Remote Subnet	Remote Gateway	SA
Work	✓	Connected 01:05:13s	Tx: 11704 Rx: 11702	192.168.10.0 --255.255.255.0	192.168.1.0 --255.255.255.0	202.129.109.82	AH: none ESP: Hash: md5, Cipher: 3des

If VPN Tunnel can not be established:

- Make sure that the modem in front of the DFL-firewall supports VPN passthrough.
- 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 firewalls.

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):



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: Z:

Folder: \\192.168.1.20\Shared Do

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 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.