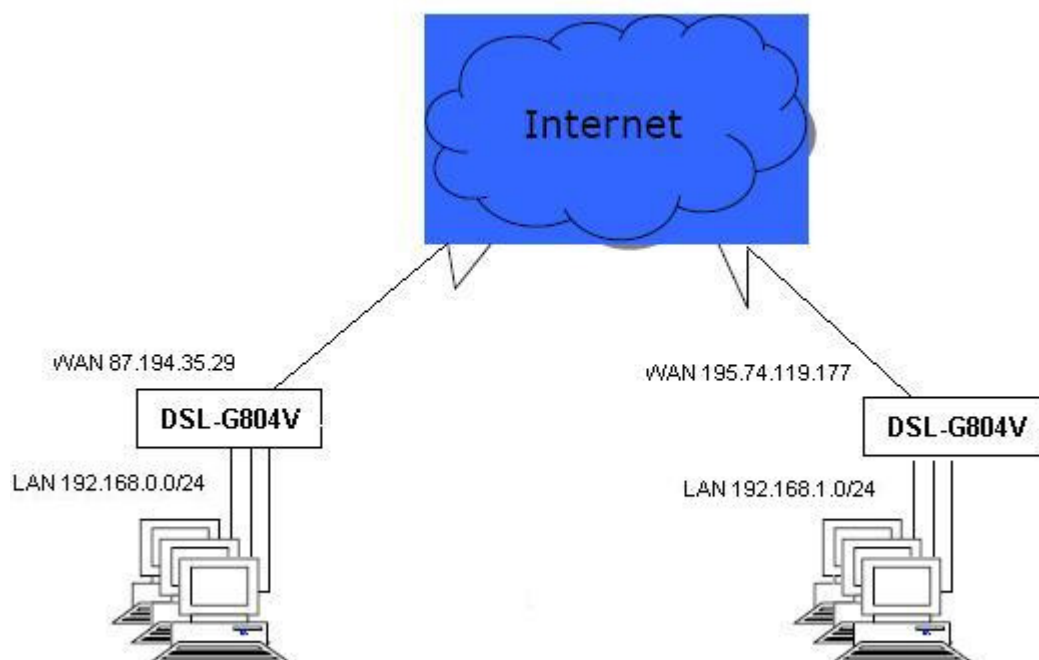


DSL-G804V CONFIGURATION EXAMPLE – LAN TO LAN USING IPSEC



PREPARATIONS

Firmware

Check that the router is updated. New firmware can be downloaded from D-Link servers, <ftp://ftp.dlink.co.uk> and <http://www.dlink.co.uk>

After update is done, please that verify the correct version is being displayed on the *Status – Device Info* page. You may need to clear the cache memory of your web browser to continue. It is advised to reset the router to factory settings after any firmware update.

Note: Firmware updating will clear our your settings. Although this is not recommended, you can save a configuration file to the hard drive, perform the update, and then reload the configuration file.

Network

In order to connect with VPN, the two networks cannot have identical LAN addresses. If **Router A** uses the default IP address 192.168.1.1 on the 192.168.1.0/24 network, set **Router B** to use, e.g. 192.168.0.1 on the 192.168.0.0/24 network.

In order to link two routers together at different locations, you will need to setup the WAN port. Go to *Home – WAN*, fill in your details then apply, save & reboot. Please verify in *Status – Device Info* if your WAN IP address is correct.

Test the connection by pinging an Internet server or browsing the Internet in your web browser.

SETTING UP THE IPSEC TUNNEL

Go to Advanced – VPN, select IPsec and enter your network settings. This is an example.

VPN		VPN	
<input type="radio"/> PPTP	<input checked="" type="radio"/> IPsec	<input type="radio"/> PPTP	<input checked="" type="radio"/> IPsec
<input type="radio"/> L2TP		<input type="radio"/> L2TP	
IPsec		IPsec	
Enable after 'Apply'	<input checked="" type="radio"/> Yes <input type="radio"/> NO	Enable after 'Apply'	<input checked="" type="radio"/> Yes <input type="radio"/> NO
Connection Name	<input type="text" value="LAN_B"/>	Connection Name	<input type="text" value="LAN_A"/>
Local Network	<input type="text" value="Subnet"/>	Local Network	<input type="text" value="Subnet"/>
IP Address	<input type="text" value="192.168.0.0"/>	IP Address	<input type="text" value="192.168.1.0"/>
Netmask	<input type="text" value="255.255.255.0"/>	Netmask	<input type="text" value="255.255.255.0"/>
Remote Secure Gateway IP	<input type="text" value="195.74.119.177"/>	Remote Secure Gateway IP	<input type="text" value="87.194.35.29"/>
Remote Network	<input type="text" value="Subnet"/>	Remote Network	<input type="text" value="Subnet"/>
IP Address	<input type="text" value="192.168.1.0"/>	IP Address	<input type="text" value="192.168.0.0"/>
Netmask	<input type="text" value="255.255.255.0"/>	Netmask	<input type="text" value="255.255.255.0"/>
Proposal	<input checked="" type="radio"/> ESP <input type="radio"/> AH	Proposal	<input checked="" type="radio"/> ESP <input type="radio"/> AH
Authentication Type	<input type="text" value="MD5"/>	Authentication Type	<input type="text" value="MD5"/>
Encryption	<input type="text" value="3DES"/>	Encryption	<input type="text" value="3DES"/>
Perfect Forward Secrecy	<input type="text" value="MODP 1024 (Group 2)"/>	Perfect Forward Secrecy	<input type="text" value="MODP 1024 (Group 2)"/>
Pre-shared Key	<input type="text" value="presharedkey"/>	Pre-shared Key	<input type="text" value="presharedkey"/>

This is an example setup from the left side router, from the diagram on the top of this document.

This is an example setup from the right side router, from the diagram on the top of this document.

In the left example, the Remote Secure Gateway IP is 87.194.35.29. This field should have the right side router's WAN IP. *Note that you can also use a domain name.*

Click **Apply, save and reboot.**

VERIFYING IPSEC TUNNEL

To see if Router A and Router B are connected properly, go to **Status – IPsec** on any of the two routers.

IPSec Status

VPN Tunnels

[View IPsec Setting](#)

Name	Active	Status	Statistics	Local Subnet	Remote Subnet	Remote Gateway	SA
LAN_B	✓	Connected 00:02:05s	Tx: 121 Rx: 121	192.168.1.0 --255.255.255.0	192.168.0.0 --255.255.255.0	87.194.35.29	AH: none ESP: Hash: md5, Cipher: 3des

You can also try PINGING from a machine connected to WLAN or LAN on router A to a machine on WLAN on LAN of router B.

```
C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
U:\>ping 192.168.0.120
```

If you can PING to a machine on the remote LAN, you can also perform other network tasks through the VPN tunnel.

Troubleshooting IPsec

If you don't get the connection like Step 4

- Reboot both routers and wait until ADSL is synchronised.
- Verify is the WAN IP address on the Status page is the same as in your VPN profiles.
- Check the Event Log for error messages relating to VPN or IPsec. The picture below shows how a successful connection will look like
- Reset the router, setup tunnel again. Alternatively test other protocols PPTP or L2TP

Event Log

```
Jan 01 00:19:49 DSL-G804V:ipforw:none: [INFO]SA Under
Negotiating, Drop Packet.
Jan 01 00:19:50 DSL-G804V:ike:none: [INFO]Add policy
00000001_0001_0002
Jan 01 00:19:50 DSL-G804V:ike:none: [INFO]Initiating Main
Mode for policy 00000001_0001_0002
Jan 01 00:19:51 DSL-G804V:ike:none: [INFO]ISAKMP SA
established for policy 00000001_0001_0002 (SA #1)
Jan 01 00:19:51 DSL-G804V:ike:none: [INFO]Initiating Quick
Mode for policy 00000001_0001_0002
Jan 01 00:19:52 DSL-G804V:ike:none: [INFO]IPsec SA
established for policy 00000001_0001_0002 (SA #2)
Jan 01 00:19:53 DSL-G804V:ike:none: [INFO]Initiating Quick
Mode for policy 00000001_0001_0002
Jan 01 00:19:53 DSL-G804V:ike:none: [INFO]IPsec SA
established for policy 00000001_0001_0002 (SA #3)
----- system log buffer tail -----
```