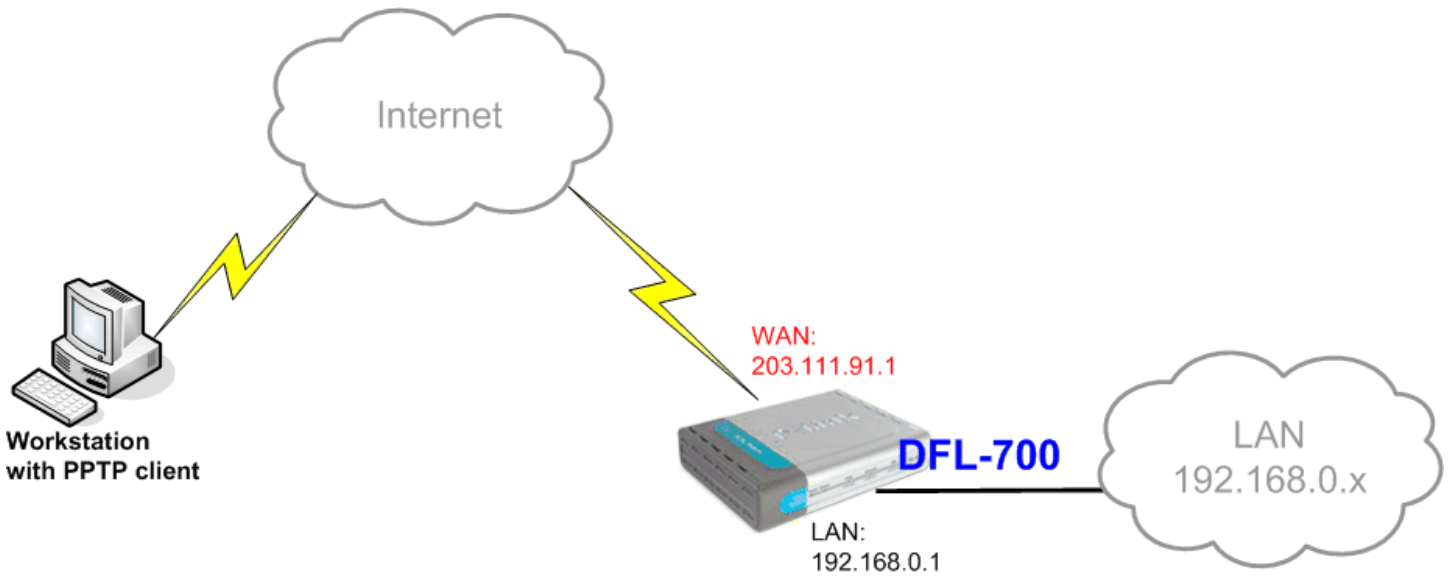


## Setting up VPN connection: DFL-700 with Windows PPTP client



### **DFL-700**

LAN IP: 192.168.0.1 Subnet Mask: 255.255.255.0

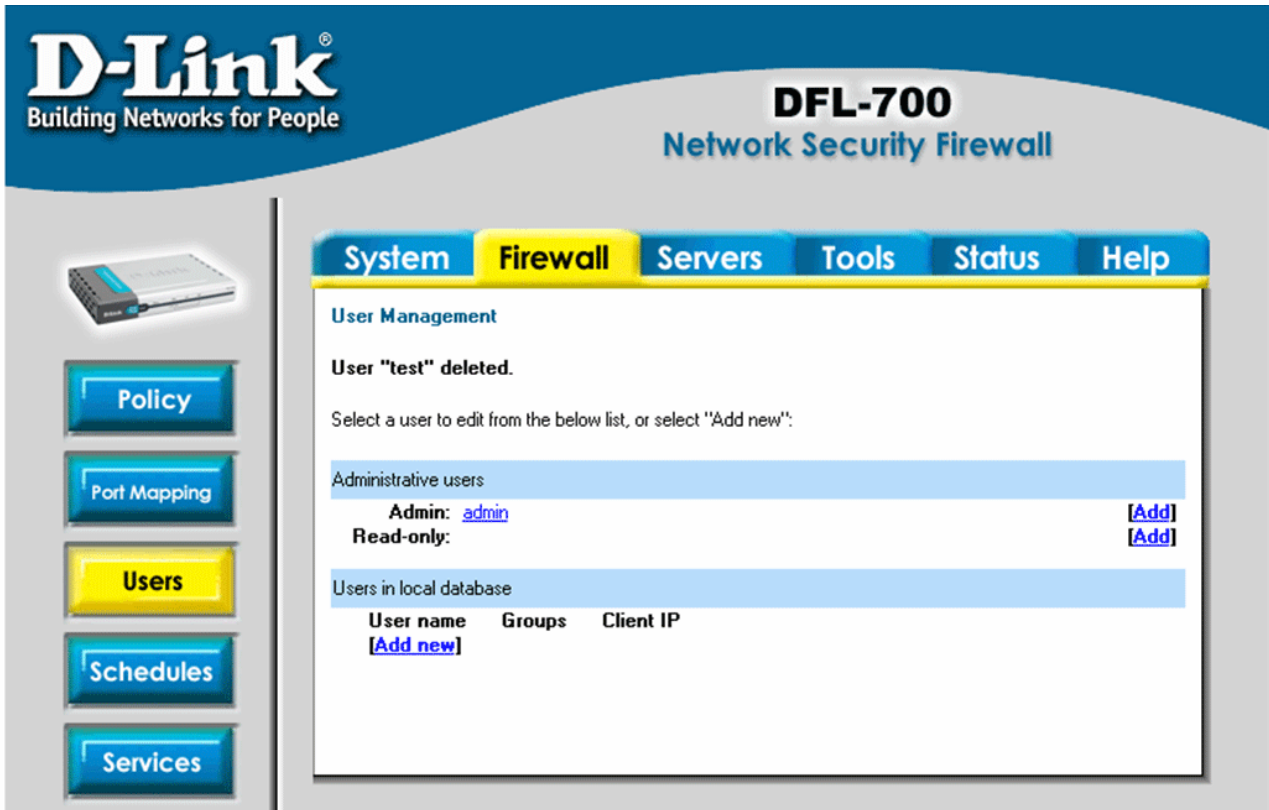
WAN IP: 203.111.91.1 Subnet Mask: 255.255.255.252

Default Gateway: 203.111.91.2

If you are using DSL-300, DSL-300+, DSL-302G modem or DSL-500, DSL-504, DSL-604+ router please see **Appendix 3** at the end of this document.

## Setting up DFL-700

Log into the router's WEB interface and go to Firewall > Users.



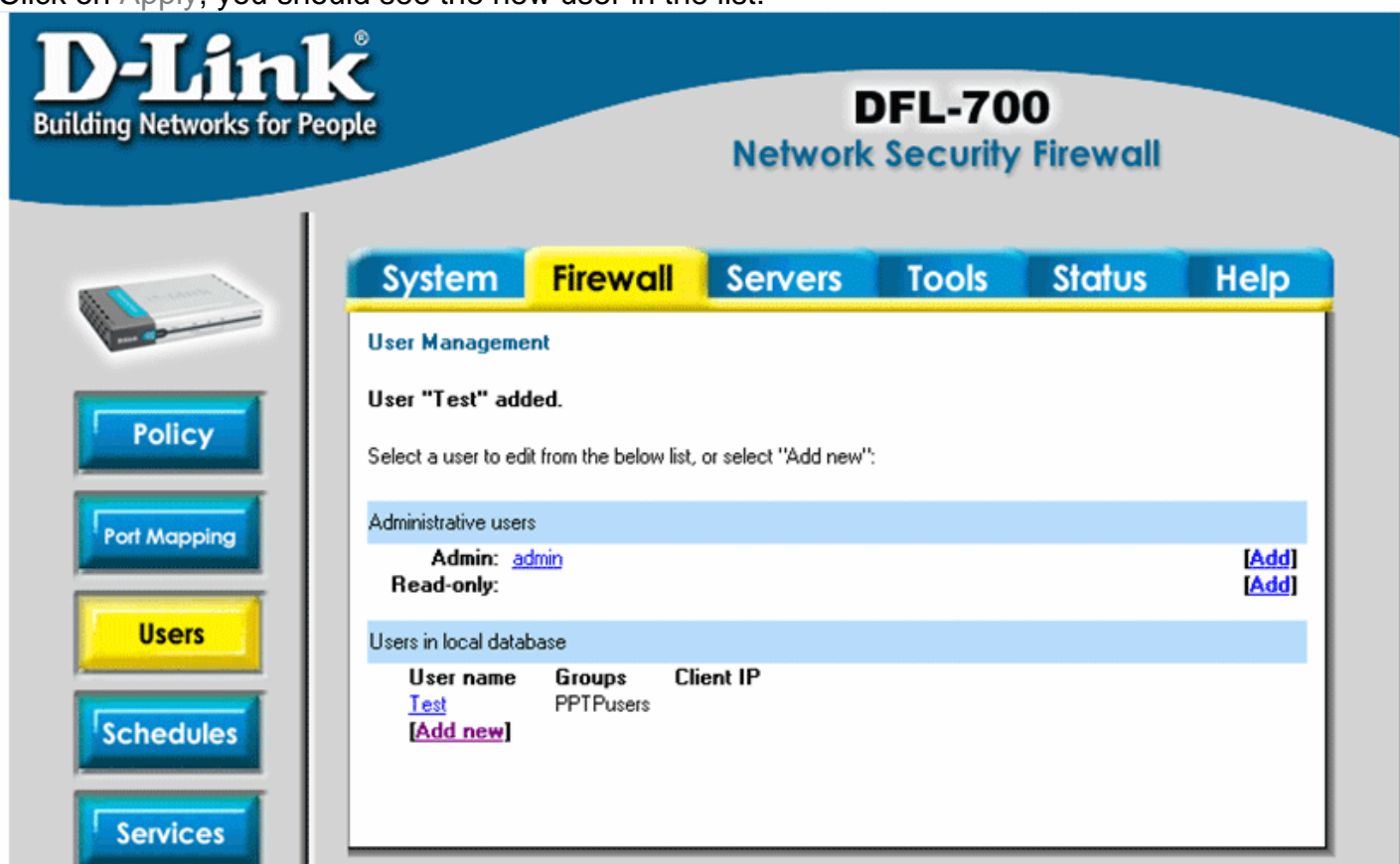
The screenshot shows the D-Link DFL-700 Network Security Firewall web interface. The top navigation bar includes System, Firewall (selected), Servers, Tools, Status, and Help. The left sidebar contains buttons for Policy, Port Mapping, Users (highlighted), Schedules, and Services. The main content area is titled "User Management" and displays a message: "User 'test' deleted." Below this, it instructs the user to "Select a user to edit from the below list, or select 'Add new':". There are two sections: "Administrative users" with "Admin: admin" and "Read-only:" both having "[Add]" links; and "Users in local database" with a table header "User name Groups Client IP" and an "[Add new]" link.

Add new user, specify User name and Password:



The screenshot shows the "Add new user" form in the D-Link DFL-700 Network Security Firewall web interface. The top navigation bar and left sidebar are the same as in the previous screenshot. The main content area is titled "User Management" and contains the "Add new user:" section. The form fields are: "User name:" with the value "Test"; "Group membership:" with the value "PPTUsers"; "Password:" and "Retype password:" both with masked input (four vertical bars). Below these is the "L2TP/PPTP settings:" section with "Static client IP:" (empty) and "Networks behind user:" (empty). A note states: "If empty, the IP address will be taken from the server's IP pool". At the bottom right, there are three buttons: "Apply" (green checkmark), "Cancel" (orange X), and "Help" (red plus).

Click on Apply, you should see the new user in the list:



**D-Link**  
Building Networks for People

**DFL-700**  
Network Security Firewall

System **Firewall** Servers Tools Status Help

User Management

User "Test" added.

Select a user to edit from the below list, or select "Add new":

Administrative users


Admin: [admin](#) [\[Add\]](#)

Read-only: [\[Add\]](#)


Users in local database

User name	Groups	Client IP
<a href="#">Test</a>	PPTUsers	
<a href="#">[Add new]</a>		

Go to Firewall > VPN. Click on Add New PPTP Server:



# DFL-700 Network Security Firewall




- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN**
- Certificates

**System** | **Firewall** | Servers | Tools | Status | Help

### VPN Tunnels

Pick a VPN tunnel to edit from the below list:



Help

### IPsec Tunnels

Name	Local Net	Remote Net	Remote Gateway
<a href="#">[Add new]</a>			


### L2TP / PPTP Client

Name	Type	Remote Gateway	User	IPsec
<a href="#">[Add new PPTP client]</a>				
<a href="#">[Add new L2TP client]</a>				

### L2TP / PPTP Server

Name	Type	Outer IP	Inner IP	IPsec
<a href="#">[Add new PPTP server]</a>				
<a href="#">[Add new L2TP server]</a>				

Specify the details of the PPTP connection. You can use the default settings, just give the tunnel the name you want and allocate the range of IP addresses for the remote PPTP tunnel users (Client IP Pool):



Building Networks for People

# DFL-700

## Network Security Firewall

**System** | **Firewall** | Servers | Tools | Status | Help

**L2TP/PPTP Servers**

Edit PPTP tunnel test:

Name:

Outer IP:  Blank = WAN IP  
Must be WAN IP if IPsec encryption is required

Inner IP:  Blank = LAN IP

**IP Pool and settings:**

Client IP Pool:

Primary DNS:  (Optional)

Secondary DNS:  (Optional)

Use unit's own DNS relay addresses

Primary WINS:  (Optional)

Secondary WINS:  (Optional)

---

**Authentication protocol:**

No authentication

PAP

CHAP

MSCHAP (MPPE encryption possible)

MSCHAPv2 (MPPE encryption possible)

---

**MPPE encryption:**

None - unencrypted

40 bit

56 bit

128 bit (best security)

Encryption is only possible when using MSCHAP or MSCHAPv2 as authentication protocol

**Require IPsec encryption**

**PSK - Pre-Shared Key**

Key:

Retype key:

**Certificate based**

Local Identity:

Certificates:

Use ctrl/shift click to select multiple certificates.  
To use ID lists below, you must select a CA certificate.

Click on Apply. Then activate the changes:

**D-Link**  
Building Networks for People

**DFL-700**  
Network Security Firewall

System Firewall Servers Tools Status Help

**Activate Changes**

Press "Activate Changes" below to save your changes and have them take effect.

If an administrator does not log in within a set time, the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.

Wait for admin login for: 1 minute before reverting.

Activate Changes

Administration  
Interfaces  
Routing  
Logging  
Time

Changes:  
Activate  
Discard

System Firewall Servers Tools

**Activate Changes**

**The configuration was successfully finalized.**

Current configuration available for editing:

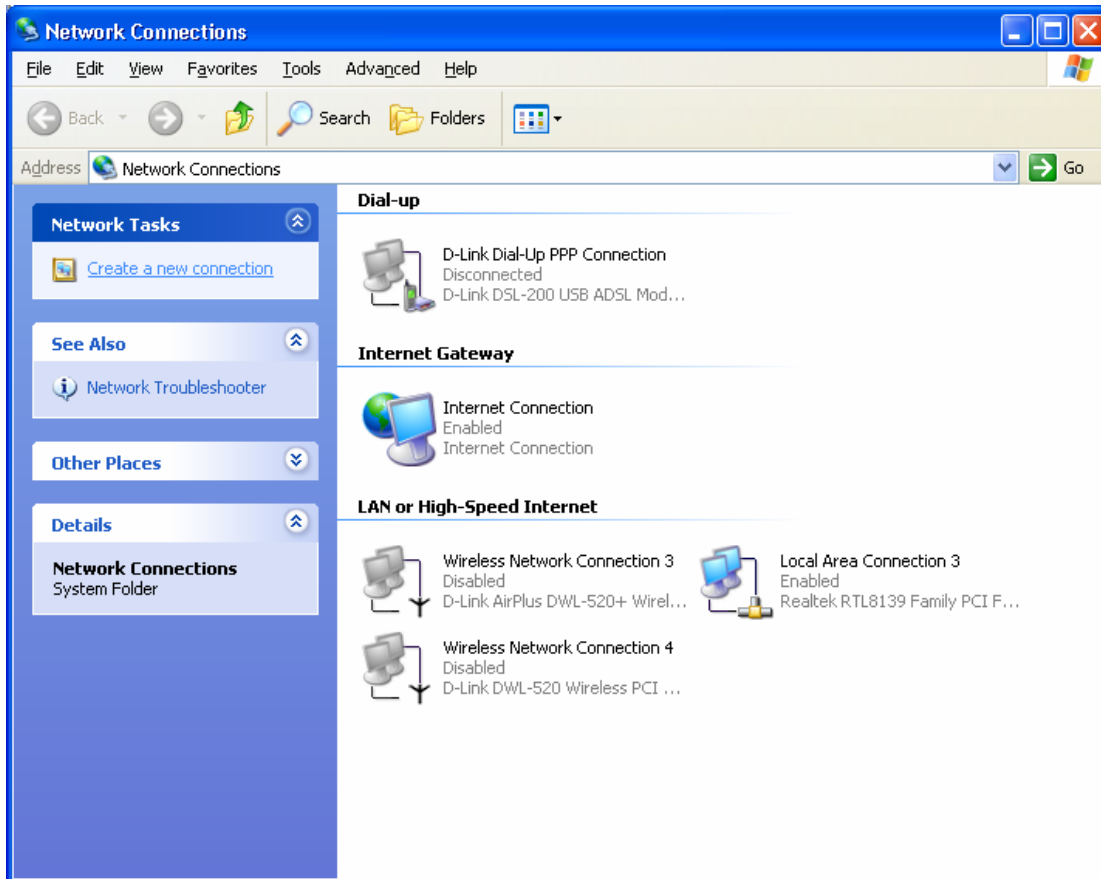
Version: 6  
Modified: 2005-02-10 23:48:50  
... by: "admin"  
... from: 192.168.1.149

## Setting up PPTP connection in Windows

Click on Start > My Network Places, Then click on View Network Connections under the Network tasks on the left hand side.

You should see a window similar to the one below.

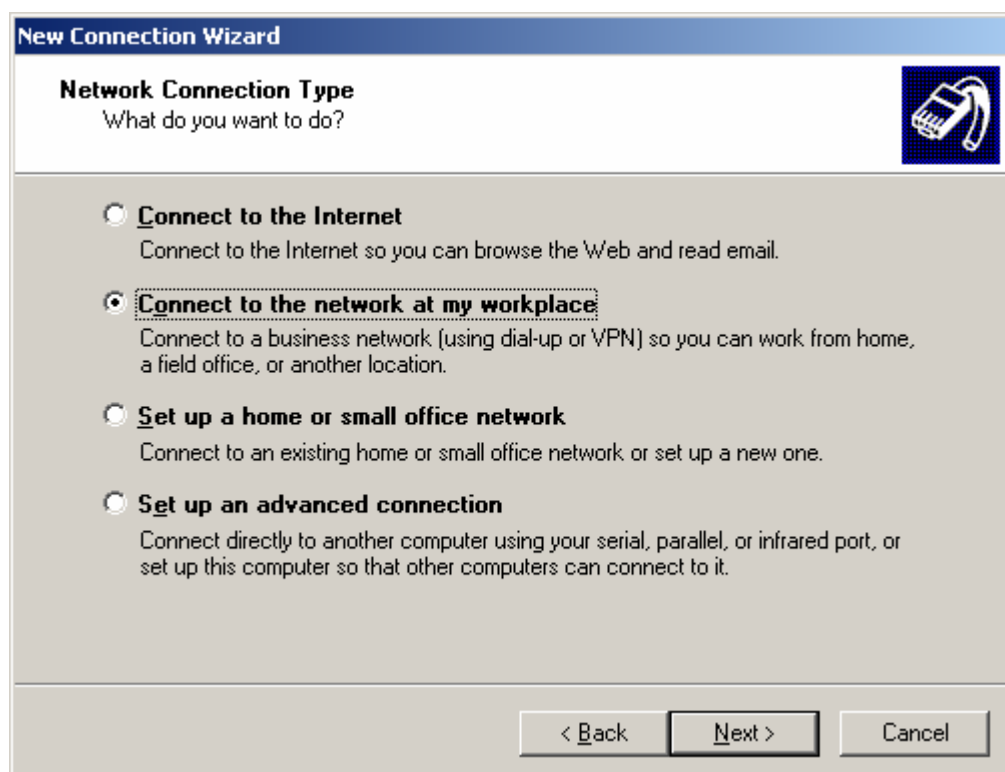
Click on Create a new connection.



Click on Next when you get the Wizard as below.



Then select **Connect to the network at my workplace**.  
Click on Next.






Click on Virtual Private Network connection, then click on Next.

**New Connection Wizard**

**Network Connection**  
How do you want to connect to the network at your workplace?



Create the following connection:


- Dial-up connection**  
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.
- Virtual Private Network connection**  
Connect to the network using a virtual private network (VPN) connection over the Internet.

< Back   Next >   Cancel

Enter a name for your PPTP connection:

**New Connection Wizard**

**Connection Name**  
Specify a name for this connection to your workplace.



Type a name for this connection in the following box.

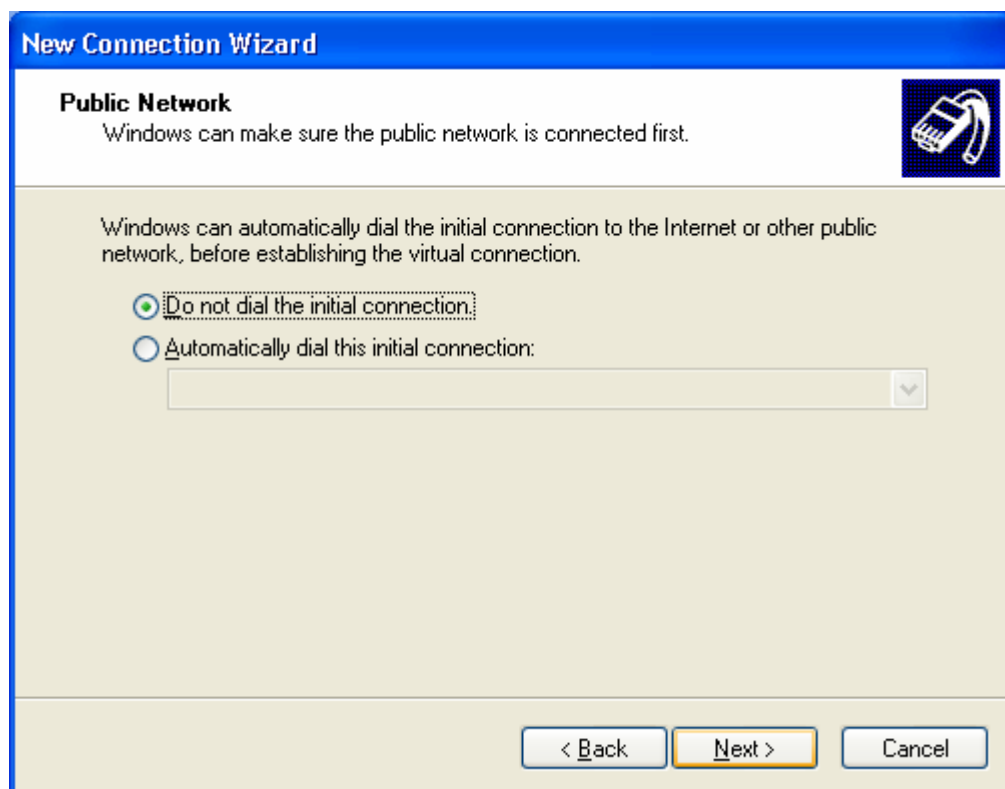
Company Name

D-Link VPN

For example, you could type the name of your workplace or the name of a server you will connect to.

< Back   Next >   Cancel

Optional step: select Do not dial the initial connection, if you use dial up you can change this later on, Click on Next.



**New Connection Wizard**

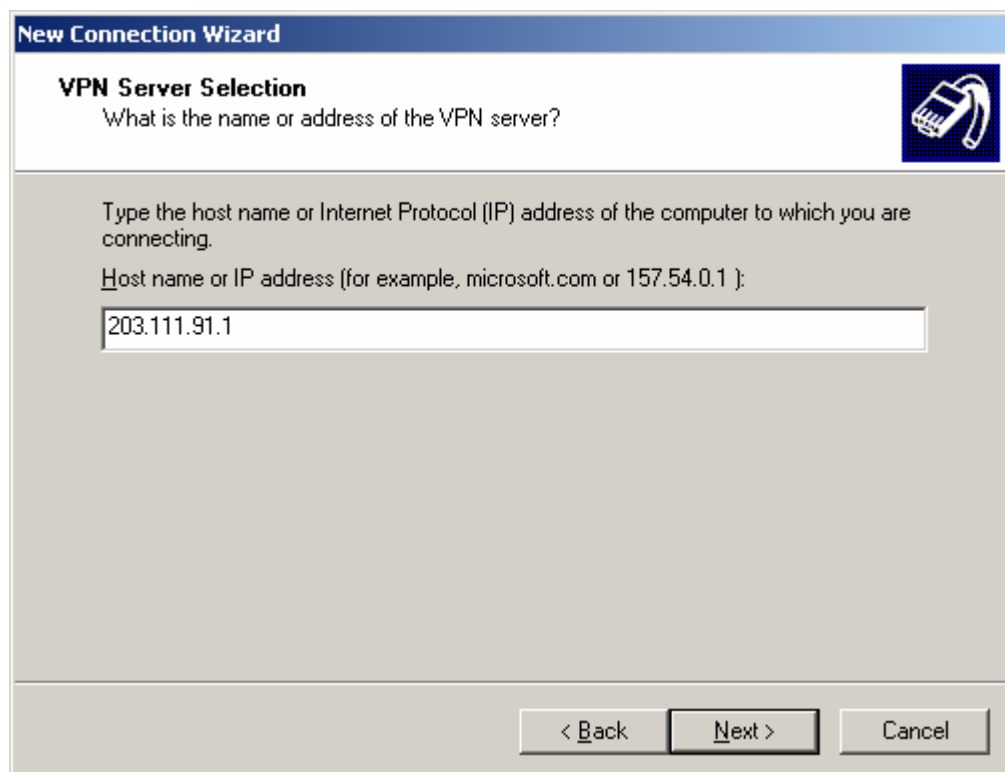
**Public Network**  
Windows can make sure the public network is connected first.

Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.

Do not dial the initial connection:  
 Automatically dial this initial connection:

< Back   Next >   Cancel

Next enter in the public IP address of the VPN server (the one given by ISP). You can find this IP under the status page of the DFL-600 (if you have a router or NAT modem in front of the DFL-600, you need to look up the IP address there).



**New Connection Wizard**

**VPN Server Selection**  
What is the name or address of the VPN server?

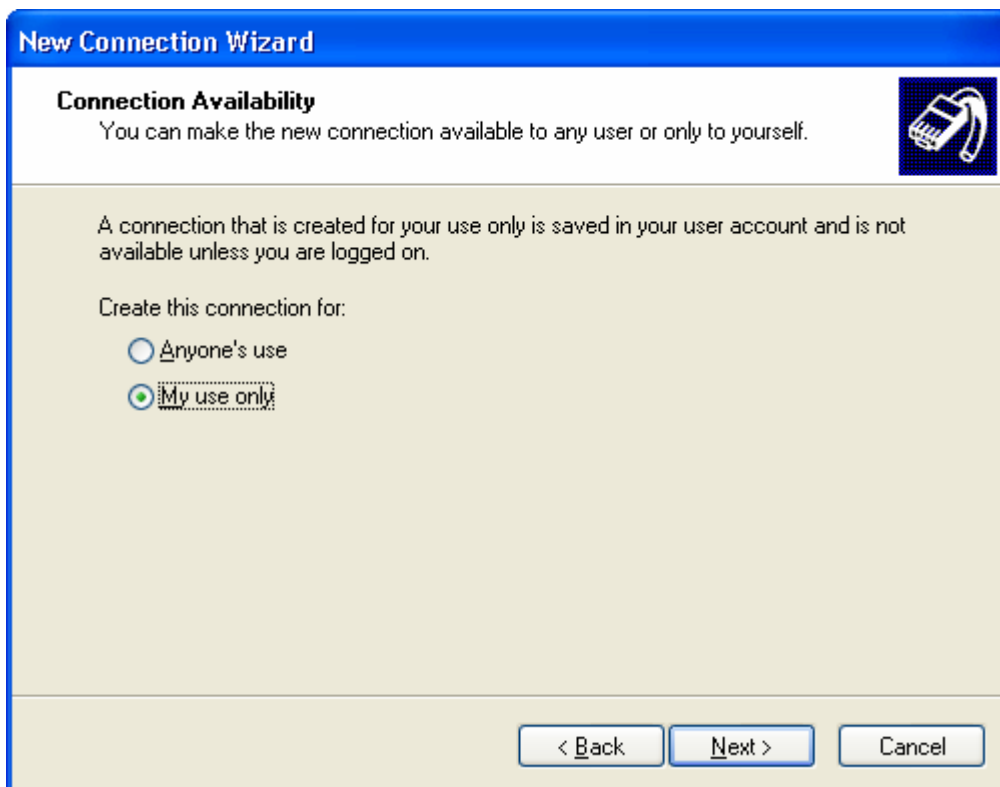
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1):

203.111.91.1

< Back   Next >   Cancel

Optional step: to make your VPN safer in the home environment click on My use only, If you want other people to use this connection, click on Anyone's use.



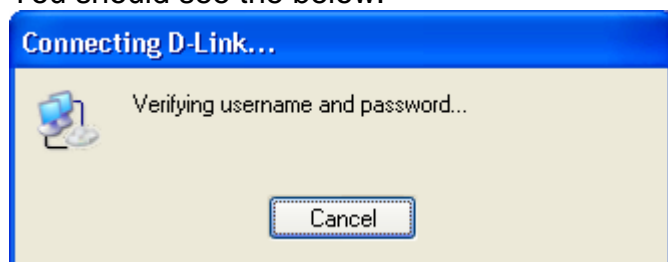
To complete the connection Wizard click on Finish.



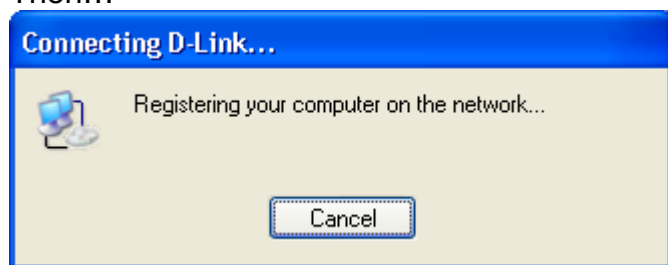
Enter in the User name and password that you entered into the PPTP page of the DFL-600, then click connect.



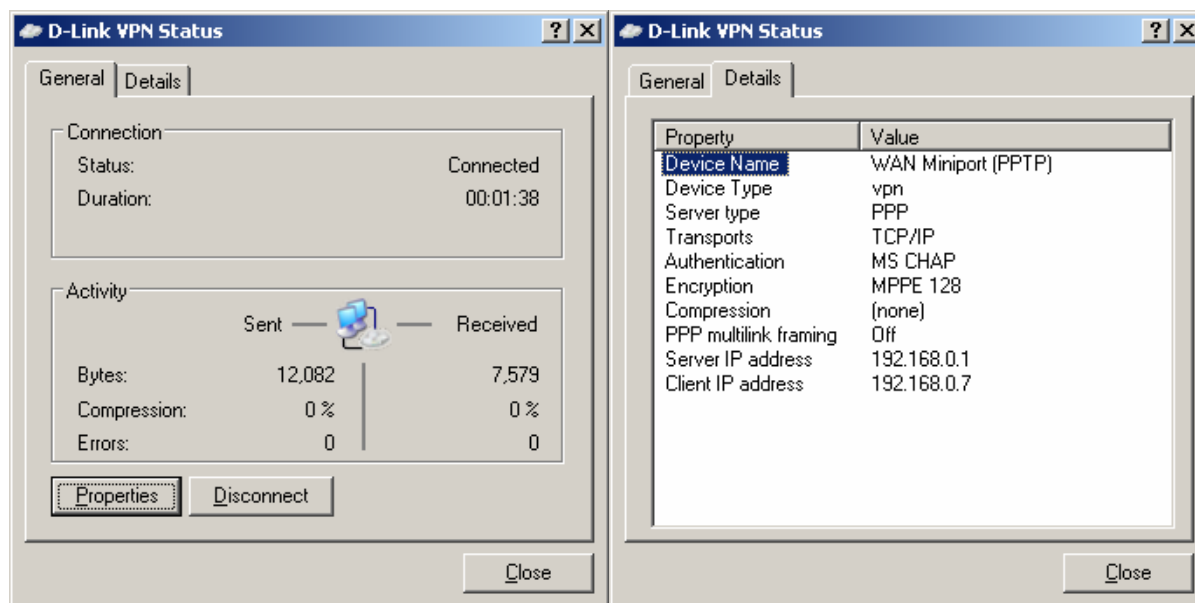
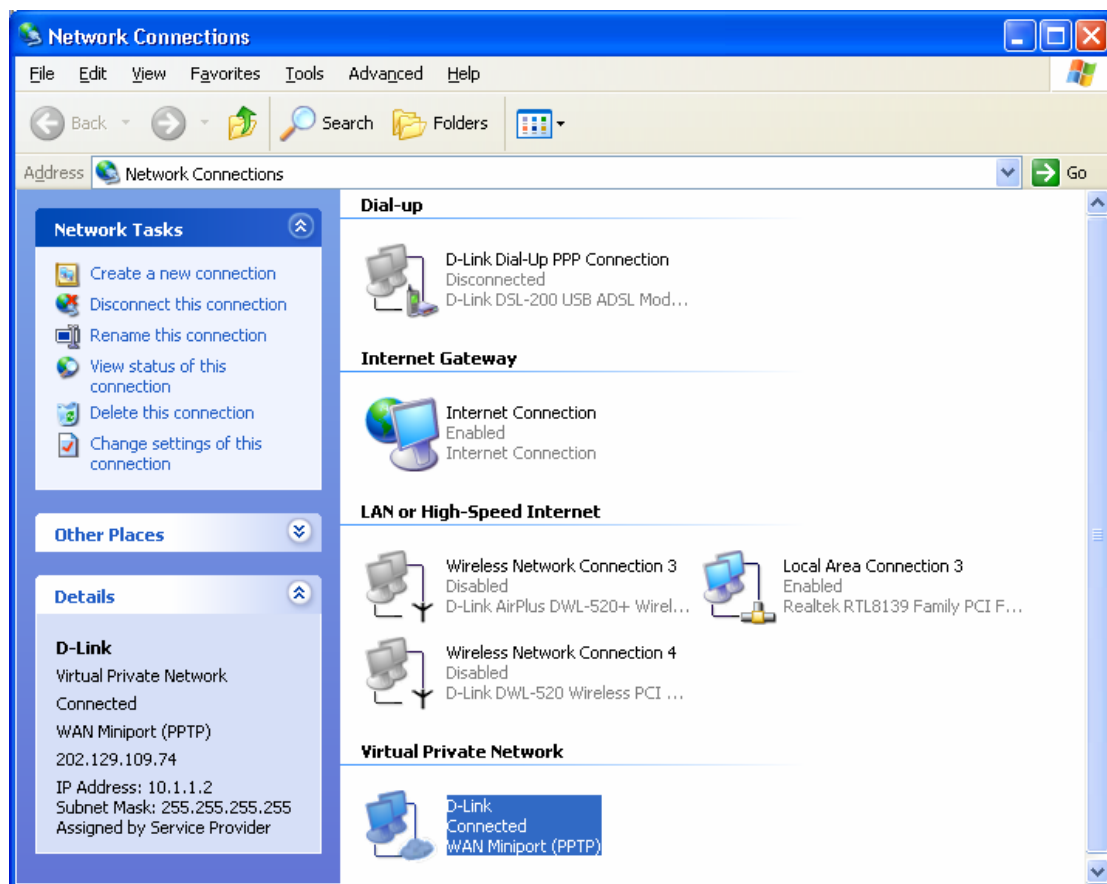
You should see the below.



Then...



Once the PPTP connection is established you should see a window similar to the one below. The Virtual Private Network icon is now blue, and says “Connected”



You can check your IP settings and VPN connectivity:

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 203.111.91.2
    Subnet Mask . . . . . : 255.255.255.252
    Default Gateway . . . . . : 203.111.91.1

PPP adapter {546DB0F7-AD1F-4C9C-A975-FBA8DB211EE0}:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.0.7
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 192.168.0.7

C:\>ping 192.168.0.149

Pinging 192.168.0.149 with 32 bytes of data:

Reply from 192.168.0.149: bytes=32 time=4ms TTL=128
Reply from 192.168.0.149: bytes=32 time=6ms TTL=128
Reply from 192.168.0.149: bytes=32 time=4ms TTL=128
Reply from 192.168.0.149: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.0.149:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

## Appendix 1.

### How to test your VPN connection.

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

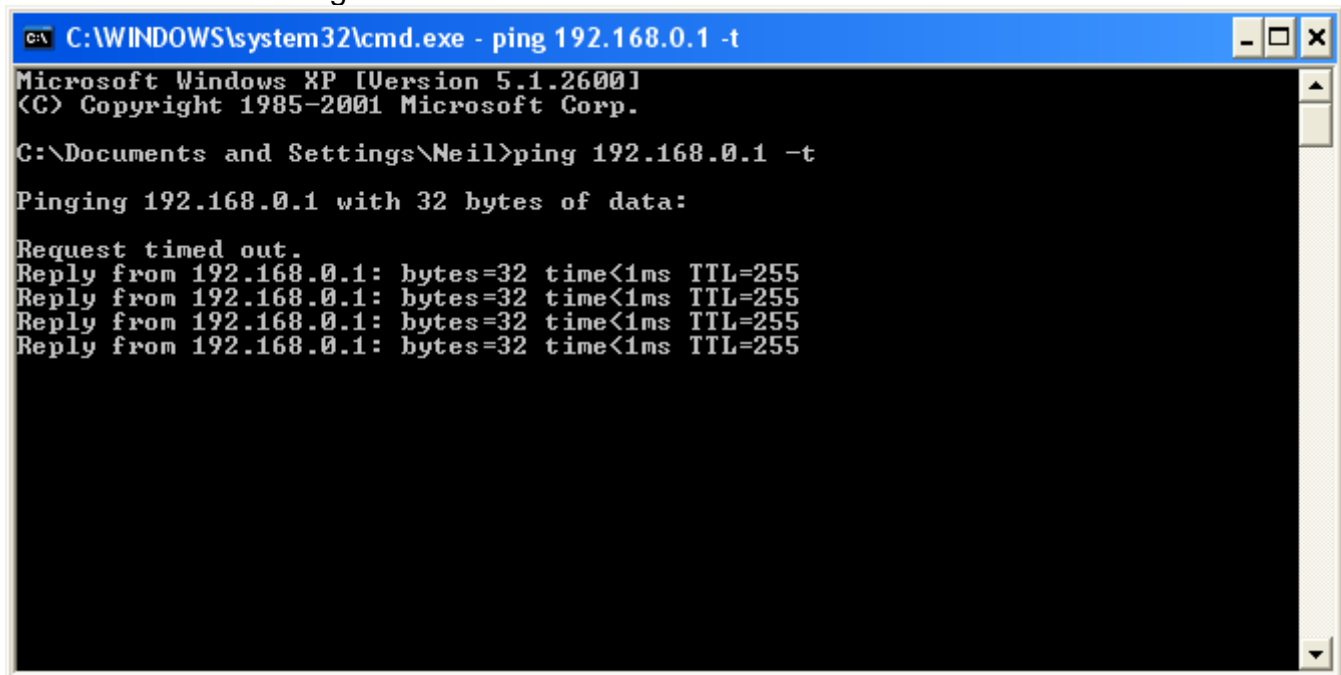
The make sure that you are on the XP's location with the PPTP connection.

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

If you type in the below then hit enter.

**ping 192.168.0.1 -t (or the LAN IP address of the DFL-600)**

You should see messages similar to the one below:



```
C:\WINDOWS\system32\cmd.exe - ping 192.168.0.1 -t
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Neil>ping 192.168.0.1 -t

Pinging 192.168.0.1 with 32 bytes of data:

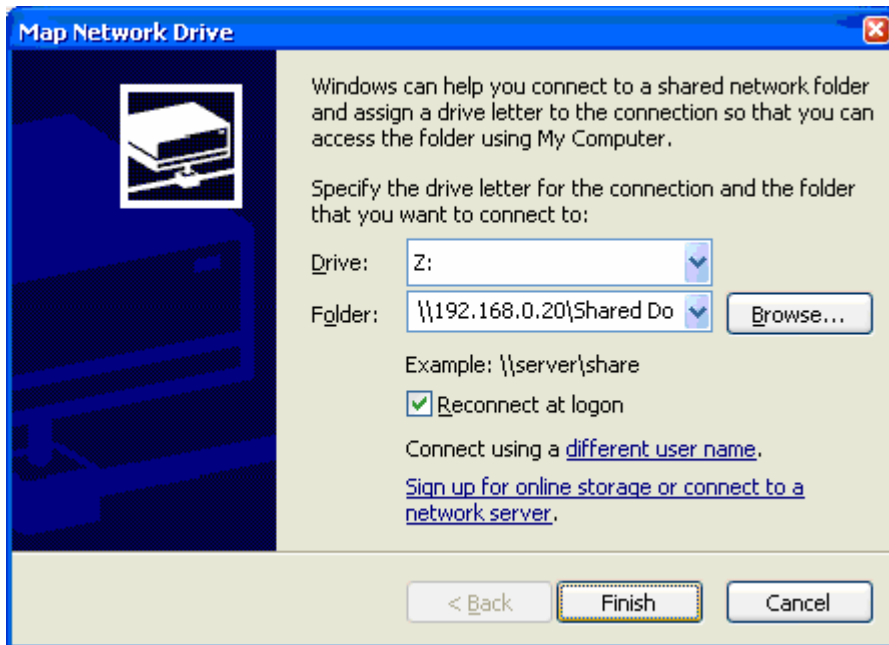
Request timed out.
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
```

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):



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. 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 DFL-600 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 DFL-600 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 DFL-600.
2. Set WAN port on DFL-600 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 DFL-600 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**.

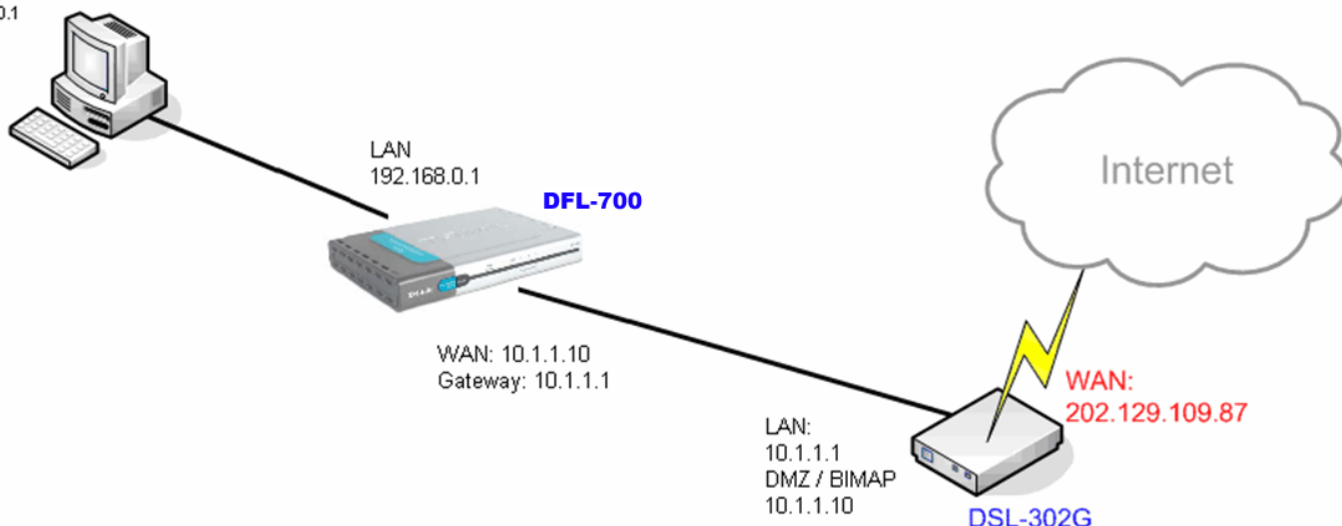
Note that you need to enable VPN pass-through on the router. Or go to **NAT Configuration** and enable **DMZ**: specify the IP address of the WAN port of DFL-600 there.

DFL-600 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 DFL-600 will have private IP address. When setting up **Remote Gateway** in VPN you will need to use public IPs 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.

WorkStation A:  
192.168.0.10  
Gateway:  
192.168.0.1



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 DFL-600 which is connected to this modem. **Global address** leave as 0.0.0.0:

#### NAT Rule - Add

NAT Rule Information				
<b>Rule Flavor:</b>	BIMAP <input type="button" value="v"/>			
<b>Rule ID:</b>	<input type="text" value="2"/>			
<b>IF Name:</b>	ALL <input type="button" value="v"/>			
<b>Local Address:</b>	<input type="text" value="10"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="10"/>
<b>Global Address:</b>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Copyright © 2002 D-Link, Inc. All rights reserved.

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.