

Wireless Broadband Gateway

Secure Configuration Guidelines

1 Introduction

The objective of this document is to provide some installation instructions / check list for wrongly named "Wireless Broadband Router" (as in most of them, no routing protocol is running, no more routing table than in PC).

Even if the principles apply to any Wireless GW, as I'm the owner of a D-Link DI-614+ Rev B box ("Wireless router") and a D-Link DWL-650+ PCMCIA card, this document will be a little oriented to D-Link products.

This document is published on :
<http://users.swing.be/id-phy/WLAN/WLAN-Config.html>



1.1 Wireless ...

If you want more info about Wireless or Wi-Fi, you could start with :

[Wi-Fi Alliance index](#)
[Wi-Fi Planet - The Source for Wi-Fi Business and Technology](#)
[Wi-Fi Security at Work and on the Road](#)

... or just ask Google !

1.2 Security concerns

A wireless access point (WAP), is a **public** access, just like connecting your LAN (wired or not) to the Internet, but with one major difference : only your neighborhood can access it. Is this worse or better than Internet ? Think about it and provide your own answer ... From my point of view, even with a broadband connection, when connected to the Internet, I change regularly form IP address and nobody knows it : I *feel* completely *anonymous* ! Anonymous is not synonymous of security, I agree, but this is out of scope of a wireless security. Now, with a WAP, my home LAN is *extended* to my neighborhood, it is not anonymous anymore ! If I have very good relationship with my neighbors, first I don't know all of them, second this is not a reason to invite everybody on my home LAN, to share my broadband access with anyone (if some one uses your broadband connection "for free" to surf, it isn't really a security concern, he will just "eat" some of your bandwidth !), and third I don't want them to know what I do at home (I switch my connection on, only when needed): a little *privacy* please. Other said, my first concern is to convert this **public** access to a **private** one !

This said, aside the *privacy* aspect, the wireless gateway is not a security issue by itself : it can just provide you some extra security, and without it, your PC is/was directly connected to the Internet. If you configure your *router* with the biggest security holes, you'll never be less secure than without it : the true security must rely on each PC security, provided with personal firewall.

Now, the wireless gateway gives you also a **home LAN**, and you can use it not only to share the Internet access, but also to share private resources like printers, disks, folders, files, ... and those shares resources are *exposed* to the Internet, accessible in wireless. And here, you open security issues, open holes on your hosts, PCs. Remember, as soon as wireless is activated on the *Wireless router*, your wired connections are exposed

as well : the *router* makes no distinction, at IP level, between wired and wireless connections : both are part of one single LAN ! The only way to share resources in a complete secure way is to do it only through wired connections, and disable the Wireless (and Internet connection) the time you transfer data, the time you set shared resources (folders), and immediately "unshare" the folder prior to re-enable wireless (Internet). That will comply with the most strict business security policies.





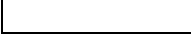
Regarding business security, using your broadband connection for "*teleworking*", if you connect to your corporate network using a sound VPN client with IPSec encryption and have a *Personal Firewall*, you're safe, that PC is safe. But are you always connected to your Corporate network, and when not, **is your Personal Firewall always active** on your Wireless/Wired interfaces ? The concern is more when you directly surf on Internet without going through Corporate network, or if you have other PCs connected (wired or wireless) to the gateway. If you also use another PC to backup your (Company) data (which is a good idea), is that PC well protected ?

Resumed, with a Personal Firewall on each PC, you're safe. The concern is more the PCs without FW, or *opened FW* (for games, sharing, ...) with "*sensitive*" data, on your home LAN (wired or not). And remember, enabling a Wireless Access Point on your LAN, is putting it on the *public space* !

2 Configuration guidelines

Lets start with the “Wireless Router” configuration, then have a look at the PC (USB / PCMCIA / ...) card.

I suggest to use (print) the tables below to write down the configuration changes you made, and safe it in a “secure” place. The first column indicates in which order I did the configuration, number are underlined when the *router* re-booted, and the color indicate the security requirement level, from *required* to *no security impact*, as illustrated in the table below. (NB : you may not agree with my classification.) You can also use it as *checkbox*, and use the third one to write parameter value you selected or chose (some examples being provided).

Color code	Requirement level
	Highly recommended WLAN security feature
	Best practice WLAN security feature
	Additional security feature recommended
	Limited security impact
	No security impact

But, first to *deeply* secure it, you may want see it work ! So, first install it with **Quick start ...** settings (first section below), at least to access the *wireless router ...* in order to configure it !!! Also take this first step opportunity to record MAC addresses of connected equipments (this is the easiest way to get those).

2.1 IPCONFIG

Remember this DOS command : `IPCONFIG [/ALL]` (running in a DOS box (Command prompt : Start/run cmd), on all Windows version) shows the IP address assigned to interfaces. With the `/all` option, you also see the MAC address (Physical address) of the interface. **This command is very useful when debugging LAN IP addressing on the router.**

On Windows 95 / 98, you can also run the ‘winipcfg’ command (in start/run).

2.2 “Wireless Router” configuration

In this section, I’ll try to list all elements you should take care of to get an *as safe as possible* Wireless LAN Gateway configuration.

Note that section & item order in the table below doesn’t exactly reflect the order/section of D-Link DI-614+ Rev B configuration tool. However, I’ll try to refer to D-Link DI-614+ sections / items, putting comments between square brackets [].

This document is based on the DI-614+ Rev B2 (One external antenna + one internal, instead of 2 externals. Note the 2d antenna is not used to transmit/receive, but only to measure the “echo” and enforce the reception (dixit D-LINK support)). Rev B has also a ARM9 processor : 300 Mips (with 130 Mips for ARM7 in rev A : I expect thus better performances, for example with 256 bits encryption (other equipment only use 64 or 128 bits encryption)).

Concerning the Firmware version, even if it is recommended to always upgrade to the latest version (3.35), after a lot of mails exchanged with D-Link support, it seems the 3.20 is less bugged (Static DHCP working), but some features are not yet present. The version number is added between parenthesis when a parameter or a value is specific to that version. Note I didn’t make extensive tests with version 3.28, I only tested Static DHCP on it, which also failed. Last remark, as I finally downgraded from version 3.35 to 3.20, I first saved the 3.38 config with the idea to reload it in 3.20, but it failed.

By hosts, I understand any device, connected to your home LAN, wired (Ethernet interface) or wireless. Those are of course PCs (and your laptop first, with both wired and wireless interfaces), but also include PDA, Linux / Unix server, ... IBM 3090 Mainframe you may have at home, without forgetting your (kid’s) *video game*, IP enabled fridge, ...

You've noticed (if not, you will !), the wireless router is ... a wireless router, not a Web server ! Hence the poor performance of the configuration tool. So be patient when configuring, most of "Apply" lead to a "reboot". I also recommend to configure it wired, rather than over the wireless. I also tested the remote management, with the *feeling* that it worked quicker (don't ask me why !).

Configuration section / item		Parameter value
Quick Start ... This is the first info you need !		
1	Plug cables !	
2	HTTP to <i>Wireless router</i> IP address [Default : 192.168.0.1], And run Wizard with ...	
2	New admin password	
2	PPPoE info, if behind ADSL (see below)	
2	SSID : start with an easy like ...	MY_HOME
2	Enable WEP, 64K and use an easy key like ... (10 HEX digits)	A1B2C3D4E5
<i>... and that's it ... you're in business ! But continue directly with ...</i>		
3	Change the SSID broadcast to disable in [Advanced/Performance] so that your neighbors will no "see" your router	Disable
4	Save this config [Tools/System] and start advanced, more secure configuration !	MyBasicConfig.bin
5	For the WiFi card, use directly the latest driver available at D-Link TechSupport - Products - DWL-650+ (no need to insert any CD !), use same <i>easy</i> parameters as above. Follow install procedure below ! (Section 3.2)	
6	Upgrade as soon as possible, as when doing so, you'll lose your configuration (at least I did, and didn't saved it before !)	
Firmware upgrade [Tools / Firmware]		
6	<p>First upgrade to latest version Use the 'Browse' button to find the previously downloaded firmware file. CAUTION : D-LINK manufactured 2 versions of the DI-614+ router. Be sure to use the correct one : Revision B for box with <u>one</u> external antenna. Remember FOR EVER where you bought your D-LINK router, as Firmware are different (and said <i>incompatible</i>) ! You could end with a stuck box !</p> <p>NB : Do it asap, save current configuration first (I lost mine afterwards!), and do it wired !</p> <p><u>D-Link instructions:</u></p> <p>Do NOT upgrade firmware on any D-Link product over a wireless connection. Failure of the device may result. Use only hard-wired network connections.</p> <p style="text-align: center;">Attention:</p> <div style="border: 1px solid black; padding: 5px; text-align: center;"> <p>This firmware is engineered for US products only. Using this firmware on a device outside of the United States will void your warranty and may render the device unusable.</p> <p>Please contact the D-Link office in your region for firmware updates that are compatible with your D-Link product.</p> <p style="text-align: center;">International Offices</p> </div>	<p>Version 3.20 (shipped) : Static DHCP OK</p> <p>Version 3.35 (latest) : Static DHCP bugged</p> <p>For :</p> <p>D-614+ Rev B2 <u>US</u></p>

General parameters / Administration [Tools / Admin]		
<u>7</u>	Change Administrator password	
<u>7</u>	Change User password ["read only" access]	
<u>7</u>	Remote management	Disabled
WAN (Internet) configuration [Home / WAN]		
2	For ADSL (Skynet / Easynet / Codenet) use PPPoE	PPPoE
2	Dynamic PPPoE	Selected (enabled)
2	User Name	userid@PROVIDER
2	Password	
2	Auto reconnect	Enable
2	For cable modem, Dynamic IP Address (?)	
2	MTU size (max 1492 for PPPoE, max 1500 for Dynamic/static IP address)	1492
<u>8</u>	"Discard PING from WAN side" (ICMP request) [Tools / Misc.]	Enable
<u>8</u>	WAN speed (V 3.35)	10 Mbps or Auto
LAN (private home network : "Intranet") settings [Home / LAN]		
	<p>First, some general considerations on IP addressing.</p> <p>LAN refers to both wired and wireless connections, seen, from IP point of view, as a <u>single segment</u> !</p> <p>I would recommend to change the default network (192.168.0.0), because everybody uses/knows it, and by configuring statically 192.168.0.9 on his PC, will get a valid and <i>routed</i> IP address on your WLAN ! Rather, choose an as small as possible subnet from the private 10.0.0.0 network, and not a <i>trivial</i> one.</p> <p>As reminder, a subnet start at a multiple of subnet range : for example, if you want</p> <ul style="list-style-type: none"> - a subnet of 4 – 8 – 16 – 32 addresses, - corresponding to the subnet mask 255.255.255.252 – 255.255.255.248 – 255.255.255.240 – 255.255.255.224 - the subnet (last part of IP address) must start at {0,4,8,12,16,20, ..., 252} – {0,8,16,32, ..., 248} – {0,16,32,48, ..., 240} – {0,32,64,96, ..., 224} <p>respectively. The "10" network ranges from 10.0.0.0 to 10.255.255.255.</p> <p>The first address of the range is the subnet address, and the last one is the broadcast address, both unusable for hosts (router/PC).</p> <p>To make it a little more difficult for intruders, I would suggest, if possible, to use static IP addresses or static DHCP and not use dynamic DHCP. This way, you also know which IP address have each host (router / PC). For a small home LAN, this is not too difficult to maintain.</p>	<p>For up to 1 PC :</p> <ul style="list-style-type: none"> - subnet of 4 addresses (2 valid, one for the router, one for the PC) : 10.123.231.188 - mask : 225.255.255.252 - first - last valid IP address : 10.123.231.189 10.123.231.190 <p>For up to 5 PCs :</p> <ul style="list-style-type: none"> - subnet of 8 addresses (6 valid, one for the router, 5 for PCs) : 10.123.231.184 - mask : 225.255.255.248 - first - last valid IP address : 10.123.231.185 10.123.231.190 <p>... and so on ...</p>
	Subnet of 8 addresses [not provided as parameter to the DI-614+]	10.123.231.112
<u>9</u>	Subnet mask	255.255.255.248
<u>9</u>	<p>IP Address : this is the <i>router</i> IP address as seen from your hosts/PCs</p> <p>Note : After changing IP Address and mask, you will be <u>disconnected</u> from the router, and have to reconnect with the new IP address. This is <u>after refreshing/reconfiguring your PC to get (DHCP) / set (static IP address) the new IP address, from the new subnet, on your PC wired/wireless interface !</u></p>	10.123.231.113

	Broadcast address [not provided as parameter to the DI-614+] See next DHCP section for a complete subnet addressing table "Host – Interface – IP address – MAC address"	10.123.231.119		
	DNS relay (V3.35)	Enabled		
DHCP (private home network : "Intranet") settings [Home / DHCP]				
	As said, disable Dynamic DHCP if possible. Unfortunately, as we use DHCP at the office, and if you want to connect you PC with a cable (wired) at home as well, you need a DHCP server with at least one IP address. Fortunately, some <i>router</i> (and D-Link one, in latest firmware (not yet documented)) has Static DHCP implemented : this allows to give/reserve a fix/static IP address to a host (Hostname and MAC address check).	So, I recommend to use a small DHCP pool, and reserve <u>all</u> of them to specific Hosts.		
10	DHCP Server	Enabled		
<u>10</u>	Starting IP address (Do not include <i>router</i> address in the pool !)	10.123.231.116		
<u>10</u>	Ending IP address	10.123.231.118		
<u>10</u>	Leased time (choose max value)	1 Week		
<u>10</u>	Static DHCP OK in Firmware 3.20 *** BUGGED in Firmware 3.28 & 3.35: router continuously reboot *** Static DHCP is used to allow DHCP server to assign same IP address to specific MAC address.	Enabled, and for <u>each IP address</u> in the pool ...		
	Name Host name, as configured in your PC : Right click on 'My Computer', 'Properties', 'Network Identification' : first part of 'Full computer name' Do not modify any parameter here !	YOURPC1		
	IP Static DHCP IP address reserved for this host NOTE: When creating a Static DHCP entry, the IP address that you choose to have assigned needs to be in the range of the DHCP scope. Entries created with IP addresses outside of this range will not take effect.	10.123.231.116		
	MAC address	____-____-____-____-____-____		
Host name	Interface	Address type Dynamic/Static DHCP / Static	IP address	MAC address
Wireless router	WAN	Dynamic PPPoE	xxx.xxx.xxx.xxx	00-0D-88-____-____-____
Wireless router	LAN	Static	10.123.231.113	00-0D-88-____-____-____
PC002	Ethernet	Static	10.123.231.114	____-____-____-____-____-____
_____		Static	10.123.231.115	____-____-____-____-____-____
YOURPC1	Ethernet (wired)	Static DHCP	10.123.231.116	____-____-____-____-____-____
YOURPC1	Wireless	Static DHCP	10.123.231.117	00-80-C8-____-____-____
PC002	Ethernet	Static DHCP	10.123.231.118	____-____-____-____-____-____
	... Or ... Under the Static DHCP section next to DHCP Client , select one of the DHCP clients from the list and click Clone .			

Wireless settings [Home / Wireless]																	
	Disable when not used / when sharing "Proprietary/Confidential resources"	Disable / Enable															
11	Change SSID default (Long & non trivial SSID : not your name, address,...). This is to be configured on your Wireless card / PC.	#Yµor\$pc1f!c&n0t3sy!															
11	Channel Find a free channel (this not the same as your neighbor !)	6 / Auto scan (3.35)															
11	Authentication On D-Link, when Authentication set to Shared Key, the devices (PCs) must be listed in the MAC Address Control List in order to access the DI-614+ on the network.	Shared Key															
3	SSID broadcast [Advanced / Performance]	Disable															
11	WEP	Enable															
11	WEP encryption	256 bits															
	Key type Note that KEY must be "strong" (too much zero <i>weaken</i> it). Here Web site generating strong keys (as they claim!) and providing more info on WEP: http://www.warewolfabs.com/portfolio/programming/wepskg/wepskg.html	HEX															
11	Key 1	5f316b3b512e7669275a3b337d3e456f6b5e783d575b746c334e6c2b54															
11	Key 2	2c5c7c34233a4542465d394e654564323a314c2749716f342f2b565238															
11	Key 3	643f3b715b363e626c50665136293b4c404e387975343479416d22276d															
11	Key 4	26517b76395e48236b4d5b37555a61305941262e202a6c685851564954															
Security / Firewall settings [Advanced / ...]																	
	Virtual Server Only required if you plan to set some of you home PC as Web server, FTP server, Webcam server, ...	Nothing to configure															
	Special Application	Nothing to configure															
	Parental control	Nothing to configure															
12	Filters : only MAC Filter required (also for "Authentication mode") You should include all your MAC addresses (wired or wireless) in the list. Refer to the table in DHCP section above for the list of MAC addresses. The <i>wireless router</i> can automatically discover the MAC addresses of connected (wired / wireless) equipments (and be sure you don't register your neighbor !). Another way to get the MAC address of your interface, is to run 'ipconfig /all' from a DOS box. MAC address is the Physical address. MAC address are also written on the PC card (but for internal cards ...).	Only allow MAC address listed below to access Internet from LAN															
	Firewall (no additional rules required) Firewall Rules List	Nothing to configure															
	<table border="1"> <thead> <tr> <th>Action</th> <th>Name</th> <th>Source</th> <th>Destination</th> <th>Protocol</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> Deny</td> <td>Default</td> <td>*,*</td> <td>LAN, *</td> <td>IP (0),*</td> </tr> <tr> <td><input checked="" type="checkbox"/> Allow</td> <td>Default</td> <td>LAN, *</td> <td>*, *</td> <td>IP (0),*</td> </tr> </tbody> </table>	Action	Name	Source	Destination	Protocol	<input checked="" type="checkbox"/> Deny	Default	*,*	LAN, *	IP (0),*	<input checked="" type="checkbox"/> Allow	Default	LAN, *	*, *	IP (0),*	But ensure the rules listed here aside are active
Action	Name	Source	Destination	Protocol													
<input checked="" type="checkbox"/> Deny	Default	*,*	LAN, *	IP (0),*													
<input checked="" type="checkbox"/> Allow	Default	LAN, *	*, *	IP (0),*													
	Note that adding Virtual Servers (and I guess also for Special applications, DMZ) will automatically create/add rules in the Firewall section.																

	DMZ	Disable
8	VPN Pass-Through [Tools / Misc.] ["Allow VPN connections to work through the DI-614"]	Enable IPsec Disable all others
8	UPNP Settings [Tools / Misc.]	Disable
8	Gaming mode [Tools / Misc.]	Disable
Performances settings [Advanced / Performance]		
	<p>D-Link provides a 4X mode :</p> <p>4X mode is a <u>proprietary</u> method of gaining increased throughput exclusive to the D-Link Airplus family.</p> <p>4X mode enables you to get <u>up to</u> 4 times actual throughput increase over 802.11b devices when using D-Link Airplus products that also support 4X mode.</p> <p>The 4X mode option is available with a driver upgrade for the DWL-650+ or DWL-520+ and a firmware upgrade for DWL-900AP+ and the DI-614+.</p> <p>Note: When upgrading firmware or drivers, 4X mode is enabled by default. If you are using non-4X adapters in your wireless network, performance will degrade if 4X is enabled.</p> <p>When 4X is enabled, some settings on the DI-614+ are altered from their default values and can not be changed. The RTS Threshold and Fragmentation are both now 4095 instead of 2432, 2346 and the Preamble is set to Short instead of Long.</p> <p>If using non-4X wireless adapters when the router has 4X enabled, the wireless connection may degrade or drop completely with those adapters. If you are not using a complete D-Link Airplus Wireless network with the 4X mode option (mixed environment), it is recommended not to use 4X : you must disable 4X mode on the DI-614+ and DWL-650+.</p>	
14	4X mode	Enable (see above)
14	Preamble type	Short (see above)
	<p>Antenna transmit power</p> <p>You can adjust the strength of your antenna transmission. This may be beneficial for security purposes.</p>	100%
14	Antenna Selection (V3.35)	Diversity Antenna
	<p>I let you play with other performance parameters ...</p> <p><u>Note</u> : Performances can be affected by other 2.4 GHz equipments, like cordless phones, ... I don't know if changing channel can help.</p>	... up to you !

2.3 PC Card

Here, the range of cards and interfaces is still wider. However, as all support WiFi, they should *answer* the same basic parameters, and the configuration is quite simpler : it only have to match the router's one !

Note : As the *wireless router* is supposed to be configured with "SSID broadcast disabled", you should not see it with the *Site Survey* tool coming with your utility. You must then configure it manually.

Again, this section is D-Link DWL-650+ oriented.

There are basically two modes of networking with wireless interfaces :

- **Infrastructure** – using a Router/ Access Point, such as the DI-614+
- **Ad-Hoc** – directly connecting to another computer (PC), for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DWL-650+ Cardbus adapters.

The Ad-Hoc or peer-to-peer mode, suppose direct connection between PCs. From IP point of view, one will **initiate** a session to the other, which will see it as an **incoming call**. To allow incoming calls, you must **deactivate (or at least open) the Personal Firewall** on the incoming interface (wireless in this case).

Ad-Hoc mode violates basic WLAN security rules !

Other said, as long as you Personal Firewall is active on your wired and wireless interfaces, you're quite safe !

Remember the `ipconfig [/all] [/renew] [/?]` command !

Configuration section / item	Parameter value
D-LINK DWL-650+ installation	
First download the latest version of the DWL-650+ card	Version 3.07
Install driver before inserting PCMCIA in your laptop ... up to Finish	
Shut down your laptop : don't use "restart" option !	
Insert the DWL-650+	
Restart you PC	
Continue driver installation	
Configuration	
Start Configuration utility. On most configuration utility, you have possibility to save/edit a profile for each wireless connection type (Home Wireless LAN, Public HotSpot, Ad-Hoc with ..., ...) With D-LINK Configuration Utility, configuration parameters are under "Configuration" and "Encryption" section, and through "SiteSurvey", "Profile" frame then Properties button.	As said, Wireless interface parameters must match router settings !
15 Profile name	<i>Your sweet home ...</i>
15 Change SSID default (Long & non trivial SSID ...).	#Yμor\$pc1flc&n0t3sy!

15	Wireless mode : to connect to the <i>router</i> ...	Infrastructure
	Channel	6
15	4x configuration (enable only if all D-LINK AirPlus devices) <i>Note: If 4X mode is enabled on the Access Point/Wireless Router you are connecting to the SSID will appear gold in the Available Networks box.</i>	4x Enable
15	TxRate	Auto
15	Preamble (Short for 4x mode)	Short Preamble
	Power mode	<i>Up to you...r battery!</i>
15	Data encryption	Checked / Enable
	Authorization mode Open Authentication – communicates the key across the network Shared Authentication – allows communication only with other devices with identical WEP settings Auto – will automatically adjust to the Authentication mode of the wireless client	Shared authentication Use the same key as the one defined on the router !
	Key format / type	HEX
15	Key length	256 bits
	Key 1-4	<i>See router configuration : must be the same !</i>
LAN configuration (Local Area Connection in Windows 2000)		
	To configure your LAN / 'Local Area Connection' wired/wireless interface(s) of your PC, you must go to (in Windows 2000) : 'Control Panel' / 'Network and Dial-up Connection', then select the correct 'Local Area Connection' (LAN). Keeping the pointer on it, provides the underlying HW device detail. Right click and select 'Properties'. Then on 'General' tab ... DO NOT TOUCH ANY 'System / Network Identification' parameters (from Control Panel) !	
	Net Firewall (This is only for AT&T Global Network Client users) Similar option should be available for other Personal FW.	Checked (enable)
	File and Printer Sharing for Microsoft Networks ... to comply to Company WLAN Security Requirements.	Unchecked (disable)
	Internet Protocol (TCP/IP)	Checked (enable)
	Internet Connection Sharing (ICS, on 'Sharing' tab) The purpose of this is to use this PC as GW to Internet, by <i>sharing</i> this interface. This will be precisely the job of <i>the Wireless router / GW !</i>	Unchecked (disable)

IP configuration...		
	To configure the TCP/IP stack, from 'Local Area Connection Properties' window (see previous section), select 'Internet Protocol (TCP/IP)' and press 'Properties' button, and on 'General' tab ...	
... for DHCP (Dynamic or Static on router side) DHCP configuration is required on the LAN interface used to connect to most Company office		
	Obtain an IP address automatically	Selected (enabled)
	Obtain DNS server address automatically	Selected (enabled)
... for Static IP address better/safer for home PCs wired and all wireless connections Must match 'LAN settings' section of the GW configuration		
	Use the following IP address	Selected (enabled)
	IP address (PC002 example)	10.123.231.114
	Subnet mask	255.255.255.248
	Default gateway (this is the IP address of the <i>Wireless router</i>)	10.123.231.113
	Use the following DNS server addresses	Automatically selected
	Preferred DNS server (this is again the IP address of the <i>Wireless router</i>)	10.123.231.113

2.4 AT&T Global Network Client issue

Some have experienced a problem to build a VPN tunnel to corporate network using the AT&T NetClient. The *common symptom* (not specific to D-Link) being that you can connect wired, but fail over the wireless.

If you have the same kind of problem, try the following :

In "Start / Settings / Network and Dial-up Connections" , right click the "Wifi LAN connection" (also displayed as "Local Area Connection 4"), select Properties : the second component should say Net Firewall and should be "*checked*". (If already so, uncheck it, validate the change : OK, ... (reboot if necessary), and re-check it, OK, ... *reboot is always a good idea under Windows*). If the Net Firewall doesn't appear at all, you should re-install the full AT&T Global Network Client (NetClient).

Now you're there, select the TCP/IP component, Properties, Advanced, Options tab, IP security, Properties : 'Do not use IP Sec' should be selected (don't ask me why, but it works).

And what D-Link says at <http://support.dlink.com/supportfaq/default.asp?Model=&TemplateId=150500> :

ATnT VPN

Upgrade your router to the latest firmware. You can download firmware at <http://support.dlink.com/downloads>.
Disable all Firewall Software (ZoneAlarm, Windows XP Firewall, etc.).

Step 1 Open your web browser and enter the IP address of the router (192.168.0.1). Enter username (admin) and your password (blank by default).

Step 2 Click on Tools and then Miscellaneous.

Step 3 Disable Gaming mode, PPTP, and UPnP.

Step 4 Enable IPSec.

Step 5 Click Apply and then Continue.

If you still have problems connecting, in your ATnT Client software, uncheck the Negotiate UDP Encapsulation with VPN server for NAT traversal in the Client Properties. If this is already unchecked, then check it and try to connect again.

3 ... and then ...

3.1 Some more fun : DDNS & Virtual servers

You Want to access your home PC configured as Web/FTP/Webcam/... Server from the Internet ?

Great, but you then have to face several problems :

1. What is your public IP address ? The main problem is that most ISPs give you a dynamic IP address, changing continuously (at least at each reboot, reconnect) !
2. Your *router* should be Firewall enabled, which will prevent incoming sessions to reach your *server*.
3. The request must reach the right private IP address (home PC) behind the public IP address (gateway)
4. Hence the static IP address requirement on your LAN.

Fortunately, *broadband routers* designers and Internet services designers anticipated your dreams ... and here are the solutions ...

3.1.1 DDNS : Dynamic DNS

Here is the answer to your first problem : a free DDNS server like No-IP :

<http://www.no-ip.com/services/page/free/dynamic/dns>

DDNS is a way to publish, advertise, the dynamic IP address you receive from your ISP (Telenet, Skynet, ...) to a Dynamic DNS server. So, whatever is your public IP address, you can always access it under the same name, like yourhost.no-ip.info. All you have to do is : register, chose a name, configure DDNS on the D-Link to "advertise" its new IP address to No-IP and ... you're in business !

All this (and much more) for free ! I tested it, and it works that easy !

On No-IP, when adding a host, chose the first option as Host type : DNS Host (A). You'll find in next section how to configure the D-Link for this.

3.1.2 Virtual Server

D-Link Virtual Server option (under Advanced tab) answers the second and third problem at once.

To access a host behind your *router*, configure a pre-defined *Virtual Server*, or define a new one. This will :

1. Enable "Port Forwarding" : map a pre-defined *public* port number to a *private* IP address and port number (traffic to your public (and dynamic) IP address with that port, will be forwarded to the specified private IP address, with eventually another port number).
2. Add the corresponding rules to the Firewall, to allow the specific incoming sessions.

3.1.3 Static IP address

The IP address of your *server* must be constant, invariable on your LAN : you need a static IP address ! This topic is already widely discussed in the *router* configuration section; you can go for a pure static IP address or for the "*static DHCP*" option.

3.1.4 D-Link configuration

Here now how to translate all this into the D-Link configuration.

In the D-LINK Firmware 3.35, 3 DDNS servers are pre-configured, and one is No-IP !

In Firmware 3.20, you must code the server address manually .:

Configuration section / item		Parameter value
Dynamic DNS [Tools / Misc.]		
	DDNS	Enabled
	Server Address (V3.20) DDNS Server (V3.35)	dynupdate.no-ip.com No-IP
	Host Name (put the full name you registered)	yourhost.no-ip.info
	Username (typically your (private) e-mail address)	your.name@your.provider
	Password	
Port Forwarding & Firewall rules definition [Advanced / Virtual Server]		
	For each <i>service</i> you want to activate on you LAN, you need one definition. You can configure several <i>services</i> (Web server, FTP server, ...) on the same PC, and the same <i>service</i> (Netmeeting) on several PCs. In the later case, you will need to access the subsequent <i>same service</i> from the Internet through different port numbers : For example, you will map the default port (1720) to IP address1, default port (1720), then map another free port (1721) to IP address2, default port (1720). To access the second defined <i>service</i> from the Internet, you must tell that application to use another port number than the default (typically by adding "colon new_port_number" (:1721) to the IP address (or name).	
	Name (edit one of the pre-defined list or set your own)	YourName
	Private IP (IP address of the <i>server</i>)	10.123.231.113
	Protocol Type (application dependant)	UDP / TCP
	Private Port (as configured on your server, use default where possible)	
	Public Port (use default for the first <i>service</i> , a free/unused for subsequent <i>same services</i> , or to "hide" your application (Internet users will not see your <i>service</i> (for example your Webcam) if they don't know which port you configured!)).	
	Firewall rules (if not automatic on your <i>router</i> , consult your doc)	Automatically updated

3.2 House keeping

- Check on regular basis who / which PC (MAC addresses) are connected [Status / Wireless]
- Disable Wireless when not used, and, to comply to Company Security Policy Requirements, when transferring Company data between PCs on your LAN.
- Have a look at logs [Status / Log]
- Save the router configuration on you PC [Tools / System]
- Upgrade to the latest firmware : current is **3.35** for **DI-614+ Rev B** (26 FEB 2004)
- Upgrade to the latest driver : current is **3.07** for **DWL-650+** (03 DEC 2003)
- Use WPA instead of WEP if possible : here an extract of D-Link devices supporting WPA :

Product	Driver/Firmware version
DI-614+ (Rev B)	3.28 or higher
DI-624 (Rev B)	1.25 or higher
DI-624 (Rev C)	2.25 or higher
DWL-650+	3.06 or higher

3.3 D-LINK web sites :

D-LINK himself : [D-Link Systems, Inc.](#)
DI-614+ support : [D-Link TechSupport - Products - DI-614+ revB](#)
DI-614+ emulator : [DI-614+](#)
DWL-650+ support : [D-Link TechSupport - Products - DWL-650+](#)

Note that the latest manuals are not at the level of the latest firmware/driver !

3.4 Need some Hotspots ?

If you're looking for free Hotspots in Belgium, here two providers to start with :

For SKYNET ADSL users : [ADSL Hotspot](#)

For Telenet cable users : [Sinfilo - Access on the spot](#)

3.5 Performances

Once all configured, I started some performance tests, done by copying (DOS copy) a file of 18 357 960 bytes.

Each test consisted of 3 transfers :

- copy from the "server" (LAN) to my PC (->)
- copy from PC to server (<-)
- copy from server to server (file transit by my PC, so I took twice the file size for throughput calculation) (<->)

I measure the time to transfer it, and converted the result in Mbps. This is **true throughput** : I mean actual payload throughput, without the TCP/IP and underlying protocols overhead !

The *wireless router* is on the second floor, in the front of my house, and tested, with WEP 256 bits, over :

- 100Mbps Ethernet,
- 10Mbps half duplex (HD) on the PC, 100Mbps on the "server" (LAN)
- 10Mbps HD on both
- Wireless 22 Mbps + 4X mode at 1 meter from the *router*
- Wireless 22 Mbps at 1 meter from the *router*
- Wireless 11 Mbps mode at 1 meter from the *router*
- Wireless 22 Mbps + 4X mode at 7 meter from the *router*, on the ground floor, in my living room (same corner)
- Wireless 22 Mbps + 4X mode at 14 meter from the *router*, on the ground floor, in my kitchen (opposite corner)
- Wireless 11 Mbps mode at 14 meter from the *router*, on the ground floor, in my kitchen (opposite corner : 2 floors and many walls to cross, all in diagonal)
- No connection from my garden (at the back of my house !)

Here the outcome results I made ('D-Link Peak' are the peak values I saw on the "Link status" window during the transfer):

Type	Mode	WEP	Dist. (m)	Link Quality	Signal Strength	Throughput					
						Mbps			D-Link Peak		
						->	<-	<->	->	<-	<->
Ethernet	100 Mbps					24.78	11.22	14.33			
Ethernet	10 Mbps HD PC					6.80	4.26	4.93			
Ethernet	10 Mbps HD PC & LAN					4.96	4.41	4.73			
WAP	24 Mbps 4X	-	1			4.85	3.90	4.62	5.20	4.7	2.7
WAP	24 Mbps 4X	64	1			4.48	3.73	4.22	4.90	4.2	2.5
WAP	22 Mbps 4X	256	1	100%	82%	4.52	3.81	4.27	5.00	4.40	2.70
WAP	22 Mbps	256	1	100%	75%	3.79	3.62	4.00	4.40	4.10	2.40
WAP	11 Mbps	256	1	100%	75%	3.46	3.11	3.40	3.70	3.5	2.1
Both WAP	22 Mbps 4X	256	1			2.46	1.52	1.38	2.80	2.8	1.5
Ad-hoc	22 Mbps 4X	-	1			5.13	5.05	5.28	5.60	5.6	3.1
Ad-hoc	22 Mbps 4X	256	1			4.18	3.94	4.31	4.40	4.6	2.4
WAP	22 Mbps 4X	256	7	100%	80%	4.75	3.88	4.56	5.20	4.50	2.70
WAP		256	14	90%	63%	1.52	1.37	1.58	2.05	2.3	1.4

Except in my kitchen and garden, I found the results quite good. I also noticed that, by just moving the PC a few centimeters, rotating it, or moving myself a little, the signal strength change, with impact on throughput. I'll try to move the *wireless router* around (the second floor, where my ADSL connection arrives) to get *signal* in the garden, where I want to get it (I truly don't care receiving any signal in the kitchen !).

If you're interested, you can have a look at the full spreadsheet (to make your own tests !).



WLAN_Test.xls

To measure the transfer time, I simply used the following MS-DOS commands (in batch (.bat) file) :

```
cls
del *.bin
rem
rem The 'rtn.cmd' file just have a CR/LF (empty line)
rem This is to answer the 'time' command prompt withsingle 'Enter' !
rem
time < rtn.cmd
copy e:testfile.bin c:
time < rtn.cmd
copy c:testfile.bin e:tstfile.bin
time < rtn.cmd
copy e:tstfile.bin e:tstfile.xxx
time < rtn.cmd
del e:tst*.*
```