

PIN SERVICES NETWORK CONFIGURATION AND ADMINISTRATION

This document describes the high level network, PC, and router/firewall configuration.

1. General Network Information



All devices (computers, laptops, iPods, cell phones, printers, etc.) connected to any network must have a unique *IP (Internet Protocol) Address* in order to communicate with other devices.

IP addresses consists of 4 sets of 3 digit numbers ranging from 0 to 255 separated by 3 dots

For example, **192.159.15.7** is an IP address



There are currently not enough IP addresses available to connect every device with a **Network Interface Card (NIC)** directly to the Internet. To get around this problem the use of **Network Address Translation (NAT)** routers have become very common. These devices connect directly to the Internet and receive an IP address from an Internet Service Provider. They then act as a **DHCP server** and automatically provide local IP addresses to devices behind the router. This allows any number of PCs on the **local area network (LAN)** behind the router to share one Internet Connection as well as protecting these PCs from being directly accessed from the Internet. Most routers used in homes and small and medium sized businesses today are combination NAT routers and **Hardware-based Firewalls**. A Firewall limits access into and out of the local network and can be configured to allow or disallow certain types of data to pass through **ports**. These ports are identified by numbers ranging from 1 to 65535. Many of these ports are registered for specific applications such as port 80 for the http protocol that allows most Internet communications.



These ports are not physical; they are virtual. All data of any kind actually passes through the same bundles of wire or fibre-optic cable. It is the server and client software - FTP, Browser, On-line Games, BitTorrent, etc. - that uses these ports to facilitate connections according to how the software and firewall are configured. In addition, most PC's are running **Windows Firewall**. This is a software based firewall that monitors communication with other computers on the local network or on the Internet (**the Wide Area Network or WAN**) to prevent unwarranted access. Windows Firewall controls the sending of data in or out of the PC when it involves other computers. Windows Firewall must also be configured to allow certain types of services, such as the Virtual Private Network Server, to run.



IP addresses can be static or dynamic. Most devices and networks are configured to receive IP addresses automatically (this is what a DHCP server or service does). The problem with dynamic IP addresses is that they can change without warning and this might cause some remote applications on remote computers to no longer be able to find the original computer. Static IP addresses fix this problem but must be manually managed. In the final analysis it is not really the IP address that uniquely identifies a device on a network - it is actually its network card's MAC address!



The MAC address has nothing to do with Apple Computers. It stands for **Media Access Control** Address. Every network card has an absolutely unique MAC address. This MAC address is tied to any IP address the network card receives, either from a DHCP server or one that configured statically, when it is connected to any local network local or directly to the Internet.



The Internet Connection you have assigns your Shaw Modem, and therefore your Router/Firewall, with a dynamic IP address. As computers on your network are running

services that are accessed remotely from the Internet they are actually reached indirectly by using the router's IP address. In addition any PC running a remote service on the local network has a static IP address. The router firewall is configured so that requests for remote services are directed to the appropriate PC based on its fixed IP address.



If remote services are accessed through the router IP address and this address changes these services will not be available until the new IP address is determined.

It is not difficult to determine the router's IP address but this must be done in the office. To make the system more fault tolerant the router and your network is configured to use a Dynamic DNS service.



On the local network devices should be configured to be part of the **PINSERVICES** Workgroup (*right-click* on **My Computer** and *select* **Manage**, then *click* on the **Computer Name** tab on the window that opens). This is not essential but makes finding shared resources or folders easier.

2. PIN Service Dynamic DNS registration

DNS (Domain Name System) is an Internet based network of servers and database software that keeps track of the IP addresses for all those web sites you love. When you type in www.google.ca and hit return the domain address is checked by the closest DNS server, which then determines the IP address of the server that hosts the website. Your network has its own free domain name and is configured with a free service that keeps the IP address of your router up-to-date and associated with your network domain name. This service uses a built-in feature of your router and a free service provided by Dyndns.com.

Dynamic DNS Configuration and Account Information



Network Domain Name: **pin.dyndns.biz**

Website of Service Provider: <https://www.dyndns.com/>

Account Name: **XXXX**

Password: Stored in Secure File Vault on PIN00-oldPC and on System Backup DVD

To check your current router IP address enter this address into your browser in the office:
<http://checkip.dyndns.com/>

The router configuration for Dynamic DNS is covered in the section below.

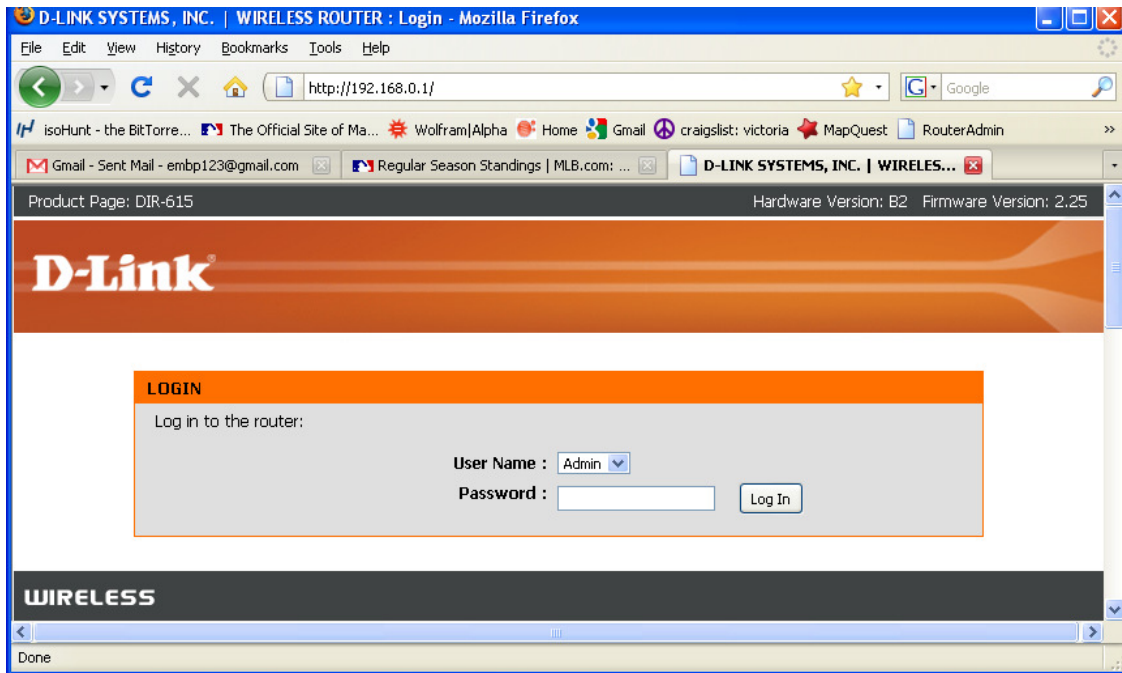
3. Router/Firewall Configuration and Administration



The majority of consumer routers are preconfigured to use an internal IP address of 192.168.0.1 as the **Gateway** and 255.255.255.0 as the **Subnet**. We do not have to be too concerned with the significance of these numbers. This particular subnet configuration provides for 255 dynamic and/or static IP addresses from 192.168.0.1 to 192.168.0.255.

What matters is that by convention the router, in this case referred to as the **Gateway**, receives the first IP address on the subnet. This is required to facilitate accessing the router's administration panel and to provide a route to the Internet. PC's send requests to access resources on the Internet to the address 196.168.0.1 and the router then forwards these requests appropriately.

To access the router's Administration Panel simply type the following into any web browser's address field and *press* **Enter**: <http://192.168.0.1> The following web page will open.



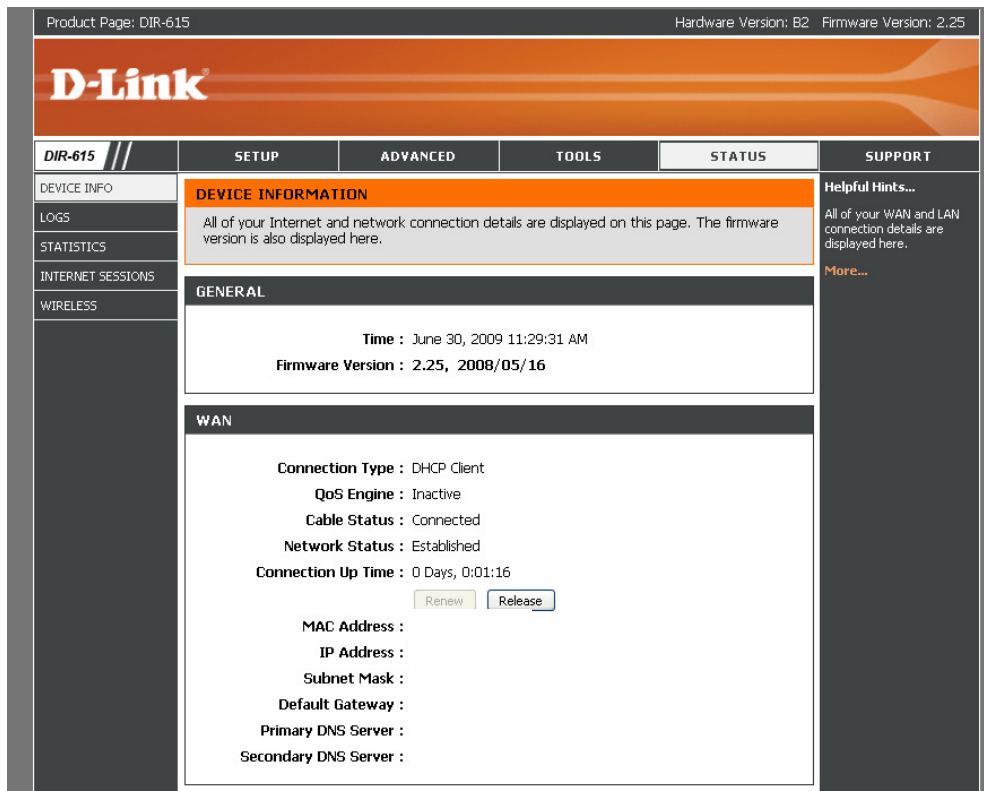
User Name: **Admin**

Password: ***** (Password stored in XXXXXXXXXXXXXXXXXXXXXXXX)



If the router password is compromised the entire network and all data can be compromised. Do not provide this password to anyone other than trusted and technically savvy users. It is recommended that this password be changed every 6 months, or immediately if there is any suspicious activity on the network.

Once you have successfully logged on the following page opens.



The **Status** page displays both the current dynamic IP address and MAC address for the router. This is another method of determining the IP address for **pin.dyndns.biz**.

The following pages show the current configuration of the router specific to your Internet Connection and your remote services. They are provided to assist in trouble-shooting.

a) Tools | Admin

Click the **TOOLS** link at the top on the menu bar to see the **Admin** settings

The screenshot shows the D-Link DIR-615 router's web interface. The top navigation bar includes links for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration options like ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'ADMINISTRATOR SETTINGS' and contains several sections: 'ADMIN PASSWORD' and 'USER PASSWORD' both require entering and verifying a password; 'SYSTEM NAME' has a 'Gateway Name' field set to 'PINDOTCA'; and 'ADMINISTRATION' includes an 'Enable Remote Management' checkbox, a 'Remote Admin Port' field set to 8080, a 'Remote Admin Inbound Filter' dropdown set to 'Allow All', and a 'Details' field set to 'Allow All'. A 'Save Settings' button is located at the top left of the settings area. On the right side, there is a 'Helpful Hints...' section with text about security and remote management.

This is where the router password is changed. In addition you may enable **Remote Management** of the router by simply *clicking* the **Enable Remote Management** checkbox and then *clicking* the **Save Settings** button. This allows the Administration Panel of the router to be accessed remotely by typing in the external IP address of the router and the remote administration port (8080) into any browser and then logging on.



Saving settings on the router may require a reboot. This only takes a few seconds and will not normally cause any problems.

For example, assuming the current IP address, enter: <http://XXXXXXXXXXXX:8080> or if Dynamic DNS is working <http://pin.dyndns.biz:8080> to bring up the logon window remotely. Port 8080 is the default port for remote administration.



Enabling remote administration of the router allows anyone with the router admin password to modify settings remotely and should only be used in emergencies. Remote management should normally be disabled for security reasons

b) Basic Internet and Wireless Configuration

Click **SETUP** on the menu bar and then *click* the **Manual Internet Connection Setup** button

Product Page: DIR-615 Hardware Version: B2 Firmware Version: 2.25

D-Link

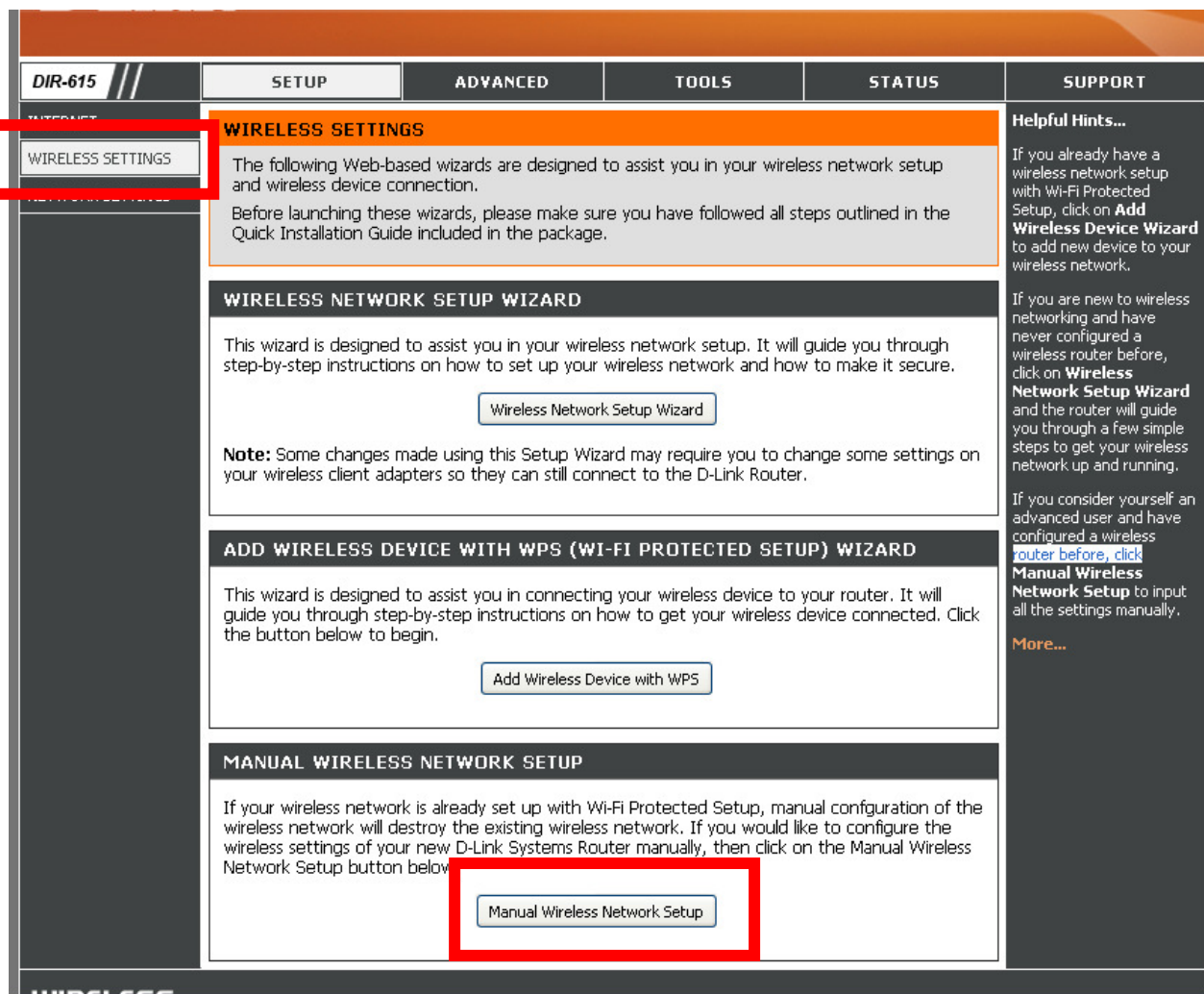
DIR-615	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
INTERNET	INTERNET CONNECTION				Helpful Hints... If you are new to networking and have never configured a router before, click on Internet Connection Setup Wizard and the router will guide you through a few simple steps to get your network up and running. If you consider yourself an advanced user and have configured a router before, click Manual Internet Connection Setup to input all the settings manually. More...
WIRELESS SETTINGS	There are two ways to set up your Internet connection: you can use the Web-based Internet Connection Setup Wizard, or you can manually configure the connection.				
NETWORK SETTINGS	INTERNET CONNECTION SETUP WIZARD If you would like to utilize our easy to use Web-based Wizards to assist you in connecting your new D-Link Systems Router to the Internet, click on the button below. Internet Connection Setup Wizard Note: Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package. MANUAL INTERNET CONNECTION OPTIONS If you would like to configure the Internet settings of your new D-Link Systems Router manually, then click on the button Manual Internet Connection Setup .				
WIRELESS					

That will bring up the following page. This page shows how your router is configured for Shaw.

D-Link

DIR-615	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
INTERNET	WAN				Helpful Hints... When configuring the router to access the Internet, be sure to choose the correct Internet Connection Type from the drop down menu. If you are unsure of which option to choose, contact your Internet Service Provider (ISP) . If you are having trouble accessing the Internet through the router, double check any settings you have entered on this page and verify them with your ISP if needed. More...
WIRELESS SETTINGS	Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP and L2TP. If you are unsure of your connection method, please contact your Internet Service Provider. Note : If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers. Save Settings Don't Save Settings				
NETWORK SETTINGS	INTERNET CONNECTION TYPE Choose the mode to be used by the router to connect to the Internet. My Internet Connection is : Dynamic IP (DHCP) DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE : Use this Internet connection type if your Internet Service Provider (ISP) didn't provide you with IP Address information and/or a username and password. Host Name : Use Unicasting : ☒ (compatibility for some DHCP Servers) Primary DNS Server : 0.0.0.0 Secondary DNS Server : 0.0.0.0 MTU : 1500 (bytes) MTU default = 1500 MAC Address : 00:00:00:00:00:00 Clone Your PC's MAC Address				
WIRELESS					

Next we will look at your Wireless Setup. *Click* the **WIRELESS SETTINGS** tab (to the top left) and then *click* the **Manual Wireless Setup** button.



That will bring up the page shown following.

The wireless Internet connection needs to be secured or anyone within broadcast range will be able to connect to the router and directly access the local network. To control who gets access and how the data is transmitted wireless security is enabled using WPA encryption. This requires that anyone who wishes to connect a device to the network must supply a password and that all the data that is transmitted is encrypted so that it can't be intercepted and reconstructed. The following snap shot shows how the wireless network is configured to provide wireless security.



The key piece of information is the **Pre-Shared key**
This is a password stored in the in Secure File Vault on **XXXXXXXXXXXX**



It is recommended that this password be changed every 6 months, or immediately if there is any suspicious activity on the network. If people require temporary access to the network it is better to type in the password yourself rather than providing the password.



You may also use the **Wi-Fi Protected Setup** feature (shown on the page above) to create temporary connections to the local network. This is currently disabled to maximize security.



DIR-615	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
INTERNET	WIRELESS Use this section to configure the wireless settings for your D-Link Router. Please note that changes made on this section may also need to be duplicated on your Wireless Client. Save Settings Don't Save Settings				Helpful Hints... Changing your Wireless Network Name is the first step in securing your wireless network. Change it to a familiar name that does not contain any personal information. Enable Auto Channel Scan so that the router can select the best possible channel for your wireless network to operate on. Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they scan to see what's available. For your wireless devices to connect to your router, you will need to manually enter the Wireless Network Name on each device. If you have enabled Wireless Security, make sure you write down the Key or Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network. More...
WIRELESS SETTINGS	WIRELESS NETWORK SETTINGS Enable Wireless : ☒ Always Add New Wireless Network Name : PINDOTCA (Also called the SSID) 802.11 Mode : Mixed 802.11n, 802.11g and 802.11b Enable Auto Channel Scan : ☒ Wireless Channel : 2.437 GHz - CH 6 Transmission Rate : Best (automatic) (Mbit/s) Channel Width : 20 MHz Visibility Status : ☒ Visible ☐ Invisible				
NETWORK SETTINGS	WIRELESS SECURITY MODE To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server. Security Mode : WPA-Personal				
	WPA Use WPA or WPA2 mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use WPA2 Only mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use WPA Only . This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode. To achieve better wireless performance use WPA2 Only security mode (or in other words AES cipher). WPA Mode : Auto (WPA or WPA2) Cipher Type : TKIP and AES Group Key Update Interval : 3600 (seconds)				
	PRE-SHARED KEY Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase. Pre-Shared Key :				

WIRELESS

Copyright © 2004-2007 D-Link Systems, Inc.

4. Special Internet and Wireless Router Firewall Configuration

The following pages show how the router is configured for remote services (FTP, Remote Control, VPN) and Dynamic DNS

a) Virtual Server for UltraVNC Remote Control



Click the **ADVANCED** menu bar and the following page will load. This shows how the router is configured to allow remote connections using UltraVNC. There are two sets of two ports configured.

PIN03-NewPC is configured to use ports **XXXX** and **XXXX** to allow other properly configured PC's to control it remotely. Specifically PIN02-newlaptop and PIN01-oldlaptop.



Port **XXXX** is used by the UltraVNC client. Port **XXXX** allows a remote connection using only an Internet browser with JAVA installed. This port has been disabled by *un-checking* the check box.



The Internet Browser port can be enabled to allow remote access if and when UltraVNC client is not available, for example, if your pre-configured laptop is lost, broken, or stolen. The checkbox must be re-checked by accessing the router in the office or by enabling remote management of the router first, either in the office or remotely, if possible.

PIN01-oldlaptop is configured to connect through port **XXXX** and **XXXX** to remote control PIN00-oldPC

Product Page: DIR-615 Hardware Version: B2 Firmware Version: 2.25

D-Link

DIR-615 // SETUP **ADVANCED** TOOLS STATUS SUPPORT

VIRTUAL SERVER

PORT FORWARDING
APPLICATION RULES
QOS ENGINE
NETWORK FILTER
ACCESS CONTROL
WEBSITE FILTER
INBOUND FILTER
FIREWALL SETTINGS
ADVANCED WIRELESS
WI-FI PROTECTED SETUP
ADVANCED NETWORK

The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

Save Settings Don't Save Settings

24--VIRTUAL SERVERS LIST

	Name	IP Address	Port	Traffic Type	Schedule	Inbound Filter
☒	VNC	192.168.0.3	<< Application Name >>	Protocol TCP	Schedule Always	Inbound Filter Allow All
☐	VNCweb	192.168.0.3	<< Application Name >>	Protocol TCP	Schedule Always	Inbound Filter Allow All
☒	VNC2	192.168.0.2	<< Application Name >>	Protocol TCP	Schedule Always	Inbound Filter Allow All
☐	VNC2web	192.168.0.2	<< Application Name >>	Protocol TCP	Schedule Always	Inbound Filter Allow All
☐			<< Application Name >>	Protocol TCP	Schedule Always	Inbound Filter Allow All

Helpful Hints...

Check the **Application Name** drop down menu for a list of predefined server types. If you select one of the predefined server types, click the arrow button next to the drop down menu to fill out the corresponding field.

You can select a computer from the list of DHCP clients in the **Computer Name** drop down menu, or you can manually enter the IP address of the computer at which you would like to open the specified port.

Select a schedule for when the virtual server will be enabled. If you do not see the schedule you need in the list of schedules, go to the **Tools --> Schedules** screen and create a new schedule.

Select a filter that restricts the Internet hosts that can access this virtual server to hosts that you trust. If you do not see the filter you need in the list of filters, go to the **Advanced --> Inbound Filter** screen and create a new filter.

More...

b) Port Forwarding for Filezilla FTP Service and OpenVPN Virtual Private Network service



At the **ADVANCED** page (shown above) *click* the **PORT FORWARDING** tab (to the left towards the top of the page). This page shows how certain ports when accessed via the Internet through the router's IP address are 'forwarded' to the correct PC running the service through its static IP address on the local network. The virtual server configuration for remote control is similar. There are four ports configured.



Ports **XXXXX-XXXXX** are configured to allow unsecure FTP connections to PIN00-OldPC
Port **XXXX** is configured to allow encrypted (secure) FTP connections to PIN00-OldPC



Port **XXXX** is configured using two different protocols to allow access to two separate VPN's at PIN Services. The UDP port is configured to allow VPN connections to PIN03-newPC with PIN02-newlaptop and the TCP port is configured to allow VPN connections to PIN00-OldPC through PIN01-oldlaptop.



Opening ports on the firewall almost guarantees that people will try to access your system remotely (they will try in any event but having open ports provides specific modes of attack that having all ports closed does not allow). As long as you properly create and secure your passwords and security certificates, and update your operating system, and the software providing your remote services regularly the likelihood of being severely compromised is very low. If you are not regularly using any of the remote services they can be disabled here (by *un-checking* checkboxes and saving settings) to maximize security.

Product Page: DIR-615 Hardware Version: B2 Firmware Version: 2.25

D-Link

DIR-615 // SETUP ADVANCED TOOLS STATUS SUPPORT

PORT FORWARDING

This option is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in various formats including, Port Ranges (100-150), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689).

Save Settings Don't Save Settings

24 -- PORT FORWARDING RULES

	Name		Ports to Open	Schedule	Inbound Filter
☒	FTP Server	<< Application Name		Always	Allow All
☒	OpenVPNeric	<< Computer Name		Always	Allow All
☒	OpenVPNadmin	<< Application Name		Always	Allow All
☒	SFTP Server	<< Application Name		Always	Allow All
☐		<< Application Name		Always	Allow All

Helpful Hints...

Check the **Application Name** drop down menu for a list of predefined applications. If you select one of the predefined applications, click the arrow button next to the drop down menu to fill out the corresponding field.

You can select a computer from the list of DHCP clients in the **Computer Name** drop down menu, or you can manually enter the IP address of the LAN computer to which you would like to open the specified port.

Select a schedule for when the rule will be enabled. If you do not see the schedule you need in the list of schedules, go to the **Tools → Schedules** screen and create a new schedule.

You can enter ports in various formats:
Range (50-100)
Individual (80, 68, 888)
Mixed (1020-5000, 689)
More...

c) Dynamic DNS Router Configuration

To keep the right IP address associated with your domain **pin.dyndns.biz** the built-in DNS updating component of the router has been enabled as shown on the page below. This page is accessed by **clicking the TOOLS button** on the menu bar and then the **DYNAMIC DNS** tab.

Product Page: DIR-615 Hardware Version: B2 Firmware Version: 2.25

D-Link

DIR-615 // SETUP ADVANCED **TOOLS** STATUS SUPPORT

ADMIN
TIME
SYSLOG
EMAIL SETTINGS
SYSTEM
DYNAMIC DNS
SYSTEM CHECK
SCHEDULES

DYNAMIC DNS

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.

Sign up for D-Link's Free DDNS service at www.DLinkDDNS.com.

Save Settings Don't Save Settings

DYNAMIC DNS

Enable Dynamic DNS: ☒

Server Address: << Select Dynamic DNS Server

Host Name: (e.g.: me.mydomain.net)

Username or Key:

Password or Key:

Verify Password or Key:

Timeout: (hours)

Status: Connected

WIRELESS

Helpful Hints...
To use this feature, you must first have a Dynamic DNS account from one of the providers in the drop down menu.
More...

 The username and password entered on this page are recorded earlier in this document. They are the user account and password for the free DynDNS.com service.

c) Backup of Router settings

The current router configuration can be backed up on the **TOOL | SYSTEM's** page (shown below). The current configuration used to make this document has been backed up and stored in the File Vault on **XXXXXXXXXX** and on the **XXXXXXXXXX** in a file called **PINServicesRouterSettings0609.gws**

Product Page: DIR-615 Hardware Version: B2 Firmware Version: 2.25

D-Link

DIR-615 // SETUP ADVANCED **TOOLS** STATUS SUPPORT

ADMIN
TIME
SYSLOG
EMAIL SETTINGS
SYSTEM
SYSTEM
FIRMWARE
DYNAMIC DNS
SYSTEM CHECK
SCHEDULES

SYSTEM SETTINGS

The System Settings section allows you to reboot the device, or restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you have created.

The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by device can be uploaded into the unit.

SYSTEM SETTINGS

Save To Local Hard Drive:

Load From Local Hard Drive:

Restore To Factory Default:
Restore all settings to the factory defaults.

Reboot The Device:

WIRELESS

Helpful Hints...
Once your router is configured the way you want it, you can save the configuration settings to a configuration file.
You might need this file so that you can load your configuration later in the event that the router's default settings are restored.
To save the configuration, click the **Save Configuration** button.
More...

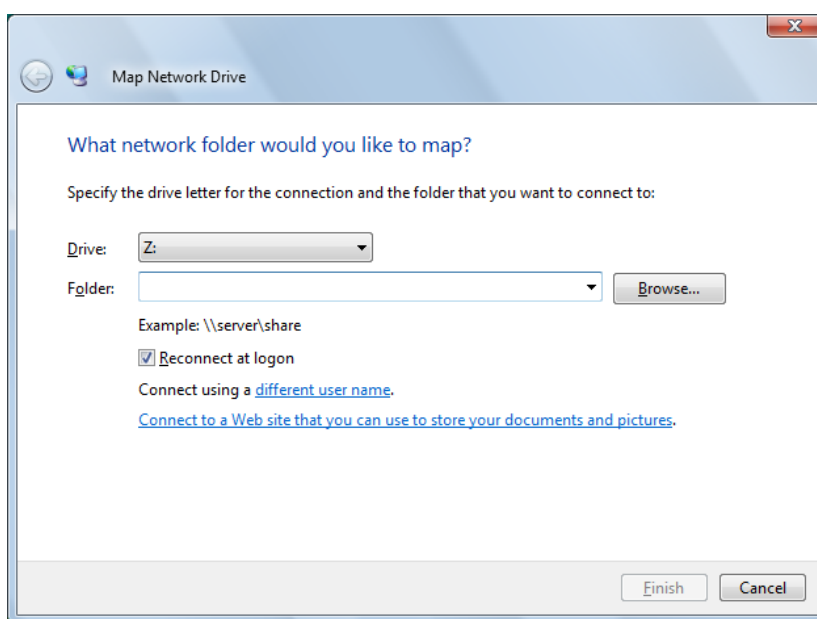
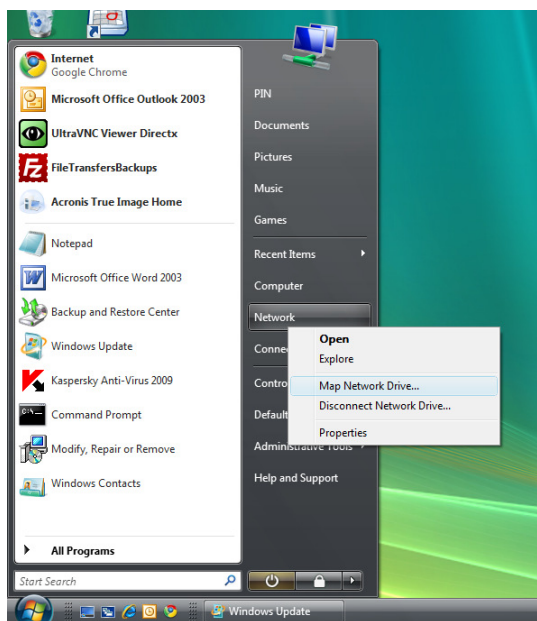
5. Mapping Network Drives and accessing shared network resources.

Various resources - folders, printers, USB drives, etc. – are shared on the network. When certain shared folders need to be made generally available, such as **My Documents** on PIN03-newPC a **drive letter** can be **mapped** to the specific folder. These links are re-established when the PC reboots. It is possible that these mappings could break, new mappings need to be made, or you simply want to browse for folders or other resources on the network. This is a relatively simple thing to do. The following will describe how to map a network drive and in parallel how to browse for resources on the network.

There are several ways to map a network drive or access network resources. This document will outline two.

a) Map a Network Drive

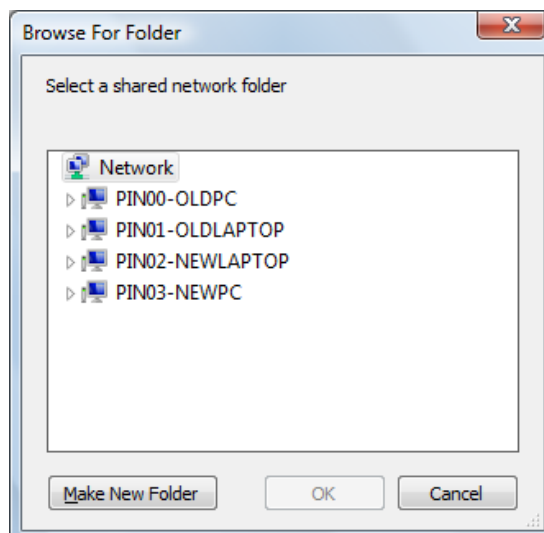
Click the **Start** button and then *right-click* on **Network** and select **Map Network Drive** as shown below (left) and the **Map Network Drive** dialogue box (right) will open:



You may select a free drive letter. In this example we will use **Z:**. Click the **Browse** button to *browse* for the computer and folder you wish to connect to. The following browse window will open:



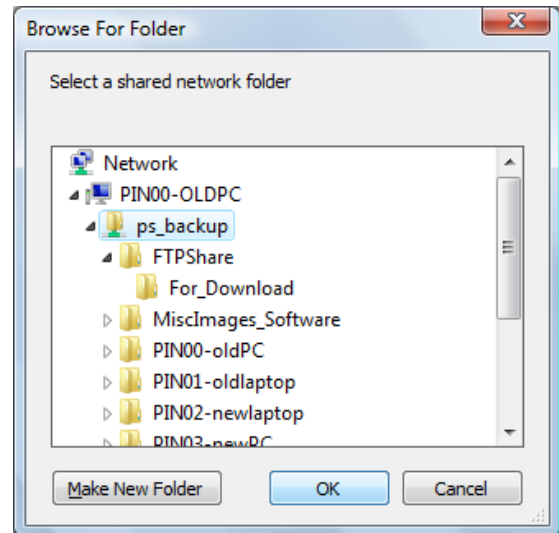
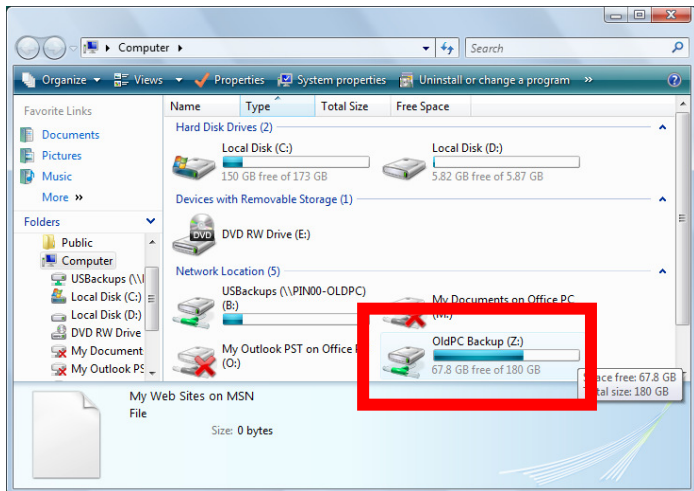
NOTE: Depending on the operating system and how it is configured you may need to browse for the **Workgroup** first. If the PC's don't show up in the list look for the Workgroup **PIN SERVICES** and open it first to see the PC's.



To find the shared folder simply *click* on the **browse arrow** to open the resource and continue this process until you find the folder you wish to map to. In this example we are mapping **Z:** to the **ps_backup** folder on PIN00-oldPC (this is the folder where the FTPShare is located).

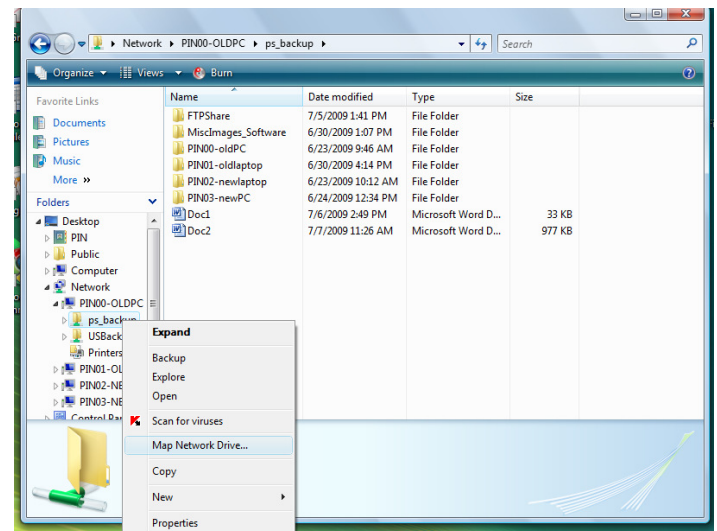
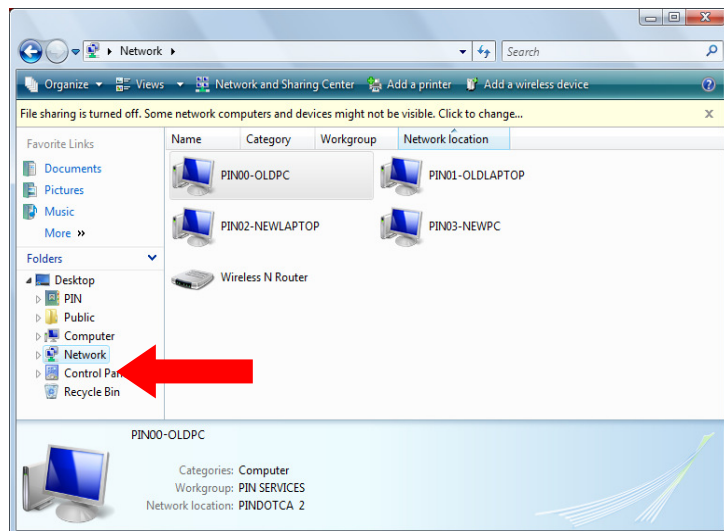
Simply *click* on the folder you wish to map to and *click* **OK** to complete the mapping.

The drive letter **Z:** will now show up in **My Computer** (see below)



b) Browsing network folders

The easiest way to browse network resources or shared folders is through the **Network Control Panel**. *Click* **Start | Network** to open the Network window (shown below):



Simply *double-click* the icon for the computer you wish to access or browse through the **Network** icon (shown above). If you wish to map a network drive simply *right-click* on any shared folder and *select* **Map Network Drive** from the context menu (as shown below) and follow the instructions from a) above.

6. Network Share Access on PIN Services Local Area Network



There are several folders, on either PIN00-oldPC or PIN03-newPC, that are shared on the network. To protect these folders from being directly accessed by non-PIN Services PC's connected to the network these shares are password protected. As file sharing on XP Home is accomplished through the **Guest** account the only way to secure the shared folders on PIN00-oldPC that appear on the network is to password protect the Guest Account on PIN00-oldPC.

If the Guest account has never been password protected the following steps must first be completed:

Log on to this computer with an Administrator account.

Click **Start | Run** then type '**cmd**' and click **OK**.

Input the following command and press **Enter**: **Net user guest password**

Go to **Control Panel | User Accounts**.

Click the **Guest** account and now you can change the password.



The password on PIN02-newlaptop and for the Guest Account on PIN00-oldPC are currently set to be the same as the PIN Services account on PIN03-newPC. If any one of these passwords is changed they all need to be changed to keep shared access transparent. If these passwords become unsynchronized it will be necessary to keep track of and use multiple passwords.

7. Backup Administrator accounts

Every PIN Services computer has a backup administrator account to protect against inadvertent account lock-out due to system corruption, or loss of passwords. This account has been given the same name and the same password on every computer.

Account Name: **XXXXXXXXXX**

Password: Stored in Secure File Vault on **XXXXXXX** and on **XXXXXXXXXXXXXX**

8. Use of static IP addresses on PIN03-newPC and PIN00-oldPC

To facilitate connection to remote services the PC hosting the remote service(s) requires a fixed IP addresses. If the IP address is dynamically assigned if and when it changes remote services will fail. The router always needs to 'know' the IP addresses of the computer running a remote service so that when requests for connectivity come from the Internet these connection request can be properly forwarded to the appropriate PC on the local area network.

The router is currently configured to provide dynamic IP addresses as follows

192.168.0.10 – 192.168.0.49 are made available for the PIN03-newPC VPN for assigning IP addresses to remote clients (typically PIN02-newlaptop and/or PIN01-oldlaptop)

192.168.0.50 – 192.168.0.99 are made available for the PIN00-oldPC VPN for assigning IP addresses to remote clients (typically PIN01-oldlaptop)

192.168.0.100 – 192.168.0.199 are made available for computers connected locally either using a network cable or the wireless connection

192.168.0.1 is the router IP address, or **Gateway**

This leaves the following IP addresses free to be used, as required, for static IP addresses:

192.168.0.2 – 192.168.0.9 and 192.168.0.200 to 192.168.0.255

Two of these IP addresses are currently in use as static IP addresses.

The IP address of PIN00-oldPC on the local network and the VPN is 192.168.0.2

The IP address of PIN03-newPC on the local network and the VPN is 192.168.0.3

Configuring a static IP address is relatively simple. The network adapter properties dialogue box in the **Control Panel** gives access to the TCP/IP settings. This procedure is described in more detail in the document, **PIN Services OpenVPN Configuration.doc**, Part B, section 4.

9. Miscellaneous Network Configuration and Administration Information

In order to keep file-sharing in place on the USB Drive there must be a mapping set to **Reconnect at Login** in order for the drive to be re-shared on reboot. If the USB drive (**B**) ever becomes unavailable but is still accessible on PIN00-oldPC check to ensure a drive mapping to the folder **Backups** is still in place. If not this drive mapping will have to be recreated.

Due to a bug in XP even though the main Administrator account on PIN00-oldPC is was renamed from **Eric Jordan** to **Admin** some remote applications still see the user account as **Eric Jordan**. If you are prompted for a user name to connect to PIN00-oldPC and **Admin** is not working try using the account name **Eric Jordan** instead.