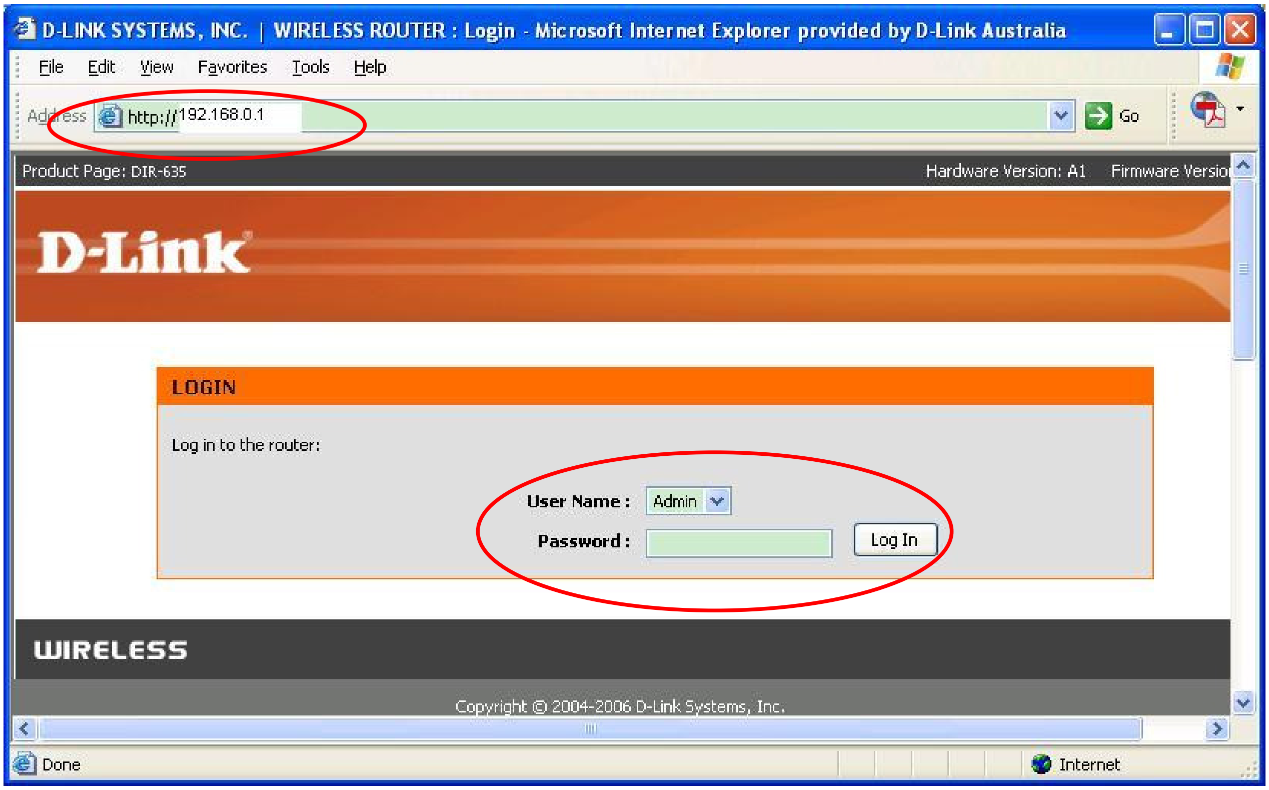
How to Enable Wireless Security on DGL-4500

It is recommended to secure your wireless network. To do that you can enable encryption on your router. As a result of this only the users who know the encryption key (“password”) you have set on your router, could access the wireless network. It is recommended to use WPA-Personal encryption, especially if your have 802.11n wireless card. Please kindly note that 802.11n standard on supports WPA encryption. If your wireless card does not support it, use WEP.

To enable wireless and encryption please follow these steps:

Step 1. Open your web browser and enter the IP address of the router (http://192.168.0.1). Enter user name and password (default username 'admin' and password is blank (nothing)).



D-LINK SYSTEMS, INC. | WIRELESS ROUTER : Login - Microsoft Internet Explorer provided by D-Link Australia

Address http://192.168.0.1

Product Page: DIR-635 Hardware Version: A1 Firmware Versio

LOGIN

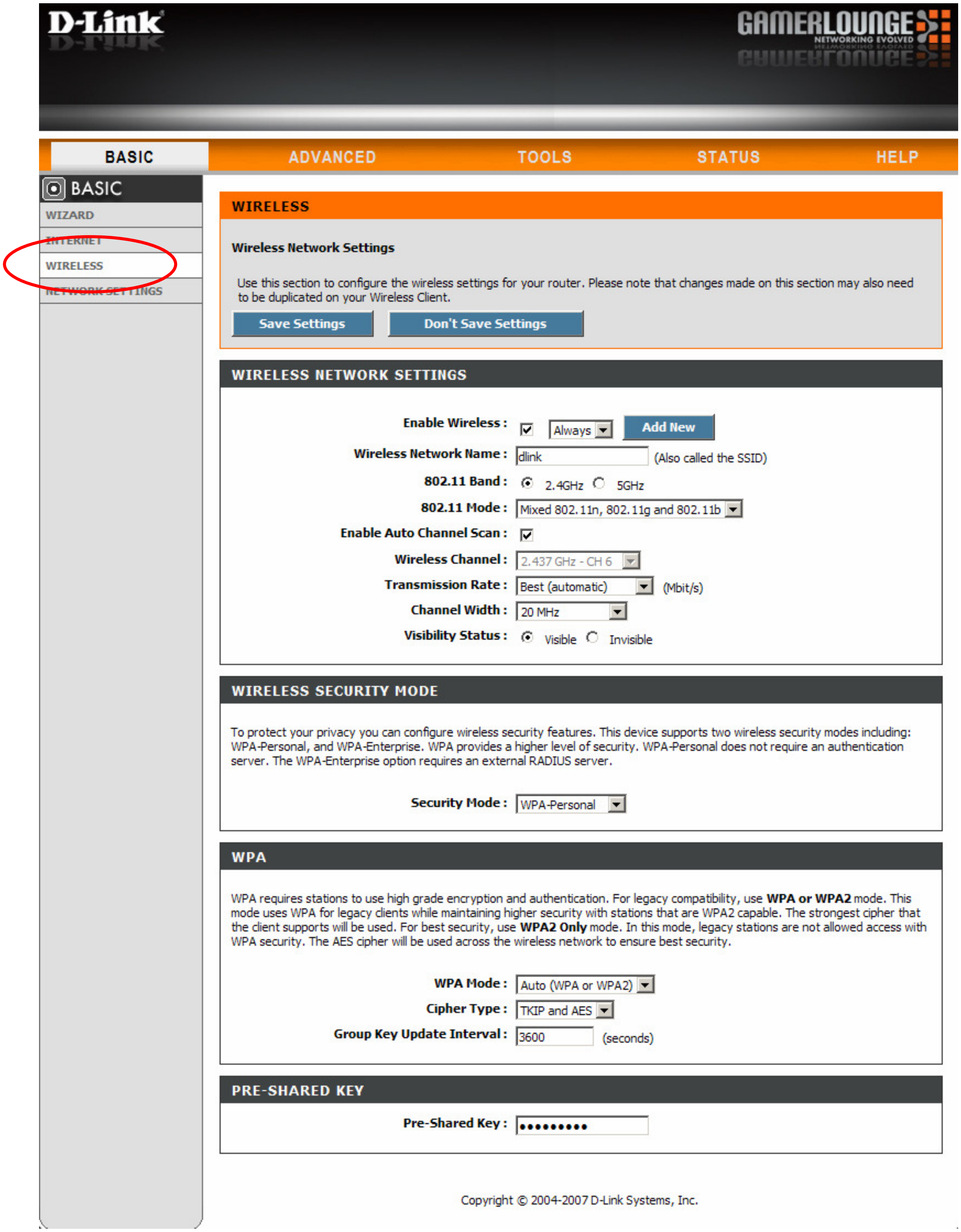
Log in to the router:

User Name : Admin

Password :

Copyright © 2004-2006 D-Link Systems, Inc.

Step 2. Click on ‘WIRELESS’ button on the left side of your screen.



WIRELESS

Wireless Network Settings

Use this section to configure the wireless settings for your router. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

WIRELESS NETWORK SETTINGS

Enable Wireless : ☑ Always

Wireless Network Name : dlink (Also called the SSID)

802.11 Band : ● 2.4GHz ○ 5GHz

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

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports two wireless security modes including: WPA-Personal, and WPA-Enterprise. 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

WPA requires stations to use high grade encryption and authentication. For legacy compatibility, use **WPA or WPA2** mode. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. In this mode, legacy stations are not allowed access with WPA security. The AES cipher will be used across the wireless network to ensure best security.

WPA Mode : Auto (WPA or WPA2)

Cipher Type : TKIP and AES

Group Key Update Interval : 3600 (seconds)

PRE-SHARED KEY

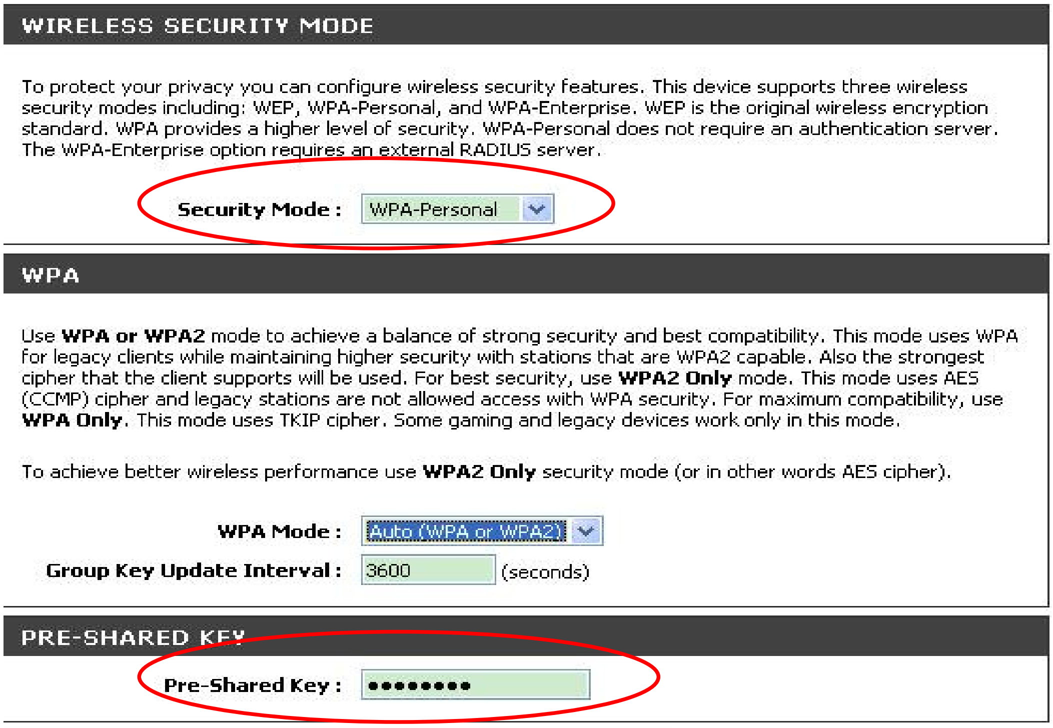
Pre-Shared Key : •••••••••

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

Step 3. Enable security and specify your security key ("password").

Option 1: WPA-PSK (more secure)

Under **Security Mode** select "WPA-Personal".
Under **Pre-shared Key** type in a password/key (you can just make it up). The key should be at least 8 characters long.
Click on 'Save 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.

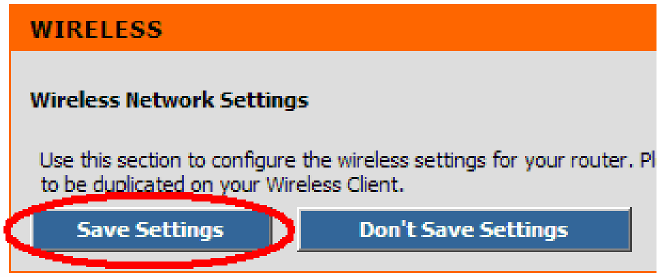
To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode : Auto (WPA or WPA2)

Group Key Update Interval : 3600 (seconds)

PRE-SHARED KEY

Pre-Shared Key : ●●●●●●●●●



WIRELESS

Wireless Network Settings

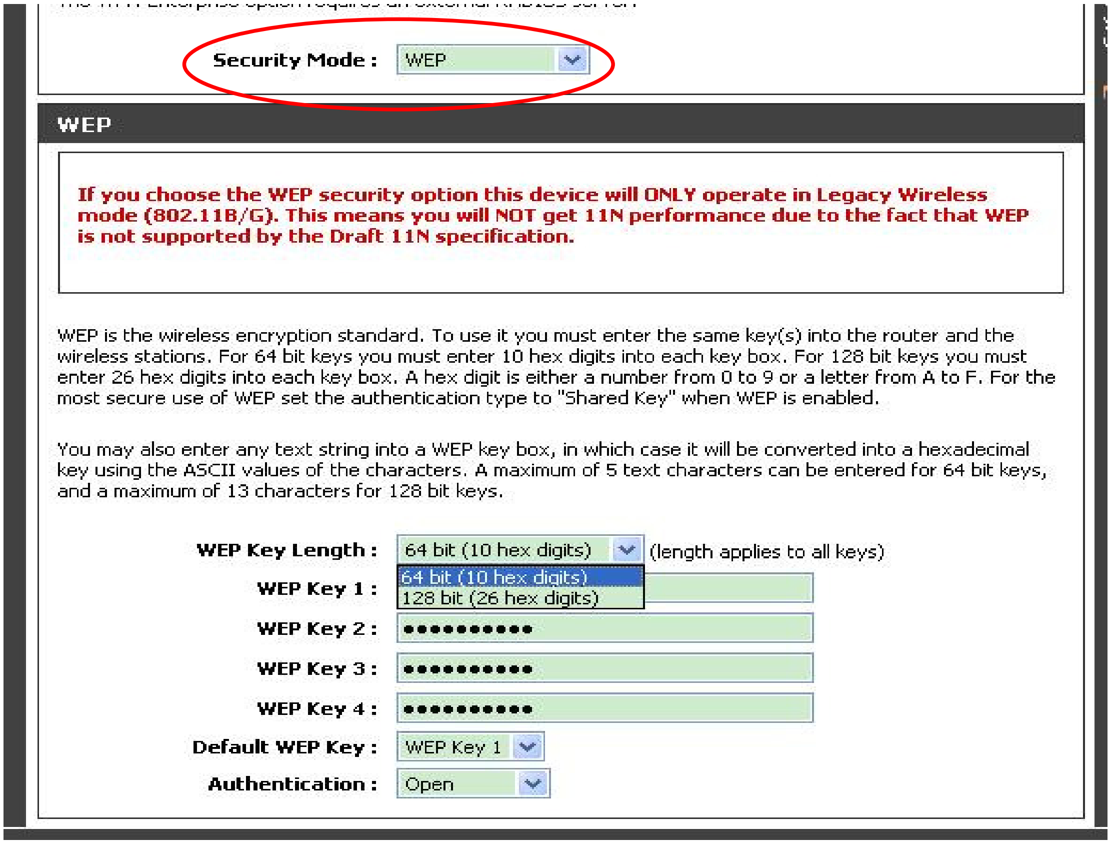
Use this section to configure the wireless settings for your router. Pl
to be duplicated on your Wireless Client.

Option 2: WEP (less secure)

Under **Security** select “WEP”.

Under **WEP Key** type in the encryption key you want to use. 64-Bit encryption requires a 10 character HEX key and 128 bit encryption requires a 26 character HEX key. (HEX characters include numbers from 0 to 9 and letters from A to F).

Click on ‘Save Settings’.



Security Mode : WEP

WEP

If you choose the WEP security option this device will ONLY operate in Legacy Wireless mode (802.11B/G). This means you will NOT get 11N performance due to the fact that WEP is not supported by the Draft 11N specification.

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length : 64 bit (10 hex digits) (length applies to all keys)

64 bit (10 hex digits)
128 bit (26 hex digits)

WEP Key 1 :

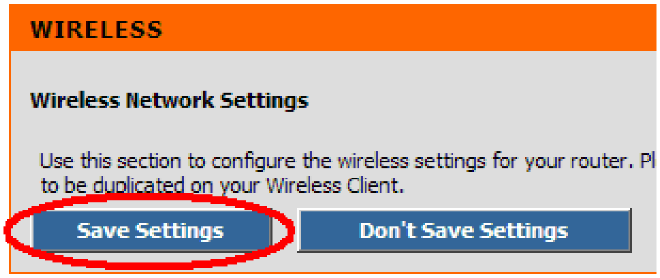
WEP Key 2 : ●●●●●●●●●●

WEP Key 3 : ●●●●●●●●●●

WEP Key 4 : ●●●●●●●●●●

Default WEP Key : WEP Key 1

Authentication : Open



WIRELESS

Wireless Network Settings

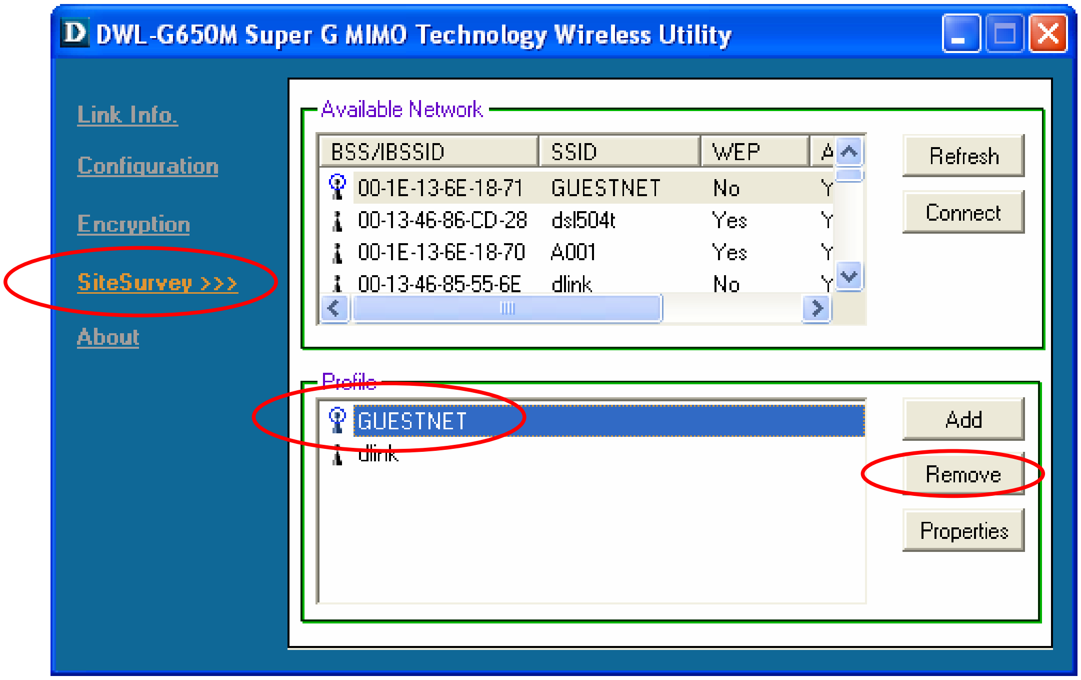
Use this section to configure the wireless settings for your router. Pl
to be duplicated on your Wireless Client.

Step 4. Reconnect your wireless clients (computers) to the wireless network using the specified key (“password”). Note that after applying the security on your router, your wireless clients will lose wireless connectivity until you specify the correct key (“password”).

To reconnect to the wireless network:
On your wireless computers delete the old profile for the wireless network connection (if present). Attempt to connect to your wireless network again. You will be prompted to enter the encryption key (“password”) or key you have entered in Step 2. Note that the WPA/WPA2-PSK key is case sensitive.

To delete the old profile:
<u>D-Link Air Utility</u>

Click on ‘Site Survey’. Highlight the WLAN profile under “Profiles” field and click on Remove.

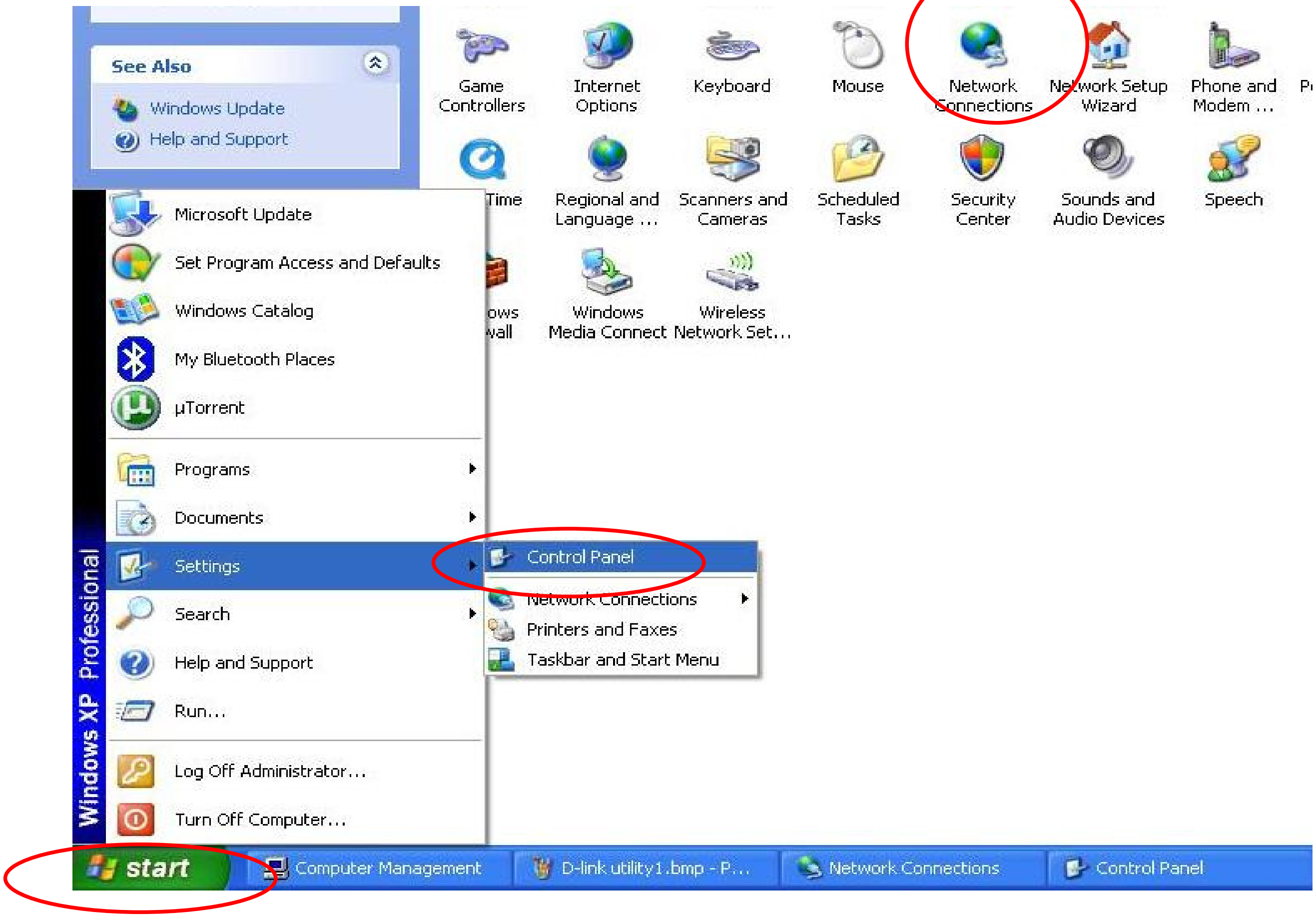


BSS/IBSSID	SSID	WEP	A
00-1E-13-6E-18-71	GUESTNET	No	Y
00-13-46-86-CD-28	dsl504t	Yes	Y
00-1E-13-6E-18-70	A001	Yes	Y
00-13-46-85-55-6E	dlink	No	Y

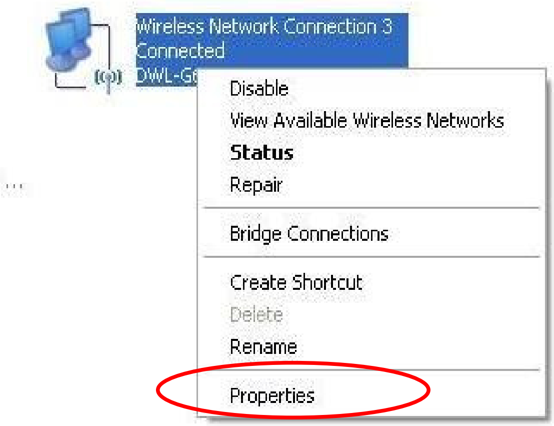
GUESTNET
dlink

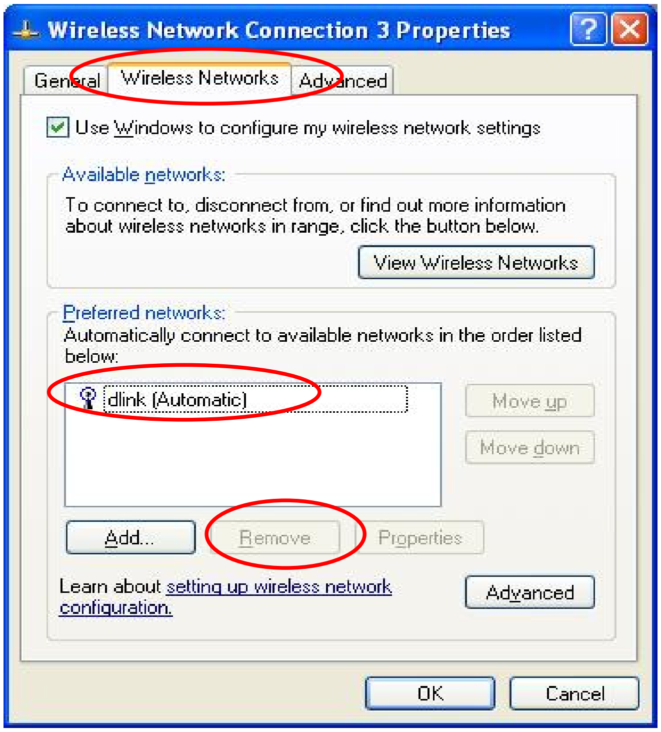
Windows XP Utility

Go to Start>Control panel>Network Connections folder, right-click Wireless Connection > Properties > Wireless Networks. Highlight the profile under “Preferred networks” field and click on Remove.



aaa




Wireless Network Connection 3 Properties

☑ Use Windows to configure my wireless network settings

Available networks:

To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

Preferred networks:

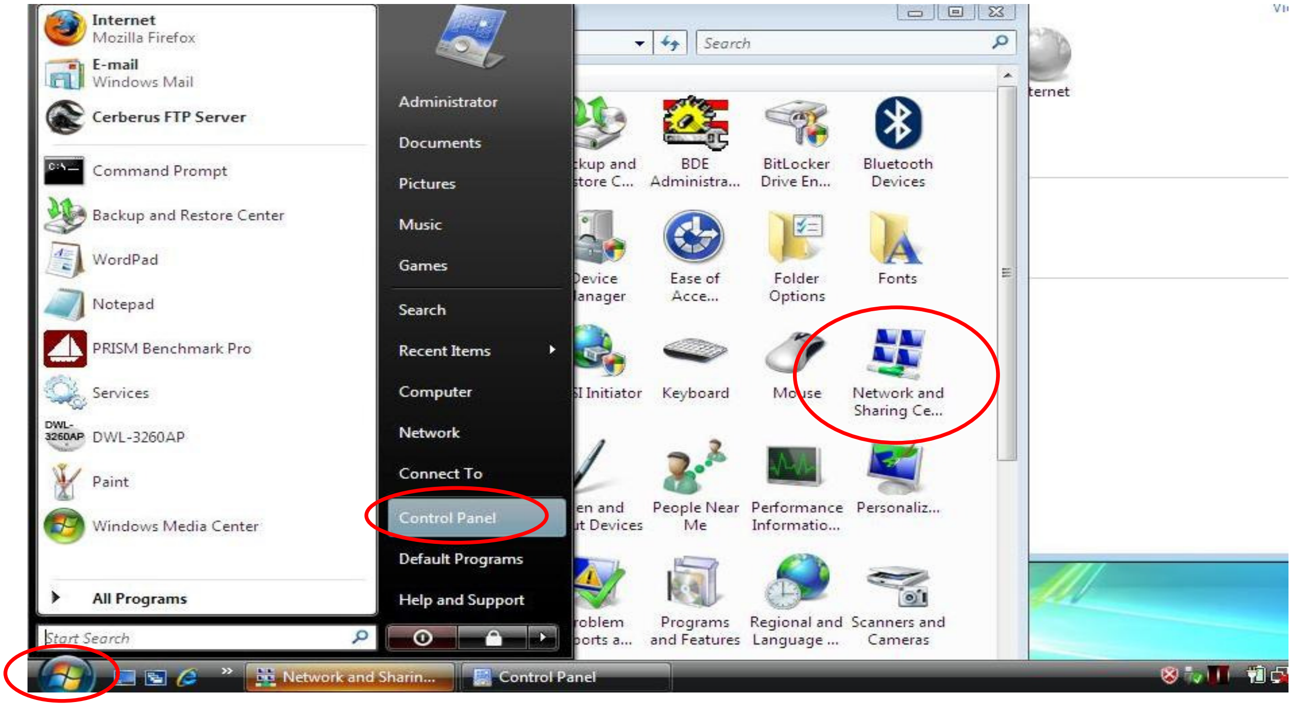
Automatically connect to available networks in the order listed below:

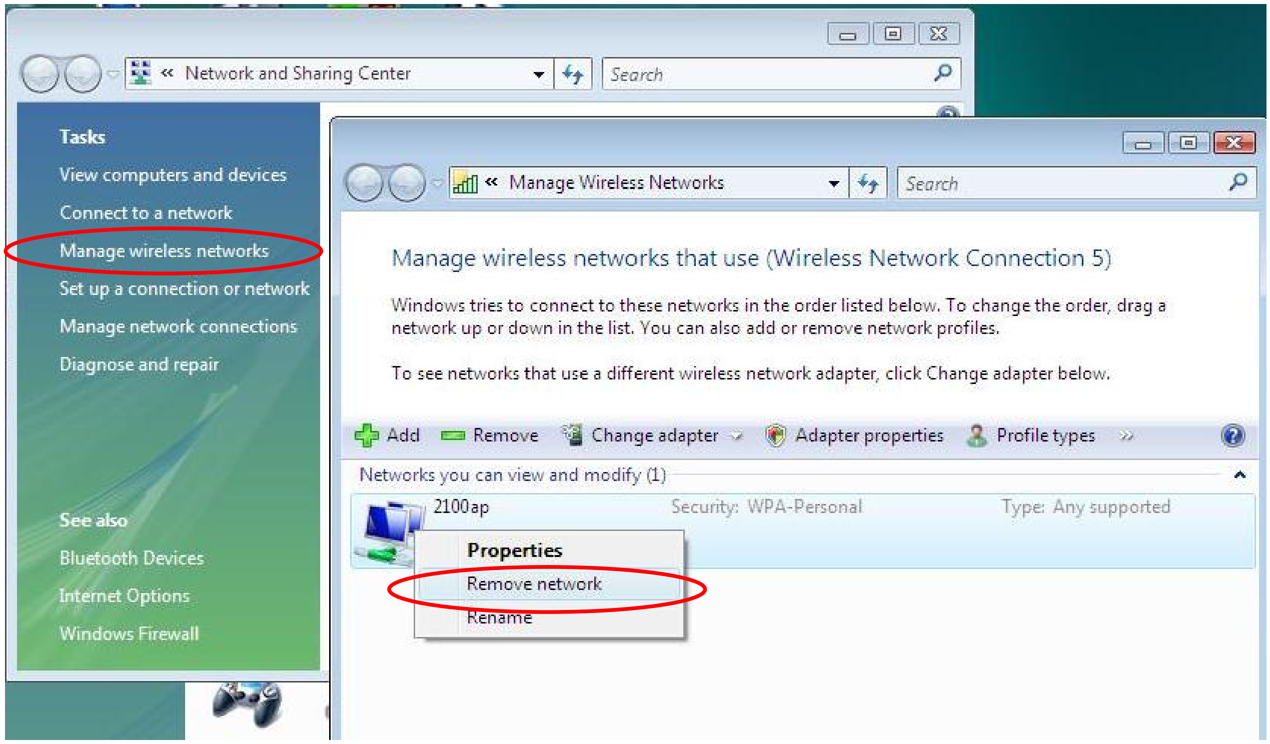
dlink (Automatic)

Learn about setting up wireless network configuration.

Windows Vista

Control Panel > Network and Internet > Network and Sharing Centre. Click on “Manage wireless networks”. Right-click on the network you want to remove and select “Remove network”.





Manage wireless networks that use (Wireless Network Connection 5)

Windows tries to connect to these networks in the order listed below. To change the order, drag a network up or down in the list. You can also add or remove network profiles.

To see networks that use a different wireless network adapter, click Change adapter below.

Networks you can view and modify (1)

2100ap Security: WPA-Personal Type: Any supported

The new profile will be created automatically after successful connection to the secured network.

Other security options (WPA2-PSK, WPA, 802.1x)
WPA2-PSK offers even better protection but not all clients may support WPA2-PSK. Advanced security options like WPA-Enterprise require a RADIUS server installed on a network, these mostly used in corporate environment.