Wireless security myth:

SSID Broadcast:
There is a common myth in industry that hiding SSID increases security. **Pune Police** & **ClubHack** would like to inform that hiding SSID will not add much to the security but in case of a corporate user, hiding SSID will facilitate other kind of attack.

No harm in connecting to open networks:
Connecting to Open SSID is equally dangerous and can expose the user to attacks like passive sniffing, MITM, Surf Jacking, ARP poising, local file access, remote exploits on client machines and a lot more.

Hotspot must be Open only:
Keeping hotspot with Open security can lead to above mentioned attacks on the users connected. Captive portal webpage which asks for username and password can only restrict connectivity to Internet but without a username and password many of the above mentioned attacks can be launched.

"Free Internet Access" or "Free public wifi" will connect to internet for free:
"Free Internet Access" or "Free public Wi-Fi" is known as Viral SSID and it does spread from one computer to another if a user tries to connect to it. They are ad-hoc connections and DONOT give you a free internet access.

Recommendation:

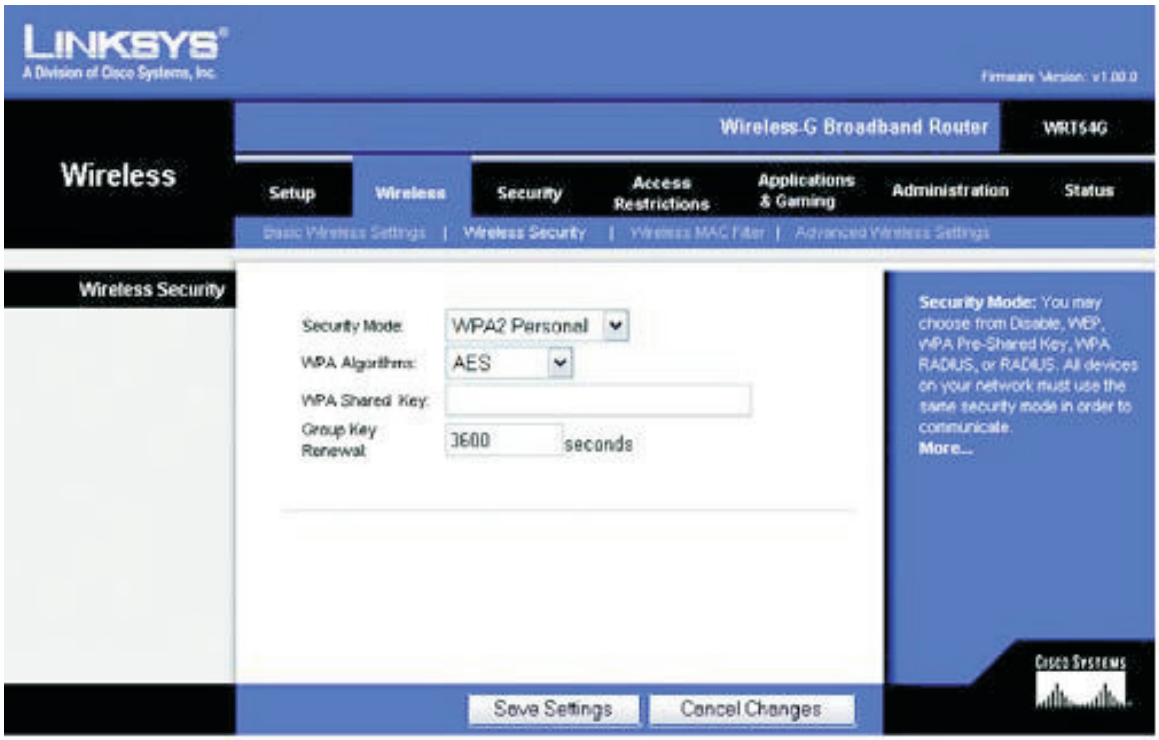
Pune Police and **ClubHack** recommends smart configuration of access points to secure the home/corporate Wi-Fi. Though these steps will not give 100% security but surely increase the security level and make breaking into the networks very difficult.

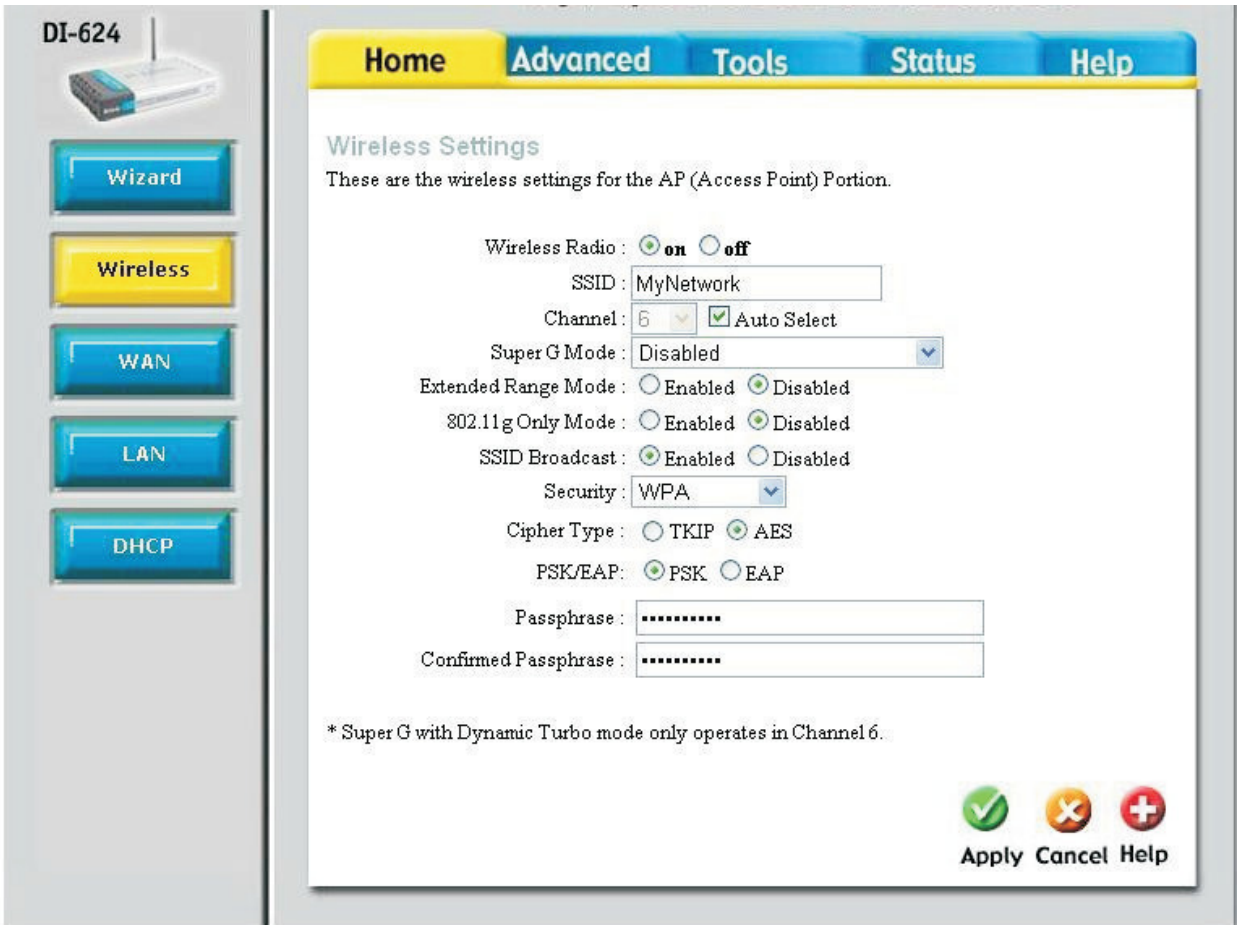
With immediate effect users should move their devices to WPA or WPA2 security level Steps to achieve WPA.

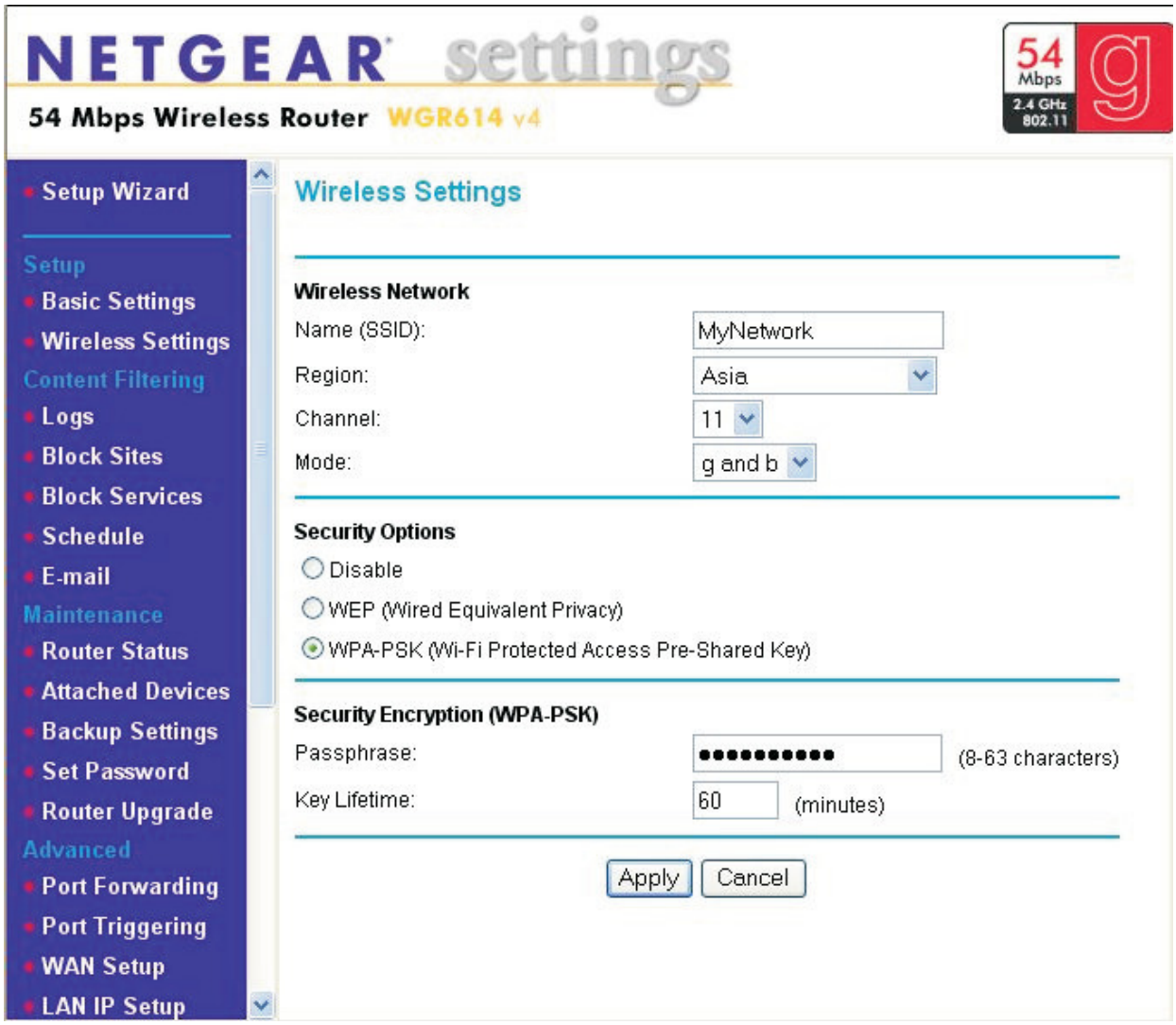
• Open the configuration of your

Wi-Fi device
• Go to wireless setting
• Under security option, select any one (whichever available)
– WPA
– WPA - PSK
– WPA - Personal
– WPA - AES
– WPA2 - Personal
– WPA2 - PSK
• Set a complex password
• Change the login password of the wireless router.
• Change the SSID to something classy
• Don't disable SSID broadcast
• Done

Please refer to the following sample screenshots of few common access points for quick reference.


LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: v1.00.0
Wireless-G Broadband Router
WRT54G
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings
Wireless Security
Security Mode:
WPA2 Personal
WPA Algorithms:
AES
WPA Shared Key:
Group Key Renewal:
3600
seconds
Security Mode: You may choose from Disable, WEP, WPA Pre-Shared Key, WPA RADIUS, or RADIUS. All devices on your network must use the same security mode in order to communicate.
More...
Cisco Systems
Save Settings
Cancel Changes


DI-624
Home
Advanced
Tools
Status
Help
Wizard
Wireless
WAN
LAN
DHCP
Wireless Settings
These are the wireless settings for the AP (Access Point) Portion.
Wireless Radio : on off
SSID : MyNetwork
Channel : 6 Auto Select
Super G Mode : Disabled
Extended Range Mode : Enabled Disabled
802.11g Only Mode : Enabled Disabled
SSID Broadcast : Enabled Disabled
Security : WPA
Cipher Type : TKIP AES
PSK/EAP: PSK EAP
Passphrase : ••••••••••
Confirmed Passphrase : ••••••••••
* Super G with Dynamic Turbo mode only operates in Channel 6.
Apply
Cancel
Help



Additionally to be secure on wireless networks keep in mind:

- Keep away from Open networks.
- Even if you use VPN, make sure your VPN encrypts all your internet traffic too and not only the internal traffic.
- Never connect to “Free Internet Access” or “Free public wife”.
- Create a DHCP pool on your wireless router of a limit which you know will be sufficient for you.
- Add reservations in DHCP pool to safeguard your IP allocation.
- If possible add MAC address filtering, although it will not make you super secure but still will add one more pain point for attacker.