Instructions for use and security of Wifi network

Wireless networks are one of the great inventions of the 21st century. Instead of using cables to connect computers and devices together, you can now use radio waves to connect. This technology has been widely known as 'Wifi'. Once set up correctly, Wifi will not encounter any problems.

Wireless networks are one of the great inventions of the 21st century. Instead of using cables to connect computers and devices together, you can now use radio waves to connect. This technology has been widely known as 'Wifi'. Once set up correctly, Wifi will not encounter any problems. However, to configure the standard at the first time, you will encounter many difficulties.

Wifi connection is easy to encounter some confusing problems. Besides, just like the types of communication sent via radio waves, it requires users to focus more on security settings to avoid being blocked by bad guys.

That's why we wrote this article. The article will provide all you need to make the Wi-Fi network run smoothly and securely, but does not include information or ideas for safe web surfing with public wireless networks.

1. 10 extremely important things that you should remember when using free Wifi

Start by checking

Whether setting up a new wireless network or when you need to help a network work well, you should first check the entire network, everything that makes up the Wifi network.

In the best conditions, Wifi networks need to be configured as fast and secure as possible. However, this is very difficult for older devices. For example, new devices can support the latest Wifi standards, but devices that were produced many years ago may not.

So, by checking all connected devices (or about to connect) to the Wifi network to see which Wi-Fi support is available, users can set the best configuration for the router.

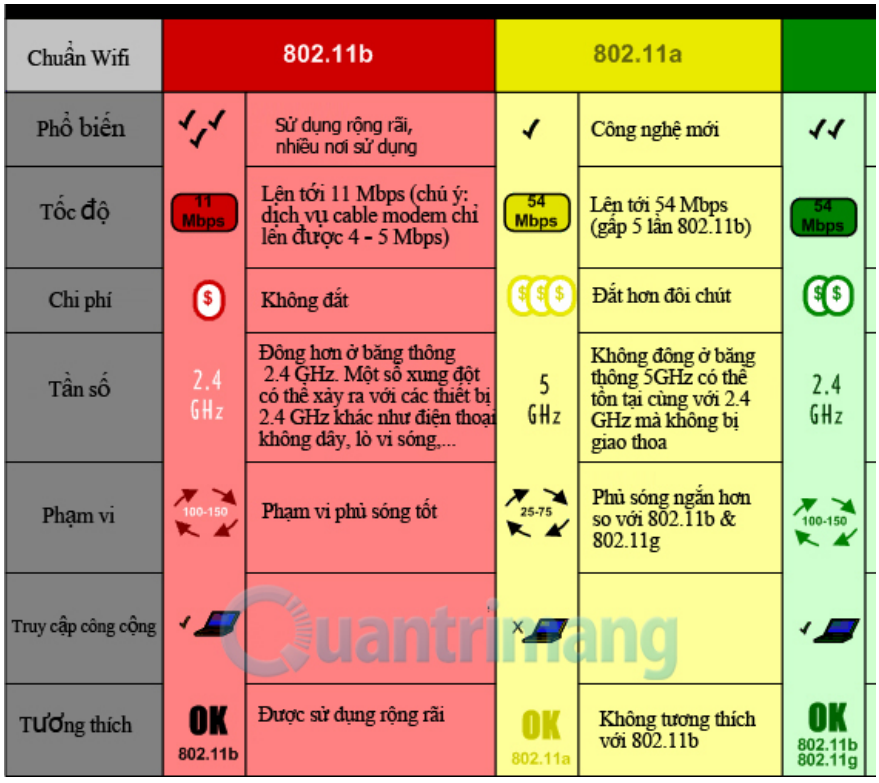
There are three important pieces of information to record about each device, be it a laptop, smartphone, game console, Internet radio, wireless security camera or any device that uses Wifi.

First, standard Wifi devices support; Next, the type of encryption it can use; Finally, the device's **Media Access Control (MAC)** address. You may need to consult the accompanying instructions to find the first two pieces of information, or search them online. However, the third information you can find right on the device (we will show you how to do it later).

Discover Wifi standards

Wifi is an umbrella term for three other but related wireless communication standards: **802.11b** , **802.11g** and **802.11n** . There is still a fourth standard - **802.11a** - but it is less frequently mentioned today.

These standards don't mean anything, but they represent technical data provided by the Institute of Electrical and Electronics Engineers (IEEE). These data are very long, detailed description of how wireless devices interact.



Even so, it's easy to 'refine' from this detailed information. For example, **802.11n** is the new and fastest standard today, can provide the best coverage.

802.11b is the oldest and slowest standard, with the shortest coverage range while **802.11g** seems to be a combination of the two. Another lucky thing is that the new Wifi standards are still compatible with the old standards. So if you have an **801.11n** Wifi-standard laptop with a router that only supports **802.11g** , both devices can still connect to each other at speed and range of **802.11g** .

Unless you discover a speed-related problem on wireless networks, you won't have to worry about deploying a new device, working fast with an old router, running slowly.

If the router is a newer model than **802.11n** , it needs to be set up correctly to fully exploit its capabilities.

A Wifi network only works at the lowest speed of the connected device. This means that if an old **802.11b** laptop connected to an **802.11n** router and actively used a wifi connection, the Wifi connection of all other Wifi devices would have to slow down to accommodate the laptop. .

However, this is not always true in practice. In theory, some high-end routers can maintain many different speeds at the same time - but in most cases, the network will slow down to the speed of the slowest device.

Determine the speed of the router

By understanding the Wifi standard supported by Wi-Fi devices, users can determine the right speed for the wireless network - it will run at the speed of the slowest device being connected.

The next step is to see what can be changed in the wireless router's configuration to increase speed. It is important to remember that the options that appear in the configuration depend a lot on the model and router manufacturer. Even so, we will try to explain as much as possible.

Start by logging in to the router's configuration page. The easiest way to do this is to open a web browser and enter the IP address, such as **192.168.2.1** , into the **Address** or **Location** bar at the top. However, you will need to refer to the manual to get more accurate information.

Next, find the option named **Wifi** or **Wireless** and click on it. In this settings panel there are options for you to choose the type or mode of wireless network.

For example, the test router has a lot of options: **802.11b-only, 802.11g-only, both 802.11b and g (802.11b / g)** , along with 2 other high-speed options.

If all of your Wifi devices support **802.11g** , choose **802.11g-only** network to ensure full Wi-Fi for all devices by preventing all devices from being connected. **802.11b** standard.

On the other hand, if you have a new **802.11n** router labeled 'dual-band', there is another option to get the best WiFi speed.

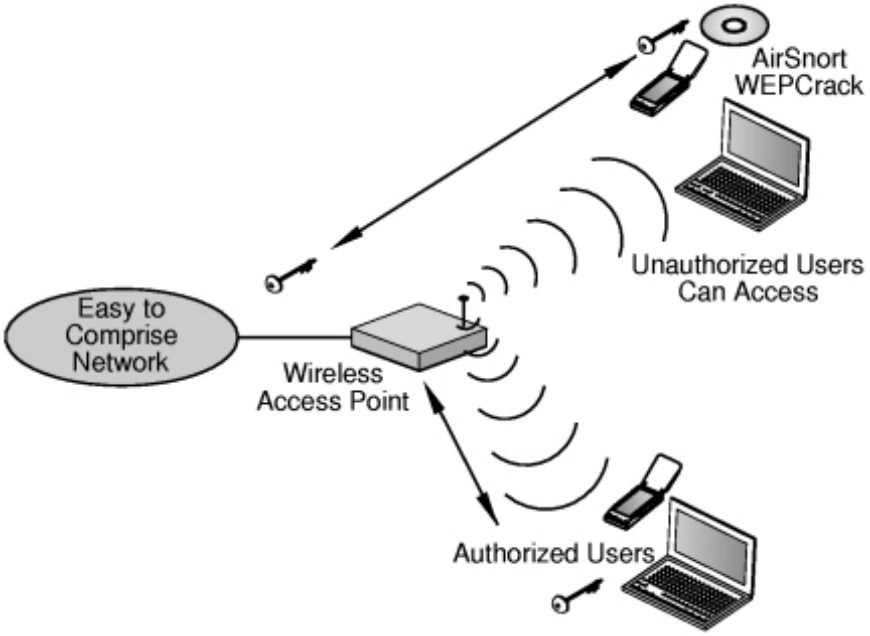
Dual-band routers can operate two different wireless networks simultaneously - one for **802.11b / g** devices and one for **802.11n** devices. This means that devices that support **802.11n** can connect to this router and not be slow when connecting **802.11b** or **802.11g devices** . This will help users get the perfect combination of speed and high flexibility.

However, another problem arises. Dual-band routers only work when running **802.11n** networks in areas with 5GHz radio frequency instead of the usual 2.4GHz frequency.

The problem is that not all **802.11n** devices can operate at high frequencies, so check your device (via the manual or the manufacturer's website) before Activate this option or spend money to upgrade the router.

Enable encryption

The next thing to check is the type of wireless network encryption that the router supports. There are two options - **Wired Equivalent Privacy (WEP)** and **Wifi Protected Access (WPA)** - and both prevent devices from connecting to the wireless network without the necessary password.



WEP is the old standard and most widely supported, but now it is also considered that the network is less secure because a Wi-Fi network protected by WEP encryption can be completely broken within minutes. The truth is that you should not use the WEP standard at all, but it is the only option for older Wi-Fi devices.

If you still own a Wi-Fi device that supports only WEP standards, we recommend replacing them with similar devices but supporting WPA standards or stopping them completely from using them.

Obviously, this is not a perfect choice when the computer is still running well. However, the built-in Wifi can be updated using a new USB Wifi adapter that supports WPA. Although it is not a perfect choice, it helps improve the security of your device.

On the other hand, if your router only supports WEP standards, our advice is to replace them immediately.

With Wifi standard, you need to refer to the appropriate instructions or through the manufacturer's website to see which coding standard your device supports. If they all support WPA, the next thing is to check whether WPA encryption is enabled.

Search the router configuration page to see Wi - Fi security settings or encryption and then choose **WPA-TKIP** or **WPA2-PSK** .

If necessary, create a new password (choose a password that combines numbers, characters and punctuation to make it harder to hack). Besides, remember that all devices connected to the network will need to enter the correct password.

Set up other security options

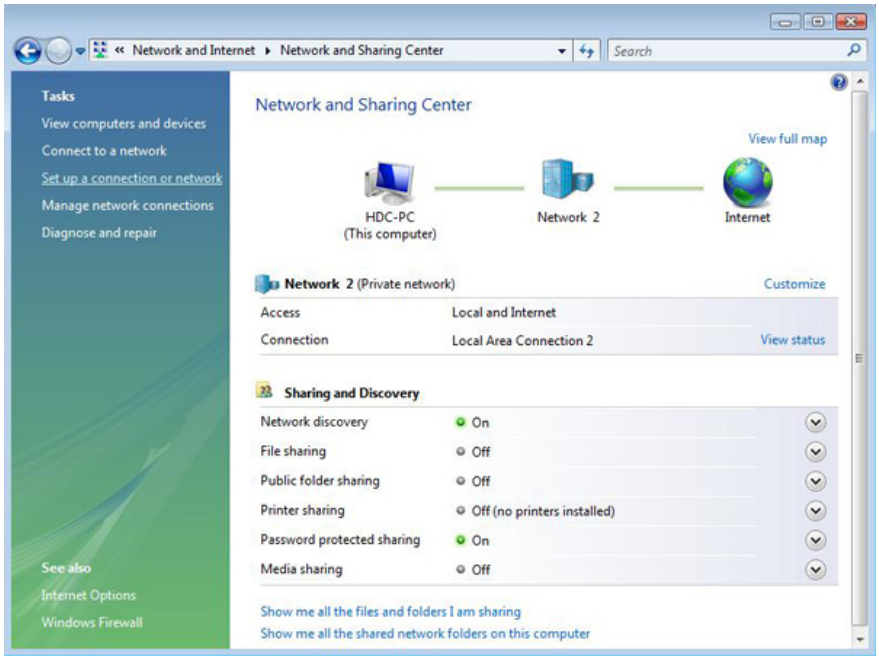
Using WPA encryption can quickly improve the quality of wireless security. However, if you still feel worried that someone can still use your WiFi network, there are 2 other ways you can use it.

Any device connected to the network (wireless or wired) has a special 12-character address code to identify it. It is usually pasted on the device's label.

If not, in Windows XP, select **Control Panel** from the **Start** menu, then click **Network and Internet Connections ? Network Connections** .

When a window appears, double-click this entry to give Wifi adapter a different dialog box to appear. Click the **Support ? Details** tab and the serial number that appears in the **Physical Address** field is the **MAC** address.

In Windows Vista and Windows 7, open the **Control Panel** from the **Start** menu, and select **Network and Internet ? Network and Sharing Center.**



Look in the Network section to see the Wifi adapter option and click on the **View status** option right next to it. In the dialog that appears afterwards, click the **Details** button to see the **Physical Address section** .

With the list of **MAC addresses** in hand, log back into the router's configuration page and look for ' **Wireless clients** ' or ' **Connected devices** ' options.

After that, the **MAC** address of all devices connected to the router will be displayed. If this list does not match what you have recorded, either you have written a missing device or have an unauthorized device to access the

network.

If it is unauthorized access, switch WPA encryption (as explained above) or change the WPA password as these devices are no longer able to steal your network. With that, remember to reconnect your devices when using a new password.

Some routers provide filtering options to allow only some **MAC addresses to** be connected to Wifi, from which the out-of-list **MAC addresses** will be blocked.

However, even if this helps you add another layer of security (and the router has the option of restricting **MAC** address access at some point in the day is very useful when managing the Internet), it is still difficult to apply use with reality.

High-speed hackers can bypass **MAC** address filtering very easily, so you should only use it when enabling WPA encryption.

Counter fake points

The last point about Wifi security. All Wifi networks have names, called ' **service set identifier** ' (or **SSID**) to distinguish them from other networks. It is used to identify networks.

When accessing a wireless network, the Wifi device will display the **SSID** of all nearby Wifi networks, select an appropriate network, enter the correct password and you have successfully logged in.

Maybe when exploring the configuration page for the router you will see the option to hide the **SSID** and then select it with the idea that if you don't see it, unauthorized users will not connect to the network. However, do not treat it as a security method.

Current Wi-Fi scanning software on the market can now find hidden **SSID** , making it a useless security method.

One of the potential risks of using public Wifi services is connecting to a fake access point, or 'evil twin' hotspot. Simply put, there are wireless access points set up by hackers. These networks have the same **SSID** as valid networks for the purpose of deceiving users. From there, the hacker will retrieve personal data of the visitor.

So, if you're sitting in a cafe or public place and seeing two Wi-Fi hotspots with the name TipsMake.com, is there any way to tell if the real network is still a evil twin? Sadly, this is very difficult.

However, common sense may help in this case. All paid or free Wifi hotspots send a login page or welcome page on the browser before starting to surf the web. Remember this, try it before continuing to surf the web or if possible, try asking the network owner if it is correct.

If in doubt, do not use public access points to access important services, such as bank accounts.

Wifi wave communication

Although Wifi uses 2.4GHz or 5GHz frequency radio to communicate, it divides each frequency into multiple channels to avoid interference with neighboring networks.

If you often find the network speed is slow or disconnected from the WiFi while the computer is connected to the network with the wire still running normally, you should probably check the channel settings.

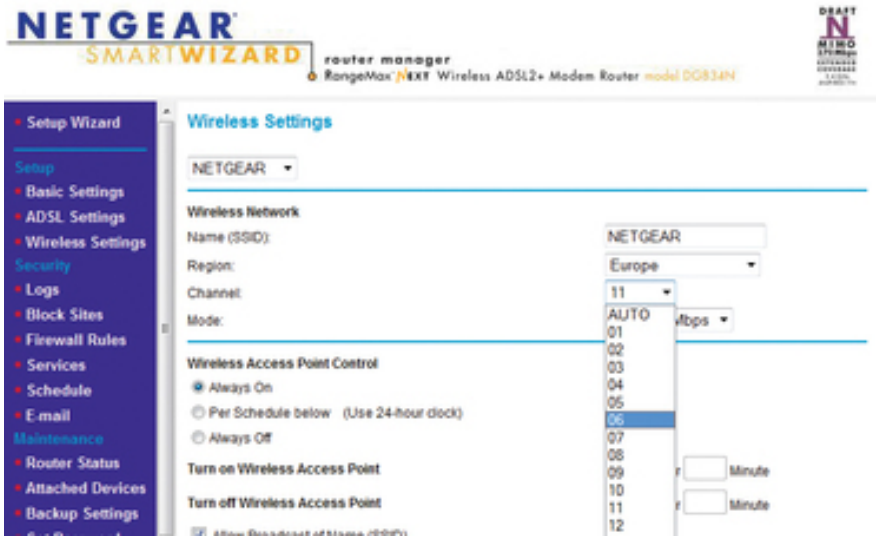
In the UK, 2.4GHz Wifi (used by **802.11b / g** and **802.11n devices**), has 13 channels and users can see how much their routers use in the configuration page. To solve the wave interference problem, you need to know which channels the neighboring network is using and then switch to other channels.

Detect nearby Wifi networks

If you suspect that a nearby WiFi network is interfering with your network, try making a small test to know what is the 'pathfinder' and the channels they are using.

Users can use the software to do this. There are many software to choose from, such as Inssider. When active, this software will display a list of nearby Wifi networks, its speed and number of channels.

Ideally, change the Wifi router's channel so that it does not overlap with other networks. If not, just select the channel with the weaker networks. Any Wifi device connected to the router will automatically change the channel.



Change channel for Wifi network on router

Other networks are just a small cause of Wifi interference. 2.4GHz radio frequency is not only used by Wifi network, it is also used by many other devices, including wireless phones, Bluetooth devices or even microwave devices.

If such devices are located near the router or Wifi device, try moving it elsewhere to solve the problem.

Sometimes, users of dual-band routers can activate the 5GHz **802.11n** network to overcome wave interference problems, as part of this radio wave is less obstructed (only available when Wi-Fi devices are supported). 5GHz **802.11n** support).

Internet access faster

If the Wi-Fi network works well, but you have problems accessing the Internet, there are a few other things on the router you should check. For example, if your web browser needs a lot of time to open web pages, or if the website sometimes doesn't access successfully, the first thing to notice is installing the router's **Domain Name System (DNS) server** .

Web addresses like TipsMake.com are just names for convenience and when it is filled in the browser, the router will have to search for the IP address needed to download the page.

The router does this through a DNS server. At the present time, your router almost uses only the DNS server settings provided by the ISP. In general, these settings work fine, but some respond slowly.

Others are even designed to block certain websites or content types. In such a case, switching to another DNS server can help solve the problem or two other types of DNS servers that are quite popular provided by **Google** and **OpenDNS** .

Install DNS server from 2 types of IP addresses - for example, Google is **8.8.8.8** and **8.8.4.4** . Look for the DNS settings in the router's configuration page.

Record the current settings and then disable the ' **automatic** ' option and then enter the alternate **DNS server** address there. Apply faster, better settings and web browsing experience. If not, switch back to previous settings or install automatically.

Google 's DNS server is the quickest and best option if you have problems downloading web pages. However, **OpenDNS** 's DNS server provides a kind of parental control installation, very useful for families with young children and wants to manage their child's Internet usage.

On the other hand, if the problem is that you have an application that cannot connect to the Internet, such as a game or chat software, it is likely that it has been blocked by the built-in firewall.

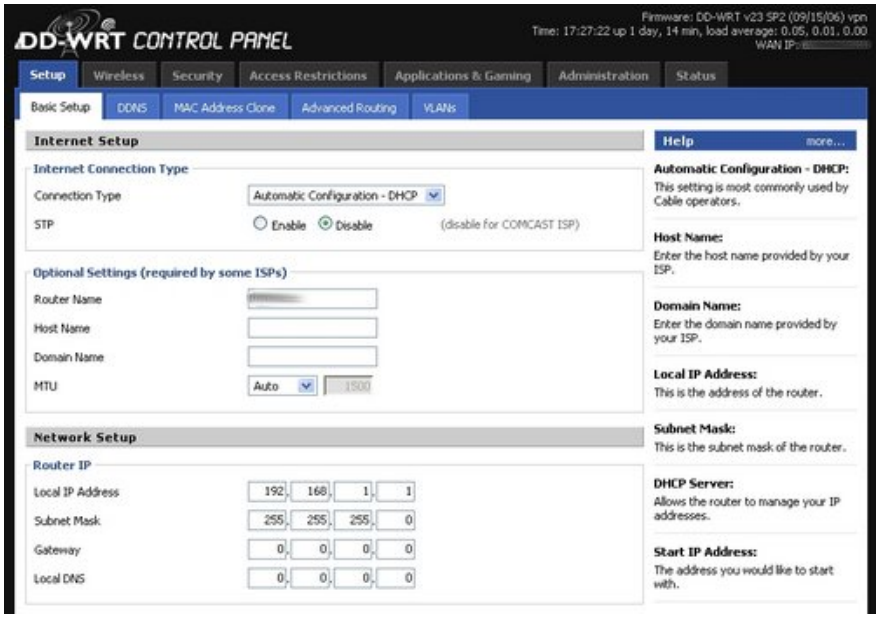
By default, routers tend to allow applications to connect to the Internet using some common ports: any access that is not using an invalid port will be blocked to protect security.

However, ports can be opened or 'forwarded' to solve this problem, but you need to know the ports that the software needs and how to do it on the router.

Option to upgrade

In case you have tried all of these ways, the router still doesn't run as you want, try updating it (**Note** : updating here doesn't mean you need to buy a new router). Start by checking on the manufacturer's website to see if new firmware is available as firmware updates can also help solve the problem related to performance.

Many routers are also updated with open source firmware called DD-WRT. It will help to add a lot of features.



Finally, if you use a wireless router provided by the ISP and don't want to be restricted, there is no reason to force it to use it. Any router is useful, except for some cases that need more attention.

Users need to know ISP settings for cables or connect ADSL to copy them on the replacement router.

Often users can find this information on the service provider's technical support page. Even so, some ISPs make it difficult for users to force them to use their routers and inevitably refuse to request technical assistance. If so, double-check the ISP before buying a new router.

Windows XP, Vista and 7 together on a network

Sharing files or other types of data on one computer between Windows-based computers may be a little problematic when Windows 7 appears.

Although Windows 7 has a 'Homegroups' feature that helps users share data and printers with everyone on the same network, it only works between Windows 7 computers. This feature doesn't work if you want to share between machines running Windows XP, Vista and Windows 7.

Although communication between different versions of the operating system is not too difficult, it is complicated because you will have to do many different methods in each version of Windows.

Microsoft provides its own instructions to help all 3 recent versions of Windows operating systems share data with the printer patch.

Above we have provided you with basic instructions for making wireless networks run smoothly, stable and always at the highest speed. Hopefully they will help you read.