

Basic knowledge to set up a home wireless network

This article will show you how to perform step-by-step programs: plan, build, and test a home wireless network. Although many typical wireless networks have made incredible strides in

This article will show you how to perform step-by-step programs: plan, build, and test a home wireless network. Although many typical wireless networks have made incredible strides over the past few years, technology and wireless is still quite difficult for us to fully comprehend. about it. This tutorial focuses primarily on how to build a home wireless network, but will also help small business network operators.

Steps to build a wireless LAN



You can build any typical wireless home network (often called wireless LAN - WLAN) through the following three steps:

1. Choose the best WLAN design for your case.
2. Choose a good wireless device.
3. Set up the device and check if the WLAN is configured.

In the section below, we will detail each step above.

Are you ready for a wireless network?

Admittedly, using a wireless network instead of building a traditional fiber optic network is a wise decision.

In the past, wireless networking was a 'luxury', because the device for it was quite expensive. But over the past few years, the cost of wireless networking equipment has dropped significantly, providing opportunities for many home users, including small and medium businesses. Are you sure the wireless network will fully meet your requirements? Please check back and consult more from experienced people to make the best decision.

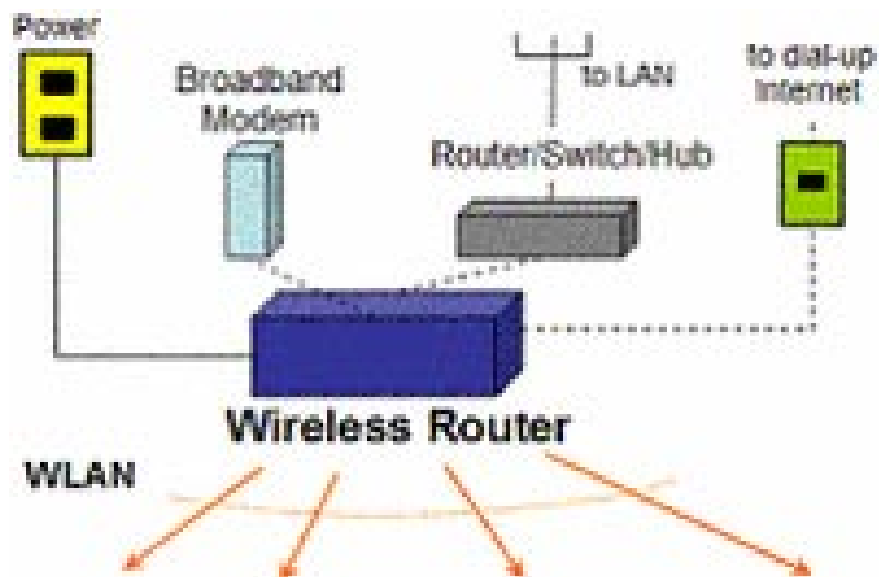
Benefits of wireless

The benefit of wireless networks that are validated is much larger than traditional wired networks. Have you ever looked up a recipe on the Internet while cooking in the kitchen? Do kids need a networked computer in their bedroom for their homework? Have you ever dreamed of sending an e-mail, a message or playing a game while relaxing on the porch? That's just some of the many things wireless networking can do for you.

Technical terms

The field of computer networks is usually located directly on the technical area. Device manufacturers, service providers, and network researchers often tend to go deep into technical terms. The wireless networking industry is gradually improving this legacy system, creating more user-friendly and easier-to-integrate products. However, they still have much to do now. Let's take a quick look at some of the following universal wireless network terms along with their meanings.

Terms and technical words wireless



WLAN network with wireless router

When learning to buy some wireless devices, or when talking about wireless networks with family and friends, you should understand some of the following basic terms.

What is WLAN?

As mentioned above, WLAN is a 'typical' home wireless network. This is because WLAN is a wireless LAN, a group of networked computers that are physically interconnected, physically close to each other. LANs can be found in many families, schools and businesses. Technically, many LANs can be used for one family. But in fact, this is very rare. In this tutorial, we will explain how to build a standard single WLAN for your family.

What is Wi-Fi?

Wi-Fi is the industry name for the wireless network product market. You will see a black and white Wi-Fi logo or a symbolic virtual certificate on any newly purchased wireless device.

Technically, Wi-Fi denotes the 802.11 wireless communication standard (described below). But since all mainstream wireless home appliances now use the 802.11 standard, basically the term 'Wi-Fi' is simply used to distinguish wireless devices from other network devices.

What is 802.11a / 802.11b / 802.11g?

802.11a, 802.11b and 802.11g are three popular wireless communication standards. A wireless network can be built according to any one of these three standards. But 802.11a is less compatible with other standards and tends to become expensive, only deployed for large businesses.

What is WEP and Wardriving?

Security features for home wireless networks and small business networks leave many concerns. If we can use an antenna or a relay to capture radio and television signals from a broadcast station, it is not difficult to catch a signal from a nearby wireless home network. Transactions via credit card on the Web can be safe, but are you sure your neighbor doesn't track every e-mail and message you sent?

A few years ago, some experts popularized the reality of wardriving to raise awareness about this vulnerability in WLAN. With the help of cheap self-made devices, the 'wardriver' (unauthorized wireless intruders) 'snooped' through the vicinity of wireless network traffic coming from neighborhood houses. Some even log into the computer without leaving any trace to the WLAN owners suspicious. Their main purpose is usually to steal resources in computers and access the Internet for free.

WEP is an important component of wireless networks, designed to enhance security. WEP will find its way in (technically called 'encoding') network traffic in a calculated way so that other computers can understand, but people cannot read it. WEP helps to protect WLANs against wardriver and curious neighbors. Currently, all wireless network devices support this component. Since WEP can be turned on / off arbitrarily, configuring and using it during network installation is necessary and simple.

Wireless device models

There are 5 types of devices identified in home wireless networks:

1. Wireless network adapter.
2. Wireless access point.
3. Wireless router.

4. Wireless antenna.
5. Wireless signal booster.

Some of these devices are not required, depending on your wireless network configuration. We will be back to review each device in detail.

Select the wireless device

A wireless LAN usually has a network adapter, access points, wireless routers, broadcast receivers and signal boosters. Among them, only the network adapter is a must-have component to build a home wireless network. Many networks also use some other devices as explained below.

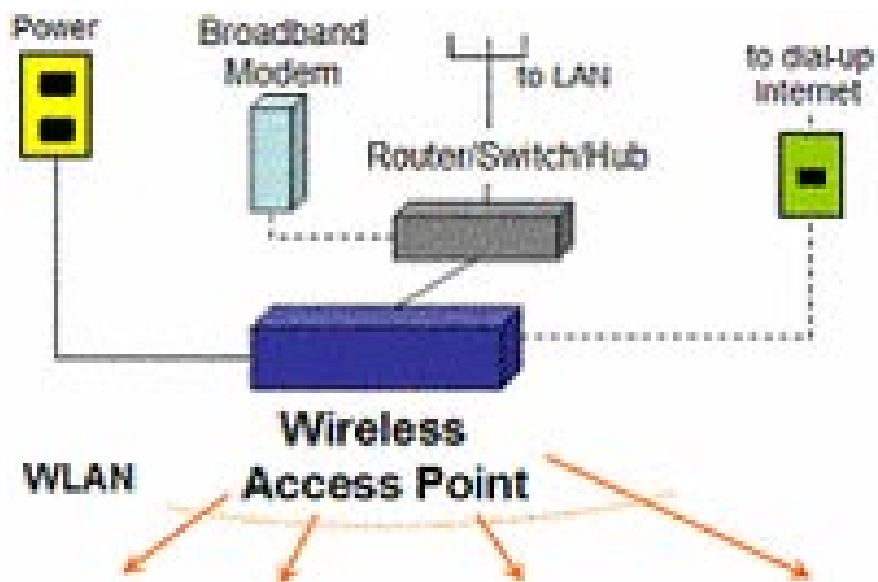
Wireless network adapter

Any computer that wants to connect to a WLAN must have a wireless network adapter. Network adapters are sometimes called NIC (Network Interface card), ie network cards. Network adapters for desktops are usually small PCI cards, sometimes USB adapters similar to cards.

The network adapter for laptops looks like a thick credit card. Today, instead of traditional cards, these laptop adapters are often built as an embedded chip inside a notebook or laptop.

Wireless network adapter includes a broadcast receiver. Wireless transmitters send and receive messages and messages and translate, format and organize them according to the flow of information between the computer and the network. Determining how many network adapters need to be purchased is the first key step in the process of building a wireless network. Check the specifications on your computers if you're not sure whether they contain built-in wireless adapter chips.

Wireless access point



WLAN network with wireless access points

A wireless access point acts as a central WLAN communication station. In fact, they are sometimes called 'base stations'. Access points are thin, light boxes with a series of LED bulbs on the surface.

Access points link a wireless LAN to a wired Ethernet network that existed before. Home network users primarily install access points after they have owned a broadband router and want to add wireless computers to their current settings. You must use either an access point, or a wireless router (described below) to deploy a 'hybrid' network between wired and wireless. If not, you may not need an access point.

Wireless router

A wireless router is a wireless access point with some other useful functions. Like a wired broadband router, the wireless router also supports sharing Internet connectivity with firewall technology to enhance network security. Wireless routers are very similar to access points.

The advantage of both wireless routers and access points is elasticity. The built-in powerful transceiver is designed to spread wireless signals throughout the home space. A home WLAN using a router or access point will signal better at the corner of the room or backyard than it does not. Likewise, if you use a router or access point, the network will support more computers. If the WLAN design scheme uses a router or access point, you must run all adapters in the infrastructure model 'to call' (so-call infrastructure mode) or special model (ad Infrastructure infrastructure).

Wireless routers are a good choice for those who build their first home network.

Wireless antenna

Wireless network adapters, access points and routers all use an antenna that supports WLAN reception. Some wireless antennas are like on the adapter hidden inside. Others, like on many access points, are outside. Ordinary antennas can also successfully complete their effective wave reception. But if installing an additional antenna, the signal reception process will be enhanced. Usually you will not know whether you need this component or not after finishing installing the basic network.

Increase the wireless signal

Some wireless access point manufacturers and routers also sell a small device called a signal booster. Installed with an access point or wireless router, increase the signal strength to improve the base station transceiver. It is possible to increase the signal strength with additional antennas to improve wireless transmission speed and signal reception at the same time.

Both antennas and signal boosts become useful additional devices for some home networks. They can help out-of-network coverage to recover WLAN signals and in some cases improve performance.

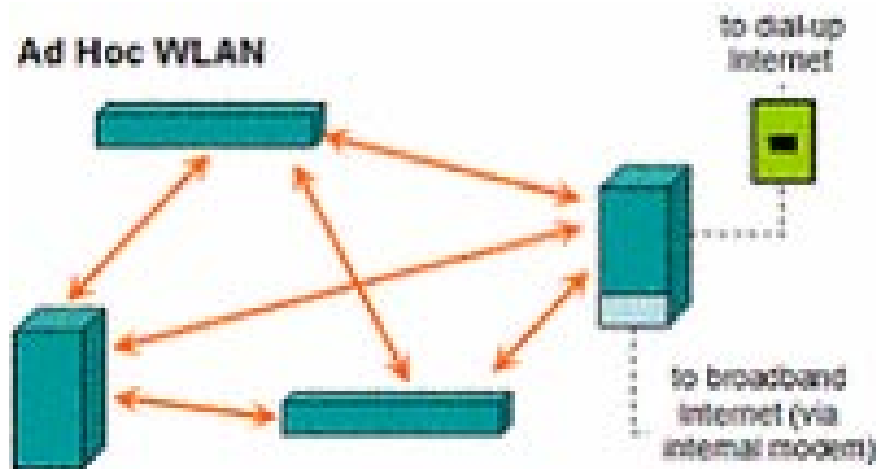
Install and configure WLAN

Now, you understand the components of a wireless LAN and are ready to install them on demand. Don't worry if you still don't have a stable configuration, we'll look at all of them.

To get the most from the guidelines below, you should have the answers to the following questions:

- Want to expand your WLAN home network or build a whole new network?
- How many wireless computers and where are they located?
- What is the operating system used for computers?
- Do you need to share your Internet connection between wireless computers? What other functions are needed? file sharing? play network game?

Wireless router installation



Arrange a special wireless LAN A wireless router supports a WLAN. Use the wireless router on the network if:

- You are building the first home network, or
- You want to rebuild your home network to be completely wireless
- You want to set up WLAN at the simplest possible level.

Try to install the wireless router in the most central location in your home space.

In Wi-Fi networks, computers located close to the router (usually in the same room or in the 'line of sight') will have higher speeds than remote computers.

Connect the wireless router to the power supply and Internet connection source (optional). All wireless routers support broadband modems and some support for connecting phones via dial-up Internet service. If you need phone support, buy a router with RS-232 port. Finally, because wireless routers have an access point built in, you have the right to connect to a wired router, switch or hub.

Next, select a network name. In Wi-Fi networks, network names are often referred to as SSIDs. The router and all computers in the WLAN must share the same SSID. Although each router is assigned a default name set by the manufacturer, it is best to change it for safety reasons. Refer to the manufacturer's documentation for the network name for each specific wireless router.

Finally, follow the instructions in the accompanying documentation when purchasing the manufacturer's router to use the WEP security function, turn on the firewall function and the required parameters.

Install wireless access point

Each wireless access point supports a WLAN network. Use the wireless access point on your home network if:

- You do not need extension components provided by the wireless router
- You are expanding a wired Ethernet home network
- You have (or will have) 4 or more wireless computers scattered throughout the house.

Try to install an access point in a central location if possible. Connect the source and connect to the Internet if you want. Also need to connect the access point cable to the LAN router, switch or hub.

Of course you will not have a firewall to configure, but you still have to set up the network name and turn on the WEP function on the access point.

Configure the wireless adapter

Configure the adapter after installing the wireless router or access point (if available). Insert the adapter into the computers as explained by the product documentation. Wi-Fi adapters require the TCP / IP protocol to be installed on the workstation.

Each manufacturer provides a configuration utility for their adapter. On Windows operating systems, for example, the adapter usually has a separate user interface (GUI) that can be accessed from the Start menu or from the taskbar after the hardware is installed. We will set the network name (SSID) and enable the WEP function here. You can also set some other parameters as described above. But remember, all wireless network adapters on computers on the network must use the same parameter settings for WLAN with proper functionality.

Configure special home WLAN network

All Wi-Fi adapters require you to choose between an infrastructure model (infrastructure mode, also known as an 'access point' model in some configuration tools) and a special model (ad-hoc infrastructure, or peer model. When using a wireless access point or router, you need to place all wireless adapters in the infrastructure model. In this model, the wireless adapter will automatically detect and set the WLAN channel number to match the access point (router).

Or set up for wireless adapters using ad-hoc models. When using this model, you will see a separate setting for the channel number. All adapters on your special wireless LAN need to match the channel number.

The ad-hoc WLAN family configuration only works well with some computers located close to each other. You can also use this configuration as a reserve option if your access point or router is broken.

Configure Internet connection sharing software

As indicated above, you can share your Internet connection via an ad-hoc wireless network. To do this, place one

of your computers as a workstation (more efficient for one machine for a router). This computer will keep the modem connected and obviously must be powered on whenever the network is used. Microsoft Windows provides a component called Internet Connection Sharing (ICS), supported in WLAN.

Debugging, tips and tricks

Now we will look at some of the more interesting points you need to know about home wireless LANs.

Signal interference wireless router or access point inside the home network

When installing an access point or 802.11b, 802.11g standard router, be cautious of signal interference from other devices. Specifically, do not install these components near a wave device that emits microwave waves within 1-3 m. Some other common sources of interference are 2.4 GHz cordless phones, a variety of baby monitors, garage door openers and some home automation devices.

If your wall is brick, cement or metal, maintaining a strong WLAN signal is difficult. The Wi-Fi network is designed to support signal areas within 300 feet, but if obstructions appear, this range will be reduced. All communication activities according to the 802.11 standard (especially 802.11a) are affected by obstructions. You need to consider this when installing your access point.

Interference with wireless router or access point from outside

In overcrowded residential areas, the case of wireless signals from this home network 'visits' neighbors' home networks and vice versa is not rare.

This happens when both households set up a communication channel that conflicts with each other. Fortunately, when configuring an access point or 802.11b, 802.11g standard router, you can (except in some areas) change the leased channel number.

For example, in the US, you can choose any WLAN channel number from 1 to 11. If you get a noise signal from your neighbor, you should coordinate the channel settings with them. Using a simple number of different channels does not always solve the problem. However, if both groups use one of the different channel numbers (1, 6 or 11), the ability to eliminate WLAN noise will be more secure.

Mac physical address filter

Newer wireless routers and access points support a useful security component called a Mac address filter. I absolutely recommend using this component. It allows registering network adapters with access points (or routers) and forcing the removal of communications from any wireless device that is not on the list. This MAC address filtering function combined with WEP encryption component provides high security.

Profile for wireless adapter

Many wireless adapters support a component called profile, which allows you to set and record multiple WLAN configurations. For example, you can create an ad-hoc configuration for your home WLAN and configure the infrastructure for the office network, then switch between the two profiles if necessary. You should set up profiles on the machines that will be used to switch between home and other WLANs. The time you save will be much greater, the more you will benefit later.

WEP encryption

In many of the introduced functions, you will find that there is a zero-second encryption mode enabled, usually WEP 128-bit. Older WEP versions (40, 64-bit) provide a defect-free protection program. Some 802.11g products support 152-bit and 2256-bit WEP. It would be great if all of your devices support this component. Some newer devices offer WPA. WPA usually has many aggregate functions that are not needed for a home WLAN, but WPA-PSK works quite well.

To set up 128-bit WEP, select and assign the number to the WEP passkey field (password for WEP). You must apply the same WEP and passkey settings to the access point (or router) and all adapters.

Some common tips

If you have all the components installed, but the home network still doesn't work properly, fix it methodically:

- Cannot connect to the Internet? Temporarily turn off the firewall and determine if there is a problem in the firewall configuration, or some other problem.
- Similarly, turn on and check each network adapter to determine whether the problem is only on one computer or on all machines.
- Use the ad-hoc style if infrastructure type is not active. And maybe you should identify the problem with the access point or router.
- To work more systematically, when building a network, you should write down the key settings such as the network name, WEP password lock, Mac address and channel number (then look at the sign later).
- Don't worry about errors that can be made during construction. You can go back and edit any WLAN settings at any time.

Conclude

With the knowledge in this tutorial, I think you must have enough equipment to start building your home wireless LAN. Welcome to the wireless world!

You finished reading the article "**Basic knowledge to set up a home wireless network**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.