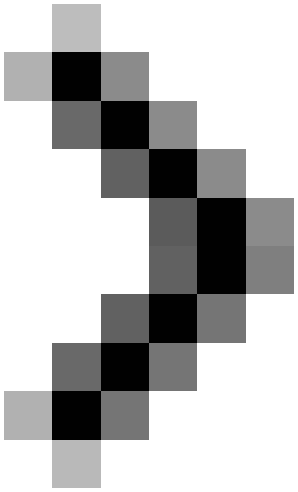
Design a small network with a broadband router (Last part)

There are now more and more people willing to build a small network to divide data files or even connect to the Internet. The network can be set up at your home or office and using a router, you can fully share your Internet connection automatically.



Design a small network with a broadband router (Part 1)

Basic security configuration

The first thing you need to know is the panel's IP address configured for your router. This information will be written on the router manual. It is usually 192.168.0.1, 192.168.1.1 or 10.0.0.1. Launch your web browser and get ***http:/// [IP address here]*** . The router used in our example has the address 192.168.1.1, so it is necessary to enter http://192.168.1.1. Obviously you need to change according to the IP address used by your router.

All configuration options will be different depending on the model of the router. Therefore, you will not have the correct name and options for each step as described in the article, but they still exist under similar names because they are basic options.

Typically, the first configuration page will ask you to choose between quick installation and advanced settings. Although quick installation is the best way to set up your network in less time, this first configuration should be done in advanced settings: set the password for the router.

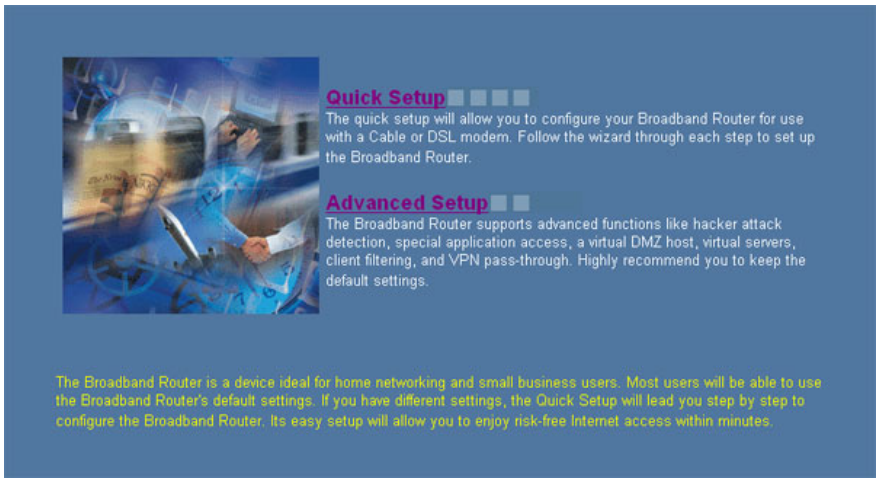


Figure 11: The first screen on the panel configuring your router

As you can see, the router configuration panel is accessible from any computer on the network. So this is a problem in small networks, the router control panel is often accessed from any computer connected to the Internet. For example, let's say your real IP address is 69.69.69.69 (the IP address that the ISP has assigned to your broadband modem). Any computer on the Internet can access your router configuration panel by opening a browser and pointing to *http://69.69.69.69* . This feature may be disabled on some routers. However, it is also a very interesting feature, because sometimes you can edit or reconfigure the office network or home network from any computer in the world. Consider whether or not to disable this feature, depending on how you will use it.

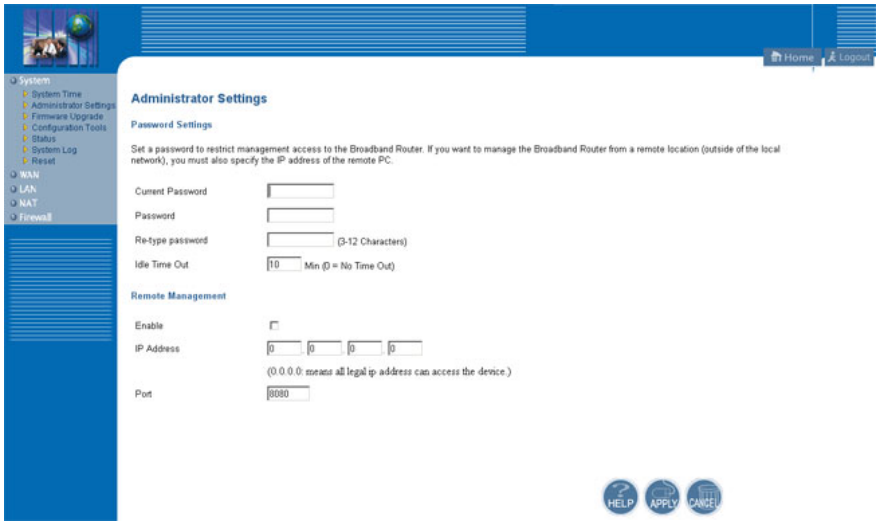


Figure 12: Set up an administrator password

On the example router, this configuration is done at **Advanced Setup** > **System** > **Administrator Settings** . On this screen you can install both the administrator password and choose to enable remote management. Now the remote management feature can be disabled but we can enable it and allow remote management with a specific IP address (for example, IP address from home computer). , so other computers will not be able to access the remote control panel of the router. You can also specify an access port. Using the router on Figure 12, we could not access it using *http://69.69.69.69* , so we need to open it with port *http://69.69.69.69:8080* . This is a simple way to avoid hackers who can open the panel to configure your router from their computers (but for a skilled hacker to know that 8080 is a commonly used port and can also use the scanner port to see which port opens into the router).

Obviously, you need to click **Apply** to make any changes take effect.

After explaining this security, let's go into the basic configuration of the router.

Configure basic settings

First, you need to choose the type of connection you have: cable, ADSL with dynamic IP (ie the IP address provided by the ISP may change over time - this is the type that providers translate still in use), ADSL with static IP (meaning that the IP address provided by the ISP remains unchanged - usually only available in case you have requested and is usually more expensive) or VPN (Virtual Private Network - usually used in corporate networks).

Please return to the basic settings and installation screens. On the router in the example, we only have to configure the time zone on the first screen, modem type on the second screen and click Next and accept all default configurations if you have a cable or ADSL connection. (If you use a VPN connection, you need to enter some additional information). Click Finish in the final screen and that's all it takes to make sure the network is working.

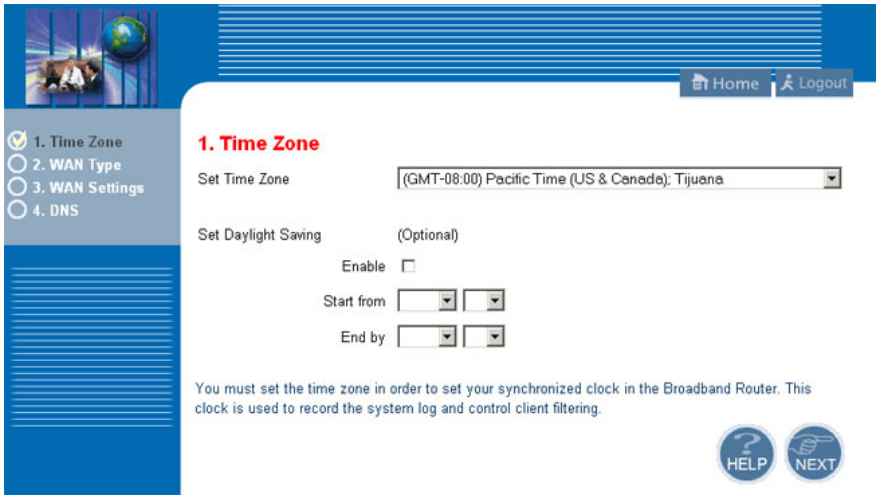


Figure 13: Basic installation, first screen (time zone configuration).

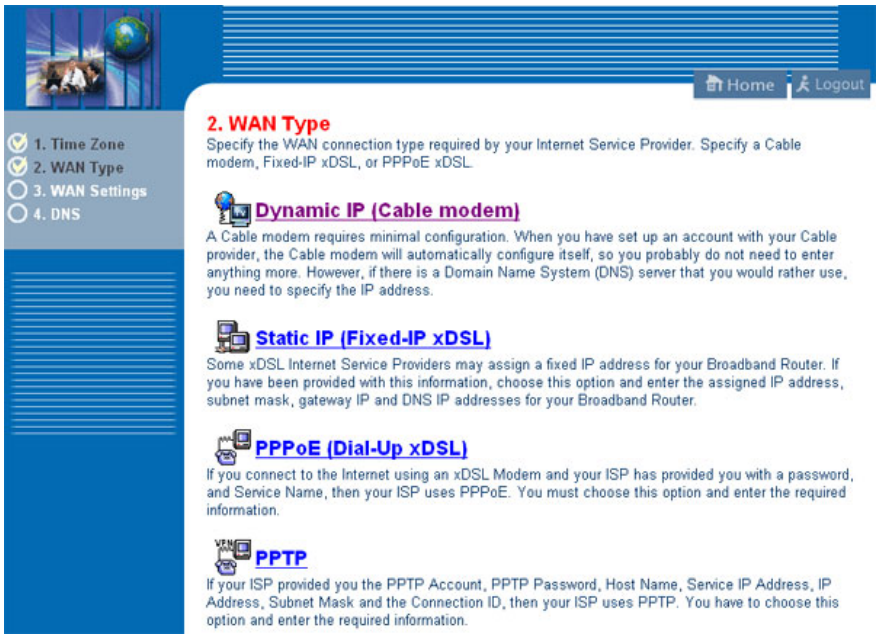


Figure 14: Basic installation, second screen (connection type)

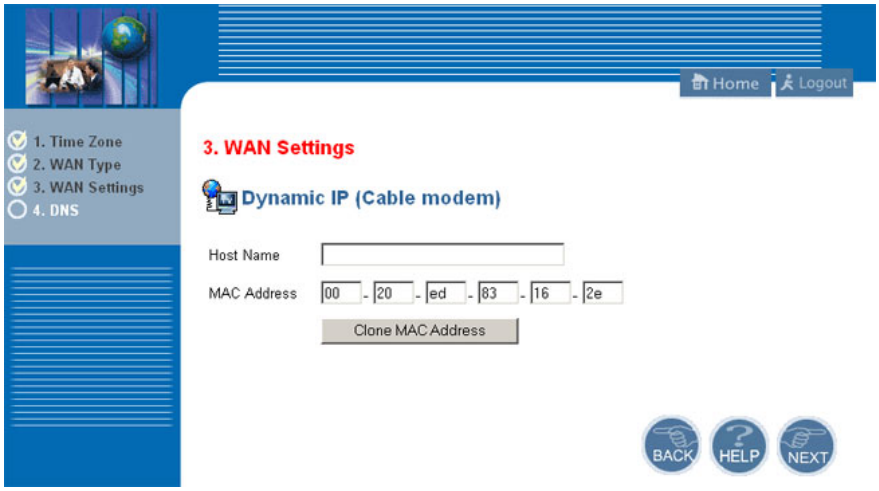


Figure 15: Basic installation, third screen (WAN settings, choose default values)

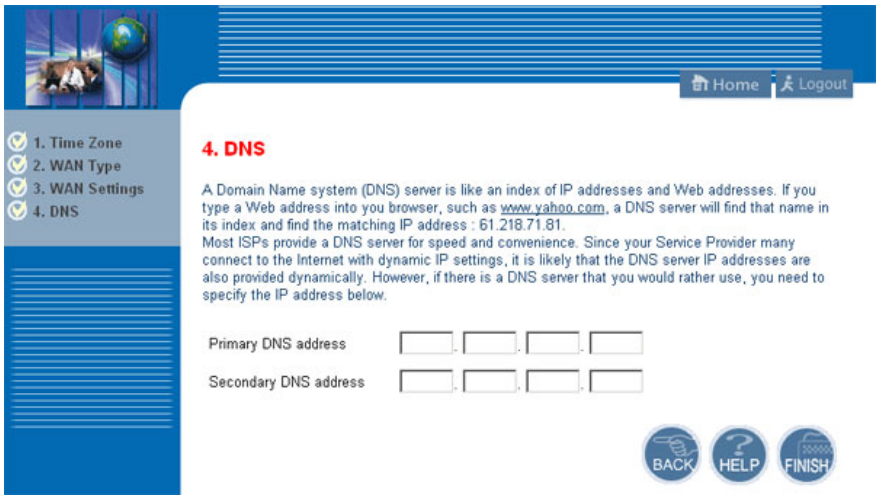


Figure 16: Basic installation, fourth screen (DNS settings, choose default values); Click *Finish*

After clicking **Finish** , try accessing the Internet from your computer and from other computers connected to the network. If it doesn't work, check out the configuration steps. If it still doesn't work, you need to call the ISP support service and explain that you have installed a router and need them to 'release' your IP address.

We also explain: When you use a broadband service, usually public IP addresses (eg 69.69.69.69) will be assigned to the computer that is connected to the broadband modem. Therefore, the ISP blocks the IP address given the MAC address connected to the modem. The MAC address is the serial number recorded on the network card. When you disconnect your modem from your computer and connect it to your router, this connection may be blocked because the ISP will want the desktop's MAC address, not the router's MAC address, these two are different. each other. 'Release' the IP address means that the ISP will scan the new MAC address connected to the modem.

Configure advanced settings

You may not need to change anything at the router's advanced settings. However, if you want to limit Internet access to a certain computer, this is the feature you need to know. If you play games online or use P2P (peer) applications, open the ports used by your software here, or the router will block your program from connecting to the Internet. In advanced settings, you will see security options, which are the ones we will cover at the end of this article.

On the example router, we can restrict time-based Internet access in the **Advanced Setup** > **Firewall** > **Client Filtering** . Blocking all computers for web browsing during business hours (for example, can be done by locking all IP addresses from *192.168.1.1* to *192.168.255.255* at port *80* (ie *www*)), then It configures the days of the week and the number of times allowed or blocked. Because the configuration allows you to specify port numbers, you can block emails (ports *25* and *110*) or even instant messengers like MSN Messenger (port *1863*).

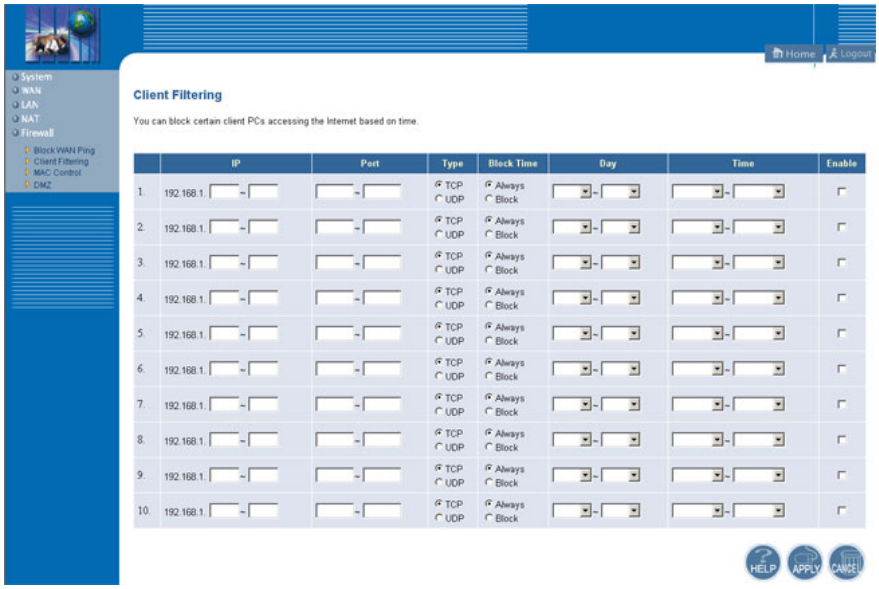


Figure 17: Lock access based on day of week and hour

You can even block some computers that are not allowed to access any Internet forms, based on firewalls and MAC controls. Here you enter the MAC address of the computer you want to block from accessing the Internet. This computer still has full access to other resources within the network such as shared folders and printers.

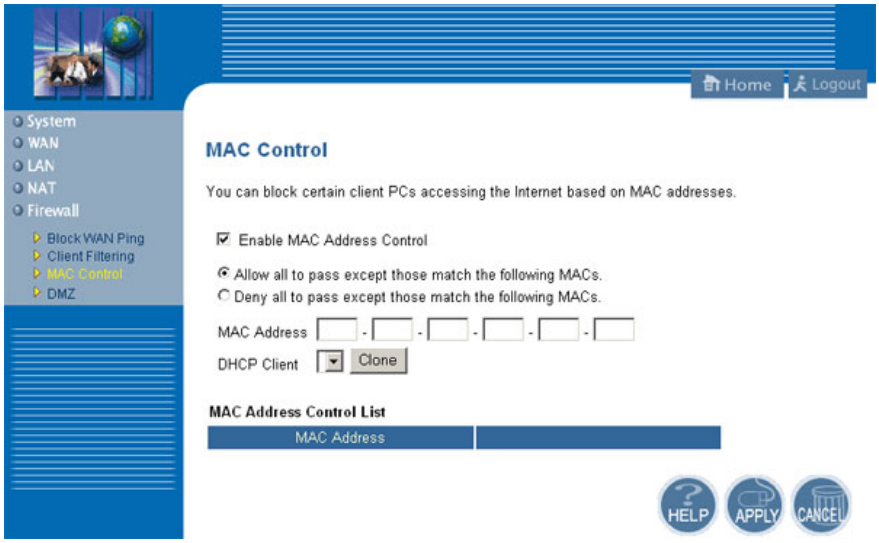


Figure 18: Access lock based on MAC address

If you have any software that uses non-standard ports, you need to open the ports on the router, or the program will not be able to access the Internet. This is true for P2P programs and online games. You should find the ports that the program uses from its instructions and open that port at **NAT** > **Special Application** . In the example of the article in Figure 19, the router opens *Overnet* ports (a P2P software).

Figure 19: Opening non-standard ports

Security

Today with a connected world, security is becoming more important than ever. We also talked about basic security configurations that you should implement on your router, such as setting up access passwords and disabling remote management.

But as mentioned, the router also works as a firewall. It will block incoming connections at non-standard ports. That is why it is necessary to open the non-standard ports used by the program to use. For example, the default configuration of the router is quite good to prevent people from playing online games.

An interesting point that all routers have is that it can lock any request to your public IP address. Ping is used to see if any computer has been installed on this IP address, this technique is used to find computers on the network. If you disable the Ping feature, people who want to find computers on the Internet using this method will not be able to find you. Therefore, I recommend that you check the ' **Discard PING from WAN side** ' option on the firewall, **Block WAN Ping** . However, if you play online games, ping is used to check the delay between you and the game server. In this case, it is better to enable ping.

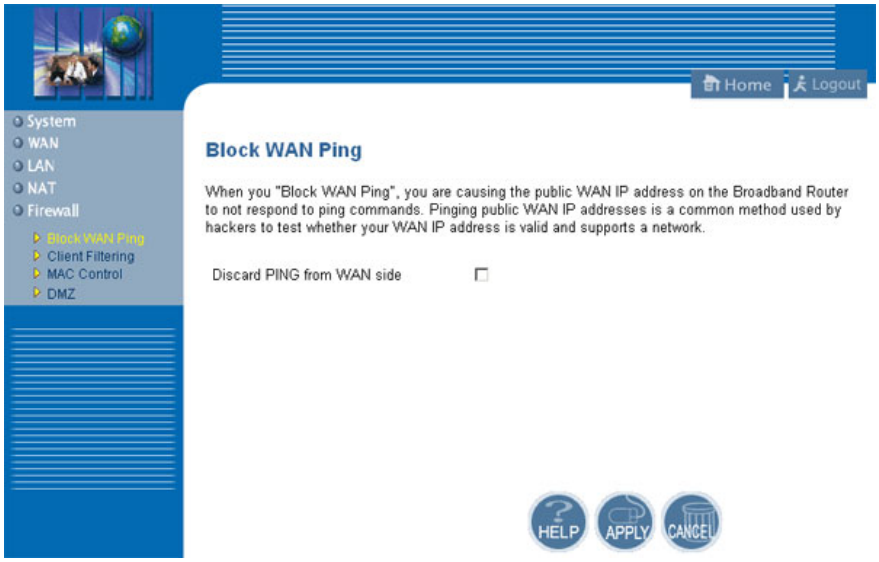


Figure 20: Disable ping feature

Another important feature available on all routers is the software upgrade. You should go to the manufacturer's website and download the latest software versions for your router and upgrade it. On the example router, we can access the **System** > **Firmware Upgrade** . This will ensure that your router is protected from security flaws that the manufacturer has discovered and released an upgrade.

All computers in your network need to be securely protected from the dangerous world. So in addition to preventing direct attacks on the network router, you still have to pay attention to the security of each computer in the network. Installing and regularly updating anti-virus, spyware and trojan software programs on network computers is the final advice we give you in this article.

You finished reading the article "**Design a small network with a broadband router (Last part)**" 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.