This will involve 3 main steps.

Part 1: Get to know your home network equipment Part 2: Configure your home network Part 3: Allow outside Internet traffic into your home network.
Part 4: ISP DHCP

However, before we get started, there's some terminology that needs to be explained. If you are a networking guru, you should be able to skip this part. For those new to networking, some of this info might be helpful. The best way to explain these terms is to use a gated community analogy.

The computer network is like a hoity-toity gated community.

The computer is like a house in that community.

The IP Address is like the house address. But in networking terms, the IP address is specified with 4 numbers, each separated by a period. For instance, 192.168.200.1 is a valid IP address.

The port number is like a door into the house. A house can have many doors, like the front door, the garage door, the backyard door, etc. A computer also has many port numbers. And each port number allows access to a certain part of the computer.

DHCP is like the home association president who determines which house gets which address. This dude assigns addresses to each house in the neighborhood. DHCP assigns IP addresses to each computer in the network.
The one small problem is that DHCP can change the address at any time. This can cause problems and we will try to work around it later.

The firewall/router/NAT is like the security post. The security guy only allows certain people in. The firewall/router/NAT restricts the type of data that goes into the network.

The MAC ID really has no counterpart. The MAC ID is a large sequence of letters and numbers that uniquely identify a computer. The MAC ID never changes. It is always the same. The MAC ID is assigned to a computer when
the computer is built. Well technically, the MAC ID is tied to the network
card and not the computer, but for our purposes, it doesn't matter. Just remember that MAC ID cannot change. IP addresses can change.

There is just one more piece of info that you should know. The entire community is hidden behind the security post. This is important. A visitor simply sees the security post and to the visitor, it just looks like one small dinky little house. In the same way, the global Internet only sees the router. The Internet does not know there are multiple computers attached behind the router. To get to the front door of a particular house, you need the address of the security post, and then the security post can tell you the address of the actual house.

When you sign up for a broadband account, the service provider uses DHCP to assign one IP address to the router. This is very important to understand.
To get to the Stoker, you need to know the IP address of your router provided by your ISP, and then your router will help you find the Stoker.
The problem is your ISP uses DHCP and so the router address can change at any time! There are ways to work around this.

Part 1: Get to know your home network eqiupment.
There are so many different combinations of network configurations that it is impossible to describe all of them. But if you have a broadband connection, you probably a pretty common configuration.

You probably have a piece of equipment from the cable company or phone company called a modem. This modem is basically an adapter. On one is is either the cable or phone line and on the other end is the ethernet cable.

Usually these modems only have one ethernet cable plug. So, you probably have a router that has a bunch of ethernet plugs (and maybe wireless internet capabilities) that allows for you to share the Internet connection with many other computers. The other main function routers provide is security. Most routers make it difficult for hackers to attack your network.

I have seen modems that have the router integrated so you might have one of those, but it's pretty much that same as the two separate pieces of equipment.

Ok, here is where it starts getting technical. When you installed your router, you should have been given a way to configure the router. Usually, this involves opening up your web browser, and typing in address like

http://192.168.1.1

Or maybe the router installation program created a shortcut on your desktop.
Either way, you need to be able to configure your router. These websites are usually password protected so you'll have to know your username and password for your router. Unfortunately, these differ from router to router and manufacturer to manufacturer, so you'll have to determine these yourself. Hopefully you wrote them down or still have the manuals handy.
The manuals have the default username and password in them.

I highly suggest just clicking on the menu options to get yourself familiar with the GUI. If you think you messed up, just click the "Cancel" button or simply close the web browser. If all else fails, unplug the power to the router and plug it back in. This seems to solve a lot of problems.

Part 2: Configure your home network

The routers usually have DHCP enabled. This means the router is the crazy HOA president assigning address to all the computers. We want to stop Mr.
Crazy DHCP, because we need the Stoker to always have the same address. This is necessary or the Stoker may sometimes work and sometimes not, depending on Mr. Crazy DHCP.

But we also want other computers to keep working. So we will not be entirely shutting off DHCP.

In your router setup, there should be a way to assign a specific IP address to a specifc MAC ID. I use a lot of Netgear products and this configuration is usually under "Address reservation" or "LAN IP setup". The GUI is pretty good and it is pretty easy to assign a specific IP address for the Stoker.

In general, I would suggest:
1) unplugging all other computers expect the Stoker and your own PC
2) make sure Stoker has a good IP address by testing it with your PC
3) Open up your router configuration
4) Look at the status and find a list of currently attached devices. The Stoker should be the entry that ISN'T your PC.
5) Write down the MAC address
6) Find the page that allows the IP address and MAC ID association
7) Associate the Stoker MAC address with the Stoker's current IP address

We are now ready for the next step.

Part 3: Allow outside Internet traffic into your home network At this point the home network is stable from the Stoker's point of view.
The Stoker is always going to get the same IP address. Now, we need to allow outside Internet traffic to access your home network. To do this, we need to talk to the security guard.

The router is built to prevent what we are trying to do. So we have to ask it to put its guard down. We do this by a process called port forwarding.
Basically, we tell the security guard "if you happen to get a visitor asking for a web page, then send that visitor to the Stoker".

Ok, back to the router configuration. You will need to find the page for port forwarding. There should be a way to create a custom entry (or service). The service requires two numbers. The IP address of the destination computer, in this case the IP address of the Stoker, and the number 80. 80 is the port number used by all web browsers to get web pages.

Once the service has been configured, all requests for a web page at the router will result in the Stoker getting that request and the Stoker serving up the web page.

The one missing piece is the router's IP address. This should be found in a status page on the router. This is the IP address you will need to access Stoker from the outside.

And that's it!

You go to your friends house with the router's IP address. You open up your friend's web browser and type in the IP address of your router. The magic of the internet generates a request at port 80 at your router. The router sees the port 80 request, sees that there is a port forwarding entry for port 80, and so forwards that request to the IP address of Stoker. The Stoker sees the request, serves up the page and voila!

Part 4: ISP DHCP

So the only part of this process you can't controll is the IP address given to your router by the ISP. The ISP can change it at any time. However, most of the time, ISP really don't change IP address. Maybe every couple of weeks. Maybe.

But if you are concerned about it, there is a way to work around it by a free service called DynDNS. http://www.dyndns.com is the website. This setup of this is out of the scope of this document, but if there is enough interest, perhaps we can write another document.