

# Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Port Forwarding For RAT's Explained \[TUTORIAL\]](#)

InZanitY - December 29, 2011, 12:55 pm

This is my first tutorial; if you have any suggestions or comments please post in this thread :)

Port Forwarding for RAT's (and other applications) explained

What is port forwarding and why do I need it?

Port forwarding is used to communicate certain services between two networks which are generally separated with a router. In our example, when we want to use a RAT, your slaves try to connect to your public IP address (your "internet" ip). This is the address of your router. In order to connect your slaves from your router to your local machine, the router needs to know where to send this traffic. This is where port forwarding kicks in.

Let's say your public IP is 12.34.56.78 and your local IP is 192.168.1.10. Your RAT uses, for example, port 100. You have set up no-ip to connect to your public IP address. Your slaves will thus try to connect to example.no-ip.com:100 which will be translated to 12.34.56.78:100 (in which 100 is the port). When your router receives this traffic, you want the router to send this traffic to your local IP address so you can connect the slaves to your RAT client. The only thing your router "knows" is the port. The router will then look in the port table to see which local IP address is associated with port 100. If you have set up port forwarding correctly, your router will look up port 100 and see this traffic needs to be routed to 192.168.1.10 (your local IP address).

I've made a drawing to explain it a bit clearer:

[img]<http://img39.imageshack.us/img39/4226/portforwardingmap.jpg>[/img]

What do I need to set up port forwarding?

## 1. Access to your router

You will need to have access to your router to configure the port you want to forward to your IP address. You can access the configuration page of your router by typing the router's IP address in the address bar of your browser. If you do not know this address, you can find it by opening a command prompt window (start -> all programs -> accessories -> command prompt), typing "ipconfig" (without quotes) and pressing enter. The default gateway address is the address of your router.

[img]<http://img856.imageshack.us/img856/5315/ipconfig.gif>[/img]

When you go to this address in your browser, you will probably be asked for a username and a password. When you do not know this, you can try the routers default password. Simply look in the routers manual or download your routers manual from the manufacturers website. Alternatively, you can google your default login or go to <http://www.routerpasswords.com/>.

## 2. A static IP address

In order to keep your IP address the same as the one in the port forwarding table, you need a static IP address. Most home networks use DHCP, this is a protocol to automatically assign an IP address

from a certain address range to a NIC (network card) when the computer boots up. It is possible that when you reboot your pc your router will assign a different IP address to your NIC then you had before, but the port will still be forwarded to your old IP address. Obviously you need to keep the same IP address all the time.

First, you have to pick the IP address you are going to assign to your NIC. This has to be an address which is not in use, so you cannot pick an address which is in the DHCP address pool (the addresses automatically assigned to other machines in the network). You can find this address range somewhere in the configuration page of your router. I've made a screenshot of my router's DHCP configuration:

[img]<http://img836.imageshack.us/img836/5559/dhcpm.jpg>[/img]

As you can see, my starting ip address of the DHCP pool is 192.168.1.31 and there are 50 addresses in the pool. This means I cannot use all the addresses between 192.168.1.31 and 192.168.1.81. Note that this may look different on your router. Other addresses I cannot use are other used static IP addresses on the network like 192.168.1.1 which is used by my router. As you can also see, I have a subnet mask of 255.255.255.0. You will most likely have the same. The subnet mask determines the number of IP addresses in your network. A subnet mask of 255.255.255.0 means all the addresses between 192.168.1.1 and 192.168.1.255 are valid network addresses on your network. Beware: one other address which is already in use is 192.168.1.255. This is not used by a machine, this is the broadcast address. With this address you contact all the other addresses on the network. This is for example used for messages which contain information about a network change. You'll never need to use this address yourself, this is all done by services. In my example, 192.168.1.10 is a free address which I'm going to use for my PC. Note that it is possible to have a different IP range on your network, for example 192.168.0.X or 10.0.0.X. Just take the same steps as I've done but with your IP range.

### Setting up port forwarding

In order to set up port forwarding there are 2 things we need to do. First we need to assign the static IP address you just chose to your network adapter. In my case this is 192.168.1.10. You also need your subnet mask and your default gateway. You can also find this through the ipconfig command.

In order to configure your network adapter you need to go to control panel -> network and sharing center. In the left pane click "Change adapter settings". You will get this screen:

[img]<http://img32.imageshack.us/img32/6020/adapterad.jpg>[/img]

Right click the adapter you are using and click properties. You will get this:

[img]<http://imageshack.us/a/img215/3848/lanproperties.jpg>[/img]

Right click "Internet Protocol Version 4 (TCP/IPv4)" and click properties. Now fill in the addresses you have found. For DNS server use the same address as your default gateway. See the example below to see how I did it with my addresses.

[img]<http://img832.imageshack.us/img832/9176/staticipy.jpg>[/img]

When you're done click OK.

Now we have configured a static IP address we need to forward our port to this address. You need to go to the router configuration page to do this. This is different for every router, so if you cannot find this yourself you could google "port forwarding <insert routertype here>".

In my router, a Draytek Vigor 2130, it's under "NAT -> Open Port".  
I've configured it using my port and local IP like this:

[img]http://img851.imageshack.us/img851/4980/forwardrtr.jpg[/img]

Use TCP+UDP; different rats use different protocols for different types of transfers, use them both to be sure.

Once you have opened this port to your local IP you're ready to test your port. You can use a website like [canyouseeme.org](http://canyouseeme.org). Note that you will need to listen on the port with an application (like your RAT) to get a response. If you're not listening on your port you will probably get a false negative.

The last step: drink beer!

[img]http://img857.imageshack.us/img857/7716/73406426.jpg[/img]

This was my tutorial on port forwarding. I hope you guys liked it for a first tutorial. If you have any questions please post in this thread, I will try to answer them as fast as I can.

Gratz and have fun ratting! ?

**x64** - December 29, 2011, 1:13 pm

Very nice tutorial about portforwarding. +1 rep

**MoneyXchang3R** - December 29, 2011, 1:17 pm

I follow all the steps correctly every time I try and portforward. But yet it doesn't work, I've disabled my firewall, tried different ports, everything. It's really frustrating

**Maple ??** - December 29, 2011, 1:35 pm

Very good tutorial. If anyone asks me how to PF because they have PF trouble I will defiantly direct them here. Keep up the good work.

**InZanitY** - December 29, 2011, 3:27 pm

Thanks for the comments! :)

@ Primacy, have you checked the firewall settings on your router? Some routers have a built in firewall with a setting to block all ports which will override any port forwarding rules. Also, if your router has a DMZ option, you need to make sure this is disabled.

**Zero®** - December 29, 2011, 4:39 pm

thanks for the help, I think my RAT is finally working...

**InZanitY** - December 30, 2011, 1:59 am

No problem mate, just trying to do something back :)

**Pr0xyg3n** - January 17, 2012, 1:57 am

Damn, i suck at Port Forwarding >\_> I think i'm stuck behind 2 routers though... Win firewall off, DMZ off, Av off, UDP and TCP forwarded and still no luck! ?

**Irreplaceable** - January 29, 2012, 3:23 am

i got 1 question. when i fill the stuff in this part: "Internet Protocol Version 4 (TCP/IPv4)" and click properties."

my ip4 shows the: 10.0.0.3 and there is no 192.168.1."x"  
how come? did i do something wrong?  
please help me out:D

PM me please.

**D3tin** - January 29, 2012, 4:02 am

Awesome tutorial mate, thanks for this.

**Ricar70** - February 4, 2012, 10:06 am

Nice tutorial about portforwarding... awesome!  
Thanks for sharing.

**Mr. RawrGasm** - February 4, 2012, 10:39 am

Umm i did the last step first, is that bad? X)

**InZanitY** - February 9, 2012, 2:06 pm

(Feb 4, 2012 11:39 AM)Mr. RawrGasm Wrote: [\[CITE\]](#) Umm i did the last step first, is that bad? X)  
Nope thats good! No port forwarding without beer! Cheers!

**undera** - February 9, 2012, 5:36 pm

very helpfull tut. helps me a lot . thanx . keep the nice work

**Justice** - February 9, 2012, 5:58 pm

NICE tutorial man, way to give back to the community! great job. =]

**dishnitup** - February 9, 2012, 6:37 pm

Ok, now i understand this. I can go home tonight and get at least this far. Now i have to figure out how to go after the people I want. Also, how do I go about hacking other computers on the same router I am on? This tut seems to get me outside my router. Any further advice is welcome. Thanks a ton!!

**Spreader** - February 9, 2012, 6:49 pm

Can I have the Beer plz!...hik...hik...

Good TUT buddy!Will be helps many new members!Keep it up!  
xBlackHatx (my acc is closed Reason: idk)

**Goldman4** - September 23, 2012, 2:44 pm

Cool but i and not the best at this stuff thanks tho ! :)

**MexxR** - September 23, 2012, 2:57 pm

Thanks ALOT man! Been sitting hours trying to figure out why my port wouldnt open, followed this step by step and now it's open!

Again, Thanks alot for sharing this! ?

**Snoilspb** - September 23, 2012, 3:17 pm

omgg all this is so confusing loli am so lost on these forums

**Jeny** - September 23, 2012, 3:36 pm

Thanks for the tutorial buddy! This will help me a lot.

mdmguyon - September 24, 2012, 10:54 pm

I got lost at the step of "go to control panel ->network and sharing center." I have no "network and sharing center." I have "Network Connections," but then there's no "Change adapter settings" in the left pane.

InZanitY - September 25, 2012, 3:48 pm

(Sep 24, 2012 10:54 PM)mdmguyon Wrote: [\[CITE\]](#) I got lost at the step of "go to control panel ->network and sharing center." I have no "network and sharing center." I have "Network Connections," but then there's no "Change adapter settings" in the left pane.

You probably have windows xp. Right click on your network adapter and click properies, then select IPv4 and click properties to change your IP.

mdmguyon - September 26, 2012, 4:24 am

(Sep 25, 2012 03:48 PM)InZanitY Wrote: [\[CITE\]](#) You probably have windows xp. Right click on your network adapter and click properies, then select IPv4 and click properties to change your IP.Yes, I have Windows XP. It took a while, since I don't know how to right click on my network adapter, but I think I found what you're referring to. I had to go to "Control Panel," then "Network Connections," and then "Local Area Connection." I right clicked on that and then clicked on "Properties." Under "General," it said "Internet Protocol (TCP/IP)," which I highlighted and then clicked on "Properties." Only then did I see something similar to what your tutorial referred to. "Obtain an IP address automatically" and "Obtain DNS server address automatically" were selected. I can see where I can enter numbers for addresses I select. If I enter an IP address and tell it to use it, does that mean that I will have that as a static IP address? Another tutorial suggested using no-ip.com to get a static IP address. Why would anyone do that when it can be done this way? How can I be sure that the address I select is available?

InZanitY - September 26, 2012, 5:33 am

(Sep 26, 2012 04:24 AM)mdmguyon Wrote: [\[CITE\]](#) Yes, I have Windows XP. It took a while, since I don't know how to right click on my network adapter, but I think I found what you're referring to. I had to go to "Control Panel," then "Network Connections," and then "Local Area Connection." I right clicked on that and then clicked on "Properties." Under "General," it said "Internet Protocol (TCP/IP)," which I highlighted and then clicked on "Properties." Only then did I see something similar to what your tutorial referred to. "Obtain an IP address automatically" and "Obtain DNS server address automatically" were selected. I can see where I can enter numbers for addresses I select. If I enter an IP address and tell it to use it, does that mean that I will have that as a static IP address? Another tutorial suggested using no-ip.com to get a static IP address. Why would anyone do that when it can be done this way? How can I be sure that the address I select is available?

As you can see in the drawing, your router has a public IP that's accessible through the internet. The public IP address of your router may change, so you can use a dynamic DNS service to link a domain name to your ip address. no-ip is such a service. When you set it up, you install a little program, no-ip duc, which checks your public IP address every few minutes and when it changes updates your no-ip hostname. Your no-ip domain will thus always be linked to your public ip address. This is the address of your router's port connected to the internet though. We use no-ip because our internet provider does not allow us to set up a static IP on our internet connection. Another advantage is that you can always update the no-ip name to another ip address, this can happen if you move or you change ISP's.

Behind your router, on your local network, every machine has it's own local address. Because your the boss of your local network you can set up a static ip, which is much easier then setting up dynamic DNS on your local network. To check which addresses are available, go into your routers configuration, find the DHCP configuration and check which addresses are in the DHCP pool. These are the addresses your router may assign to a machine requesting to get an IP address. Don't use the adresses in this range, or the address of your router (like I say in the tutorial), and you'll be fine.

Your network adapter's tcp/ip configuration should look like the one in my tutorial, just follow my

steps.

?**Dante** - *September 26, 2012, 5:55 am*

Nice work out there InZanitY...

I'd rep+ you if i can.

~dantehh...?