

Re: What Port Should I Use?

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2008-02/msg00130.html>

- *From:* ibuprofin@xxxxxxxxxxxxxxxxxxxxxxxxxxxx (Moe Trin)
 - *Date:* Fri, 15 Feb 2008 20:24:21 -0600
-

On 15 Feb 2008, in the Usenet newsgroup comp.os.linux.networking, in article <47b52835\$0\$20181\$5a62ac22@xx>, Dan N wrote:

Moe Trin wrote:

You can use any port you wish to. You need only live with the consequences.

That's really the crux of the matter, isn't it.

Yup. RFCs are interesting standards. They detail an expectation of how things are to work. You are absolutely allowed to do anything YOU want to do, but if you expect to work with others, then here are some good ideas you should follow.

If I start up my server using a port in the dynamic/private range then I run the risk that the port is already in use by some client on the same host.

```
[compton ~]$ /bin/netstat -antu | grep -c tcp
2
[compton ~]$
```

So there are 2 ports in use out of 65000 – I'd say that's pretty good odds, wouldn't you? Sure, a lot depends on what you are doing with your system and I can't answer to that. As a general statement, systems meant to be offering network services are not meant to be ALSO be being used by J. Random Luser as his workstation. Looking at the servers on my home LAN, the file servers have about 60 ports in use. The print server has two. The gateway box has three.

Re: What Port Should I Use?

When the client started, the tcp stack would have dynamically assigned it a port and that just might be the one that I want my server to listen on.

Many people tend to start running servers before any client crap is started. Depending on your kernel, you may discover that ephemeral ports used client-side TEND to run over the range of perhaps 1025–32760 or so.

So this doesn't seem like a good option. This leaves me with ports in the well known or registered ranges.

Have you looked at what is running on your server? Are there really that many ephemeral ports in use? If so, then yes you may want to consider using something in the well known range – because the original extra feature about those ports was that a server listening on those ports was not likely to be a user-land process except in really strange (individual) situations.

But if I want to adhere to standards what port do I use? IANA says that the well known and registered ports shouldn't be used without registration. And my server is using a proprietary protocol that I really don't have any need to register.

You would want to choose a port based on inter-operability. Do you expect your service will be accessed by strangers from outside? If no, then you can do exactly what you want to do. Your LAN, your rules. Are you concerned that a packet escaping from your LAN may cause the Internet Gods to cloud up and rain on you? That's a perimeter firewall issue, but probably not a major concern. If your server is using a proprietary protocol, it just means that outsiders will have to come to you to get the details. Again, probably not a big factor.

The only choice I seem to have is to not adhere to standards. The conclusion I've come to is to use a port somewhere in the registered range.

Grab a copy of RFC0793 from your favorite website:

0793 Transmission Control Protocol. J. Postel. September 1981.
(Format: TXT=172710 bytes) (Updated by RFC3168) (Also STD0007)
(Status: STANDARD)

and look at the top of page 5, in the section "Multiplexing:". Here is the second paragraph in that section:

Re: What Port Should I Use?

The binding of ports to processes is handled independently by each Host. However, it proves useful to attach frequently used processes (e.g., a "logger" or timesharing service) to fixed sockets which are made known to the public. These services can then be accessed through the known addresses. Establishing and learning the port addresses of other processes may involve more dynamic mechanisms.

```
[compton ~]$ zcat rfcs/rfc-index.* | sed 's/^\$/%/ ' | tr -d '\n' | tr '%'  
\n' | grep '^[0-9]' | tr -s ' ' | grep -v 'Not Issued' | sed 's/.*/Status:  
/' | tr -d '\n' | sort | uniq -c | column  
145 BEST CURRENT PRACTICE 1564 INFORMATIONAL  
135 DRAFT STANDARD 1667 PROPOSED STANDARD  
288 EXPERIMENTAL 88 STANDARD  
210 HISTORIC 909 UNKNOWN  
[compton ~]$ zcat rfcs/rfc-index.* | sed 's/^\$/%/ ' | tr -d '\n' | tr '%'  
\n' | grep '^[0-9]' | tr -s ' ' | grep -c 'Not Issued'  
80  
[compton ~]$
```

As of 2 February 2008, there were just over 5000 RFCs available, but not one of them **REQUIRES** that a service listening on port \$FOO must be \$BAR and \$BAR must be available on port \$FOO if it is running. There is nothing in those documents that requires anything except for interoperability. If you aren't concerned that an outsider may not know how to connect to your server, I don't think to many other people will care either. If you expect to have others connect, then you may want to be following some of the standards (did you notice that there are just 88 RFCs identified as "STANDARD" – a lot of drafts and proposals, but not that many) – like maybe RFC0894 (Ethernet), RFC0791 (IP), RFC0793 (TCP) so that your packets can pass over the wire but following the Ethernet standard[s] doesn't imply that you must **ALSO** follow IPv4 (never mind IPv6, Novell IPX, Banyan VINES, Appletalk, or any of the 65000 possible protocols including the 184 ethertypes identified by <http://www.iana.org/assignments/ethernet-numbers>).

If you've been looking at your firewall logs, you may have discovered that every zombie on every broadband network in the world is trying to connect to your 22/tcp and 25/tcp – because that's where the SSH and MTA servers should be listening **IF THEY EXIST**. Must they be on those ports only? Not really. My SSH access to my LAN uses a port quite different from 22/tcp – and the poor zombies can't connect to it. Isn't that simply terrible? I'm breaking the Internet rules – I'm gonna go to jail! Am I able to connect to my systems from outside? Yes. Do you think that I care that unauthorized hosts can't seem to do so? ;–)

Old guy
.