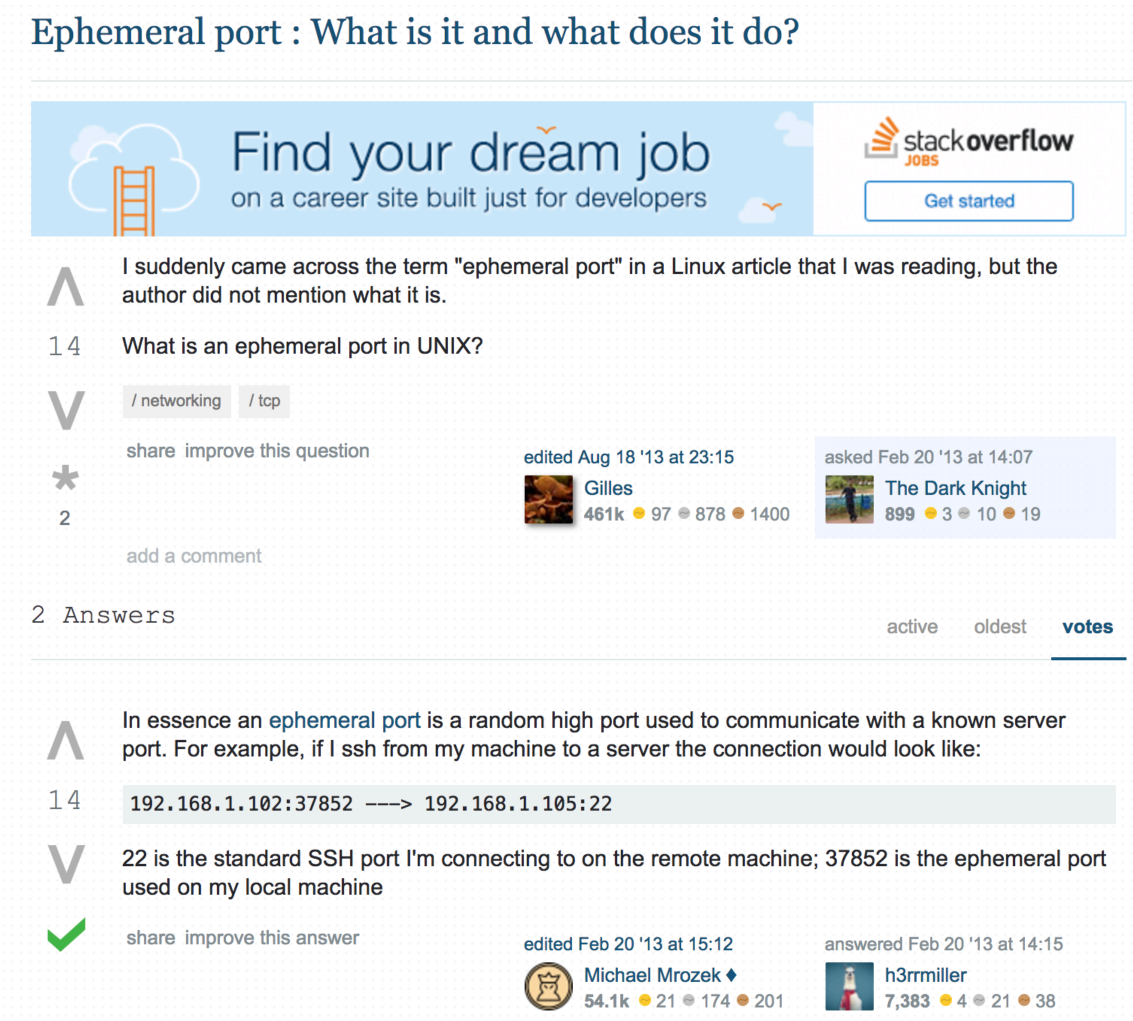
Ephemeral Ports



Ephemeral port : What is it and what does it do?

14

I suddenly came across the term "ephemeral port" in a Linux article that I was reading, but the author did not mention what it is.

What is an ephemeral port in UNIX?

/ networking / tcp

edited Aug 18 '13 at 23:15
Gilles
461k ● 97 ● 878 ● 1400

asked Feb 20 '13 at 14:07
The Dark Knight
899 ● 3 ● 10 ● 19

2 Answers

14 ✓

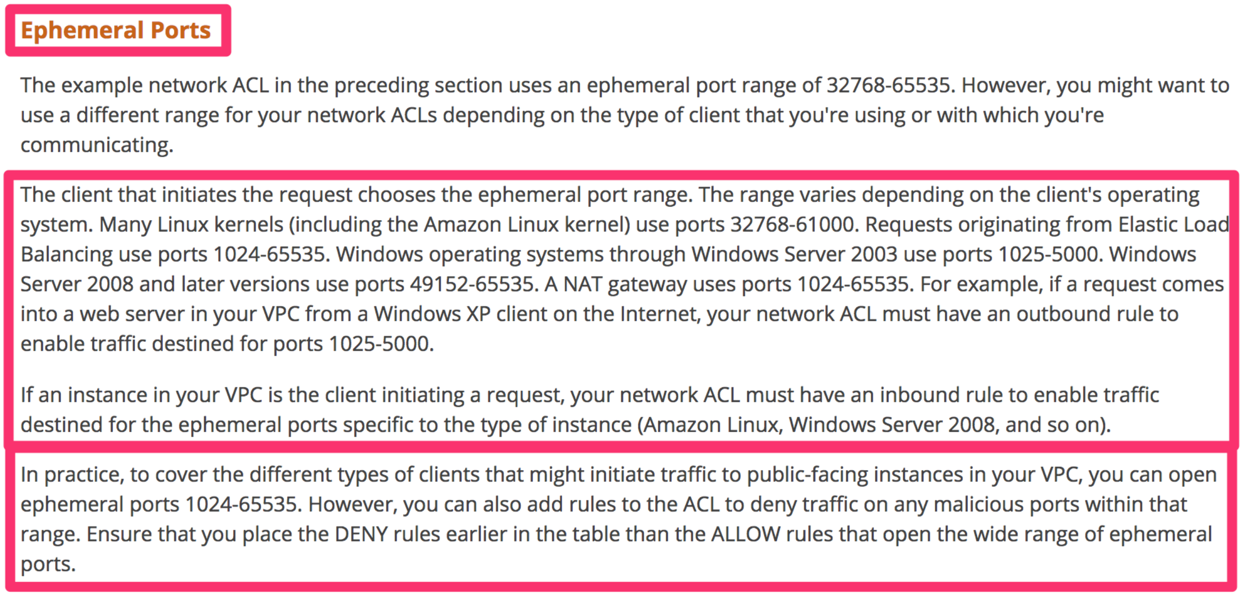
In essence an ephemeral port is a random high port used to communicate with a known server port. For example, if I ssh from my machine to a server the connection would look like:

```
192.168.1.102:37852 ---> 192.168.1.105:22
```

22 is the standard SSH port I'm connecting to on the remote machine; 37852 is the ephemeral port used on my local machine

edited Feb 20 '13 at 15:12
Michael Mrozek ♦
54.1k ● 21 ● 174 ● 201

answered Feb 20 '13 at 14:15
h3rrmiller
7,383 ● 4 ● 21 ● 38



Ephemeral Ports

The example network ACL in the preceding section uses an ephemeral port range of 32768-65535. However, you might want to use a different range for your network ACLs depending on the type of client that you're using or with which you're communicating.

The client that initiates the request chooses the ephemeral port range. The range varies depending on the client's operating system. Many Linux kernels (including the Amazon Linux kernel) use ports 32768-61000. Requests originating from Elastic Load Balancing use ports 1024-65535. Windows operating systems through Windows Server 2003 use ports 1025-5000. Windows Server 2008 and later versions use ports 49152-65535. A NAT gateway uses ports 1024-65535. For example, if a request comes into a web server in your VPC from a Windows XP client on the Internet, your network ACL must have an outbound rule to enable traffic destined for ports 1025-5000.

If an instance in your VPC is the client initiating a request, your network ACL must have an inbound rule to enable traffic destined for the ephemeral ports specific to the type of instance (Amazon Linux, Windows Server 2008, and so on).

In practice, to cover the different types of clients that might initiate traffic to public-facing instances in your VPC, you can open ephemeral ports 1024-65535. However, you can also add rules to the ACL to deny traffic on any malicious ports within that range. Ensure that you place the DENY rules earlier in the table than the ALLOW rules that open the wide range of ephemeral ports.

Make sure you don’t open unnecessary ports for inbound traffic in NACLs, as they posses a great security risk.