

## How do I know I have the right firewall ports open?

Last updated on May 28, 2015 05:35PM EDT

Livestream for Producers, Procaster, and the Livestream Studio software (as well as the Broadcaster device) stream through a number of internet ports, which need to be made open to both incoming and outgoing communication.

In (rough) order of importance, they are

- **TCP 1935**
- **TCP 80**
- **TCP 443**
- **UDP 53 \***

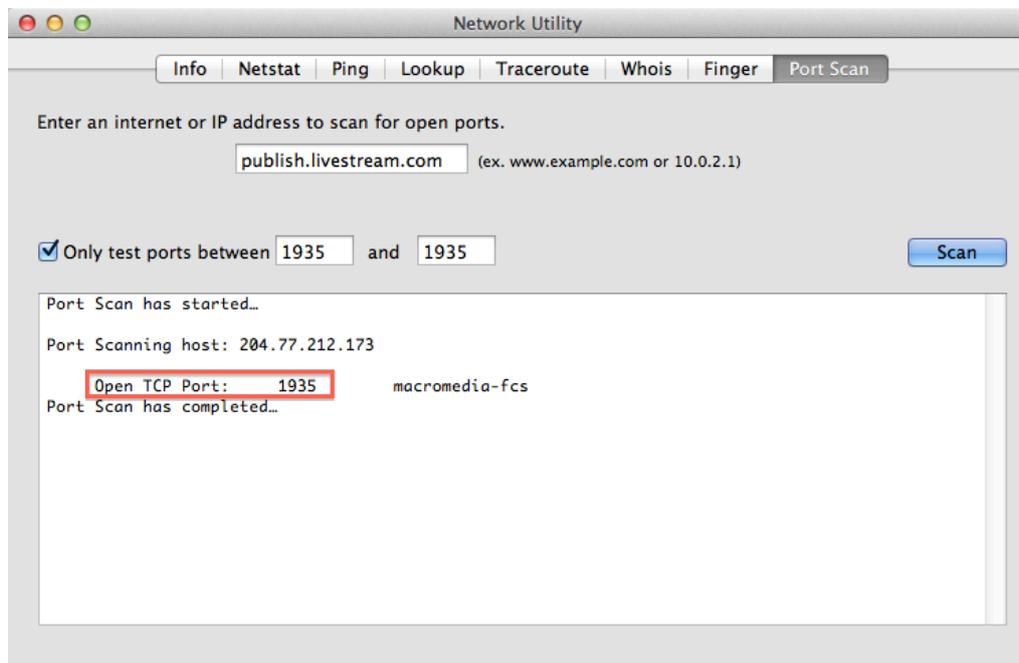
(\*Many corporate and academic networks' security policies will block this port, as it provides DNS.)

One or more of these ports may be blocked by firewalls. A firewall can be located on the network and/or on the computer itself. We generally recommend disabling any anti-virus programs at the time of your stream (ex: Norton, McAfee, AVG, Windows Security Essentials, etc. Be sure also to disable Windows Firewall). Apart from consuming valuable CPU resources, many will block one or more of the necessary ports needed for streaming.

If a firewall is on the network, these ports would need to be opened by an IT/network technician. It is possible, though, to check the status of these ports at any time:

### For OSX:

1. Open the "**Network Utility**" Tool.
2. Select the "**Port Scan**" tab.
3. Enter "**publish.livestream.com**"
4. Enter the port(s). If you want to test a specific port, enter only that port in the fields.



Port 1935 is open and ready to go.

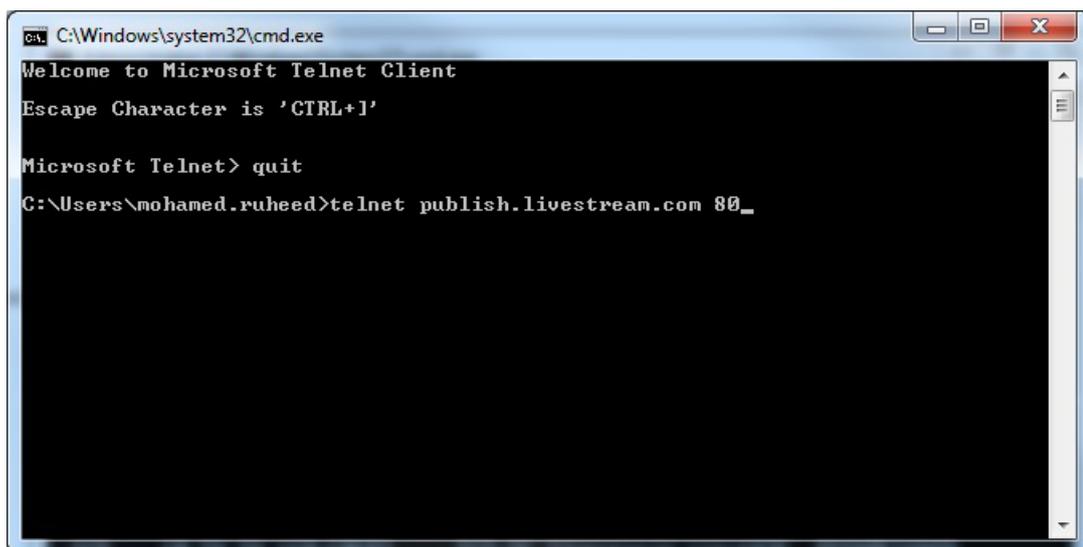
### For Windows:

*Telnet is NOT enabled by default on Windows 7 and Vista. To enable it:*

1. Start → Search for "*Turn Windows features on or off*" and select the option from the list.
2. Once the box appears, look for "**Telnet Client**". Enable it and click *OK* (it may take a few minutes for it to fully take effect).

Then:

1. Open the Command prompt (Start → Search for "*cmd*")
2. Type the command as shown in the image below (*publish.livestream.com* + "port" if testing a specific port.)

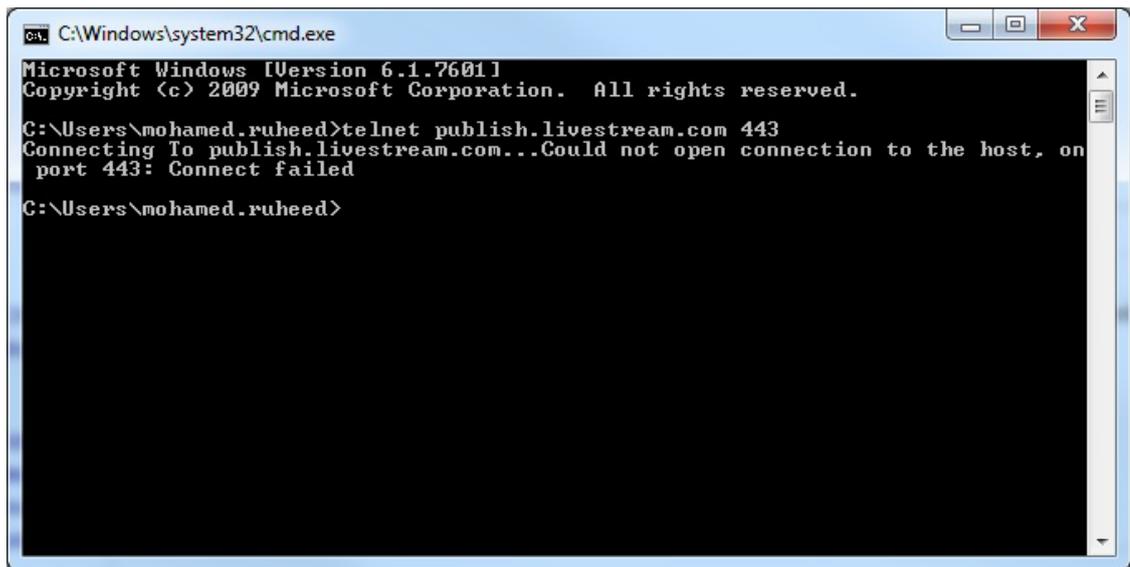


```
C:\Windows\system32\cmd.exe
Welcome to Microsoft Telnet Client
Escape Character is 'CTRL+I'

Microsoft Telnet> quit
C:\Users\mohamed.ruheed>telnet publish.livestream.com 80_
```

3. After typing the command (in this case "***publish.livestream.com 80***"), you will see a blinking cursor for a period of time, indicating that the connection was successful. (Use "***ctrl + J***" to quit telnet.)

4. If the connection fails, you'll see the following message:



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\mohamed.ruheed>telnet publish.livestream.com 443
Connecting To publish.livestream.com...Could not open connection to the host, on
port 443: Connect failed

C:\Users\mohamed.ruheed>
```

You can also listen to open ports on your network using the *netstat -f* command (the *-f* parameter forces the destination to resolve to its domain equivalent.)

```

Administrator: C:\Windows\System32\cmd.exe
.com:https CLOSE_WAIT
TCP 10.29.29.160:58589 a23-206-254-161.deploy.static.akamaitechnologies
.com:https CLOSE_WAIT
TCP 10.29.29.160:58590 a23-206-254-161.deploy.static.akamaitechnologies
.com:https CLOSE_WAIT
TCP 10.29.29.160:58591 a23-206-254-161.deploy.static.akamaitechnologies
.com:https CLOSE_WAIT
TCP 10.29.29.160:58592 a23-206-254-161.deploy.static.akamaitechnologies
.com:https CLOSE_WAIT
TCP 10.29.29.160:58593 a23-206-254-161.deploy.static.akamaitechnologies
.com:https CLOSE_WAIT
TCP 10.29.29.160:58813 event.ia3.adxpose.com:http CLOSE_WAIT
TCP 10.29.29.160:58980 213-31.livestream.com:http CLOSE_WAIT
TCP 10.29.29.160:59354 maa03s04-in-f13.1e100.net:http CLOSE_WAIT
TCP 10.29.29.160:59689 nsemar.com:http CLOSE_WAIT
TCP 10.29.29.160:59692 nsemar.com:http CLOSE_WAIT
TCP 10.29.29.160:59952 ec2-184-72-50-95.us-west-1.compute.amazonaws.com
:https CLOSE_WAIT
TCP 10.29.29.160:60252 linkedin-ela4.com:http ESTABLISHED
TCP 10.29.29.160:60593 ec2-54-243-105-116.compute-1.amazonaws.com:http
CLOSE_WAIT
TCP 10.29.29.160:60594 ec2-54-243-105-116.compute-1.amazonaws.com:http
CLOSE_WAIT
TCP 10.29.29.160:60681 212-71.livestream.com:1935 ESTABLISHED
TCP 10.29.29.160:60683 212-71.livestream.com:1935 ESTABLISHED
TCP 10.29.29.160:60693 212-71.livestream.com:http ESTABLISHED
TCP 10.29.29.160:60712 117.206.245.52:15816 TIME_WAIT
TCP 10.29.29.160:60812 115.244.239.123:42631 ESTABLISHED
TCP 10.29.29.160:60819 115.244.225.240:55573 ESTABLISHED
TCP 10.29.29.160:60820 static-49.71.99.14-tataidc.co.in:10127 ESTABLIS
HED
TCP 10.29.29.160:60821 124.253.45.146:23956 ESTABLISHED
TCP 10.29.29.160:60822 232.124.206.49-ras.beantele.net:48734 ESTABLISH
ED
TCP 10.29.29.160:60826 221x240x217x162.ap221.ftth.ucom.ne.jp:11526 EST
ABLISHED
TCP 10.29.29.160:60832 221x240x217x162.ap221.ftth.ucom.ne.jp:11526 EST
ABLISHED
TCP 10.29.29.160:60856 static-96.49.97.14-tataidc.co.in:38102 ESTABLIS
HED
TCP 10.29.29.160:60857 pc250023.ztv.ne.jp:47088 ESTABLISHED
TCP 10.29.29.160:60934 212-130.livestream.com:https CLOSE_WAIT
TCP 10.29.29.160:60956 213-72.livestream.com:https CLOSE_WAIT
TCP 10.29.29.160:60958 115.242.11.17:58029 TIME_WAIT
TCP 10.29.29.160:60959 115.241.146.97:1497 TIME_WAIT
TCP 10.29.29.160:60967 static-247.187.98.14-tataidc.co.in:1473 ESTABLI
SHED
TCP 10.29.29.160:60968 static-141.83.97.14-tataidc.co.in:59687 ESTABLI
SHED
TCP 10.29.29.160:60975 213-72.livestream.com:https CLOSE_WAIT
TCP 10.29.29.160:60990 212-131.livestream.com:https CLOSE_WAIT
TCP 10.29.29.160:60998 maa03s04-in-f23.1e100.net:https ESTABLISHED
TCP 10.29.29.160:61004 180.215.192.85:50209 ESTABLISHED
TCP 10.29.29.160:61028 maa03s04-in-f13.1e100.net:http ESTABLISHED
^C
C:\Windows\system32>

```

From the above image, you can see that TCP connections for 212-71.livestream.com:1935 and 212-71.livestream.com:http were ESTABLISHED successfully, while TCP connection for 212-130.livestream.com:https and 213-72.livestream.com:https shows as CLOSE\_WAIT (which means the connection was closed and is waiting to be authenticated)

*Note: Ports 1935, 80, and 443 represent rtmp, http, and https respectively.*

### IP Range

New Livestream IP Range 204.77.212.0/23 & 204.77.214.0/24