ON MSFT.com

🐦 f 📌 ▶ 📡

🏠 Home   📰 How-To   🎮 Xbox   🎙 OnPodcast   📁 M365 / O365   ⊞ Windows 10

👥 Windows Insider

How to configure port forwarding on a Windows 10 PC
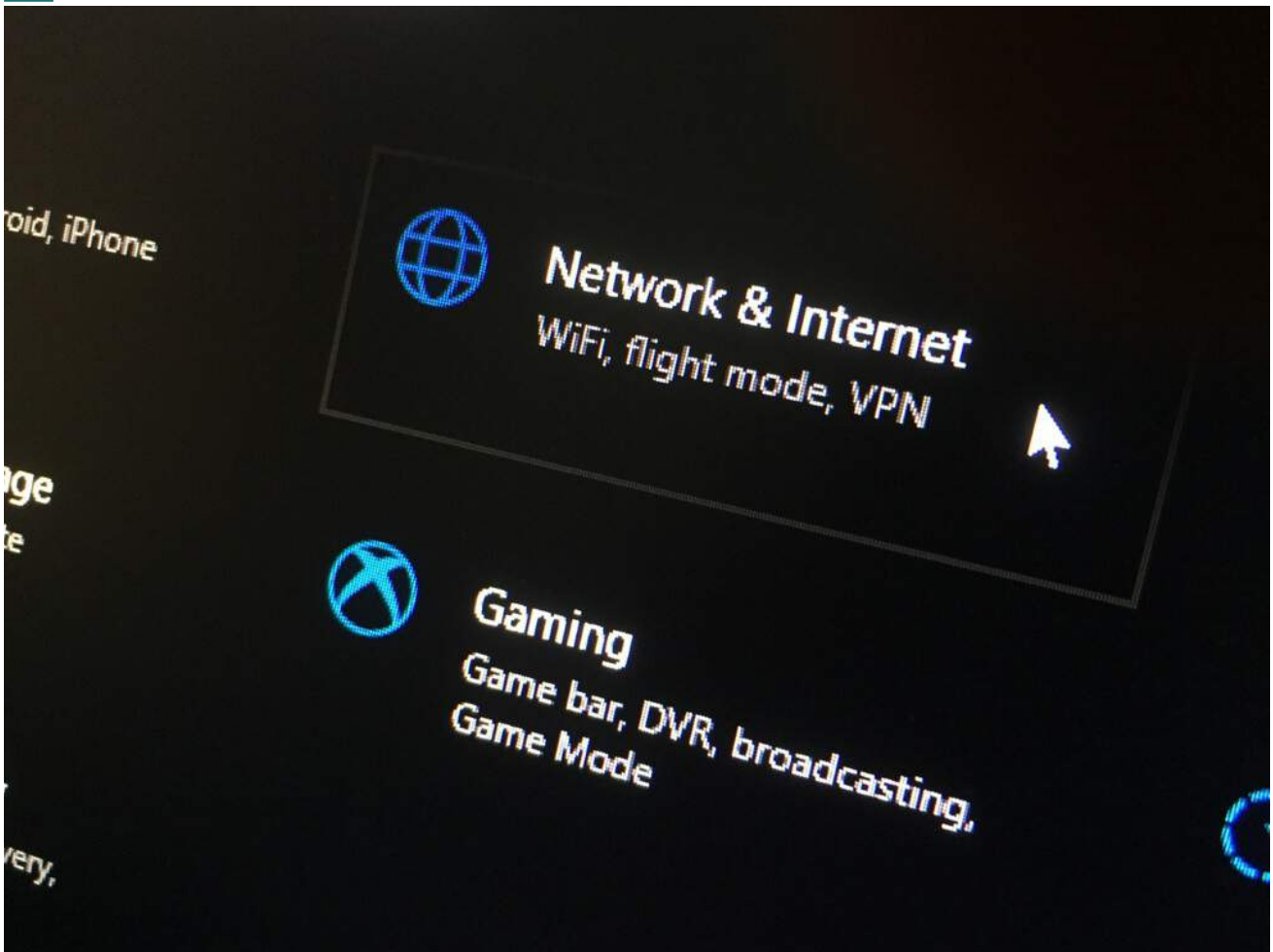
by **James Walker**

✉ **Email**   Twitter: **@jheronwalker**   Jun 3rd, 2019 in **How-To**

### 📰 How to configure port forwarding on a Windows 10 PC

To port forward 127.0.0.1:9000 to 192.168.0.10:80 in Windows 10:

1. Launch an Administrator Command Prompt.
2. Run "netsh interface portproxy add v4tov4 listenaddress=127.0.0.1 listenport=9000 connectaddress=192.168.0.10 connectport=80".

Applies to All Windows 10 Versions

Windows 10 has built-in support for port forwarding but it's not exposed in the Settings interface. Port forwarding allows you to access network resources as if they're hosted on your local machine, which can be helpful when working on a LAN (local area network) or developing with web servers.

In this guide, we'll walk you through adding your own port forwarding rule. For the purposes of this guide, we'll add a rule which routes the address "http://127.0.0.1:9000" to "http://192.168.0.10:80". You'll then be able to visit "http://127.0.0.1:9000" in a browser and view what you would have seen if you'd accessed "http://192.168.0.10:80" directly.
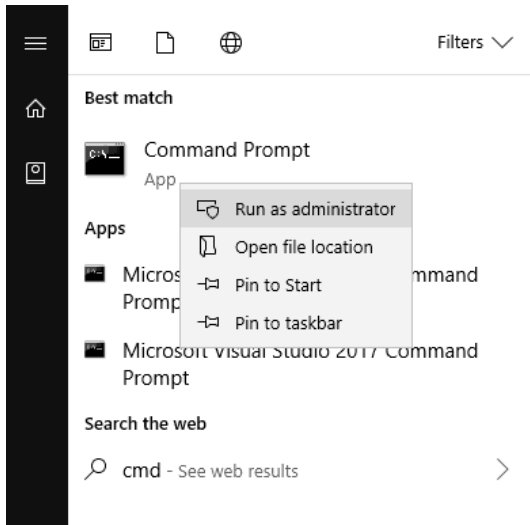
Adding the rule requires use of the command prompt. You'll need to be logged in as an administrator, too. Begin by typing "cmd" into the Start menu. Click the first search result while holding the Control and Shift keys to launch Command Prompt as an administrator.

Next, you'll use the "netsh" command to configure the port-forwarding rule. It's a somewhat long-winded command, so be sure to type it as you see below.

```
netsh interface portproxy add v4tov4 listenaddress=127.0.0.1 listenport=9000 connectaddress=192.168.0.10 connectport=80
```
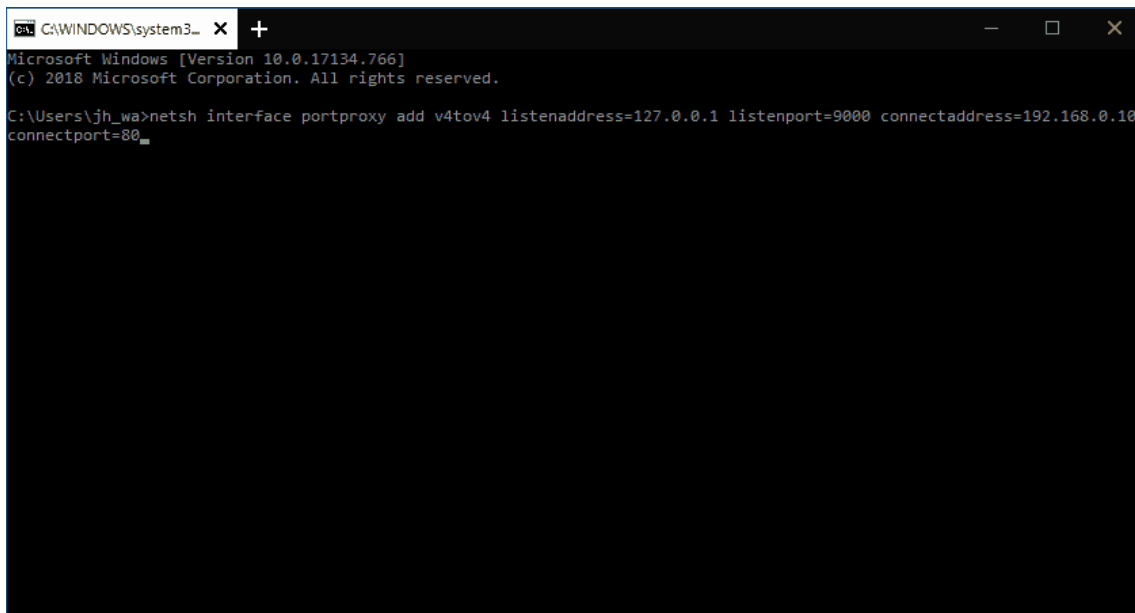

Notice how the values given for "listenaddress", "listenport", "connectaddress" and "connectport" correspond to those we stated earlier. You'll need to make adjustments here to suit the rule you're adding. For example, if you want to route to port 8888 on the device with IP 192.168.0.1, you'd use these values for the "connectport" and "connectaddress" respectively.

When you press enter, the rule will be added and applied immediately. Try visiting the listening address and port in your browser – you should see the content being served by the *connect* address and port.

When it comes time to remove the rule, return to an administrator command prompt and use the following command:
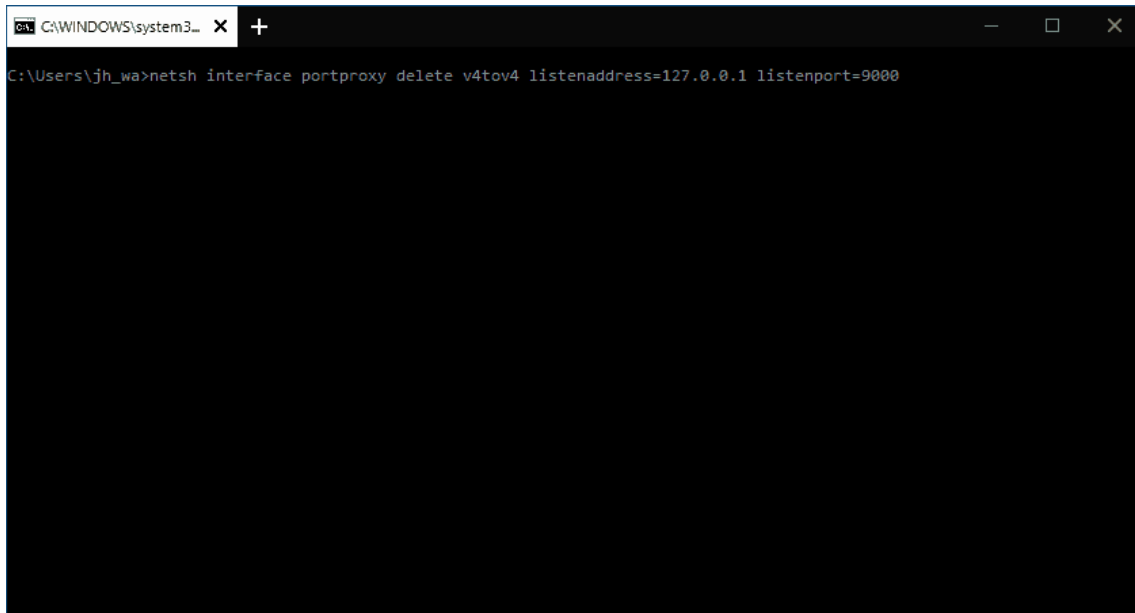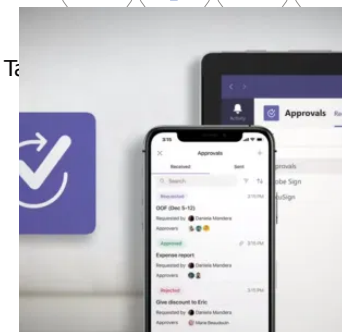
```
netsh interface portproxy delete v4tov4 listenaddress=127.0.0.1 listenport=9000
```

Again, you'll need to adjust the specified listening address and port to match the values you're using. The rule will be deleted immediately and will no longer apply to new network requests.
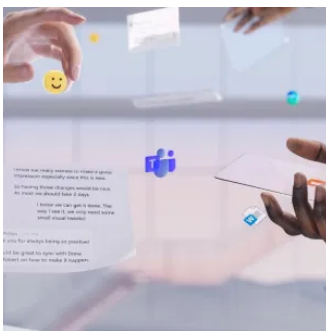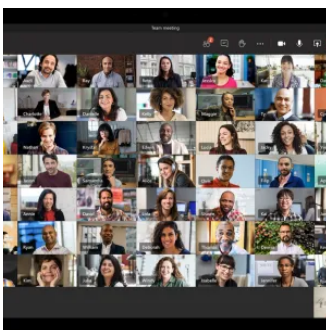
Share This Post:

Trending OnMSFT

The new Approvals app is now generally available in Microsoft Teams, here's how it works

Microsoft Teams introduces new color and styling changes in public preview

How to see everyone in a Microsoft Teams video meeting

Microsoft Forms is getting Text Formating capabilities, new Start Page experience, and more this month

How to password protect a folder or file in Windows 10

About OnMSFT.com
Contact OnMSFT
Privacy Policy
Copyright 2010-2020 OnMSFT.com LLC

Search OnMSFT

What we use:
Azure
Microsoft 365
MS Fabric Core
WordPress / Bootstrap
Simple Social Icons