How To Use Wireshark to confirm Teams Traffic is bypassing your VPN connection:

1. Get IP’s on the client machine for active network connections.

From an administrative command prompt run: ipconfig/all >c:\myipconfig.txt to output the connection info

From an administrative PowerShell: Get-NetIPConfiguration

A screenshot of a cell phone

Description automatically generated

Screenshot from https://www.whatismyip.com/

A screenshot of a cell phone

Description automatically generated

In this example: Internet ip = 10.0.0.132 and public facing is 67.162.34.162

1. If not already installed, then download and install the latest stable release of Wireshark: <https://www.wireshark.org/download.html>
2. Open an instance of Wireshark for each active network connection.

\*The interfaces may appear differently on your client.

A screenshot of a cell phone

Description automatically generated

1. Add filters, then launch and test Teams functionality, for example, join a meeting, make a call, initiate a screenshare.

Filters:

=====

udp.port == 3478 || udp.port == 3479 || udp.port == 3480 || udp.port == 3481 || tcp.port == 80 || tcp.port == 443

udp.port == 3478 || udp.port == 3479 || udp.port == 3480 || udp.port == 3481

stun

Test out whatever Teams functionality you like and review the corresponding traffic in the trace:

Relay Discovery allocation and real-time traffic (3478)

Audio (3479)

Video (3480)

Video Screen Sharing (3481)

Example of launching and joining a Teams meeting:

A screenshot of a social media post

Description automatically generated

Example after screen sharing:

A screenshot of a computer

Description automatically generated

Additionally, use netstat to check for active connections: Netstat -ano or Netstat -anob

A screenshot of a computer

Description automatically generated

As of August 12, 2020 (it is possible ip’s change or new ones are added):

Configure VPN to bypass Teams media traffic:

======================================

1. If its desired to only Split Tunnel teams traffic, then these subnets/ports will need to be added to the VPN configuration exclude access routes:  
   Ports: 3478, 3479, 3480, 3481, 80, 443  
   IP’s:  
   13.107.60.1/32 <--this one is needed if clients do not have the Teams version 1.3.00.13565 or greater 13.107.64.0/18  
   52.112.0.0/14  
   52.120.0.0/14  
   52.238.119.141/32  
   52.244.160.207/32  
   2603:1027::/48  
   2603:1037::/48

2603:1047::/48

2603:1057::/48

2620:1ec:6::/48

2620:1ec:40::/42

1. Ideally, for all O365 traffic, use the list of ip address ranges here: [https://docs.microsoft.com/en-us/office365/enterprise/office-365-vpn-implement-split-tunnel#optimize-ip-address-ranges](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Foffice365%2Fenterprise%2Foffice-365-vpn-implement-split-tunnel%23optimize-ip-address-ranges&data=02%7C01%7CMelissa.Bajric%40microsoft.com%7C074ddd5b660f4c6bba0208d83e2068b2%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637327656236100433&sdata=SHGe%2BJgNjp0fzuiJNxCoIyRPZpDhcaXxFjGx6Q7%2Blss%3D&reserved=0) and include 13.107.60.1/32
2. Pending any issues or to confirm the routing is working and desired, we’ll need to take/review a data collection.
3. To automate any updates to endpoints:
   1. Use the [How To guide](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Foffice365%2Fenterprise%2Foffice-365-vpn-implement-split-tunnel%23howto-guides-for-common-vpn-platforms&data=02%7C01%7CMelissa.Bajric%40microsoft.com%7C074ddd5b660f4c6bba0208d83e2068b2%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637327656236030472&sdata=1CUYxk5gqE4NyPRh%2F%2FDbu8%2BYLK9xEEwwN%2FYurH1SOBY%3D&reserved=0) for your specific VPN concentrator
   2. OR use [the script](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fgithub.com%2Fmicrosoft%2FOffice365NetworkTools%2Ftree%2Fmaster%2FScripts%2FDisplay%2520URL-IPs-Ports%2520per%2520Category&data=02%7C01%7CMelissa.Bajric%40microsoft.com%7C074ddd5b660f4c6bba0208d83e2068b2%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637327656236020473&sdata=yS6BMKByW2ZGbkHxNfmASoW9pS55LJ9fDE0PbH7Nmss%3D&reserved=0) referenced from [https://docs.microsoft.com/en-us/office365/enterprise/office-365-vpn-implement-split-tunnel#optimize-ip-address-ranges](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Foffice365%2Fenterprise%2Foffice-365-vpn-implement-split-tunnel%23optimize-ip-address-ranges&data=02%7C01%7CMelissa.Bajric%40microsoft.com%7C074ddd5b660f4c6bba0208d83e2068b2%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637327656236030472&sdata=16VFSwQMCI15JbWDSLrMfIjSEL0gbttzLKI22SDVCBI%3D&reserved=0)

Data Collection Plan: (If you want to open a support case, go ahead and collect the following data)

=====================

1. UNFILTERED Wireshark traces running on:
   1. Egress to internet
   2. Client machine
2. Screenshot from https://www.whatismyip.com/
3. Browse to https://connectivity.office.com/
   1. Enter your city and the prefix of your tenant name
   2. You may be prompted to download https://dotnet.microsoft.com/download/dotnet-core/thank-you/runtime-aspnetcore-3.1.3-windows-x64-installer
   3. Share the results
4. OS version
5. Teams client logs per https://docs.microsoft.com/en-us/microsoftteams/log-files
   1. Debug logs: Keyboard shortcut: Ctrl + Alt + Shift + 1
   2. Media logs:
   3. %appdata%\Microsoft\Teams\media-stack\\*.blog
   4. %appdata%\Microsoft\Teams\skylib\\*.blog
   5. %appdata%\Microsoft\Teams\media-stack\\*.etl
   6. Desktop log: %appdata%\Microsoft\Teams\logs.txt
6. Client machine output of ipconfig /all

More Information:

================

Urls, IP’s and Ports for Teams:

<https://docs.microsoft.com/en-us/office365/enterprise/office-365-vpn-implement-split-tunnel#optimize-urls>

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide#skype-for-business-online-and-microsoft-teams>

Set how you want to handle real-time media traffic for Teams meetings:

<https://docs.microsoft.com/en-us/microsoftteams/meeting-settings-in-teams#set-how-you-want-to-handle-real-time-media-traffic-for-teams-meetings>

Microsoft Teams Call Flows:

<https://docs.microsoft.com/en-us/microsoftteams/microsoft-teams-online-call-flows>

Get-NetIPConfiguration:

<https://docs.microsoft.com/en-us/powershell/module/nettcpip/get-netipconfiguration?view=win10-ps>

Get-NetAdapter: <https://docs.microsoft.com/en-us/powershell/module/netadapter/get-netadapter?view=win10-ps>

Netstat: <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat>