Spectera

Network & Security Guide for IT Administrators, System Integrators and Event Technicians

Sennheiser electronic SE & Co. KG

Am Labor 1, 30900 Wedemark, Germany, www.sennheiser.com

v1.0

SENNHEISER

Contents

1. Introduction

This document is intended for IT administrators, system integrators and event technicians and serves as an planning and configuration guide for integrating components of the Spectera offering into diverse network environments from small home networks up to enterprise networks.

The guide contains recommendations on network setup for transmission of control data and audio content (via Dante®).

2. General requirements

2.1. Operating systems

The Spectera Base Station as network device is able to be controlled by network-capable PC or Mac devices.

The following system requirements apply for operation with Spectera Web UI and Sennheiser LinkDesk:

- Intel i5 Dual Core processor/M1 Mac/or similar
- 16 GB RAM
- at least 4 GB hard disk space (5 GB for Mac devices)
- Gigabit LAN interface
- Windows® 10, 11, Server 2019, Server 2022 (x64) or higher
- IPv4 network
- Windows: 10 or later
- MacOS: 13 or later

Supported browsers for Spectera Web UI:

- Google Chrome: 125 or later
- Microsoft Edge: 125 or later
- Mozilla Firefox: 128 or later
- Apple Safari: 17 or later

2.1. Network

Bandwidth and speed

When it comes to bandwidth requirements for high-quality audio, there are a number of factors that can affect the input and output of the audio. The network speed required for especially audio transmission via Dante® should be as high as possible to ensure a smooth listening experience. As a rule, the minimum bandwidth for transmitting and receiving audio at the Spectera Base Station is approximately the following:

> The majority of audio used in professional settings is PCM (uncompressed), sampled at 48 kHz and a bit depth (word length) of 24 bits. Dante® audio is unicast by default but can be set to use multicast for cases of one-to-many distribution.
>
> - Dante® packages audio into flows to save on network overhead.
> - Unicast Audio flows contain up to 4 channels. The samples-per-channel can vary between 4 and 64, depending on the latency setting of the device. Bandwidth usage is about 6 Mbps per typical unicast audio flow.
> - Bandwidth for multicast flows is dependent on the number of audio channels used. Bandwidth is about 1.5 Mbps per channel
>
> Source: Dante Information for Network Administrators

Internet access

For both components Spectera Base Station and Sennheiser LinkDesk we recommend to provide permanent Internet access. Please refer to chapter “4. Ports, protocols and services” to get more details about used Internet services.

> At least for the initial product activation of the Spectera Base Station and for the use of the optional Sennheiser Account Login in Sennheiser LinkDesk it is mandatory to have a direct Internet access and DNS support.

> At the moment it is not possible to manually configure any network proxy and DNS server at Spectera Base Station. Please make sure to provide direct Internet access e.g. via white-listing the device and any used port, protocol and domain and using DHCP to provide DNS server settings.

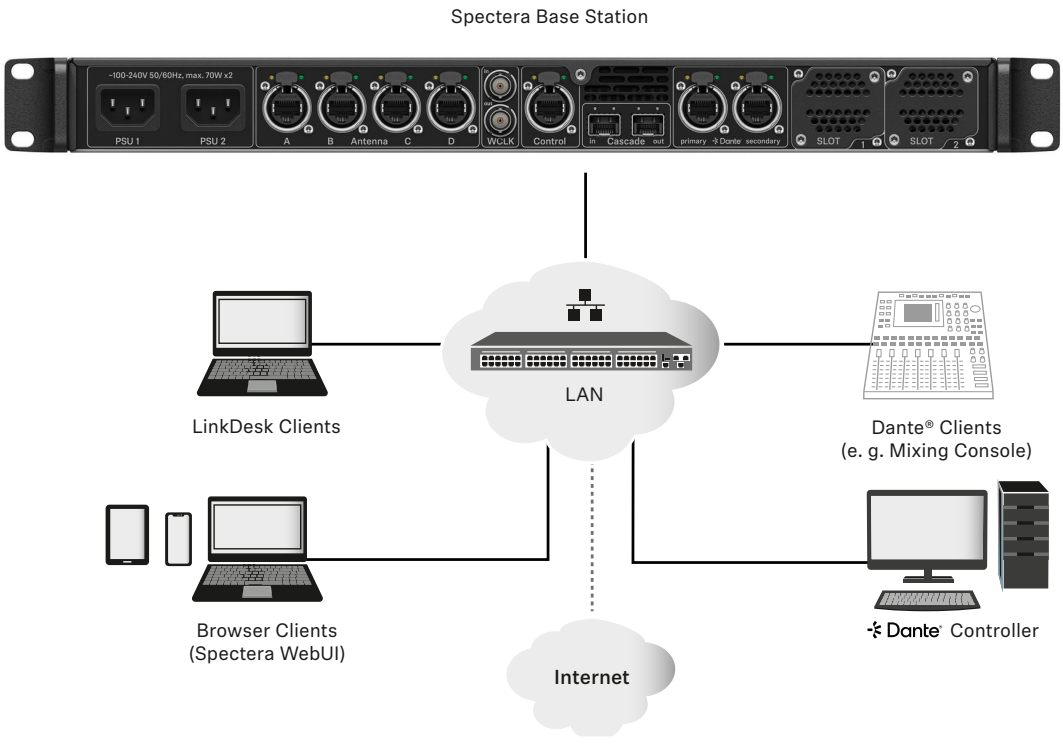
Cabeling

As long as a good Internet speed is guaranteed, the network cable used determines the actual transmission speed of data sent and received in the network.

> To ensure a reliable transmission speed of audio and control data with the Spectera Base Station, please use an RJ45 network cable with the CAT5e S/FTP standard or higher

3. Network setups

To operate the several components of the Spectera offering they need to be integrated into a network setup, either existing or new. Following figure shows a general overview of the network setup and their participants.



Spectera Base Station

This Sennheiser device has 3 network interfaces. One interface dedicated for control data and two interfaces for audio data (specifically Dante®). There is a primary and a secondary interface for redundancy of the audio transmission.

Sennheiser LinkDesk client

This client can be any host computer (PC or Mac), with the LinkDesk software application installed.

Browser Client (Spectera WebUI)

This client can be any host computer (PC, Mac, Tablet, Smartphone), with a supported web browser installed, accessing the Spectera WebUI.

Dante® client

This can be any device with a Dante® network interface installed. This ranges from Virtual Dante® Soundcards installed on a host computer up to dedicated devices like a Mixing Console.

Dante® Controller

This is typically host computer (PC or Mac), with the Dante® Controller software application installed. This application configures and controls all the Dante® devices and audio streams inside the network.

Network router

This can be any router device for routing the network communication inside the Local Area Network (LAN) and providing the gateway to other networks and to the Internet.

3.1. Spectera Base Station - network configuration

Depending on the desired network address configuration all network interface (Control and both Dante®) can be operated in following IP Modes with IPv4 only:

- Fixed/Static IP
- Auto IP (DHCP or Zeroconf)

Additionally it can be configured if mDNS/DNS-SD information shall be published by the device or not.

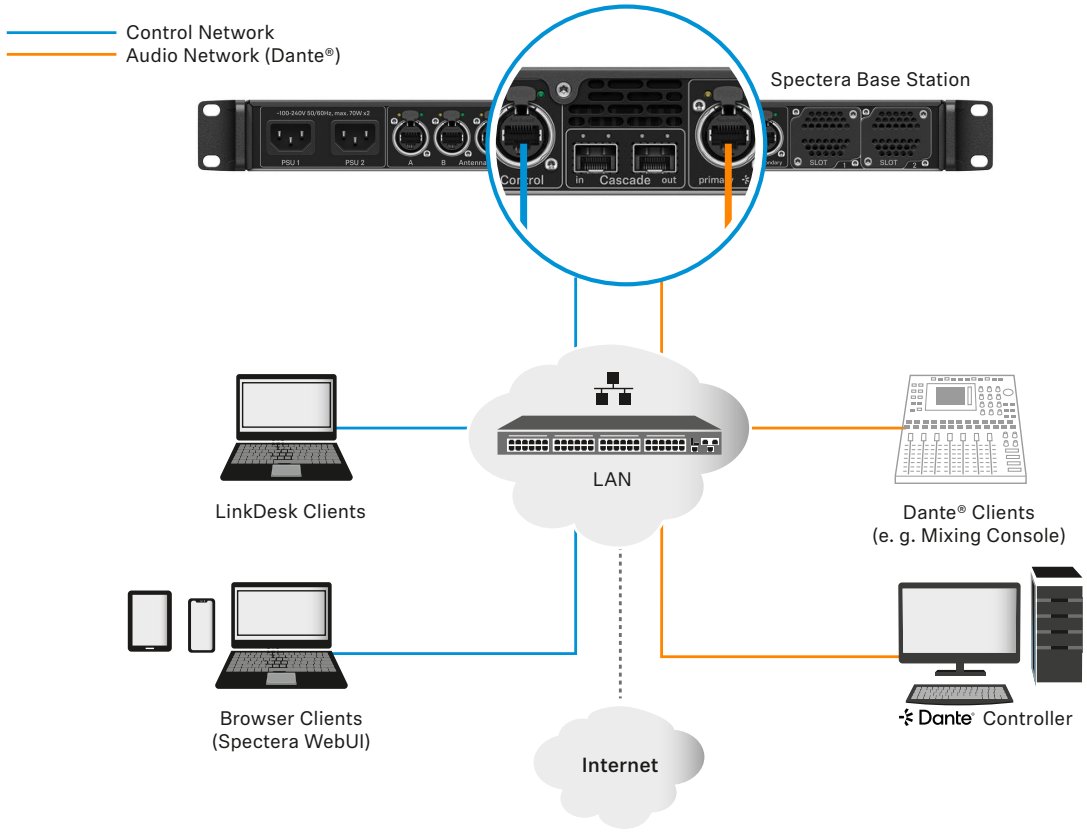
Dante® restrictions

- It is not possible to deactivate the Dante® functionality for the both Dante® ports.
- Dante® ports are shutdown when the device is in standby mode.
- Network configuration of Dante® ports can only be done via Dante® Controller software application.
- By default the Dante® ports are configured to Auto IP. If Fixed/Static IPs have been configured and the device cannot be reached anymore, the IP Mode can only be reset to Auto IP by a Factory Reset of the device.
- The Dante primary and secondary networks must not be directly connected to each other (network loop). Make sure you always connect the Base Station Dante network ports to two different networks that do not run via a common switch.

Shared Network Mode

In Shared Network Mode both networks for Control and Dante® are using the same physical network infrastructure.

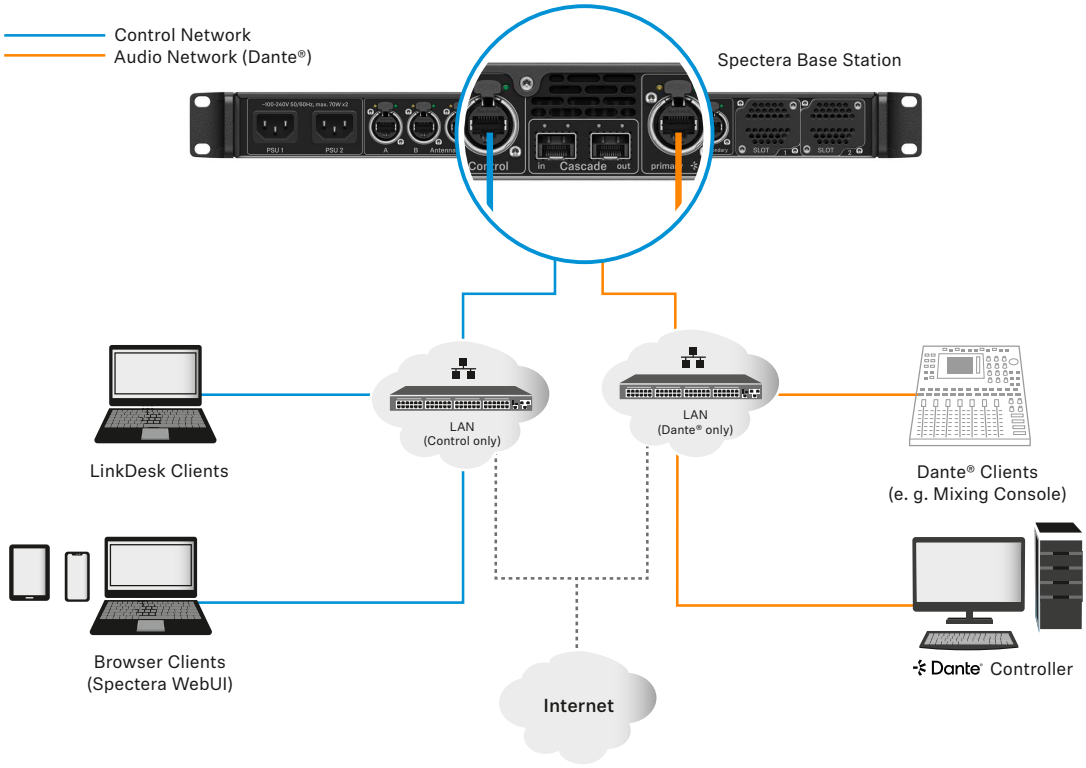
- Configure both Control and Dante® networks over one switch / router.
- Use two different IPs to address the Control network and the Dante® network separately.



Split Network Mode

In Split Network Mode both networks for Control and Dante® are using different physical network infrastructure.

- Configure both Control and Dante® networks over two different switches / routers.
- Use two different IPs to address the Control network and the Dante® network separately.



4. Ports, protocols and services

4.1. Sennheiser LinkDesk

In order to use the Sennheiser LinkDesk software, certain ports must be enabled (especially for the organization/enterprise firewall) for communication between software and devices. If necessary, please contact the local administrator to configure the required ports.

Address	Port	Protocol	Type	Service	Usage
Host Internal					
LOCALHOST	54352	HTTPS (TCP)	Unicast	LinkDesk backend	Internal backend communication
Host Outbound					
ANY	443	HTTPS (TCP)	Unicast	Spectera Base Station API	Communication to devices
Pro Emea Accounts[1] B2C Config[2]	443	HTTPS (TCP)	Unicast	Sennheiser CIAM	Sennheiser account sign-in/log-in
User insights[3] Matomo[4]	443	HTTPS (TCP)	Unicast	Sennheiser User Insights	Analytics of usage and operational data
Host Inbound					
ANY	443	HTTPS (TCP)	Unicast	Spectera Base Station API	Base Station API Communication from devices
224.0.0.251	5353	mDNS (UDP)	Multicast	mDNS, DNS-SD	(optional - if desired) device/service discovery

[1] accounts-pro-emea.sennheiser-cloud.com
[2] b2c-config.sennheiser-cloud.com
[3] sennheiseruserinsights.matomo.cloud
[4] cdn.matomo.cloud

4.2. Spectera Base Station

In order to use the Spectera Base Station device in a network, certain ports must be enabled (especially for the organization/enterprise firewall) for communication between software and devices. If necessary, please contact the local administrator to configure the required ports.

Address	Port	Protocol	Type	Service	Usage
Device Outbound					
ANY	443	HTTPS (TCP)	Uni-cast	Spectera Base Station API	Device Communication to Clients
User insights[1] Matomo[2]	443	HTTPS (TCP)	Uni-cast	Sennheiser User Insights	Analytics of usage and operational data
my.nalpeiron.com	80	HTTP (TCP)	Uni-cast	Sennheiser License Server	Activation of devices
ANY (see list of NTP servers)	123	NTP	Uni-cast	NTP Time Server	Synchronize system time
224.0.0.251	5353	mDNS (UDP)	Multi-cast	mDNS, DNS-SD	(optional - if enabled) Device/Service Discovery
ANY (see list of Dante® ports)					
Device Inbound					
ANY	443	HTTPS (TCP)	Uni-cast	Spectera Base Station API	Device Communication from Clients
ANY (see list of Dante® ports)					Dante® audio and control data

[1] sennheiseruserinsights.matomo.cloud

[2] cdn.matomo.cloud

NTP servers

To correctly operate with licenses and certificates, the Spectera Base Station needs a correct system time. The device will use the well-established NTP mechanism from the IP protocol stack to synchronize clock between a time server in a network and the client inside the device.

Currently for an IT administrator or system integrator it is not possible to manually configure a dedicated NTP server to be used by the Spectera Base Station. Being able to configure a dedicated NTP server manually is a planned feature for an upcoming release.

The device behaves the following way:

- If a time server configuration has been provided via DHCP or manually, it tries to connect and sync to that time server first.
- Otherwise the device is trying to access any server of following list of time server pools worldwide publicly available.

> **i** An IT administrator has to assure to provide Internet access to at least one of the server pools and to provides DNS settings via DHCP to the device.

List of NTP time server pools:

- pool.ntp.org
- time.nist.gov
- time.aws.com
- time.cloudflare.com

4.3. Dante® ports

To set up a Dante® network, defined port information is required. The table below shows which ports, URLs and servers are used. For detailed information, please refer directly to the website: https://www.getdante.com/support/faq/which-network-ports-does-dante-use/

External Dante® ports

Address	Port	Usage	Type
239.255.0.0/16	4321	ATP Multicast Audio	Multicast
239.69.0.0/16	5004	AES67 Multicast Audio	Multicast
224.0.1.129-132	319, 320	PTP	Multicast & Unicast (DDM)
224.0.0.251	5353	mDNS	Multicast
224.0.0.230 – 233	8700 – 8708	Multicast Ctrl & Monit.	Multicast
239.254.1.1	9998	Logging	Multicast
239.254.3.3	9998	TP Logging (if enabled)	Multicast
239.254.44.44	9998	Logging	Multicast
239.255.255.255	9875	SAP (AES67 discov.)	Multicast
UDP	28800, 28700-28708	Ctrl. & Monitoring.(ext)	Unicast
UDP	38800, 38700-38708	DVS control & monitoring (ext)	Unicast

Internal Dante® Ports

Protocol	Port	Usage	Type
UDP	14336 -14591	Unicast Audio [Excluding Via]	Unicast
UDP	34336-34600	Unicast Audio [Via Only]	Unicast
UDP	4440, 4444, 4455	Audio Control [Excluding Via]	Unicast
UDP	24440, 24441, 24444, 24455	Audio Control [Via Only]	Unicast
UDP	4777	Via Control [Via Only]	Unicast
TCP	4777	Via Websocket	Unicast
UDP	8850,28900, 24445	Via control & Monitoring (int.)	Unicast
UDP	8850, 38900, 8899	DVS control & monitoring (int.)	Unicast
UDP	8000	Dante Domain Manager Device Port	Unicast
UDP	8001	Dante Millau Device Proxy (int.)	Unicast
UDP	8002	Dante Lock Server	Unicast
UDP	8751	Dante Controller metering port	Unicast
UDP	8800	Control & Monitoring	Unicast
TCP	8753	mDNS clients (Internal only)	Unicast
TCP	16100-16131	HDCP Authent. for Video Endpoints	Unicast
UDP	61440-61951	FPGA level audio flow keepalive	Unicast
TCP	4778	DVS websocket (Apple Silicon only)	Unicast

5. Security

5.1. Certificates

Spectera Base Station is using a self-signed certificate for network communication. Currently it is not possible to replace it with a CA-signed certificate. The certificate is generated in factory and will be renewed with every factory reset.

When accessing the Spectera WebUI with a browser for the first time you will get a security warning informing about an unknown certificate. The security warning depends on the browser you are using. Depending on your browser, click on **Advanced** or **Show Details** (Safari) and then on:

- Microsoft Edge: **Continue to localhost (unsafe)**
- Google Chrome: **Proceed to localhost (unsafe)**
- Firefox: **Accept the Risk and Continue**
- Apple Safari: **[...] visit this Website** -> **Visit Website**
- or similar (other browsers)

In order to prevent man-in-the-middle (MITM) attacks, Sennheiser LinkDesk has some built-in security measures. Because of these measures, you might receive a certificate mismatch warning while working with a Base Station. In some cases, these can occur even though there is actually no security issue. These are:

- The Base Station has been factory reset since the last connect. In this case you can safely confirm the connection and proceed when encountering the mismatch warning.
- A different Base Station has been connected via the same IP address. In this case please verify if the IP Address you are using is indeed the correct IP Address of the intended Base Station.

5.2. Device password

The device access via network control API and Web UI of Spectera Base Station and via Sennheiser LinkDesk is password protected, to avoid configuring the device by unauthorized actors inside the network.

After unboxing and after every factory reset of the device a new password has to be configured by the user to claim the access to the device. Every instance of Sennheiser LinkDesk remembers the passwords of the devices it has claimed already. Protecting the access by unauthorized actors to the Sennheiser LinkDesk application on a host, other mechanisms have to be applied, e.g. password protected user accounts in Windows or MacOS.

With every new browser session of the Spectera WebUI the configured password has to entered again.

5.3. Encrypted data transmission

All control data transmission on HTTPS protocol is encrypted using Transport Layer Security (TLS).

All control data transmission on HTTP protocol to the Sennheiser License Server is encrypted on Application Level.

All audio data transmission via Dante® is not encrypted, since not supported yet.

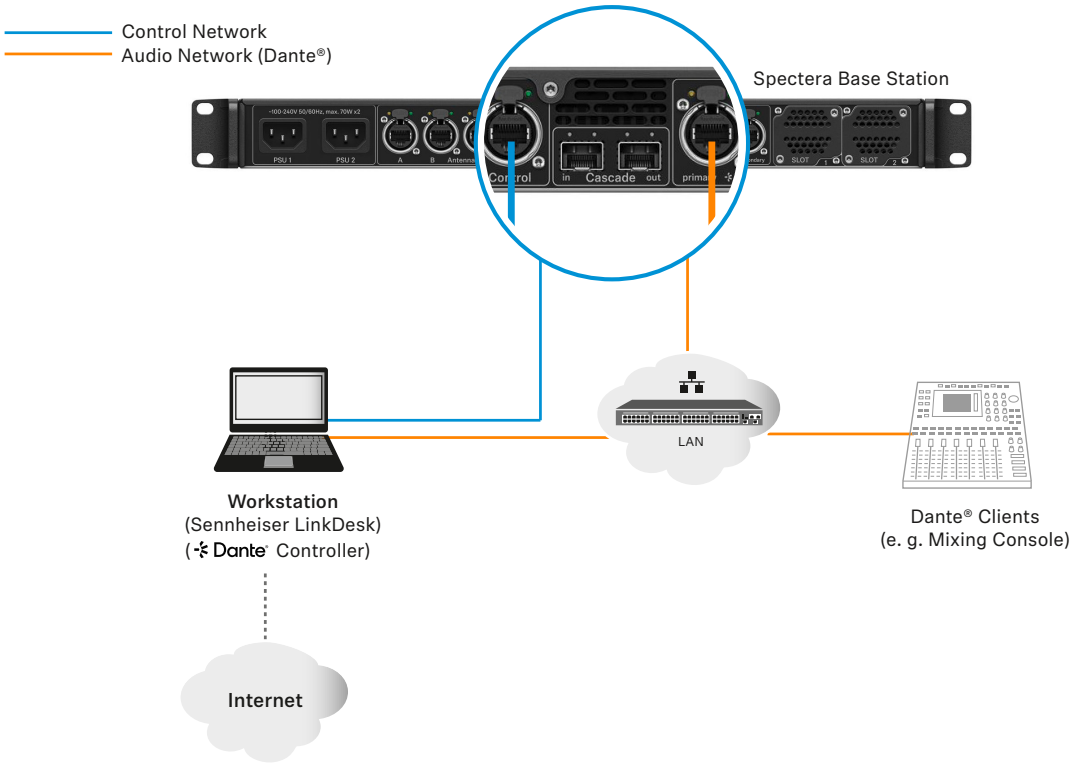
6. Best practice

6.1. Sharing Internet connection in small network setups

It is possible to operate the Spectera offering without dedicated router networks e.g. in really small setups, but we do recommend to always use some kind of home network router for trouble-free usage. Especially for providing Internet access to Spectera Base Station it is possible to use the built-in functionality of Windows and MacOS for Internet Connection Sharing.

> For enterprise networks we DO NOT RECOMMEND the usage of Internet Connection Sharing. Most of the times it is even prohibited by enterprise IT policy to use such service.

The network setup could look like this.



Inside this setup one workstation is used for all client software applications (Sennheiser LinkDesk, Spectera WebUI, Dante® Controller). Either two separated wired network interface are used for control and audio (Dante®) or one interface gets shared. Please be aware that in such setups (typically) no DHCP service is activated. Use either manual IP settings or ZeroConf configuration.

For Internet Connection Sharing typically an existing network connection (Wi-Fi or Ethernet) with Internet access gets shared with another selected network interface of the host.

In order to share your Internet connection on Windows:

1. Connect your client device to your host PC using an Ethernet cable. If either device doesn't have a free Ethernet port, use a USB-to-Ethernet adapter.
2. Go to the **Network Connections** menu. The easiest way to get there is by searching for "Network Connections" in the Windows Search box.
3. Right-click on the network adapter connected to the Internet (for example, Wi-Fi or modem), and then select **Properties**.
4. Toggle **Allow other network users to connect** to **ON** from the Sharing tab and select the relevant Ethernet port from the pull-down menu.

> Note that, if you have VPN software installed, you may see a lot of virtual Ethernet ports on your list and you'll need to pick the real one.

After you click **OK**, Internet should flow to your client device over its Ethernet port.

For more details on sharing an Internet connection please refer to the Microsoft Support page.

In order to share your Internet connection on MacOS:

1. On your Mac, choose **Apple menu** > **System Settings**.
2. Click on **General** in the sidebar and then on **Sharing** (you may need to scroll down).
3. Turn on **Internet Sharing** and click on **Configure**.
4. Click the **Share your connection from** pop-up menu.
5. Choose the Internet connection you want to share.
   (For example, if you're connected to the Internet over Wi-Fi, choose Wi-Fi).
6. Below To devices using, turn on the port other devices can use to access the shared internet connection.
   (For example, if you want to share your Internet connection over Ethernet, select Ethernet).
   If you're sharing to devices using Wi-Fi, configure the Internet-sharing network, then click **OK**.
7. Click on **Done**.
   Your Internet connection will be shared on MacOS.

For more details on sharing an Internet connection please refer to the Apple Support page.