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

v1.2

SENNHEISER

Contents

1. Introduction

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

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

2. General requirements

2.1. Operating systems

As a network device, the Spectera Base Station can be controlled by network-capable PC or Mac devices.

The following system requirements apply to 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

As regards the bandwidth requirements for high-quality audio, a number of factors can affect the input and output of the audio. In particular, the network speed required for 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 as follows:

> 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 one-to-many distribution.
>
> - Dante® packages audio into flows to save on network overheads.
> - 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.
> - The bandwidth for multicast flows depends on the number of audio channels used. The bandwidth is about 1.5 Mbps per channel
>
> Source: Dante Information for Network Administrators

Internet access

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

> For the initial product activation of the Spectera Base Station and the use of the optional Sennheiser Account Login in Sennheiser LinkDesk, direct Internet access and DNS support are compulsory requirements.

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

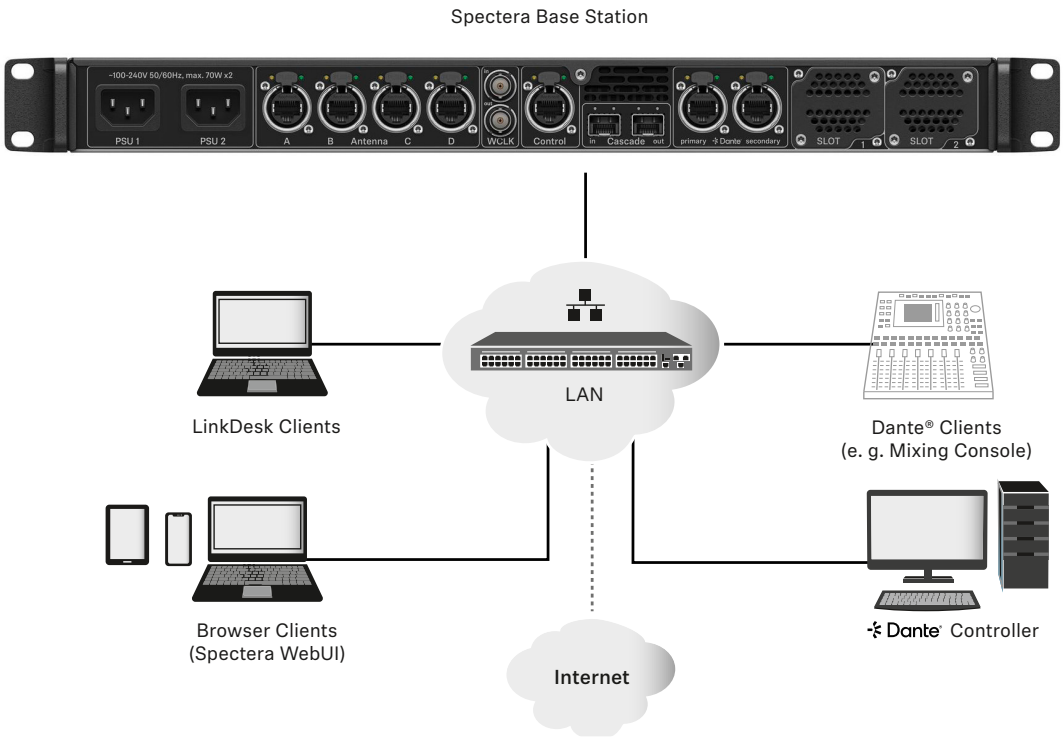
Cables

Assuming 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, use an RJ45 network cable with the CAT5e S/FTP standard or higher

3. Network setups

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



Spectera Base Station

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

Sennheiser LinkDesk client

This client can be any host computer (PC or Mac) on which the LinkDesk software application is installed.

Browser client (Spectera WebUI)

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

Dante® client

This can be any device on which a Dante® network interface is installed. This ranges from Virtual Dante® Soundcards installed on a host computer through to dedicated devices such as a mixing console.

Dante® Controller

This is typically the host computer (PC or Mac) on which the Dante® Controller software application is 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 the Internet.

3.1. Spectera Base Station - network configuration

Depending on the preferred network address configuration, the network interfaces (Control and Dante®) can be operated in the following IP modes with IPv4 only:

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

It is also possible to configure whether mDNS/DNS-SD information is published by the device or not.

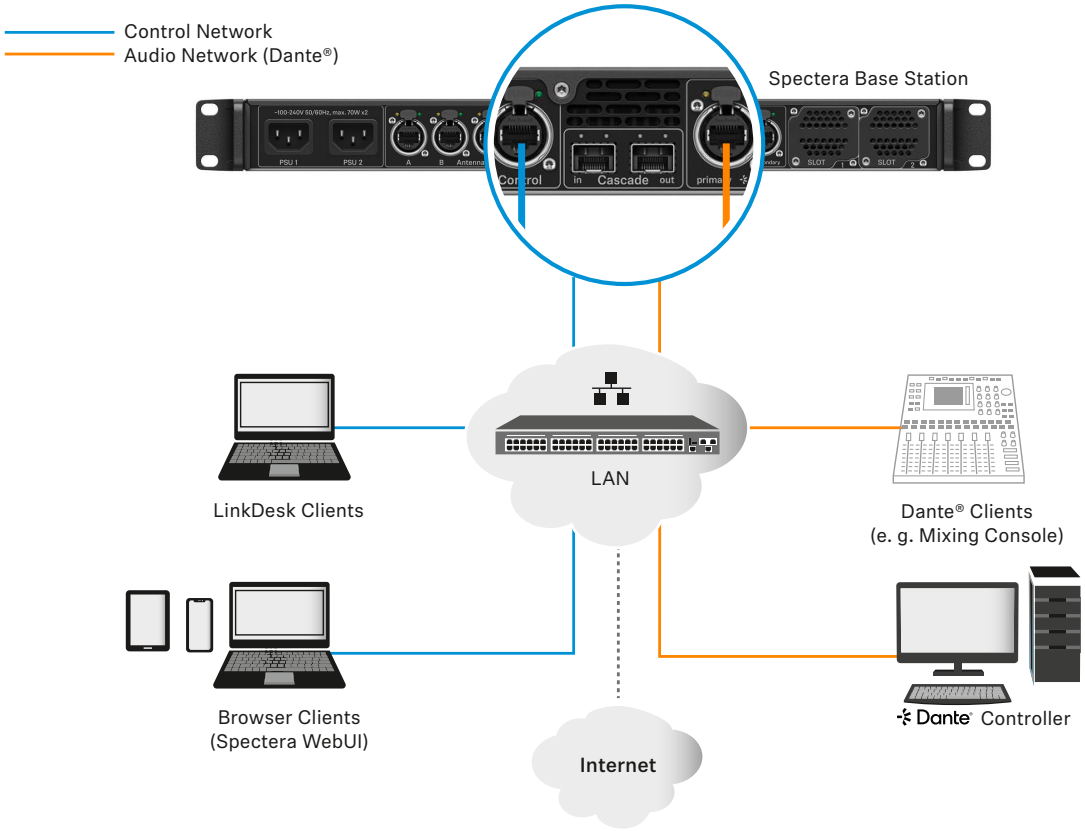
Dante® restrictions

- It is not possible to deactivate the Dante® functionality for both Dante® ports.
- The Dante® ports are shutdown when the device is in standby mode.
- The network configuration of the Dante® ports can only take place via the Dante® Controller software application.
- The Dante® ports are configured to Auto IP by default. If Fixed/Static IPs have been configured and the device cannot be reached anymore, the IP Mode can only be reset to Auto IP with 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 the Shared Network Mode, both networks for Control and Dante® use the same physical network infrastructure.

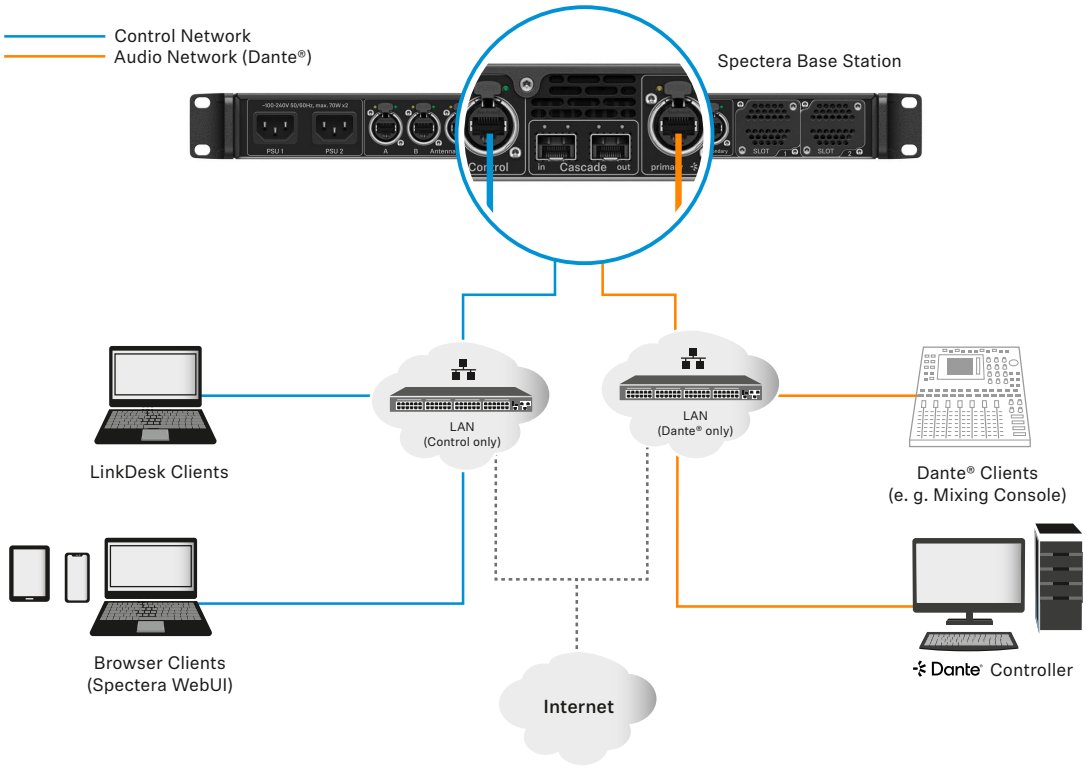
- Configure both Control and Dante® networks via one switch / router.
- Use two different IPs to address the Control network and the Dante® network separately.



Split Network Mode

In Split Network Mode, both the networks for Control and Dante® use different physical network infrastructure.

- Configure the Control and Dante® networks via 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

To use the Sennheiser LinkDesk software, certain ports must be enabled (especially for the organization/enterprise firewall) for the 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
Outbound host					
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
Inbound host					
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 preferred) 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

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

Address	Port	Protocol	Type	Service	Usage
Outbound device					
ANY	443	HTTPS (TCP)	Unicast	Spectera Base Station API	Device communication to clients
User insights[1] Matomo[2]	443	HTTPS (TCP)	Unicast	Sennheiser User Insights	Analytics of usage and operational data
my.nalpeiron.com	80	HTTP (TCP)	Unicast	Sennheiser License Server	Activation of devices
ANY (see list of NTP servers)	123	NTP	Unicast	NTP Time Server	Synchronize system time
224.0.0.251	5353	mDNS (UDP)	Multicast	mDNS, DNS-SD	(optional - if enabled) Device/service discovery
ANY (see list of Dante® ports)					
Inbound device					
ANY	443	HTTPS (TCP)	Unicast	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 be able to operate with licenses and certificates, the Spectera Base Station needs a correct system time. The device uses the well-established NTP mechanism from the IP protocol stack to synchronize the clock between a time server in a network and the client inside the device.

It is not currently possible for an IT administrator or system integrator to manually configure a dedicated NTP server for use 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 in 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 tries to access any server from the following list of time server pools publicly available worldwide.

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

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
239255255255	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 and 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. It is not currently possible to replace it with a CA-signed certificate. The certificate is generated in the factory and is renewed with every factory reset.

When accessing the Spectera WebUI with a browser for the first time you will receive 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)

To prevent man-in-the-middle (MITM) attacks, Sennheiser LinkDesk features built-in security measures. These measures mean that you may receive a certificate mismatch warning while working with a Base Station. In some cases, these can occur even though there is no current 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 whether the IP Address you are using is 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 prevent the configuration of the device by unauthorized actors inside the network.

After unboxing and after every factory reset of the device, a new password must be configured by the user to access the device. Every instance of Sennheiser LinkDesk remembers the passwords of the devices it has claimed. To protect the Sennheiser LinkDesk application against access by unauthorized actors on a host, other mechanisms must be applied, such as password-protected user accounts in Windows or MacOS.

The configured password must be entered again with every new Spectera WebUI browser session.

5.3. Encrypted data transmission

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

Transmission to Sennheiser license server

All control data transmission on HTTP protocol to the Sennheiser license server is encrypted on Application Level.

Dante Media Encryption (available as of Spectera Dante® firmware Brooklyn3 version 1.1.0)

Dante media encryption extends the security benefits of using Dante® on your network by concealing the media content during transmission between devices. Dante® utilizes the Advanced Encryption Standard (AES) with a 256-bit key to provide industry-leading media protection. Concealing the contents of media packets prevents malicious or unauthorized users eavesdropping or interfering with Dante media traffic.

> By default, Dante Media Encryption is disabled, since encryption can only be configured by using the Dante Director application. Please refer to the Audinate documentation for detailed information on Dante® encryption, on how to enable and configure encryption and to update the Dante® firmware:
>
> - Dante Media Encryption: Audinate/Media-Encryption
> - Updating Dante® firmware: Dante Updater

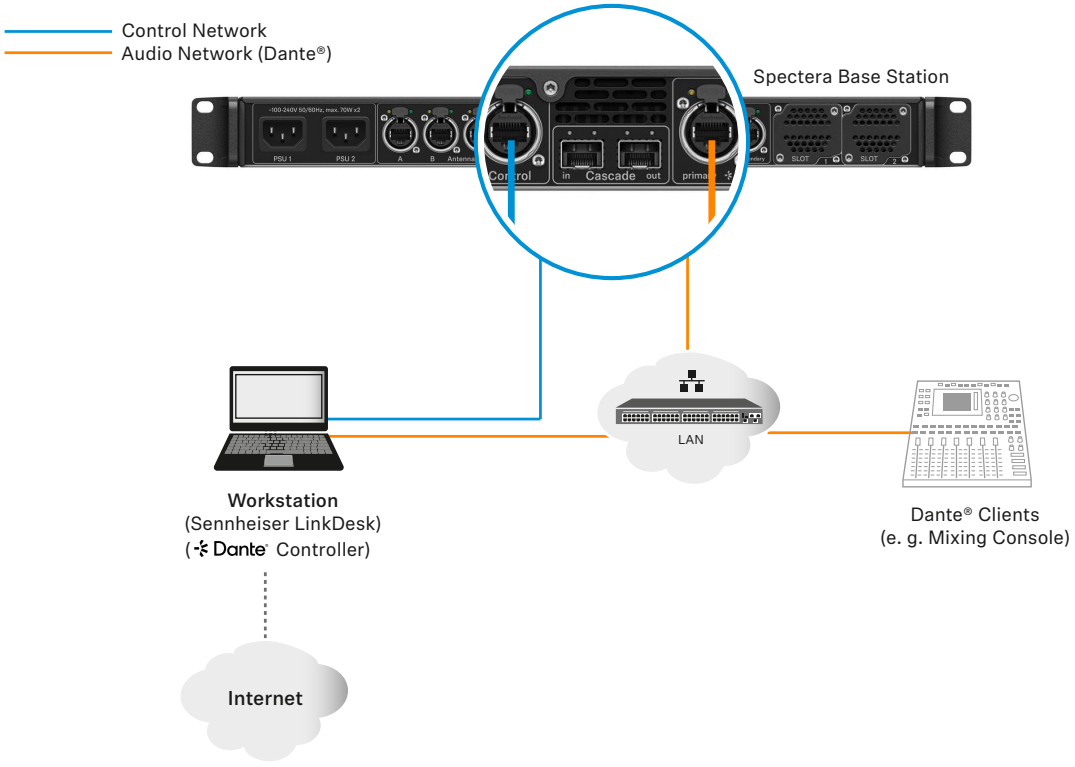
6. Best practice

6.1. Sharing Internet connection in small network setups

It is possible to operate the Spectera offering without dedicated router networks e.g. in very small setups, although we recommend you always use some kind of a home network router for trouble-free usage. To provide Internet access to the Spectera Base Station in particular, 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 time, the use of this service is also prohibited by the Enterprise IT Policy.

The network setup might look like this:



In 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 the control and audio (Dante®), or one interface is shared. Please note that in such setups (typically) no DHCP service is enabled. Use either manual IP settings or ZeroConf configuration.

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

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.

> Please note: if you have installed VPN software, you may see a lot of virtual Ethernet ports on your list and you will need to pick the specific port.

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

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

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. Enable **Internet Sharing** and click on **Configure**.
4. Click on the **Share your connection from** pop-up menu.
5. Choose the Internet connection you want to share.
   (If you're connected to the Internet via Wi-Fi, for example, choose Wi-Fi).
6. Under **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 via Ethernet, select Ethernet).
   If you're sharing devices using Wi-Fi, configure the Internet-sharing network, then click **OK**.
7. Click on **Done**.
   Your Internet connection will now be shared on MacOS.

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