Spectera

Netzwerk- und Sicherheitsleitfaden für IT-Administratoren, Systemintegratoren und Veranstaltungstechniker

Sennheiser electronic SE & Co. KG

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

v1.1

SENNHEISER

Inhalt

1. Einführung

Dieses Dokument richtet sich an IT-Administratoren, Systemintegratoren und Veranstaltungstechniker und dient als Planungs- und Konfigurationsleitfaden für die Integration von Komponenten des Spectera-Angebots in verschiedene Netzwerkumgebungen, von kleinen Heimnetzwerken bis hin zu Unternehmensnetzwerken.

Der Leitfaden enthält Empfehlungen zur Netzwerkeinrichtung für die Übertragung von Steuerdaten und Audioinhalten (über Dante®).

2. Allgemeine Anforderungen

2.1. Betriebssysteme

Die Spectera Base Station als Netzwerkgerät kann von netzwerkfähigen PC- oder Mac-Geräten gesteuert werden.

Für die Nutzung mit Spectera WebUI und Sennheiser LinkDesk gelten folgende Systemvoraussetzungen:

- Intel i5 Dual Core Prozessor/M1 Mac oder vergleichbar
- 16 GB Arbeitsspeicher
- Mindestens 4 GB Festplattenspeicher (5 GB für Mac-Geräte)
- Gigabit LAN Schnittstelle
- Windows® 10, 11, Server 2019, Server 2022 (x64) oder höher
- IPv4 Netzwerk
- Windows: 10 oder höher
- MacOS: 13 oder höher

Unterstützte Browser für Spectera WebUI:

- Google Chrome: 125 oder höher
- Microsoft Edge: 125 oder höher
- Mozilla Firefox: 128 oder höher
- Apple Safari: 17 oder höher

2.1. Netzwerk

Bandbreite und Geschwindigkeit

Wenn es um Bandbreitenanforderungen für qualitativ hochwertige Audioinhalte geht, gibt es eine Reihe von Faktoren, die sich auf die Eingabe und Ausgabe von Audiosignalen auswirken können. Die erforderliche Netzwerkgeschwindigkeit, insbesondere für die Audioübertragung über Dante®, sollte möglichst hoch sein, um ein reibungsloses Hörerlebnis zu gewährleisten. In der Regel liegt die Mindestbandbreite für das Senden und Empfangen von Audio an der Spectera Base Station ungefähr bei Folgendem:

> Der Großteil der in professionellen Einstellungen verwendeten Audiodaten ist PCM (unkomprimiert), das mit 48 kHz und einer Bittiefe (Wortlänge) von 24 Bit abgetastet wird. Audio über Dante® ist standardmäßig Unicast, kann aber so eingestellt werden, dass Multicast für den Fall einer Verteilung von 1:n verwendet wird.
>
> - Dante® packt Audio in Ströme, um das Netzwerk zu entlasten.
> - Unicast-Audioströme enthalten bis zu 4 Kanäle. Die Abtastwerte pro Kanal können zwischen 4 und 64 variieren, abhängig von der Latenzeinstellung des Geräts. Die Bandbreitennutzung beträgt ca. 6 Mbit/s pro typischem Unicast-Audiostrom.
> - Die Bandbreite für Multicast-Ströme hängt von der Anzahl der verwendeten Audiokanäle ab. Die Bandbreite beträgt ca. 1,5 Mbit/s pro Kanal
>
> Quelle: Dante-Informationen für Netzwerkadministratoren

Internet-Zugang

Für beide Komponenten Spectera Base Station und Sennheiser LinkDesk empfehlen wir einen permanenten Internetzugang. Siehe Kapitel „4. Ports, Protokolle und Services“ für weitere Informationen zu den verwendeten Internetdiensten.

> **i** Zumindest für die erste Produktaktivierung der Spectera Base Station und für die Nutzung des optionalen Sennheiser Account Login im Sennheiser LinkDesk ist ein direkter Internetzugang und DNS-Support zwingend erforderlich.

> **i** Derzeit ist es nicht möglich, einen Netzwerk-Proxy und DNS-Server an der Spectera Base Station manuell zu konfigurieren. Stellen Sie sicher, dass Sie einen direkten Internetzugang bereitstellen, z.B. über Whitelisting des Geräts und aller verwendeten Ports, Protokolle und Domänen sowie über DHCP, um DNS-Servereinstellungen bereitzustellen.

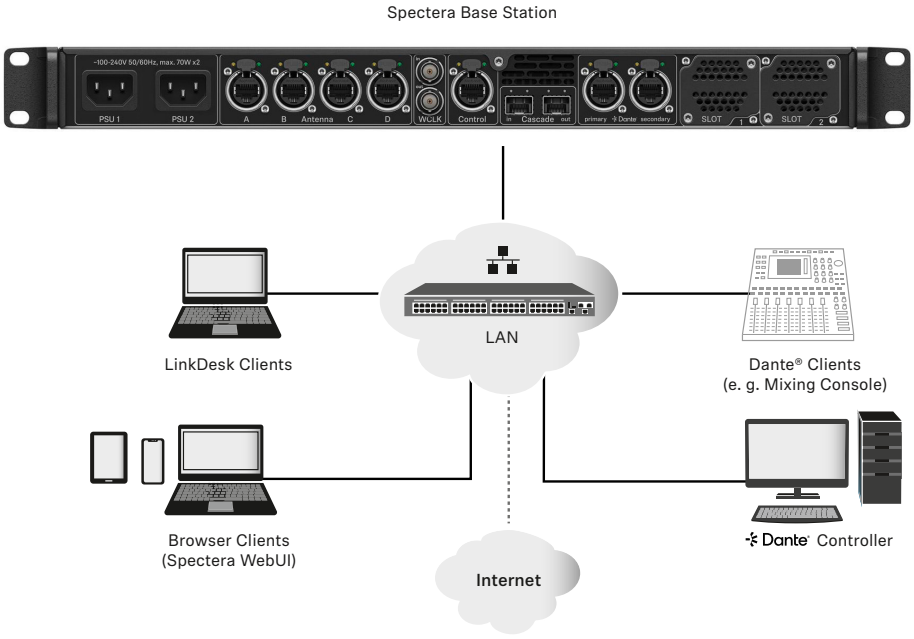
Verkabelung

Solange eine gute Internetgeschwindigkeit gewährleistet ist, bestimmt das verwendete Netzwerkkabel die tatsächliche Übertragungsgeschwindigkeit der im Netzwerk gesendeten und empfangenen Daten.

> **i** Um eine zuverlässige Übertragungsgeschwindigkeit von Audio- und Steuerdaten mit der Spectera Base Station zu gewährleisten, verwenden Sie bitte ein RJ45-Netzwerkkabel mit dem CAT5e S/FTP-Standard oder höher

3. Netzwerk-Setups

Um die verschiedenen Komponenten des Spectera-Angebots bedienen zu können, müssen sie in ein bestehendes oder neues Netzwerk-Setup integriert werden. Die folgende Abbildung zeigt eine allgemeine Übersicht über das Netzwerk-Setup und deren Teilnehmer.



Spectera Base Station

Dieses Sennheiser-Gerät verfügt über 3 Netzwerkschnittstellen. Eine Schnittstelle für Steuerdaten und zwei Schnittstellen für Audiodaten (speziell Dante®). Es gibt eine primäre und eine sekundäre Schnittstelle zur Redundanz der Audioübertragung.

Sennheiser LinkDesk-Client

Bei diesem Client kann es sich um einen beliebigen Host-Computer (PC oder Mac) handeln, auf dem die LinkDesk-Softwareanwendung installiert ist.

Browser-Client (Spectera WebUI)

Bei diesem Client kann es sich um einen beliebigen Host-Computer (PC, Mac, Tablet, Smartphone) handeln, auf dem ein unterstützter Webbrowser installiert ist, der auf die Spectera WebUI zugreift.

Dante®-Client

Dies kann jedes Gerät sein, auf dem eine Dante®-Netzwerkschnittstelle installiert ist. Dies reicht von virtuellen Dante®-Soundkarten, die auf einem Host-Computer installiert sind, bis hin zu dedizierten Geräten wie einem Mischpult.

Dante®-Controller

Hierbei handelt es sich in der Regel um einen Host-Computer (PC oder Mac), auf dem die Dante®-Controller-Softwareanwendung installiert ist. Diese Anwendung konfiguriert und steuert alle Dante®-Geräte und Audiostreams innerhalb des Netzwerks.

Netzwerk-Router

Dabei kann es sich um ein beliebiges Routergerät handeln, das die Netzwerkkommunikation innerhalb des LANs leitet und das Gateway für andere Netzwerke und das Internet bereitstellt.

3.1. Spectera Base Station - Netzwerkkonfiguration

Abhängig von der gewünschten Konfiguration der Netzwerkadresse können alle Netzwerkschnittstellen (Steuerung und beide Dante®) nur in folgenden IP-Modi mit IPv4 betrieben werden:

- Feste/statische IP
- Auto IP (DHCP oder Zeroconf)

Zusätzlich kann konfiguriert werden, ob mDNS/DNS-SD-Informationen vom Gerät veröffentlicht werden sollen oder nicht.

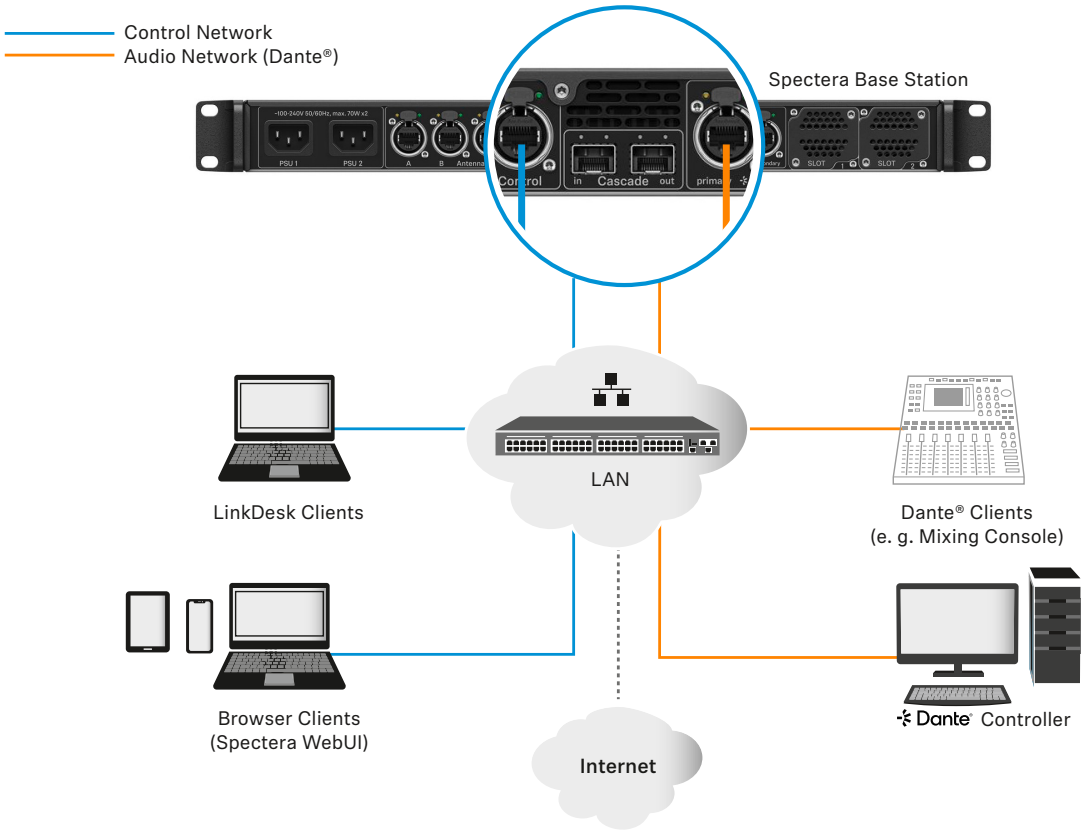
Dante®-Einschränkungen

- Es ist nicht möglich, die Dante®-Funktionalität für beide Dante®-Ports zu deaktivieren.
- Dante®-Ports werden heruntergefahren, wenn sich das Gerät im Standby-Modus befindet.
- Die Netzwerkkonfiguration von Dante®-Ports kann nur über die Dante®-Controller-Softwareanwendung erfolgen.
- Standardmäßig sind die Dante®-Ports auf Auto IP konfiguriert. Wenn feste/statische IPs konfiguriert wurden und das Gerät nicht mehr erreichbar ist, kann der IP-Modus nur durch eine Werkseinstellung des Geräts auf Auto-IP zurückgesetzt werden.
- Die primären und sekundären Dante-Netzwerke dürfen nicht direkt miteinander verbunden sein (Netzwerkschleife). Stellen Sie sicher, dass Sie die Dante-Netzwerkanschlüsse der Base Station immer mit zwei verschiedenen Netzwerken verbinden, die nicht über einen gemeinsamen Switch ausgeführt werden.

Shared Network-Modus

Im Shared Network-Modus nutzen beide Netzwerke für Steuerung und Dante® die gleiche physische Netzwerkinfrastruktur.

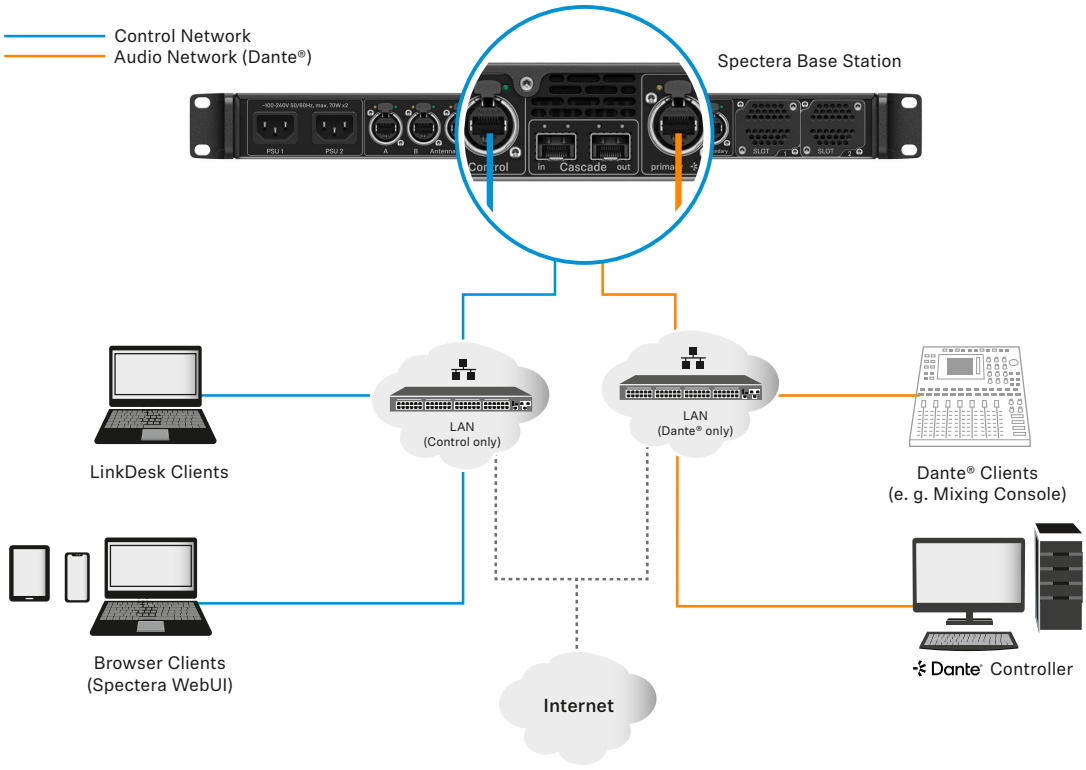
- Konfigurieren Sie Steuerungs- und Dante®-Netzwerk über einen Switch/Router.
- Verwenden Sie zwei verschiedene IPs, um das Steuerungsnetzwerk und das Dante®-Netzwerk getrennt zu adressieren.



Split Network-Modus

Im Split Network-Modus nutzen beide Netzwerke für Steuerung und Dante® unterschiedliche physische Netzwerkinfrastrukturen.

- Konfigurieren Sie Steuerungs- und Dante®-Netzwerk über zwei verschiedene Switches/Router.
- Verwenden Sie zwei verschiedene IPs, um das Steuerungsnetzwerk und das Dante®-Netzwerk getrennt zu adressieren.



4. Ports, Protokolle und Services

4.1. Sennheiser LinkDesk

Um die Sennheiser LinkDesk-Software nutzen zu können, müssen bestimmte Ports (insbesondere für die Unternehmensfirewall) für die Kommunikation zwischen Software und Geräten aktiviert sein. Wenden Sie sich bei Bedarf an den lokalen Administrator, um die erforderlichen Ports zu konfigurieren.

Adresse	Port	Protokoll	Typ	Service	Nutzung
Host intern					
LOCALHOST	54352	HTTPS (TCP)	Unicast	LinkDesk-Backend	Interne Backend-Kommunikation
Host ausgehend					
ANY	443	HTTPS (TCP)	Unicast	Spectera Base Station API	Kommunikation an Geräte
Pro EMEA-Konten[1] B2C-Konfiguration[2]	443	HTTPS (TCP)	Unicast	Sennheiser CIAM	Sennheiser-Konto Anmeldung
Anwenderberichte[3] Matomo[4]	443	HTTPS (TCP)	Unicast	Sennheiser-Anwenderberichte	Analyse von Nutzungs- und Betriebsdaten
Host eingehend					
ANY	443	HTTPS (TCP)	Unicast	Spectera Base Station API	Base Station API Kommunikation von Geräten
224.0.0.251	5353	mDNS (UDP)	Multicast	mDNS, DNS-SD	(Optional - falls gewünscht) Geräte-/Service-Erkennung

[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

Um die Spectera Base Station in einem Netzwerk nutzen zu können, müssen bestimmte Ports (insbesondere für die Unternehmensfirewall) für die Kommunikation zwischen Software und Geräten aktiviert sein. Wenden Sie sich bei Bedarf an den lokalen Administrator, um die erforderlichen Ports zu konfigurieren.

Adresse	Port	Protokoll	Typ	Service	Nutzung
Gerät ausgehend					
ANY	443	HTTPS (TCP)	Unicast	Spectera Base Station API	Gerätekommunikation an Clients
Anwenderberichte[1] Matomo[2]	443	HTTPS (TCP)	Unicast	Sennheiser-Anwenderberichte	Analyse von Nutzungs- und Betriebsdaten
my.nalpeiron.com	80	HTTP (TCP)	Unicast	Sennheiser-Lizenzserver	Aktivierung von Geräten
ANY (siehe Liste der NTP-Server)	123	NTP	Unicast	NTP-Zeitserver	Systemzeit synchronisieren
224.0.0.251	5353	mDNS (UDP)	Multicast	mDNS, DNS-SD	(Optional - falls aktiviert) Geräte-/Service-Erkennung
ANY (siehe Liste der Dante®-Ports)					
Gerät eingehend					
ANY	443	HTTPS (TCP)	Unicast	Spectera Base Station API	Gerätekommunikation von Clients
ANY (siehe Liste der Dante®-Ports)					Dante® Audio- & Steuerdaten

[1] sennheiseruserinsights.matomo.cloud

[2] cdn.matomo.cloud

NTP-Server

Um mit Lizenzen und Zertifikaten korrekt zu arbeiten, benötigt die Spectera Base Station eine korrekte Systemzeit. Das Gerät verwendet den etablierten NTP-Mechanismus aus dem IP-Protokollstapel, um die Uhr zwischen einem Zeitserver in einem Netzwerk und dem Client im Gerät zu synchronisieren.

Derzeit ist es für einen IT-Administrator oder Systemintegrator nicht möglich, einen dedizierten NTP-Server manuell für die Spectera Base Station zu konfigurieren. Die Möglichkeit, einen dedizierten NTP-Server manuell zu konfigurieren, ist eine geplante Funktion für eine kommende Version.

Das Gerät verhält sich wie folgt:

- Wenn eine Zeitserverkonfiguration über DHCP oder manuell bereitgestellt wurde, versucht sie zuerst, eine Verbindung mit diesem Zeitserver herzustellen und eine Synchronisierung durchzuführen.
- Andernfalls versucht das Gerät, auf einen Server der folgenden Liste von Zeitserverpools zuzugreifen, die weltweit öffentlich verfügbar sind.

> **i** Ein IT-Administrator muss sicherstellen, dass er Internetzugang zu mindestens einem der Serverpools bereitstellt und dem Gerät DNS-Einstellungen über DHCP bereitstellt.

Liste der NTP-Zeitserverpools:

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

4.3. Dante®-Ports

Für den Aufbau eines Dante®-Netzwerks sind definierte Port-Informationen erforderlich. Die folgende Tabelle zeigt, welche Ports, URLs und Server verwendet werden. Detaillierte Informationen finden Sie direkt auf der Website: https://www.getdante.com/support/faq/which-network-ports-does-dante-use/

Externe Dante®-Ports

Adresse	Port	Nutzung	Typ
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	Steuerung & Überwachung Multicast	Multicast
239.254.1.1	9998	Protokollierung	Multicast
239.254.3.3	9998	TP-Protokollierung (falls aktiviert)	Multicast
239.254.44.44	9998	Protokollierung	Multicast
239255255255	9875	SAP (AES67 Discov.)	Multicast
UDP	28800, 28700-28708	Steuerung & Überwachung (ext.)	Unicast
UDP	38800, 38700-38708	DVS-Steuerung & -Überwachung (ext.)	Unicast

Interne Dante®-Ports

Protokoll	Port	Nutzung	Typ
UDP	14336 -14591	Unicast-Audio [ohne Via]	Unicast
UDP	34336-34600	Unicast-Audio [nur Via]	Unicast
UDP	4440, 4444, 4455	Audiosteuerung [ohne Via]	Unicast
UDP	24440, 24441, 24444, 24455	Audiosteuerung [nur Via]	Unicast
UDP	4777	Via-Steuerung [nur Via]	Unicast
TCP	4777	Via-Websocket	Unicast
UDP	8850,28900, 24445	Via-Steuerung & -Überwachung (int.)	Unicast
UDP	8850, 38900, 8899	DVS-Steuerung & -Überwachung (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	Messanschluss Dante Controller	Unicast
UDP	8800	Steuerung & Überwachung	Unicast
TCP	8753	mDNS-Clients (nur intern)	Unicast
TCP	16100-16131	HDCP-Authent. für Video-Endpunkte	Unicast
UDP	61440-61951	FPGA-Audiopegelstrom, Keepalive	Unicast
TCP	4778	DVS-Websocket (nur Apple Silicon)	Unicast

5. Sicherheit

5.1. Zertifikate

Die Spectera Base Station verwendet ein selbstsigniertes Zertifikat für die Netzwerkkommunikation. Derzeit ist es nicht möglich, es durch ein von der Zertifizierungsstelle signiertes Zertifikat zu ersetzen. Das Zertifikat wird werkseitig generiert und bei jedem Werksreset erneuert.

Wenn Sie zum ersten Mal mit einem Browser auf die Spectera WebUI zugreifen, erhalten Sie eine Sicherheitswarnung, die über ein unbekanntes Zertifikat informiert. Die Sicherheitswarnung hängt vom verwendeten Browser ab. Klicken Sie je nach Browser auf **Erweitert** oder **Details anzeigen** (Safari) und dann auf:

- Microsoft Edge: **Weiter zu localhost (unsicher)**
- Google Chrome: **Weiter zu localhost (unsicher)**
- Firefox: **Risiko akzeptieren und fortfahren**
- Apple Safari: **[...] diese Website besuchen** -> **Website besuchen**
- oder ähnlich (andere Browser)

Um Man-in-the-Middle-Angriffe (MITM) zu verhindern, verfügt Sennheiser LinkDesk über einige integrierte Sicherheitsmaßnahmen. Aufgrund dieser Maßnahmen erhalten Sie möglicherweise eine Warnung zu einem Zertifikatkonflikt, wenn Sie mit einer Base Station arbeiten. In einigen Fällen können diese auftreten, obwohl tatsächlich kein Sicherheitsproblem vorliegt. Diese sind:

- Die Base Station wurde seit der letzten Verbindung auf die Werkseinstellungen zurückgesetzt. In diesem Fall können Sie die Verbindung sicher bestätigen und fortfahren, wenn eine Konfliktwarnung auftritt.
- Eine andere Base Station wurde über dieselbe IP-Adresse verbunden. Überprüfen Sie in diesem Fall, ob die verwendete IP-Adresse tatsächlich die richtige IP-Adresse der vorgesehenen Base Station ist.

5.2. Geräte-Passwort

Der Gerätezugriff über Netzwerk-Steuerungs-API und WebUI der Spectera Base Station sowie über Sennheiser LinkDesk ist passwortgeschützt, um eine Konfiguration des Geräts durch nicht autorisierte Akteure innerhalb des Netzwerks zu vermeiden.

Nach dem Auspacken und nach jedem Werksreset des Geräts muss ein neues Passwort vom Benutzer konfiguriert werden, um den Zugriff auf das Gerät zu beanspruchen. Jede Instanz von Sennheiser LinkDesk merkt sich die Passwörter der Geräte, die sie bereits beansprucht hat. Zum Schutz vor unberechtigtem Zugriff auf die Sennheiser LinkDesk-Anwendung auf einem Host müssen andere Mechanismen angewendet werden, z. B. passwortgeschützte Benutzerkonten in Windows oder MacOS.

Bei jeder neuen Browsersitzung der Spectera WebUI muss das konfigurierte Passwort erneut eingegeben werden.

5.3. Verschlüsselte Datenübertragung

Die gesamte Übertragung von Steuerdaten über das HTTPS-Protokoll wird mithilfe von Transport Layer Security (TLS) verschlüsselt.

Übertragung zum Sennheiser-Lizenzserver

Die gesamte Übertragung von Steuerdaten über das HTTP-Protokoll an den Sennheiser-Lizenzserver wird auf Anwendungsebene verschlüsselt.

Dante Medienverschlüsselung (verfügbar ab Spectera Dante® Firmware-Version 1.1)

Dante Medienverschlüsselung erweitert die Sicherheitsvorteile der Verwendung von Dante® in Ihrem Netzwerk, indem der Medieninhalt während der Übertragung zwischen Geräten verborgen wird. Dante® verwendet den Advanced Encryption Standard (AES) mit einem 256-Bit-Schlüssel, um

branchenführenden Schutz für Medien zu bieten. Das Verbergen des Inhalts von Medienpaketen verhindert, dass böswillige oder unbefugte Benutzer den Dante-Medienverkehr abhören oder stören.

> Bitte beachten Sie die Audinate-Dokumentation für detaillierte Informationen zur Dante®-Verschlüsselung und zur Aktualisierung der Dante®-Firmware:
>
> - Dante Medienverschlüsselung: Audinate/Media-Encryption
> - Aktualisierung der Dante®-Firmware: Dante Updater

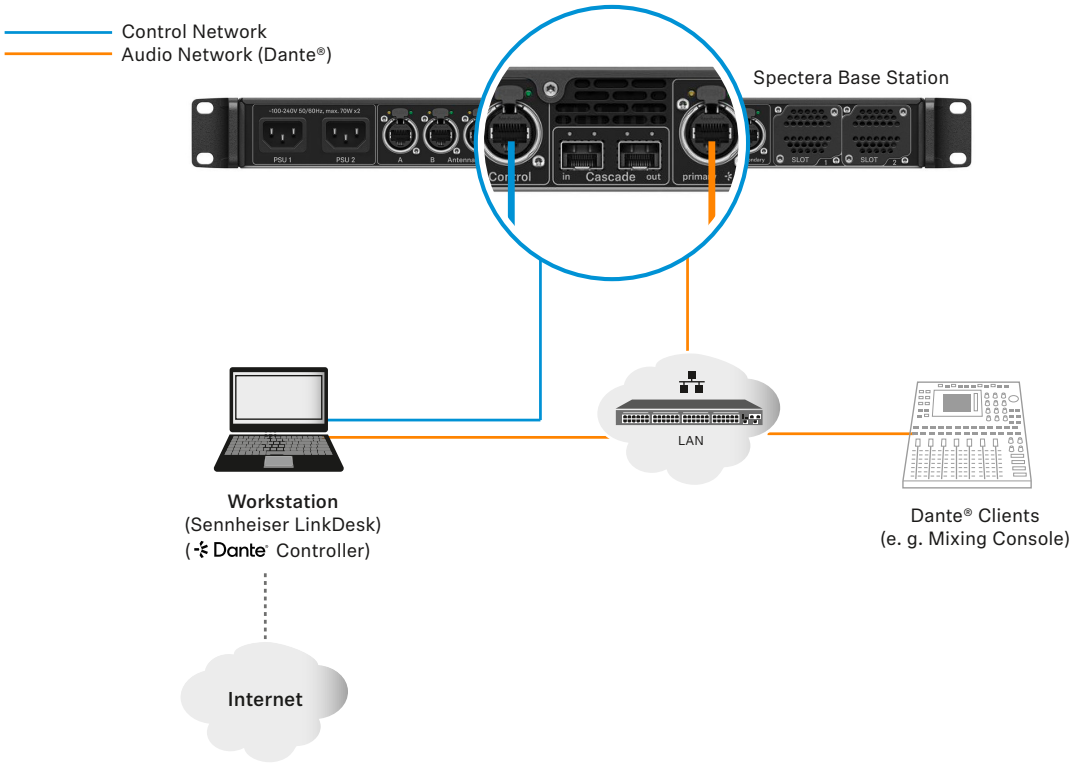
6. Best Practice

6.1. Internetfreigabe in kleinen Netzwerk-Setups

Es ist möglich, das Spectera-Angebot ohne dedizierte Router-Netzwerke zu betreiben, z.B. in wirklich kleinen Setups, aber wir empfehlen, immer eine Art von Heimnetzwerk-Router für eine störungsfreie Nutzung zu verwenden. Speziell für die Internetfreigabe für die Spectera Base Station ist es möglich, die integrierte Funktionalität von Windows und MacOS für die gemeinsame Nutzung der Internetverbindung zu nutzen.

> Für Unternehmensnetzwerke EMPFEHLEN wir NICHT, die gemeinsame Nutzung der Internetverbindung zu verwenden. In den meisten Fällen ist es sogar durch die IT-Richtlinie des Unternehmens verboten, einen solchen Dienst zu nutzen.

Das Netzwerk-Setup könnte folgendermaßen aussehen.



Innerhalb dieses Setups wird eine Workstation für alle Client-Softwareanwendungen (Sennheiser LinkDesk, Spectera WebUI, Dante®-Controller) verwendet. Entweder werden zwei getrennte kabelgebundene Netzwerkschnittstellen für Steuerung und Audio verwendet (Dante®) oder eine Schnittstelle wird gemeinsam genutzt. Bitte beachten Sie, dass bei solchen Setups (in der Regel) kein

DHCP-Dienst aktiviert ist. Verwenden Sie entweder manuelle IP-Einstellungen oder die ZeroConf-Konfiguration.

Für die gemeinsame Nutzung der Internetverbindung wird normalerweise eine vorhandene Netzwerkverbindung (WLAN oder Ethernet) mit Internetzugang mit einer anderen ausgewählten Netzwerkschnittstelle des Hosts gemeinsam genutzt.

Internetfreigabe unter Windows:

1. Schließen Sie das Client-Gerät über ein Ethernet-Kabel an den Host-PC an. Wenn keines der Geräte über einen freien Ethernet-Anschluss verfügt, verwenden Sie einen USB-to-Ethernet-Adapter.
2. Rufen Sie das Menü **Netzwerkverbindungen** auf. Der einfachste Weg dorthin ist die Suche nach „Netzwerkverbindungen“ im Windows-Suchfeld.
3. Klicken Sie mit der rechten Maustaste auf den mit dem Internet verbundenen Netzwerkadapter (z.B. WLAN oder Modem), und wählen Sie dann **Eigenschaften**.
4. Aktivieren Sie auf der Registerkarte Freigabe die Option **Anderen Netzwerkbenutzern Verbindung ermöglichen** und wählen Sie im Pulldown-Menü den entsprechenden Ethernet-Port aus.

> **i** Beachten Sie, dass Sie, wenn Sie VPN-Software installiert haben, möglicherweise viele virtuelle Ethernet-Ports auf Ihrer Liste sehen und den richtigen auswählen müssen.

Nachdem Sie auf **OK** geklickt haben, sollte die Internetverbindung über den Ethernet-Anschluss an das Client-Gerät übertragen werden.

Weitere Informationen zur Internetfreigabe finden Sie auf der Seite Microsoft-Support.

Internetfreigabe unter MacOS:

1. Wählen Sie auf Ihrem Mac das **Apple-Menü** > **Systemeinstellungen**.
2. Klicken Sie in der Seitenleiste auf **Allgemein** und dann auf **Freigabe** (möglicherweise müssen Sie nach unten scrollen).
3. Aktivieren Sie die **Internetfreigabe**, und klicken Sie auf **Konfigurieren**.
4. Klicken Sie im Popupmenü auf die Option **Verbindung freigeben**.
5. Wählen Sie die Internetverbindung aus, die Sie freigeben möchten.
   (Wenn Sie z.B. über WLAN mit dem Internet verbunden sind, wählen Sie WLAN).
6. Aktivieren Sie unter „An Geräte“ den Port, den andere Geräte für den Zugriff auf die freigegebene Internetverbindung verwenden können.
   (Wenn Sie beispielsweise Ihre Internetverbindung über Ethernet freigeben möchten, wählen Sie Ethernet aus.)
   Wenn Sie an Geräte im WLAN freigeben, konfigurieren Sie das Netzwerk für die gemeinsame Nutzung des Internets, und klicken Sie dann auf **OK**.
7. Klicken Sie auf **Fertig**.
   Ihre Internetverbindung wird unter MacOS freigegeben.

Weitere Informationen zur Internetfreigabe finden Sie auf der Seite Apple-Support.