Spectera

Guide réseau et sécurité pour administrateurs informatiques, intégrateurs de systèmes et techniciens d'événements

Sennheiser electronic SE & Co. KG

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

v1.1

SENNHEISER

Sommaire

1. Introduction

Ce document est destiné aux administrateurs informatiques, aux intégrateurs de systèmes et aux techniciens d'événements et sert de guide de planification et de configuration pour l'intégration des composants de la gamme Spectera dans divers environnements réseau, des petits réseaux domestiques aux réseaux d'entreprise.

Le guide contient des recommandations sur la configuration du réseau pour la transmission des données de commande et du contenu audio (via Dante®).

2. Exigences générales

2.1. Systèmes d'exploitation

La Base Station Spectera, en tant qu'appareil réseau, peut être commandée par des appareils PC ou Mac compatibles avec le réseau.

La configuration système requise suivante s'applique au fonctionnement avec Spectera WebUI et Sennheiser LinkDesk:

- Processeur Intel i5 Dual Core/M1 Mac/ou similaire
- 16Go de RAM
- Au moins 4Go d'espace sur le disque dur (5Go pour les appareils Mac)
- Interface LAN Gigabit
- Windows®10, 11, Server2019, Server2022 (x64) ou version supérieure
- Réseau IPv4
- Windows: version10 ou supérieure
- MacOS: version13 ou supérieure

Navigateurs pris en charge pour Spectera WebUI:

- Google Chrome: version125 ou supérieure
- Microsoft Edge: version125 ou supérieure
- Mozilla Firefox: version128 ou supérieure
- Apple Safari: version17 ou supérieure

2.1. Réseau

Bande passante et vitesse

En ce qui concerne les exigences en matière de bande passante pour une qualité audio élevée, un certain nombre de facteurs peuvent affecter l'entrée et la sortie du son. La vitesse du réseau requise spécialement pour la transmission audio via Dante® doit être la plus élevée possible afin de garantir une expérience d'écoute fluide. En règle générale, la bande passante minimale pour la transmission et la réception de données audio dans la Base Station Spectera est approximativement la suivante:

> La majorité des fichiers audio utilisés dans les environnements professionnels sont des PCM (non compressés), échantillonnés à 48kHz et avec une profondeur de bits (longueur de mot) de 24bits. L'audio Dante® est de type unicast par défaut mais peut être configuré pour une utilisation multicast dans le cas d'une distribution «one-to-many» (d'un à plusieurs).
>
> - Dante® regroupe les données audio en flux pour réduire la surcharge du réseau.
> - Les flux audio unicast contiennent jusqu'à 4canaux. Le nombre d'échantillons par canal peut varier entre 4 et 64, en fonction du réglage de la latence de l'appareil. L'utilisation de la bande passante est d'environ 6Mbps par flux audio unicast typique.
> - La bande passante pour les flux multicast dépend du nombre de canaux audio utilisés. La bande passante est d'environ 1,5Mbps par canal.

Source: Informations Dante pour les administrateurs de réseau

Accès Internet

Pour les deux composants Spectera Base Station et Sennheiser LinkDesk, nous recommandons de prévoir un accès permanent à Internet. Veuillez vous référer au chapitre «4. Ports, protocoles et services» pour obtenir plus de détails sur les services Internet utilisés.

> **i** Au moins pour l'activation initiale du produit de la Base Station Spectera et pour l'utilisation de la connexion optionnelle au compte Sennheiser dans Sennheiser LinkDesk, il est obligatoire de disposer d'un accès direct à Internet et d'un support DNS.

> **i** Pour le moment, il n'est pas possible de configurer manuellement un proxy réseau et un serveur DNS sur la Base Station Spectera. Veillez à fournir un accès direct à Internet, par exemple en plaçant l'appareil et tout port, protocole et domaine utilisé sur une liste blanche et en utilisant DHCP pour définir les paramètres du serveur DNS.

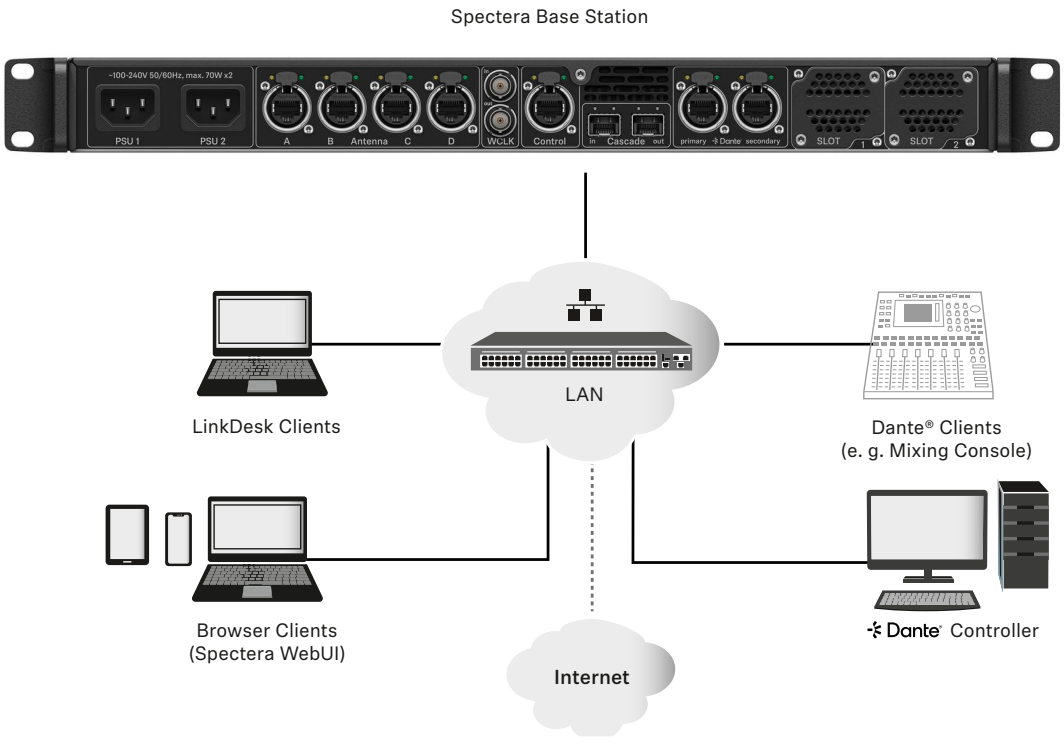
Câblage

Tant qu'une vitesse Internet correcte est garantie, le câble réseau utilisé détermine la vitesse réelle de transmission des données envoyées et reçues dans le réseau.

> **i** Pour garantir une vitesse de transmission fiable des données audio et de commande avec la Base Station Spectera, veuillez utiliser un câble réseau RJ45 avec la norme CAT5e S/FTP ou supérieure

3. Configuration du réseau

Pour fonctionner, les différents composants de la gamme Spectera doivent être intégrés dans une configuration de réseau, existante ou nouvelle. L'illustration suivante présente une vue d'ensemble de la configuration du réseau et de ses participants.



Base Station Spectera

Cet appareil Sennheiser possède 3interfaces réseau: une interface dédiée aux données de commande et deux interfaces pour les données audio (spécifiquement Dante®). Il existe une interface primaire et une interface secondaire pour la redondance de la transmission audio.

Client Sennheiser LinkDesk

Ce client peut être n'importe quel ordinateur hôte (PC ou Mac), avec l'application logicielle LinkDesk installée.

Client navigateur (Spectera WebUI)

Ce client peut être n'importe quel ordinateur hôte (PC, Mac, tablette, smartphone), avec un navigateur Web compatible installé, accédant à Spectera WebUI.

Client Dante®

Il peut s'agir de n'importe quel appareil équipé d'une interface réseau Dante®. Cela va des cartes son virtuelles Dante® installées sur un ordinateur hôte aux appareils dédiés tels qu'une table de mixage.

Contrôleur Dante®

Il s'agit généralement d'un ordinateur hôte (PC ou Mac), sur lequel l'application logicielle Dante® Controller est installée. Cette application configure et commande l'ensemble des appareils Dante® et les flux audio à l'intérieur du réseau.

Routeur réseau

Il peut s'agir de n'importe quel routeur destiné à acheminer les communications réseau à l'intérieur du réseau local (LAN) et à servir de passerelle vers d'autres réseaux et vers internet.

3.1. Base Station Spectera – configuration du réseau

En fonction de la configuration de l'adresse réseau souhaitée, toutes les interfaces réseau (commande et Dante®) peuvent être utilisées dans les modesIP suivants, avec IPv4 uniquement:

- IP fixe/statique
- IP automatique (DHCP ou Zeroconf)

En outre, il est possible de configurer si les informations mDNS/DNS-SD doivent être publiées par l'appareil ou non.

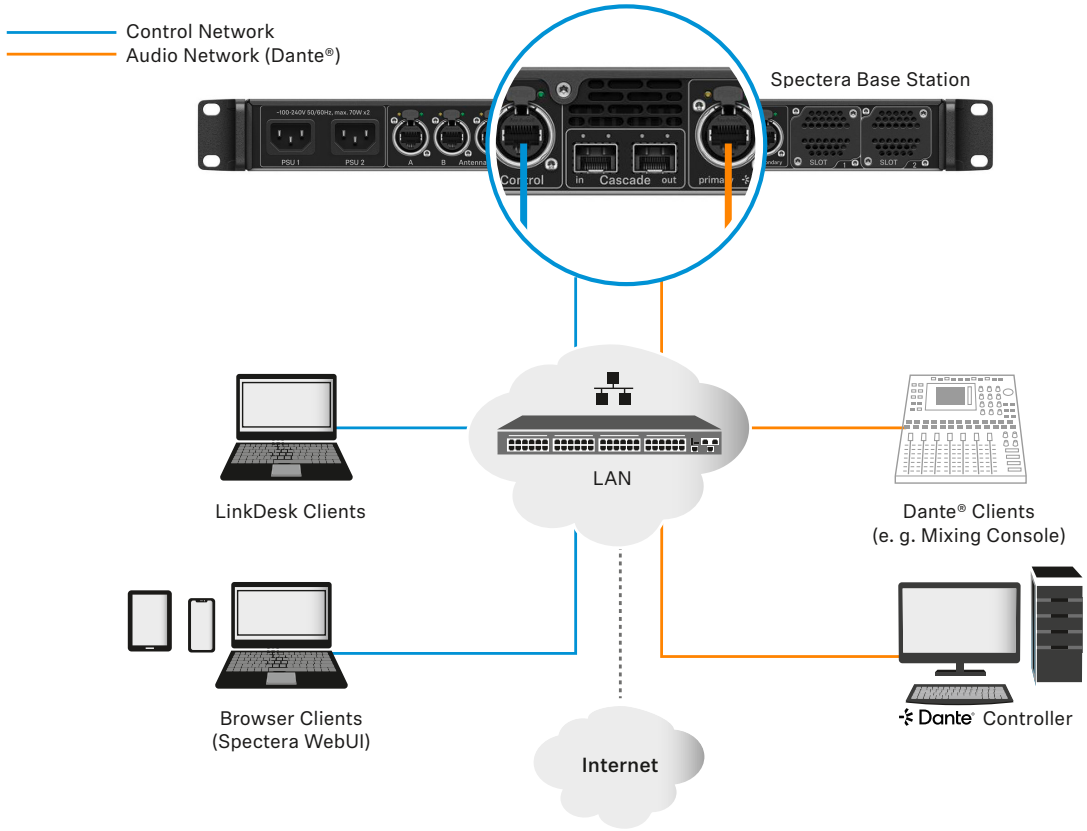
Restrictions Dante®

- Il n'est pas possible de désactiver la fonctionnalité Dante® pour les deux ports Dante®.
- Les ports Dante® sont arrêtés lorsque l'appareil est en mode veille.
- La configuration réseau des ports Dante® ne peut être réalisée que par le biais de l'application logicielle Dante® Controller.
- Par défaut, les ports Dante® sont configurés en Auto IP. Si des IP fixes/statiques ont été configurées et que l'appareil ne peut plus être atteint, le mode IP ne peut être rétabli sur Auto IP que par une réinitialisation des réglages d'usine de l'appareil.
- Les réseaux primaire et secondaire de Dante ne doivent pas être directement connectés l'un à l'autre (boucle de réseau). Veillez à toujours connecter les ports du réseau Dante de la Base Station à deux réseaux différents qui ne fonctionnent pas avec un commutateur commun.

Mode de réseau partagé

En mode de réseau partagé, les deux réseaux pour la commande et Dante® utilisent la même infrastructure de réseau physique.

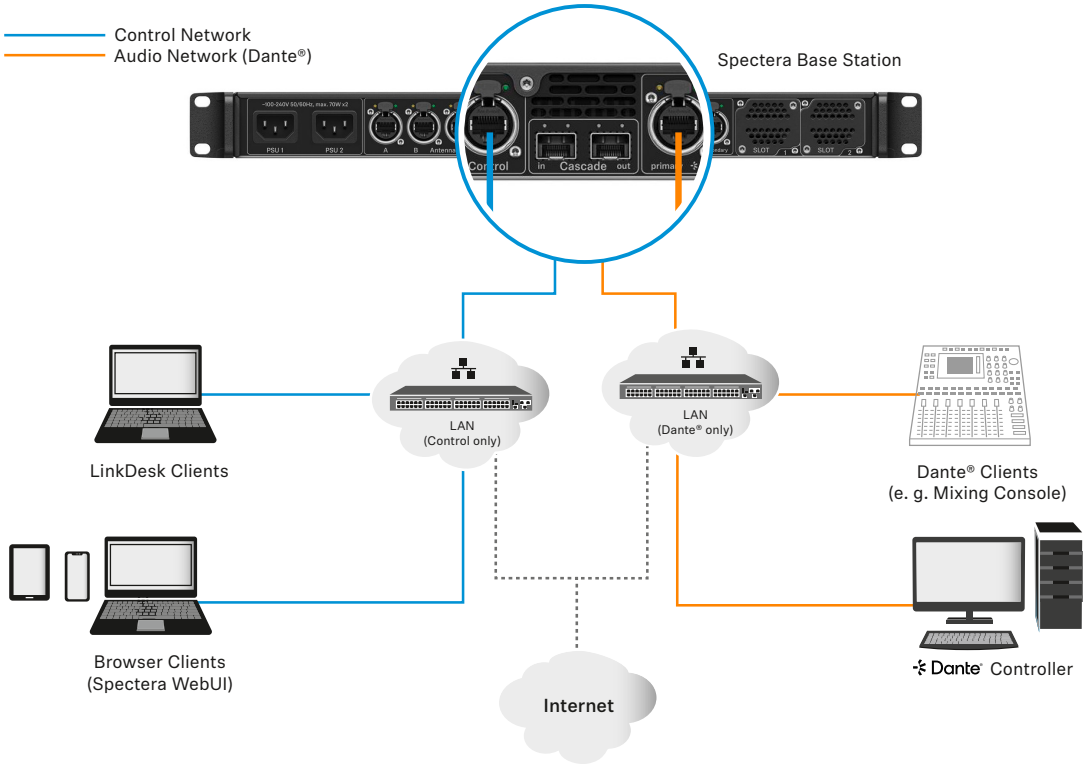
- Configurez les réseaux de commande et Dante® à l'aide d'un seul commutateur/routeur.
- Utilisez deux adresses IP différentes pour adresser séparément le réseau de commande et le réseau Dante®.



Mode de réseau fractionné

En mode de réseau fractionné, les deux réseaux pour la commande et Dante® utilisent des infrastructures de réseau physiques différentes.

- Configurez les réseaux de commande et Dante® sur deux commutateurs/routeurs différents.
- Utilisez deux adresses IP différentes pour adresser séparément le réseau de commande et le réseau Dante®.



4. Ports, protocoles et services

4.1. Sennheiser LinkDesk

Afin d'utiliser le logiciel Sennheiser LinkDesk, certains ports doivent être activés (en particulier pour le pare-feu de l'organisation/l'entreprise) pour la communication entre le logiciel et les appareils. Si nécessaire, veuillez contacter l'administrateur local pour configurer les ports requis.

Adresse	Port	Protocole	Type	Service	Utilisation
Hôte interne					
HÔTE LOCAL	54352	HTTPS (TCP)	Unicast	LinkDesk backend	Communication interne au backend
Hôte sortant					
N'IMPORTE LEQUEL	443	HTTPS (TCP)	Unicast	API de la Base Station Spectera	Communication avec les appareils
Comptes Pro Emea[1] B2C Config[2]	443	HTTPS (TCP)	Unicast	Sennheiser CIAM	Ouverture d'un compte Sennheiser/ connexion
Témoignages des utilisateurs[3] Matomo [4]	443	HTTPS (TCP)	Unicast	Témoignages des utilisateurs de Sennheiser	Analyse des données d'utilisation et des données opérationnelles
Hôte entrant					
N'IMPORTE LEQUEL	443	HTTPS (TCP)	Unicast	API de la Base Station Spectera	API de la Base Station Communication à partir d'appareils
224.0.0.251	5353	mDNS (UDP)	Multicast	mDNS, DNS-SD	(facultatif – si souhaité) découverte de l'appareil/du service

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

4.2. Base Station Spectera

Afin d'utiliser la Base Station Spectera dans un réseau, certains ports doivent être activés (en particulier pour le pare-feu de l'organisation/l'entreprise) pour la communication entre le logiciel et les appareils. Si nécessaire, veuillez contacter l'administrateur local pour configurer les ports requis.

Adresse	Port	Protocole	Type	Service	Utilisation
Appareil sortant					
N'IMPORTE LEQUEL	443	HTTPS (TCP)	Unicast	API de la Base Station Spectera	Communication de l'appareil aux clients
Témoignages des utilisateurs[1] Matomo [2]	443	HTTPS (TCP)	Unicast	Témoignages des utilisateurs de Sennheiser	Analyse des données d'utilisation et des données opérationnelles
my.nalpeiron.com	80	HTTP (TCP)	Unicast	Serveur de licences Sennheiser	Activation des appareils
N'IMPORTE LEQUEL (voir la liste des Serveurs NTP)	123	NTP	Unicast	Serveur de temps NTP	Synchroniser l'heure système
224.0.0.251	5353	mDNS (UDP)	Multicast	mDNS, DNS-SD	(facultatif – si activé) Découverte d'appareils/services
N'IMPORTE LEQUEL (voir la liste des Ports Dante®)					
Appareil entrant					
N'IMPORTE LEQUEL	443	HTTPS (TCP)	Unicast	API de la Base Station Spectera	Communication d'appareil depuis les clients
N'IMPORTE LEQUEL (voir la liste des Ports Dante®)					Données audio et de commande Dante®

[1] sennheiseruserinsights.matomo.cloud

[2] cdn.matomo.cloud

Serveurs NTP

Pour fonctionner correctement avec les licences et les certificats, la Base Station Spectera a besoin d'une heure système correcte. L'appareil utilisera le mécanisme NTP bien établi de la pile de protocoles IP pour synchroniser l'horloge entre un serveur horaire dans un réseau et le client à l'intérieur de l'appareil.

Actuellement, pour un administrateur informatique ou un intégrateur de système, il n'est pas possible de configurer manuellement un serveur NTP dédié qui sera utilisé par la Base Station Spectera. La possibilité de configurer manuellement un serveur NTP dédié est une fonctionnalité prévue pour une prochaine version.

L'appareil se comporte de la manière suivante:

- Si une configuration d'un serveur horaire a été fournie via DHCP ou manuellement, le système essaie de se connecter et de se synchroniser avec ce serveur horaire en premier.
- Dans le cas contraire, l'appareil tente d'accéder à n'importe quel serveur de la liste suivante de pools de serveurs horaires disponibles publiquement dans le monde entier.

> **i** Un administrateur informatique doit s'assurer de fournir un accès Internet à au moins un des pools de serveurs et de fournir des paramètres DNS via DHCP à l'appareil.

Liste des pools de serveurs horaires NTP:

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

4.3. Ports Dante®

Pour configurer un réseau Dante®, des informations sur les ports définis sont nécessaires. Le tableau ci-dessous indique les ports, les URL et les serveurs utilisés. Pour obtenir des informations détaillées, veuillez vous référer directement au site Web : https://www.getdante.com/support/faq/which-network-ports-does-dante-use/

Ports Dante® externes

Adresse	Port	Utilisation	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 (si activé)	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

Ports Dante® internes

Protocole	Port	Utilisation	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. Sécurité

5.1. Certificats

La Base Station Spectera utilise un certificat auto-signé pour la communication réseau. Actuellement, il n'est pas possible de le remplacer par un certificat signé par une autorité de certification. Le certificat est généré en usine et sera renouvelé à chaque réinitialisation des réglages d'usine.

Lorsque vous accédez pour la première fois à Spectera WebUI à l'aide d'un navigateur, vous recevez un avertissement de sécurité vous informant de l'existence d'un certificat inconnu. L'avertissement de sécurité dépend du navigateur que vous utilisez. En fonction de votre navigateur, cliquez sur **Avancé** ou **Afficher les détails** (Safari), puis sur:

- Microsoft Edge: **Continuer vers l'hôte local (non sécurisé)**
- Google Chrome: **Poursuivre vers l'hôte local (non sécurisé)**
- Firefox: **Accepter le risque et continuer**
- Apple Safari: **[...] consulter ce site Web** -> **Consulter ce site Web**
- ou toute autre option similaire (autres navigateurs)

Afin d'éviter les attaques de type «man-in-the-middle» (MITM), le Sennheiser LinkDesk dispose de certaines mesures de sécurité intégrées. En raison de ces mesures, il se peut que vous receviez un avertissement d'incompatibilité de certificat lorsque vous travaillez avec une Base Station. Dans certains cas, ces problèmes peuvent survenir même s'il n'y a pas de problème de sécurité. Il s'agit de:

- Les réglages d'usine de la Base Station ont été réinitialisés depuis la dernière connexion. Dans ce cas, vous pouvez confirmer la connexion en toute sécurité et continuer lorsque vous rencontrez l'avertissement d'incompatibilité.
- Une autre Base Station a été connectée au moyen de la même adresse IP. Dans ce cas, veuillez vérifier si l'adresse IP que vous utilisez est bien l'adresse IP correcte de la Base Station prévue.

5.2. Mot de passe de l'appareil

L'accès à l'appareil par le biais de l'API de contrôle du réseau et l'interface Web de la Base Station Spectera et via Sennheiser LinkDesk est protégé par un mot de passe, afin d'éviter la configuration du dispositif par des acteurs non autorisés à l'intérieur du réseau.

Après le déballage et après chaque réinitialisation des réglages d'usine de l'appareil, un nouveau mot de passe doit être configuré par l'utilisateur pour réclamer l'accès à l'appareil. Chaque instance de Sennheiser LinkDesk se souvient des mots de passe des appareils qu'elle a déjà réclamés. Pour protéger l'accès d'acteurs non autorisés à l'application Sennheiser LinkDesk sur un hôte, d'autres mécanismes doivent être appliqués, par exemple des comptes d'utilisateurs protégés par mot de passe dans Windows ou MacOS.

À chaque nouvelle session de navigation dans Spectera WebUI, le mot de passe configuré doit être saisi à nouveau.

5.3. Transmission de données cryptées

Toutes les données de commande transmises par le protocole HTTPS sont cryptées à l'aide du protocole TLS (Transport Layer Security).

Transmission au serveur de licences Sennheiser

Toute transmission de données de contrôle sur le protocole HTTP vers le serveur de licences Sennheiser est chiffrée au niveau de l'application.

Chiffrement des médias Dante (disponible à partir de la version 1.1 du firmware Spectera Dante®)

Le chiffrement des médias Dante étend les avantages de sécurité de l'utilisation de Dante® sur votre réseau en dissimulant le contenu des médias pendant la transmission entre les appareils. Dante® utilise la norme de chiffrement avancée (AES) avec une clé de 256 bits pour fournir une protection des médias de premier plan dans l'industrie. Dissimuler le contenu des paquets multimédias empêche les

utilisateurs malveillants ou non autorisés d'écouter ou d'interférer avec le trafic multimédia Dante.

> Veuillez vous référer à la documentation d'Audinate pour des informations détaillées sur le chiffrement Dante® et sur la façon de mettre à jour le firmware Dante® :
>
> - Chiffrement des médias Dante : Audinate/Media-Encryption
> - Mise à jour du firmware Dante® : Dante Updater

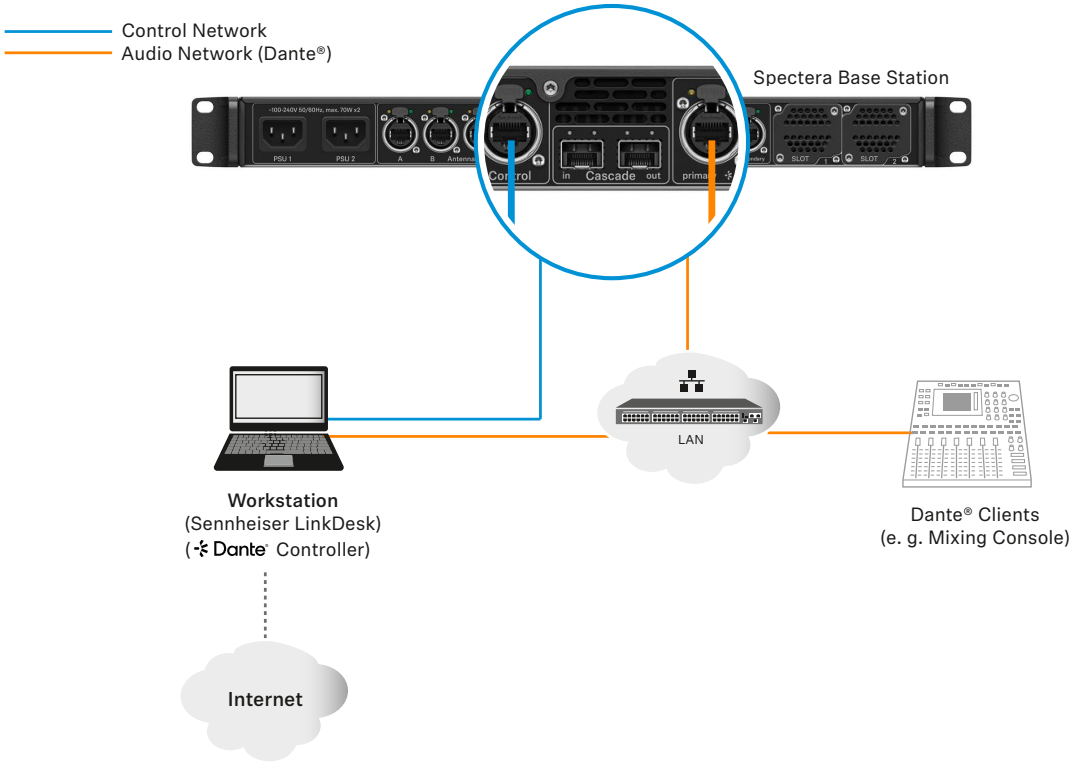
6. Meilleures pratiques

6.1. Partage de la connexion Internet dans les petits réseaux

Il est possible d'exploiter la gamme Spectera sans routeur de réseau dédié, par exemple dans les très petites configurations, mais nous recommandons de toujours utiliser une sorte de routeur de réseau domestique pour une utilisation sans problème. Notamment pour fournir un accès Internet à la Base Station Spectera, il est possible d'utiliser la fonctionnalité intégrée de Windows et de MacOS pour le partage de connexion Internet.

> Pour les réseaux d'entreprise, nous NE RECOMMANDONS PAS l'utilisation du partage de connexion Internet. La plupart du temps, les règles informatiques de l'entreprise interdisent même l'utilisation de ce type de service.

La configuration du réseau pourrait ressembler à ceci.



Dans cette configuration, un poste de travail est utilisé pour toutes les applications logicielles client (Sennheiser LinkDesk, Spectera WebUI, Dante® Controller). Soit deux interfaces de réseau filaire séparées sont utilisées pour la commande et l'audio (Dante®), soit une interface est partagée. Veuillez noter que, dans ce type de configurations (en général), aucun service DHCP n'est activé. Utilisez les paramètres IP manuels ou la configuration ZeroConf.

Dans le cas du partage de connexion Internet, une connexion réseau existante (Wi-Fi ou Ethernet) avec accès à Internet est généralement partagée avec une autre interface réseau sélectionnée de l'hôte.

Pour partager votre connexion Internet sous Windows:

1. Connectez votre appareil client à votre PC hôte à l'aide d'un câble Ethernet. Si l'un des appareils ne dispose pas d'un port Ethernet libre, utilisez un adaptateur USB-Ethernet.
2. Accédez au menu **Connexions réseau**. Le moyen le plus simple d'y parvenir est de rechercher «Connexions réseau» dans la boîte de recherche Windows.
3. Cliquez avec le bouton droit de la souris sur l'adaptateur réseau connecté à Internet (par exemple, Wi-Fi ou modem), puis sélectionnez **Propriétés**.
4. Basculez l'option **Autoriser les autres utilisateurs du réseau à se connecter** sur **ON** dans l'onglet Partage et sélectionnez le port Ethernet approprié dans le menu déroulant.

> **i** Notez que, si vous avez installé un logiciel VPN, il se peut que vous voyiez de nombreux ports Ethernet virtuels dans votre liste et que vous deviez choisir le port correct.

Une fois que vous avez cliqué sur **OK**, Internet devrait être acheminé vers votre appareil client via son port Ethernet.

Pour obtenir plus de détails sur le partage d'une connexion Internet, veuillez consulter la page d'assistance de Microsoft.

Pour partager votre connexion Internet sur MacOS:

1. Sur votre Mac, sélectionnez le **menu Apple** > **Paramètres système**.
2. Cliquez sur **Général** dans la barre latérale, puis sur **Partage** (il se peut que vous deviez faire défiler la page vers le bas).
3. Activez le **partage Internet** et cliquez sur **Configurer**.
4. Cliquez dans le menu contextuel sur **Partager votre connexion à partir de**.
5. Choisissez la connexion Internet que vous souhaitez partager.
   (Par exemple, si vous êtes connecté à Internet via Wi-Fi, choisissez Wi-Fi).
6. Sous «Vers les appareils utilisant», activez le port que d'autres appareils peuvent utiliser pour accéder à la connexion Internet partagée.
   (Par exemple, si vous souhaitez partager votre connexion Internet via Ethernet, sélectionnez Ethernet).
   Si vous partagez avec des appareils utilisant le Wi-Fi, configurez le réseau de partage Internet, puis cliquez sur **OK**.
7. Cliquez sur **Terminé**.
   Votre connexion Internet sera partagée sur MacOS.

Pour obtenir plus de détails sur le partage d'une connexion Internet, veuillez consulter la page d'assistance Apple.