
# Spectera

## Guía de redes y seguridad para administradores de TI, integradores de sistemas y técnicos de eventos

**Sennheiser electronic SE & Co. KG**

Am Labor 1, 30900 Wedemark (Alemania), www.sennheiser.com
v1.1

SENNHEISER

# Contenido

# 1. Introducción

Este documento está destinado a administradores de TI, integradores de sistemas y técnicos de eventos y sirve como guía de planificación y configuración para integrar los componentes del catálogo de Spectera en diversos entornos de red, desde redes domésticas pequeñas hasta redes empresariales.

La guía contiene recomendaciones sobre la configuración de la red para la transmisión de datos de control y contenido de audio (a través de Dante®).

# 2. Requisitos generales

## 2.1. Sistemas operativos

La Base Station Spectera, como dispositivo de red, puede controlarse desde ordenadores Windows o Mac con conexión a la red.

**Los siguientes requisitos del sistema se aplican al funcionamiento con la WebUI de Spectera o el software LinkDesk de Sennheiser:**

- Procesador Intel i5 Dual Core/M1 Mac/o similar
- RAM de 16GB
- Al menos 4GB de espacio en el disco duro (5GB para dispositivos Mac)
- Interfaz Gigabit LAN
- Windows® 10, 11, Server 2019, Server 2022 (x64) o superior
- Red IPv4
- Windows: 10 o posterior
- MacOS: 13 o posterior

**Navegadores compatibles con la WebUI de Spectera:**

- Google Chrome: 125 o posterior
- Microsoft Edge: 125 o posterior
- Mozilla Firefox: 128 o posterior
- Safari de Apple: 17 o posterior

## 2.1. Red

### Ancho de banda y velocidad

Los requisitos de ancho de banda para obtener audio de alta calidad dependen de diversos factores que afectan tanto la entrada como la salida de señal. La velocidad de red requerida para la transmisión de audio a través de Dante® debe ser lo más alta posible para garantizar una experiencia de audio fluida. Como regla general, el ancho de banda mínimo para transmitir y recibir audio en la Base Station Spectera es aproximadamente el siguiente:

> La mayor parte del audio utilizado en configuraciones profesionales es PCM (sin comprimir), muestreado a 48kHz y una profundidad de bits (longitud de palabra) de 24bits. El audio Dante® es unicast por defecto, pero se puede configurar para usar multicast en casos de distribución de uno a muchos.
>
> - Dante® agrupa el audio en flujos para reducir la sobrecarga de la red.
> - Los flujos de audio de unicast contienen hasta 4canales. Las muestras por canal pueden variar entre 4 y 64, dependiendo de la configuración de la latencia del dispositivo. El uso de ancho de banda es de aproximadamente 6Mbps por flujo de audio unicast típico.
> - El ancho de banda de los flujos multicast depende del número de canales de audio utilizados. El ancho de banda es de aproximadamente 1,5Mbps por canal
>
> Fuente: Información de Dante para administradores de red

### Acceso a Internet

Para ambos componentes, la Base Station Spectera y LinkDesk de Sennheiser, se recomienda proporcionar acceso permanente a Internet. Consulte el capítulo “4. Puertos, protocolos y servicios” para obtener más información sobre los servicios de Internet que se usan.

> **i** Al menos para la activación inicial del producto de la Base Station Spectera y para el uso del inicio de sesión opcional de la cuenta Sennheiser en LinkDesk, es obligatorio tener un acceso directo a Internet y soporte DNS.

> **i** Por el momento, no es posible configurar manualmente ningún proxy de red ni servidor DNS en la Base Station Spectera. Asegúrese de proporcionar acceso directo a Internet, por ejemplo, a través de la lista blanca del dispositivo y cualquier puerto, protocolo y dominio utilizado, y utilizando DHCP para proporcionar la configuración del servidor DNS.

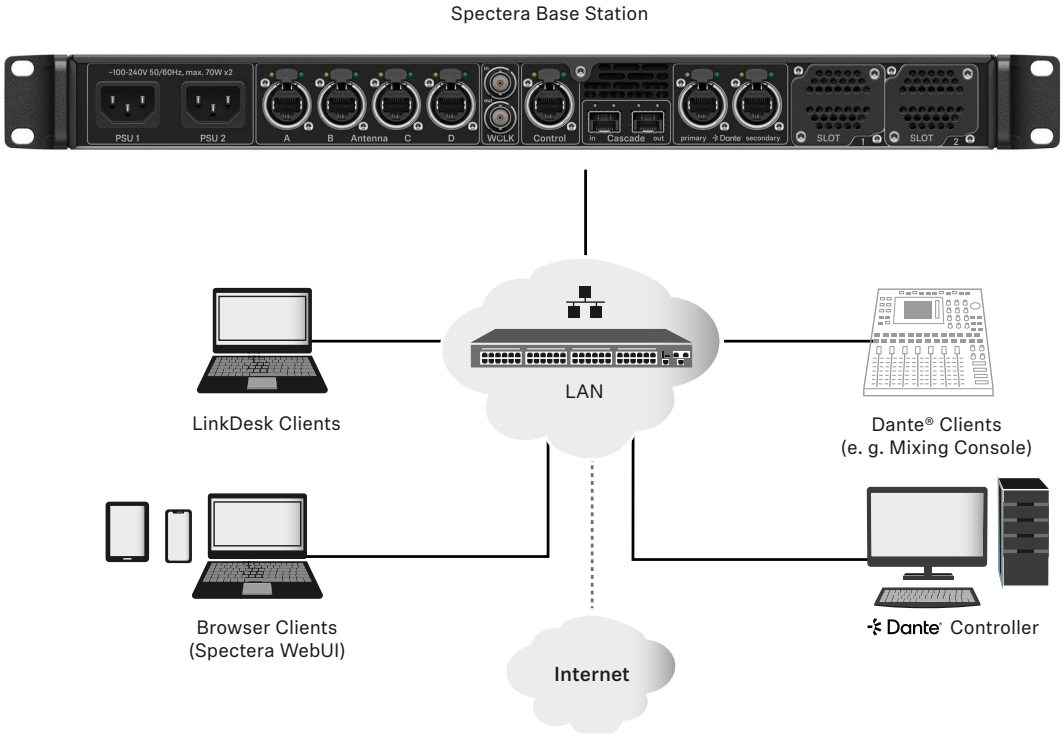
### Cableado

Siempre que se garantice una buena velocidad de Internet, el cable de red utilizado determina la velocidad de transmisión real de los datos enviados y recibidos en la red.

> **i** Para garantizar una velocidad de transmisión fiable de datos de audio y control con la Base Station Spectera, utilice un cable de red RJ45 con el estándar CAT5e S/FTP o superior.

## 3. Configuraciones de red

Para utilizar los diversos componentes del catálogo Spectera, estos deben integrarse en una configuración de red, ya sea existente o nueva. La siguiente figura muestra una vista general de la configuración de red y sus participantes.



**Base Station Spectera**

Este dispositivo Sennheiser tiene 3 interfaces de red. Una interfaz se dedica a los datos de control y dos interfaces a los datos de audio (específicamente, Dante®). Hay una interfaz primaria y una secundaria para la redundancia de la transmisión de audio.

**Cliente LinkDesk de Sennheiser**

Este cliente puede ser cualquier ordenador anfitrión (PC o Mac) con la aplicación de software LinkDesk instalada.

**Cliente navegador (Spectera WebUI)**

Este cliente puede ser cualquier ordenador anfitrión (PC, Mac, tableta, teléfono inteligente), con un navegador web compatible instalado, que acceda a la Spectera WebUI.

**Cliente Dante®**

Puede ser cualquier dispositivo con una interfaz de red Dante® instalada, como Virtual Dante® Soundcards instaladas en un ordenador anfitrión o dispositivos dedicados, como una mesa de mezclas.

**Dante® Controller**

Normalmente se trata de un ordenador anfitrión (PC o Mac), con la aplicación de software Dante® Controller instalada. Esta aplicación configura y controla todos los dispositivos de Dante® y las transmisiones de audio dentro de la red.

**Router de red**

Puede ser cualquier dispositivo router para enrutar la comunicación de red dentro de la red de área local (LAN) y proporcionar la puerta de enlace a otras redes y a Internet.

## 3.1. Base Station Spectera: configuración de red

Dependiendo de la configuración de la dirección de red deseada, toda la interfaz de red (Control y ambos Dante®) se puede utilizar en los siguientes modos IP con IPv4 solamente:

- IP fija/estática
- IP automática (DHCP o Zeroconf)

Además, se puede configurar si el dispositivo puede publicar la información mDNS/DNS-SD o no.

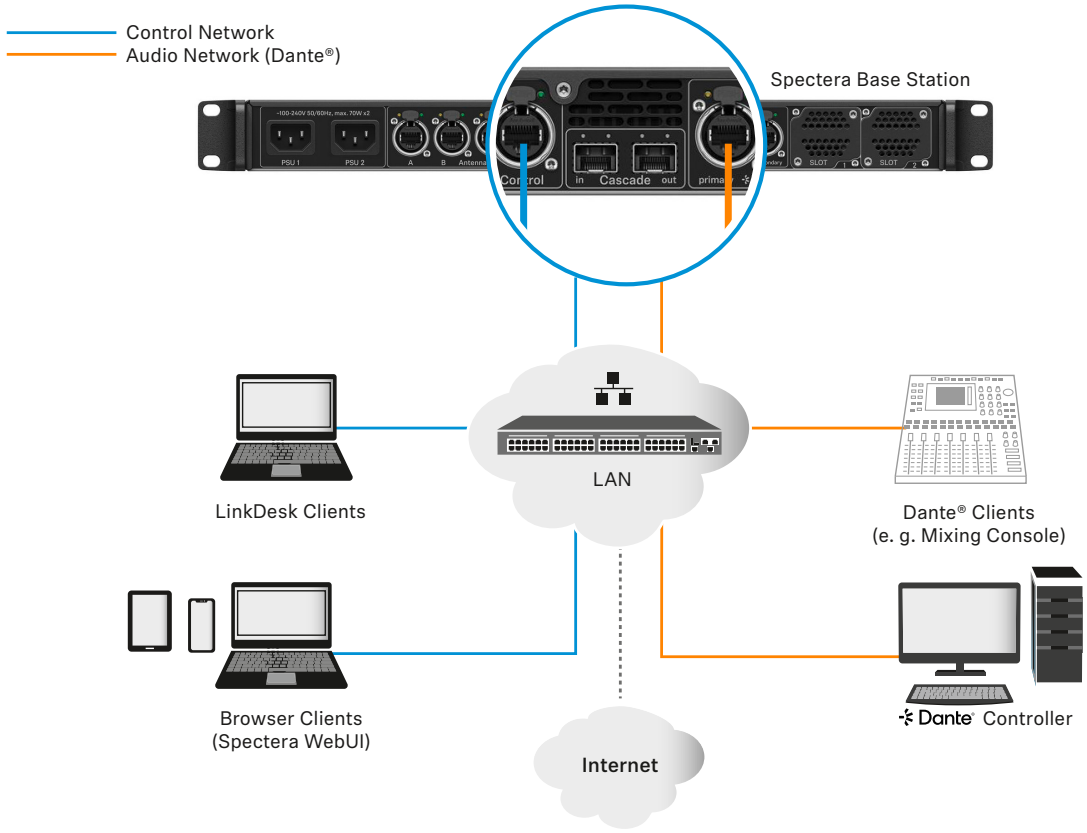
**Restricciones de Dante®**

- No es posible desactivar la funcionalidad Dante® para ambos puertos Dante®.
- Los puertos Dante® se apagan cuando el dispositivo está en modo de espera.
- La configuración de red de los puertos Dante® solo se puede realizar a través de la aplicación de software Dante® Controller.
- De forma predeterminada, los puertos Dante® están configurados con una IP automática. Si se han configurado IP fijas/estáticas y ya no se puede establecer la conexión con el dispositivo, el modo IP solo se puede restablecer a una IP automática mediante un restablecimiento de los ajustes de fábrica del dispositivo.
- Las redes primaria y secundaria de Dante no deben estar conectadas directamente entre sí (bucle de red). Asegúrese de conectar siempre los puertos de red Dante de la Base Station a dos redes diferentes que no se ejecuten a través de un conmutador común.

## Modo de red compartida

En el Modo de red compartida, tanto las redes para Control como Dante® utilizan la misma infraestructura de red física.

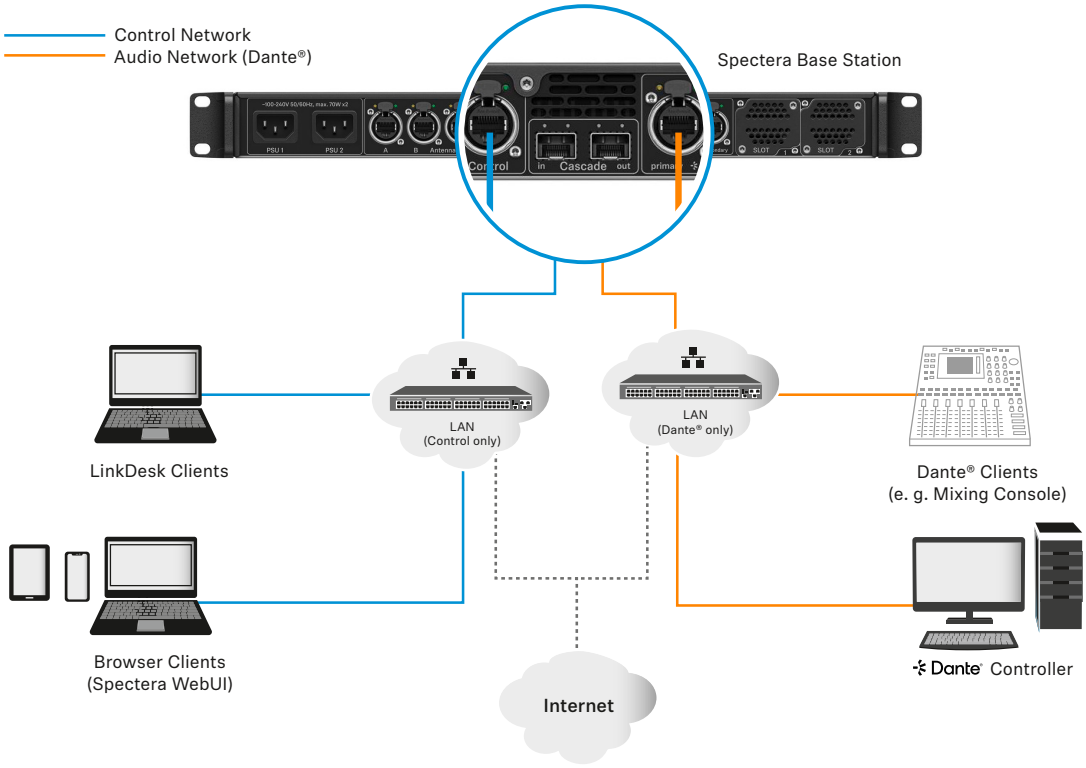
- Configure las redes de Control y Dante® a través de un interruptor o router.
- Utilice dos IP diferentes para dirigirse a la red Control y a la red Dante® por separado.



## Modo de red dividida

En el Modo de red dividida, tanto las redes para Control como Dante® utilizan una infraestructura de red física diferente.

- Configure las redes de Control y Dante® en dos interruptores y routers diferentes.
- Utilice dos IP diferentes para dirigirse a la red Control y a la red Dante® por separado.



# 4. Puertos, protocolos y servicios

## 4.1. LinkDesk de Sennheiser

Para utilizar el software LinkDesk de Sennheiser, se deben habilitar ciertos puertos (especialmente para el firewall de la organización/empresa) para la comunicación entre el software y los dispositivos. Si es necesario, póngase en contacto con el administrador local para configurar los puertos necesarios.

| Dirección | Puerto | Protocolo | Tipo | Servicio | Uso |
|---|---|---|---|---|---|
| Anfitrión interno | | | | | |
| LOCALHOST | 54352 | HTTPS (TCP) | Unicast | Backend de LinkDesk | Comunicación interna de backend |
| **Salida del anfitrión** | | | | | |
| Cualquiera | 443 | HTTPS (TCP) | Unicast | API de la Base Station de Spectera | Comunicación con los dispositivos |
| Cuentas Pro Emea[1]<br>Configuración de B2C[2] | 443 | HTTPS (TCP) | Unicast | Sennheiser CIAM | Registro/inicio de sesión de la cuenta de Sennheiser |
| Información del usuario[3]<br>Matomo[4] | 443 | HTTPS (TCP) | Unicast | Información del usuario de Sennheiser | Análisis de datos operativos y de uso |
| **Anfitrión entrante** | | | | | |
| Cualquiera | 443 | HTTPS (TCP) | Unicast | API de la Base Station de Spectera | API de la Base Station Comunicación desde los dispositivos |
| 224.0.0.251 | 5353 | mDNS (UDP) | Multicast | mDNS, DNS-SD | (Opcional, si se desea) Detección de dispositivos/servicios |

[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

Para utilizar el dispositivo Base Station Spectera en una red, se deben habilitar ciertos puertos (especialmente para el firewall de la organización/empresa) para la comunicación entre el software y los dispositivos. Si es necesario, póngase en contacto con el administrador local para configurar los puertos necesarios.

| Dirección | Puerto | Protocolo | Tipo | Servicio | Uso |
|---|---|---|---|---|---|
| **Salida del dispositivo** | | | | | |
| Cualquiera | 443 | HTTPS (TCP) | Uni-cast | API de la Base Station de Spectera | Comunicación del dispositivo hacia los clientes |
| Información del usuario[1] Matomo[2] | 443 | HTTPS (TCP) | Uni-cast | Información del usuario de Sennheiser | Análisis de datos operativos y de uso |
| my.nalpeiron.com | 80 | HTTP (TCP) | Uni-cast | Servidor de licencias Sennheiser | Activación de dispositivos |
| CUALQUIERA (véase la lista de Servidores NTP) | 123 | NTP | Uni-cast | Servidor de tiempo NTP | Sincronizar hora del sistema |
| 224.0.0.251 | 5353 | mDNS (UDP) | Multi-cast | mDNS, DNS-SD | (Opcional, si se activa) Detección de dispositivos/servicios |
| CUALQUIERA (véase la lista de Puertos Dante®) | | | | | |
| **Entrada del dispositivo** | | | | | |
| Cualquiera | 443 | HTTPS (TCP) | Uni-cast | API de la Base Station de Spectera | Comunicación de los clientes hacia el dispositivo |
| CUALQUIERA (véase la lista de Puertos Dante®) | | | | | Datos de audio y control de Dante® |

[1] sennheiseruserinsights.matomo.cloud

[2] cdn.matomo.cloud

## Servidores NTP

Para funcionar correctamente con licencias y certificados, la Base Station Spectera necesita una hora de sistema correcta. El dispositivo utilizará el mecanismo NTP, ampliamente reconocido y utilizado dentro de la pila de protocolos IP, para sincronizar el reloj entre un servidor de tiempo en la red y el cliente dentro del dispositivo.

Actualmente, un administrador informático o un integrador de sistemas no puede configurar manualmente un servidor NTP dedicado para que lo utilice la Base Station Spectera. La posibilidad de configurar manualmente un servidor NTP dedicado es una característica que se ha planificado para una futura versión.

El dispositivo se comporta de la siguiente manera:

- Si se ha proporcionado una configuración de servidor de tiempo a través de DHCP o manualmente, este primero intenta conectarse y sincronizarse con dicho servidor.
- De lo contrario, el dispositivo intenta acceder a cualquier servidor de la siguiente lista de grupos de servidores de tiempo, los cuales están disponibles de forma pública en todo el mundo.

> Un administrador informático debe asegurarse de proporcionar acceso a Internet a al menos uno de los grupos de servidores y de introducir la configuración DNS a través de DHCP al dispositivo.

**Lista de grupos de servidores de tiempo NTP:**

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

## 4.3. Puertos Dante®

Para configurar una red Dante®, se requiere la información de puerto definida. La siguiente tabla muestra qué puertos, URL y servidores se utilizan. Para más información detallada, consulte directamente el sitio web: https://www.getdante.com/support/faq/which-network-ports-does-dante-use/

### Puertos Dante® externos

| Dirección | Puerto | Uso | Tipo |
|---|---|---|---|
| 239.255.0.0/16 | 4321 | Audio ATP Multicast | Multicast |
| 239.69.0.0/16 | 5004 | Audio AES67 Multicast | Multicast |
| 224.0.1.129-132 | 319, 320 | PTP | Multicast y unicast (DDM) |
| 224.0.0.251 | 5353 | mDNS | Multicast |
| 224.0.0.230 – 233 | 8700 – 8708 | Control y monitorización multicast | Multicast |
| 239.254.1.1 | 9998 | Registro | Multicast |
| 239.254.3.3 | 9998 | Registro TP (si está habilitado) | Multicast |
| 239.254.44.44 | 9998 | Registro | Multicast |
| 239.255.255.255 | 9875 | SAP (descubrimiento AES67) | Multicast |
| UDP | 28800, 28700-28708 | Control y monitorización (ext.) | Unicast |
| UDP | 38800, 38700-38708 | Control y monitorización de DVS (ext.) | Unicast |

### Puertos Dante® internos

| Protocolo | Puerto | Uso | Tipo |
|---|---|---|---|
| UDP | 14336 -14591 | Audio unicast (excluyendo vía) | Unicast |
| UDP | 34336-34600 | Audio unicast (solo vía) | Unicast |
| UDP | 4440, 4444, 4455 | Control de audio (excluyendo vía) | Unicast |
| UDP | 24440, 24441, 24444, 24455 | Control de audio (solo vía) | Unicast |
| UDP | 4777 | Vía de control (solo vía) | Unicast |
| TCP | 4777 | Vía websocket | Unicast |
| UDP | 8850,28900, 24445 | Control y monitorización de vía (int.) | Unicast |
| UDP | 8850, 38900, 8899 | Control y monitorización de DVS (int.) | Unicast |
| UDP | 8000 | Puerto del dispositivo de Dante Domain Manager | Unicast |
| UDP | 8001 | Proxy de dispositivo Dante Millau (int.) | Unicast |
| UDP | 8002 | Servidor de bloqueo Dante | Unicast |
| UDP | 8751 | Puerto de medición de Dante Controller | Unicast |
| UDP | 8800 | Control y monitorización | Unicast |
| TCP | 8753 | Clientes mDNS (solo para uso interno) | Unicast |
| TCP | 16100-16131 | Autenticación HDCP para puntos finales de vídeo | Unicast |
| UDP | 61440-61951 | Mantenimiento de flujo de audio a nivel FPGA | Unicast |
| TCP | 4778 | Websocket DVS (solo Apple Silicon) | Unicast |

# 5. Seguridad

## 5.1. Certificados

La Base Station Spectera utiliza un certificado autofirmado para la comunicación de red. Actualmente, no es posible reemplazarlo con un certificado firmado por CA. El certificado se genera en fábrica y se renueva al restablecer los ajustes de fábrica.

Al acceder a la Spectera WebUI con un navegador por primera vez, se le mostrará un aviso de seguridad que indica que hay un certificado desconocido. Dicho aviso dependerá del navegador que use. Dependiendo de su navegador, haga clic en **Avanzado** o **Mostrar detalles** (Safari) y, posteriormente, en:

- Microsoft Edge: **Continuar a localhost (no seguro)**
- Google Chrome: **Acceder a localhost (sitio no seguro)**
- Firefox: **Aceptar el riesgo y continuar**
- Safari de Apple: **[...] visitar este sitio web** -> **Visitar este sitio web**
- o similar (en otros navegadores)

Para evitar ataques de tipo «hombre en el medio» (MITM por su sigla en inglés), LinkDesk de Sennheiser incorpora ciertas medidas de seguridad que pueden generar advertencias de error por coincidencia de certificados al utilizar una Base Station. En algunos casos, esto puede ocurrir aunque en realidad no haya ningún problema de seguridad. Los casos más comunes son los siguientes:

- Se han restablecido los ajustes de fábrica de la Base Station desde la última conexión. En este caso, puede confirmar de forma segura la conexión y continuar cuando le aparezca el aviso de no coincidencia.
- Se ha conectado una Base Station diferente a través de la misma dirección IP. En este caso, compruebe si la dirección IP que está utilizando es realmente la dirección IP correcta de la Base Station prevista.

## 5.2. Contraseña del dispositivo

El acceso al dispositivo a través de la API de control de red y la WebUI de la Base Station Spectera y a través de LinkDesk de Sennheiser está protegido por contraseña; de este modo se evita que los actores no autorizados configuren el dispositivo dentro de la red.

Después del desempaquetado o de un restablecimiento de los valores de fábrica, el usuario deberá establecer una nueva contraseña para recuperar el acceso al dispositivo. Cada instancia de LinkDesk de Sennheiser recuerda las contraseñas de los dispositivos que ya ha reclamado. Al proteger el acceso de actores no autorizados a la aplicación LinkDesk de Sennheiser en un anfitrión, se deben aplicar otros mecanismos, por ejemplo, cuentas de usuario protegidas con contraseña en Windows o MacOS.

Con cada nueva sesión del navegador de la Spectera WebUI, la contraseña configurada debe introducirse de nuevo.

## 5.3. Transmisión de datos cifrados

Toda transmisión de datos de control en el protocolo HTTPS se cifra mediante seguridad de capa de transporte (TLS, por sus siglas en inglés).

### Transmisión al servidor de licencias Sennheiser

Toda la transmisión de datos de control en el protocolo HTTP al servidor de licencias Sennheiser está encriptada a nivel de aplicación.

### Encriptación de medios Dante (disponible a partir de la versión de firmware 1.1 de Spectera Dante®)

La encriptación de medios Dante extiende los beneficios de seguridad de usar Dante® en su red al ocultar el contenido de los medios durante la transmisión entre dispositivos. Dante® utiliza el Estándar de Encriptación Avanzada (AES) con una clave de 256 bits para proporcionar una

protección de medios líder en la industria. Ocultar el contenido de los paquetes de medios previene que usuarios maliciosos o no autorizados escuchen o interfieran con el tráfico de medios Dante.

> Por favor, consulte la documentación de Audinate para obtener información detallada sobre la encriptación de Dante® y sobre cómo actualizar el firmware de Dante®:
>
> - Encriptación de Medios Dante: Audinate/Media-Encryption
> - Actualización del firmware de Dante®: Dante Updater

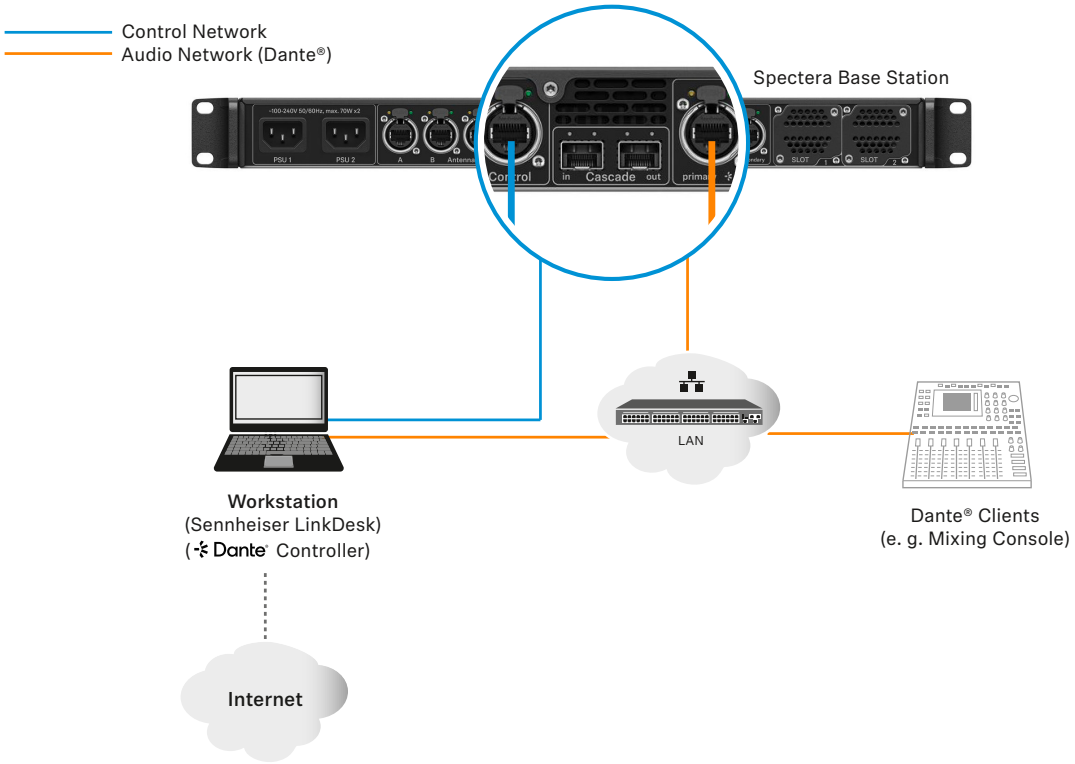
# 6. Mejores prácticas

## 6.1. Compartir la conexión a Internet en pequeñas configuraciones de red

Es posible utilizar las soluciones de Spectera sin redes de router dedicadas (por ejemplo, en configuraciones realmente pequeñas), pero recomendamos usar siempre algún tipo de router de red doméstica para disfrutar de un uso sin problemas. Especialmente para proporcionar acceso a Internet a una Base Station Spectera se puede utilizar la funcionalidad integrada de Windows y MacOS para compartir la conexión a Internet.

> Para redes empresariales NO RECOMENDAMOS el uso de una conexión compartida a Internet. La mayoría de las veces, el uso de dicho servicio incluso está prohibido por la política informática de la empresa.

La configuración de la red podría verse así.




Dentro de esta configuración, se utiliza una estación de trabajo para todas las aplicaciones de software cliente (LinkDesk de Sennheiser, Spectera WebUI, Dante® Controller). Se utilizan dos interfaces de red cableadas separadas para control y audio (Dante®) o se comparte una interfaz.

Tenga en cuenta que en estas configuraciones (normalmente) no se activa ningún servicio DHCP. Utilice la configuración manual de IP o la configuración de ZeroConf.

Para la conexión compartida a Internet, normalmente una conexión de red existente (wifi o Ethernet) con acceso a Internet se comparte con otra interfaz de red seleccionada del anfitrión.

**Para compartir su conexión a Internet en Windows:**

1. Conecte su dispositivo cliente a su PC anfitrión mediante un cable Ethernet. Si cualquiera de los dispositivos no tiene un puerto Ethernet libre, utilice un adaptador USB a Ethernet.
2. Vaya al menú **Conexiones de red**. La forma más fácil de acceder es buscando «Conexiones de red» en el cuadro de búsqueda de Windows.
3. Haga clic con el botón derecho en el adaptador de red conectado a Internet (por ejemplo, wifi o módem) y, a continuación, seleccione **Propiedades**.
4. Ponga la opción **Permitir que otros usuarios de la red se conecten** en **ON** desde la pestaña Compartir y seleccione el puerto Ethernet correspondiente en el menú desplegable.

> **i** Tenga en cuenta que, si tiene instalado un software VPN, puede ver muchos puertos Ethernet virtuales en su lista y tendrá que elegir el adecuado.

Después de hacer clic en **Aceptar**, Internet debe llegar al dispositivo cliente a través de su puerto Ethernet.

Para obtener más información sobre cómo compartir una conexión a Internet, consulte la página Soporte técnico de Microsoft.

**Para compartir su conexión a Internet en MacOS:**

1. En su Mac, seleccione el **menú Apple** > **Configuración del sistema**.
2. Haga clic en **General** en la barra lateral y, luego ,en **Compartir** (es posible que deba desplazarse hacia abajo).
3. Active la opción **Compartir Internet** y haga clic en **Configurar**.
4. Haga clic en el menú emergente **Compartir su conexión desde**.
5. Elija la conexión a Internet que desea compartir.
   (Por ejemplo, si está conectado a Internet a través de wifi, seleccione Wifi).
6. A continuación, en A dispositivos que usan, active el puerto que otros dispositivos pueden usar para acceder a la conexión a Internet compartida.
   (Por ejemplo, si desea compartir su conexión a Internet a través de Ethernet, seleccione Ethernet).
   Si va a compartirla en dispositivos que utilizan wifi, configure la red de uso compartido de Internet y haga clic en **Aceptar**.
7. Haga clic en **Hecho**.
   Su conexión a Internet se compartirá en MacOS.

Para obtener más información sobre cómo compartir una conexión a Internet, consulte la página Soporte oficial de Apple.