Spectera

Guia de Rede e Segurança para Administradores de TI, Integradores de sistemas e Técnicos de eventos

Sennheiser electronic SE & Co. KG

Am Labor 1, 30900 Wedemark, Alemanha, www.sennheiser.com
v1.1

SENNHEISER

Índice

1. Introdução

Este documento destina-se a administradores de TI, integradores de sistemas e técnicos de eventos e foi concebido como um guia de planeamento e de configuração para integrar componentes da oferta Spectera em vários ambientes de rede, desde pequenas redes domésticas a redes empresariais.

O guia contém recomendações da configuração da rede para a transmissão de dados de controlo e conteúdos áudio (via Dante®).

2. Requisitos gerais

2.1. Sistemas operativos

A Spectera Base Station como dispositivo de rede pode ser controlada por computadores ou dispositivos Mac de rede.

Os seguintes requisitos do sistema aplicam-se à operação com a Spectera WebUI e o Sennheiser LinkDesk:

- Processador Intel i5 Dual Core/M1 Mac/ou semelhante
- RAM de 16 GB
- pelo menos, 4GB de espaço no disco rígido (5GB para dispositivos Mac)
- Interface Gigabit LAN
- Windows® 10, 11, Server 2019, Server 2022 (x64) ou superior
- Rede IPv4
- Windows: 10 ou mais recente
- MacOS: 13 ou mais recente

Navegadores compatíveis com Spectera WebUI:

- Google Chrome: 125 ou mais recente
- Microsoft Edge: 125 ou mais recente
- Mozilla Firefox: 128 ou mais recente
- Apple Safari: 17 ou mais recente

2.1. Rede

Largura de banda e velocidade

Relativamente aos requisitos de largura de banda para áudio de alta qualidade, há vários fatores que podem influenciar a entrada e saída do áudio. A velocidade de rede necessária para a transmissão de áudio via Dante® deve ser a mais alta possível para garantir a melhor experiência de audição. Por regra, a largura de banda mínima para transmitir e receber áudio na Spectera Base Station é aproximadamente a seguinte:

> A maioria do áudio utilizado em configurações profissionais é PCM (não comprimido), com uma amostragem de 48kHz e uma profundidade de bits (comprimento de palavra) de 24bits. O áudio Dante® é Unicast por predefinição, mas pode ser definido para utilizar Multicast em casos de distribuição de um para muitos.
>
> - O Dante® combina o áudio em fluxos para poupar os recursos da rede.
> - Os fluxos de áudio Unicast contêm até 4 canais. As amostras por canal podem variar entre 4 e 64, dependendo das definições de latência do dispositivo. A utilização da largura de banda é cerca de 6Mbps por fluxo de áudio Unicast típico.
> - A largura de banda para fluxos Multicast depende do número de canais áudio utilizado. A largura de banda é cerca de 1,5Mbps por canal
>
> Fonte: Dante Information for Network Administrators

Acesso à Internet

Recomendamos o acesso permanente à Internet para ambos os componentes, a Spectera Base Station e o Sennheiser LinkDesk. Consulte o capítulo “4. Portas, protocolos e serviços” para mais informações sobre os serviços de Internet usados.

> **i** Pelo menos para a ativação inicial do produto na Spectera Base Station e para usar o login da conta Sennheiser opcional no Sennheiser LinkDesk é obrigatório ter um acesso direto à Internet e suporte DNS.

> **i** De momento não é possível configurar manualmente qualquer proxy de rede e servidor DNS na Spectera Base Station. Certifique-se de que disponibiliza acesso direto à Internet, por ex., através da permissão do dispositivo e de qualquer porta, protocolo e domínio usado e utilizando DHCP para fornecer as definições do servidor DNS.

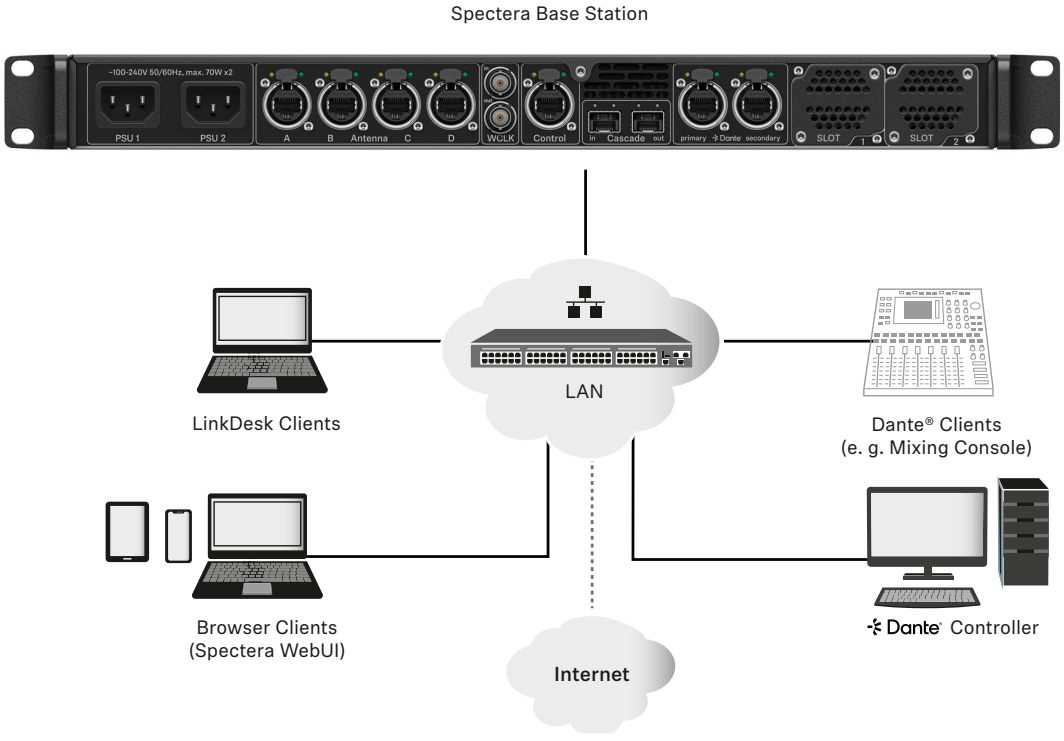
Cablagem

Desde que esteja garantida uma boa velocidade da Internet, o cabo de rede utilizado determina a velocidade de transmissão efetiva dos dados enviados e recebidos na rede.

> **i** Para garantir uma velocidade de transmissão fiável de dados de áudio e controlo com a Spectera Base Station, use um cabo de rede RJ45 com o padrão CAT5e S/FTP ou superior

3. Configurações da rede

Para operar os vários componentes da oferta Spectera, eles precisam de ser integrados numa configuração da rede, já existente ou nova. A imagem seguinte mostra uma vista geral da configuração da rede e dos respetivos participantes.



Spectera Base Station

Este dispositivo Sennheiser tem 3 interfaces de rede. Uma interface dedicada aos dados de controlo e duas interfaces para dados de áudio (especificamente Dante®). Há uma interface primária e uma interface secundária para redundância da transmissão áudio.

Cliente Sennheiser LinkDesk

Este cliente pode ser qualquer computador anfitrião (PC ou Mac) com a aplicação de software LinkDesk instalada.

Cliente do navegador (Spectera WebUI)

Este cliente pode ser qualquer computador anfitrião (PC, Mac, tablet, smartphone), com um navegador web compatível, que aceda à Spectera WebUI.

Cliente Dante®

Pode ser qualquer dispositivo com uma interface de rede Dante® instalada. Pode ir desde Virtual Dante® Soundcards instalados num computador anfitrião até dispositivos dedicados como uma mesa de mistura.

Dante® Controller

Este é geralmente um computador anfitrião (PC ou Mac) com a aplicação de software Dante® Controller instalada. Esta aplicação configura e controla todos os dispositivos Dante® e transmissões áudio na rede.

Router de rede

Este pode ser qualquer router para direcionar a comunicação de rede dentro da rede de área local (LAN) e fornecer o gateway a outras redes e à Internet.

3.1. Spectera Base Station - configuração da rede

Dependendo da configuração pretendida do endereço de rede, toda a interface de rede (Control e Dante®) pode ser operada nos seguintes modos IP apenas com IPv4:

- IP fixo/estático
- Auto IP (DHCP ou Zeroconf)

Adicionalmente, é possível configurar se as informações mDNS/DNS-SD devem ou não ser publicadas pelo dispositivo.

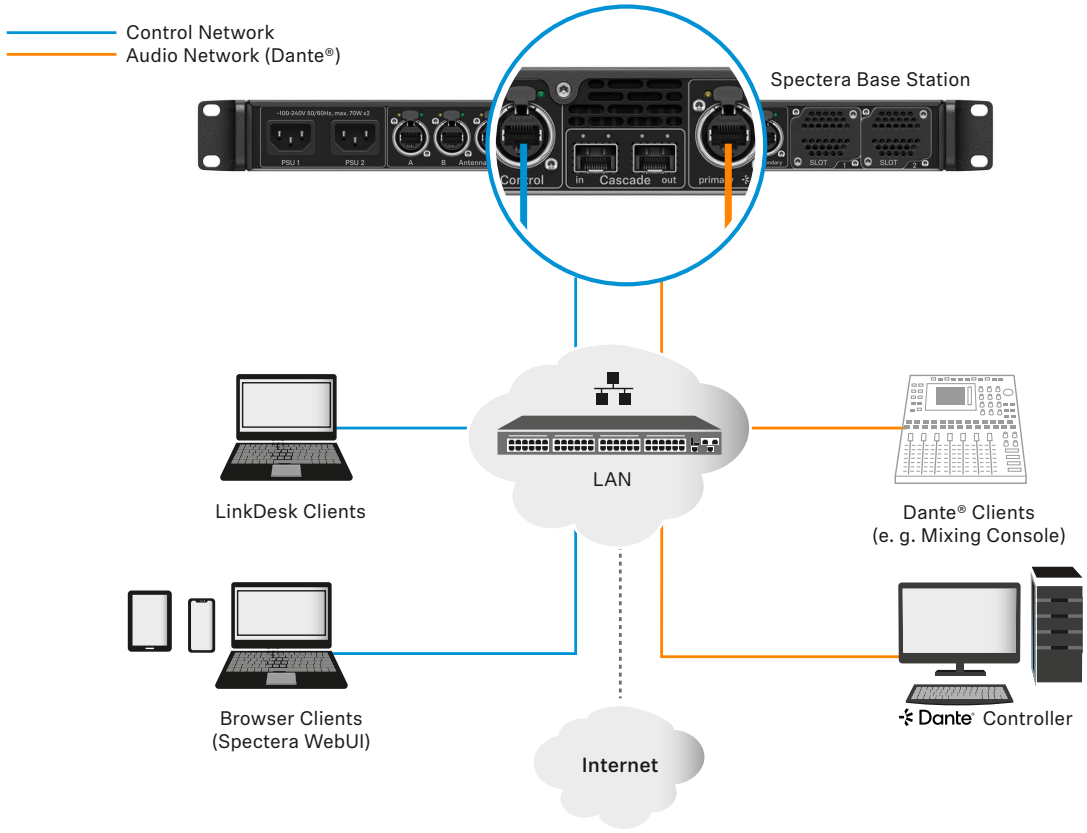
Restrições Dante®

- Não é possível desativar a funcionalidade Dante® para ambas as portas Dante®.
- As portas Dante® são desativadas quando o dispositivo se encontra no modo de espera.
- A configuração da rede das portas Dante® só pode ser realizada através da aplicação de software Dante® Controller.
- Por predefinição, as portas Dante® estão configuradas para Auto IP. Se tiverem sido configurados IP estáticos/fixos e não for possível continuar a aceder ao dispositivo, o Modo IP só pode ser reposto para Auto IP através de uma reposição do dispositivo às definições de fábrica.
- As redes Dante primária e secundária não devem estar diretamente ligadas uma à outra (loop de rede). Certifique-se de que liga sempre as portas de rede da Base Station Dante a duas redes diferentes que não funcionam através de um switch comum.

Modo de rede partilhada

No modo de rede partilhada, ambas as redes para Control e Dante® utilizam a mesma infraestrutura de rede física.

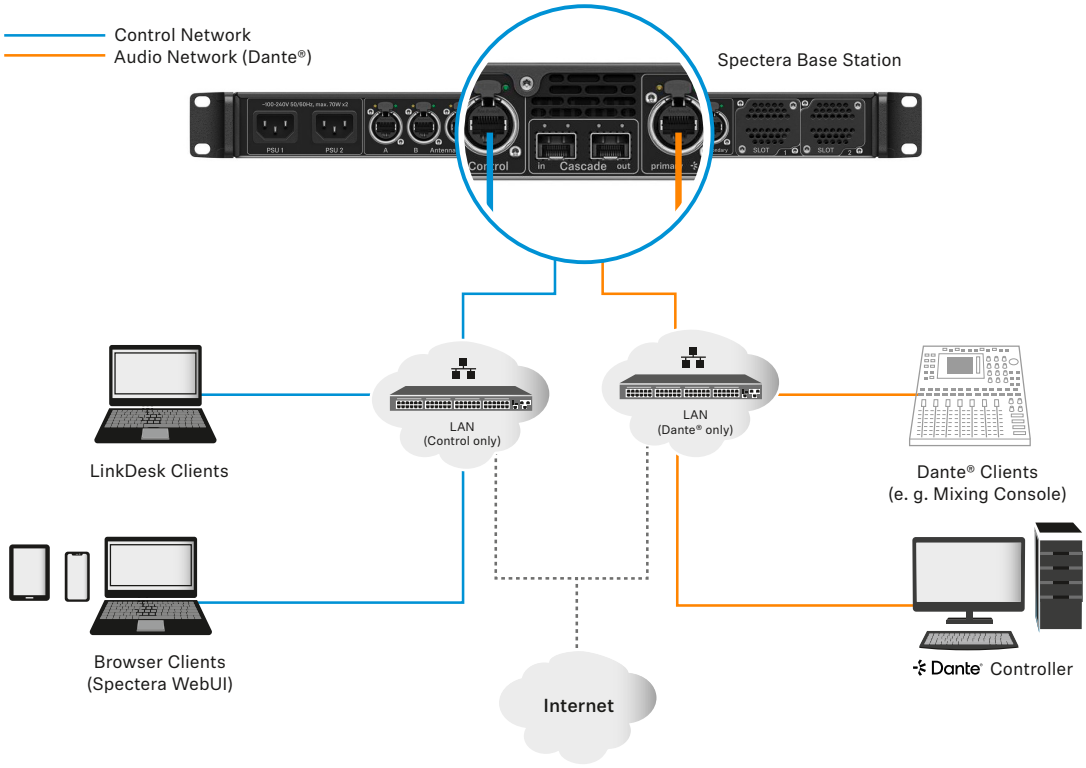
- Configure as redes Control e Dante® através de um switch/router.
- Use dois IP diferentes para endereçar separadamente a rede Control e a rede Dante®.



Modo de rede dividida

No modo de rede dividida, ambas as redes para Control e Dante® utilizam uma infraestrutura de rede física diferente.

- Configure as redes Control e Dante® através de dois switches/routers diferentes.
- Use dois IP diferentes para endereçar separadamente a rede Control e a rede Dante®.



4. Portas, protocolos e serviços

4.1. Sennheiser LinkDesk

Para usar o software Sennheiser LinkDesk, determinadas portas devem estar ativadas (especialização para a firewall da organização/empresa) para a comunicação entre o software e os dispositivos. Se necessário, contacte o administrador local para configurar as portas necessárias.

Endereço	Porta	Protocolo	Tipo	Serviço	Utilização
Anfitrião interno					
LOCALHOST	54352	HTTPS (TCP)	Unicast	Servidor Link-Desk	Comunicação com o servidor interno
Anfitrião de saída					
INDIF.	443	HTTPS (TCP)	Unicast	API da Spectera Base Station	Comunicação com dispositivos
Contas Pro Emea[1] Config. B2C[2]	443	HTTPS (TCP)	Unicast	Sennheiser CIAM	Registo/início de sessão com conta Sennheiser
User insights[3] Matomo[4]	443	HTTPS (TCP)	Unicast	Sennheiser User Insights	Análise de dados de utilização e operacionais
Anfitrião de entrada					
INDIF.	443	HTTPS (TCP)	Unicast	API da Spectera Base Station	API da Base Station Comunicação a partir de dispositivos
224.0.0.251	5353	mDNS (UDP)	Multicast	mDNS, DNS-SD	(opcional – se pretendido) descoberta de dispositivos/serviços

[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

Para usar o dispositivo da Spectera Base Station numa rede, determinadas portas devem estar ativadas (especialmente para a firewall da organização/empresa) para a comunicação entre o software e os dispositivos. Se necessário, contacte o administrador local para configurar as portas necessárias.

Endereço	Porta	Protocolo	Tipo	Serviço	Utilização
Dispositivo de saída					
INDIF.	443	HTTPS (TCP)	Uni-cast	API da Spectera Base Station	Comunicação do dispositivo com os clientes
User insights[1] Matomo[2]	443	HTTPS (TCP)	Uni-cast	Sennheiser User Insights	Análise de dados de utilização e operacionais
my.nalpeiron.com	80	HTTP (TCP)	Uni-cast	Servidor de licenças Sennheiser	Ativação de dispositivos
INDIF. (ver lista de Servidores NTP)	123	NTP	Uni-cast	Servidor de hora NTP	Sincronizar hora do sistema
224.0.0.251	5353	mDNS (UDP)	Multi-cast	mDNS, DNS-SD	(opcional – se ativado) descoberta de dispositivos/serviços
INDIF. (ver lista de Portas Dante®)					
Dispositivo de entrada					
INDIF.	443	HTTPS (TCP)	Uni-cast	API da Spectera Base Station	Comunicação do dispositivo a partir dos clientes
INDIF. (ver lista de Portas Dante®)					Dados de controlo e áudio Dante®

[1] sennheiseruserinsights.matomo.cloud

[2] cdn.matomo.cloud

Servidores NTP

Para funcionar corretamente com licenças e certificados, a Spectera Base Station precisa de uma hora correta do sistema. O dispositivo irá utilizar o mecanismo NTP consolidado da pilha de protocolos IP para sincronizar o relógio entre um servidor de hora numa rede e o cliente dentro do dispositivo.

Atualmente, não é possível um administrador de TI ou integrador de sistemas configurar manualmente um servidor NTP dedicado para ser usado pela Spectera Base Station. A possibilidade de configurar manualmente um servidor NTP dedicado é uma funcionalidade planeada para uma próxima versão.

O dispositivo comporta-se da forma seguinte:

- Se tiver sido fornecida uma configuração do servidor de hora via DHCP ou manualmente, primeiro ele tenta ligar e sincronizar com esse servidor de hora.
- Caso contrário, o dispositivo está a tentar aceder a qualquer servidor da seguinte lista de conjuntos de servidores de hora disponíveis publicamente a nível mundial.

> **i** Um administrador de TI tem de garantir que fornece acesso à Internet a, pelo menos, um dos pools de servidores e fornece definições DNS ao dispositivo através de DHCP.

Lista de conjuntos de servidores de hora NTP:

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

4.3. Portas Dante®

Para configurar uma rede Dante® são necessárias informações da porta. A tabela abaixo mostra que portas, URL e servidores são usados. Para informações detalhadas, consulte diretamente o website: https://www.getdante.com/support/faq/which-network-ports-does-dante-use/

Portas Dante® externas

Endereço	Porta	Utilização	Tipo
239.255.0.0/16	4321	Áudio Multicast ATP	Multicast
239.69.0.0/16	5004	Áudio Multicast AES67	Multicast
224.0.1.129-132	319, 320	PTP	Multicast e Unicast (DDM)
224.0.0.251	5353	mDNS	Multicast
224.0.0.230 – 233	8700 – 8708	Contr. e monit. Multicast	Multicast
239.254.1.1	9998	Logging	Multicast
239.254.3.3	9998	TP Logging (se ativado)	Multicast
239.254.44.44	9998	Logging	Multicast
239255255255	9875	SAP (AES67 discov.)	Multicast
UDP	28800, 28700-28708	Cont. e monitoriz. (ext)	Unicast
UDP	38800, 38700-38708	Controlo e monitorização DVS (ext)	Unicast

Portas Dante® internas

Protocolo	Porta	Utilização	Tipo
UDP	14336-14591	Áudio Unicast [excluindo Via]	Unicast
UDP	34336-34600	Áudio Unicast [apenas Via]	Unicast
UDP	4440, 4444, 4455	Controlo de áudio [excluindo Via]	Unicast
UDP	24440, 24441, 24444, 24455	Controlo de áudio [apenas Via]	Unicast
UDP	4777	Controlo Via [apenas Via]	Unicast
TCP	4777	Via Websocket	Unicast
UDP	8850,28900, 24445	Controlo e monitorização Via (int.)	Unicast
UDP	8850, 38900, 8899	Controlo e monitorização DVS (int.)	Unicast
UDP	8000	Porta do dispositivo Dante Domain Manager	Unicast
UDP	8001	Proxy do dispositivo Dante Millau (int.)	Unicast
UDP	8002	Servidor Dante Lock	Unicast
UDP	8751	Porta de medição Dante Controller	Unicast
UDP	8800	Controlo e monitorização	Unicast
TCP	8753	Clientes mDNS (apenas interno)	Unicast
TCP	16100-16131	Autent. HDCP para terminais de vídeo	Unicast
UDP	61440-61951	Nível de áudio FPGA fluxo keepa-live	Unicast
TCP	4778	DVS websocket (apenas Apple Si-licon)	Unicast

5. Segurança

5.1. Certificados

A Spectera Base Station utiliza um certificado autoassinado para a comunicação de rede. De momento não é possível substituir este por um certificado assinado pela CA (Autoridade Certificadora). O certificado é gerado de fábrica e será renovado a cada reset de fábrica.

Ao aceder à Spectera WebUI pela primeira vez com um navegador será apresentado um aviso de segurança sobre um certificado desconhecido. O aviso de segurança depende do navegador utilizado. Dependendo do seu navegador, clique em **Advanced** (Definições avançadas) ou em **Show Details** (Mostrar detalhes) (Safari) e depois em:

- Microsoft Edge: **Continue to localhost (unsafe) (Continuar para localhost (inseguro))**
- Google Chrome: **Proceed to localhost (unsafe) (Avançar para localhost (inseguro))**
- Firefox: **Accept the Risk and Continue (Aceitar o risco e continuar)**
- Apple Safari: **[...] visit this Website** -> **Visit Website** ([...] visitar este website -> Visitar website)
- ou semelhante (outros navegadores)

Para prevenir ataques “man-in-the-middle” (MITM), o Sennheiser LinkDesk tem algumas medidas de segurança integradas. Devido a estas medidas, pode receber um aviso de incompatibilidade de certificados durante o trabalho com uma Base Station. Em alguns casos, tal pode ocorrer mesmo não havendo qualquer problema de segurança. Estes são:

- A Base Station foi reposta às configurações de fábrica desde a última ligação. Neste caso, pode confirmar com segurança a ligação e avançar quando encontrar o aviso de incompatibilidade.
- Foi ligada uma Base Station diferente através do mesmo endereço IP. Neste caso, verifique se o endereço IP que está a usar é realmente o endereço IP correto da Base Station pretendida.

5.2. Palavra-passe do dispositivo

O acesso ao dispositivo através da API de controlo da rede e a WebUI da Spectera Base Station e através do Sennheiser LinkDesk está protegido por palavra-passe para evitar a configuração do dispositivo por elementos não autorizados dentro da rede.

Após desembalar e após cada reset de fábrica do dispositivo, é necessário o utilizador configurar uma nova palavra-passe para obter acesso ao dispositivo. Cada instância do Sennheiser LinkDesk grava as palavras-passe dos dispositivos que já reclamou. Para proteger o acesso por elementos não autorizados à aplicação Sennheiser LinkDesk num anfitrião, é necessário aplicar outros mecanismos, por exemplo, contas de utilizador protegidas por palavra-passe em Windows ou MacOS.

A cada nova sessão do navegador da Spectera WebUI, é necessário voltar a introduzir a palavra-passe configurada.

5.3. Transmissão de dados encriptados

Toda a transmissão de dados de controlo no protocolo HTTPS é encriptada através de Transport Layer Security (TLS).

Transmissão para o servidor de licenças Sennheiser

Toda transmissão de dados de controle no protocolo HTTP para o servidor de licenças Sennheiser é criptografada no Nível de Aplicação.

Criptografia de Mídia Dante (disponível a partir da versão 1.1 do firmware Spectera Dante®)

A criptografia de mídia Dante estende os benefícios de segurança do uso do Dante® em sua rede ao ocultar o conteúdo da mídia durante a transmissão entre dispositivos. O Dante® utiliza o Padrão de Criptografia Avançada (AES) com uma chave de 256 bits para fornecer proteção de mídia líder da indústria. Ocultar o conteúdo dos pacotes de mídia impede que usuários maliciosos ou não autorizados escutem ou interfiram no tráfego de mídia Dante.

> **i** Nota Por favor, consulte a documentação da Audinate para informações detalhadas sobre a criptografia Dante® e sobre como atualizar o firmware Dante®:
>
> - Criptografia de Mídia Dante: Audinate/Media-Encryption
> - Atualizando o firmware Dante®: Dante Updater

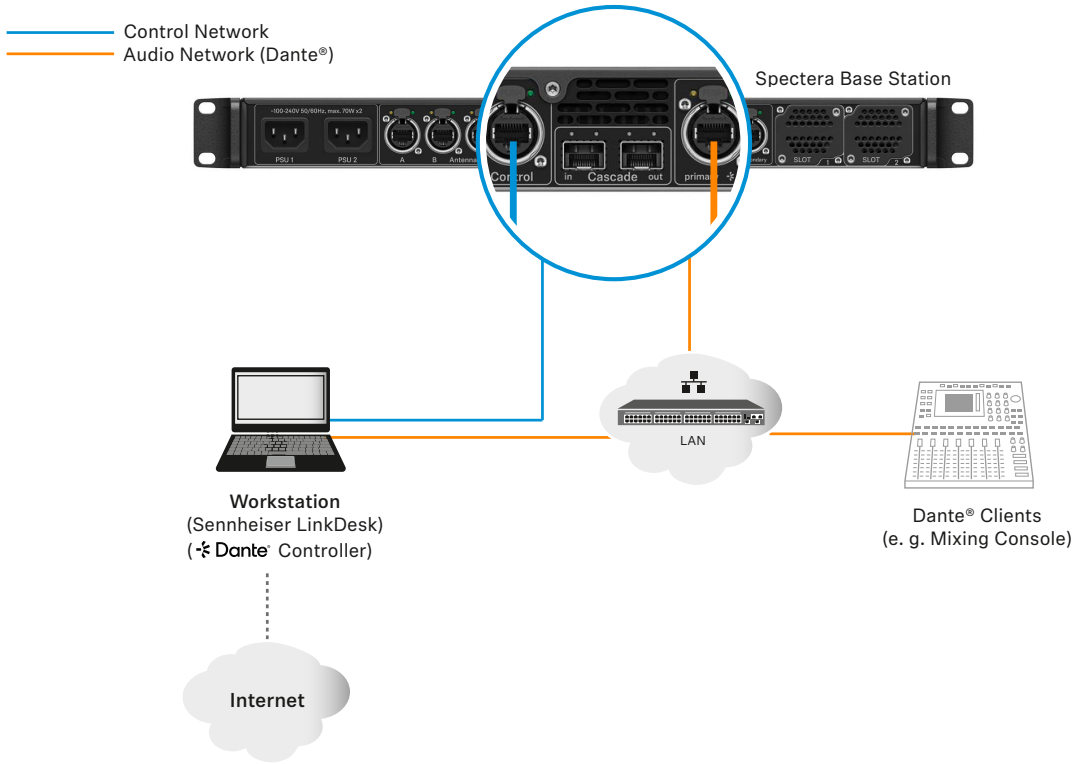
6. Melhores práticas

6.1. Partilhar a ligação da Internet em pequenas configurações de rede

É possível operar a oferta Spectera sem redes de router dedicadas, por ex., em configurações realmente pequenas, mas recomendamos usar sempre algum tipo de router de rede doméstica para uma utilização sem problemas. Especialmente para fornecer acesso à Internet à Spectera Base Station é possível usar a funcionalidade integrada de Windows e MacOS para a partilha da ligação Internet.

> **i** Para redes empresariais, NAO RECOMENDAMOS utilizar a partilha da ligação à Internet. Na maioria das vezes, é mesmo proibido usar este serviço de acordo com a política de TI da empresa.

A configuração da rede pode ter esta aparência.



Nesta configuração é utilizada uma estação de trabalho para todas as aplicações de software do cliente (Sennheiser LinkDesk, Spectera WebUI, Dante® Controller). São usadas duas interfaces de rede com fio separadas para o controlo e áudio (Dante®) ou é partilhada uma interface. Tenha em atenção que, nestas configurações, (tipicamente) não é ativado um serviço DHCP. Use definições de IP manuais ou configuração ZeroConf.

Para a partilha da ligação Internet, geralmente uma ligação da rede existente (Wi-Fi ou Ethernet) com acesso à Internet é partilhada com outra interface de rede selecionada do anfitrião.

Para partilhar a sua ligação Internet no Windows:

1. Ligue o seu dispositivo do cliente ao seu PC anfitrião com um cabo Ethernet. Se um dos dispositivos não possuir uma porta Ethernet livre, use um adaptador USB-Ethernet.
2. Aceda ao menu **Ligações de rede**. A forma mais fácil é procurar “Ligações de rede” na caixa de pesquisa do Windows.
3. Clique com o botão direito do rato no adaptador de rede ligado à Internet (por ex., Wi-Fi ou modem) e, de seguida, selecione **Propriedades**.
4. Mude **Permitir a ligação de outros utilizadores da rede** para **ON** a partir do separador Partilhar e selecione a porta Ethernet relevante no menu pendente.

> Tenha em atenção que, se tiver instalado software VPN, pode ver muitas portas Ethernet virtuais na sua lista e precisará de escolher a verdadeira.

Após clicar em **OK**, a Internet deve fluir para o dispositivo do seu cliente através da respetiva porta Ethernet.

Para mais detalhes sobre a partilha de uma rede Internet, consulte a página de Apoio da Microsoft.

Para partilhar a sua ligação de Internet no MacOS:

1. No seu Mac, selecione **Menu Apple** > **Definições do sistema**.
2. Clique em **Geral** na barra lateral e, de seguida, em **Partilhar** (pode ter de deslizar a página para baixo).
3. Ative a **Partilha de Internet** e clique em **Configurar**.
4. Clique em **Partilhar a sua ligação** no menu pop-up.
5. Selecione a ligação de Internet que deseja partilhar.
   (Por exemplo, se estiver ligado à Internet através de Wi-Fi, selecione Wi-Fi).
6. Sob Para dispositivos a usar, ative a porta que outros dispositivos podem usar para ter acesso à ligação à Internet partilhada.
   (Por exemplo, se desejar partilhar a sua ligação de Internet através de Ethernet, selecione Ethernet).
   Se estiver a partilhar dispositivos através de Wi-Fi, configure a rede de partilha de Internet e, de seguida, clique em **OK**.
7. Clique em **Terminar**.
   A sua ligação à Internet será partilhada em MacOS.

Para mais detalhes sobre a partilha de uma ligação à Internet, consulte a página de Apoio da Apple.