TI 310

Ethernet networking (1.1 ES)

d&b audiotechnik

Información general

TI 310 Ethernet networking

Versión 1.1 ES, 12/2014, D5310.ES .01

d&b audiotechnik GmbH
Eugen-Adolff-Strasse 134, D-71522 Backnang, Alemania
Teléfono: +49-7191-9669-0, Fax: +49-7191-95 00 00
Correo electrónico: support@dbaudio.com. Internet: www.dbaudio.com

Índice

1. Introducción

En la industria del entretenimiento, el método preferente para transportar contenido y controlar los datos son las redes basadas en Ethernet.

Algunos de los esquemas topológicos y de administración son muy complejos porque exigen tener conocimientos expertos y profesionales sobre el tema, y quedan fuera del ámbito de este tutorial.

Sin embargo, la gran mayoría de los tamaños y las tareas con redes se realizan en producciones que son más pequeñas que las giras nacionales e internacionales y, en consecuencia, pueden gestionarse fácilmente con un conocimiento básico de sonido en los temas siguientes:

- Cómo configurar una topología de red de trabajo.
- Direcciones MAC e IP y máscaras subred IP.
- Cómo configurar el adaptador de red del equipo informático.
- Cómo funcionan las redes WLAN.
- Seguridad de la red.

Este documento se ha concebido como unas guía básica que ofrezca precisamente estos conocimientos, pero no sustituye al especialista en redes cualificado.

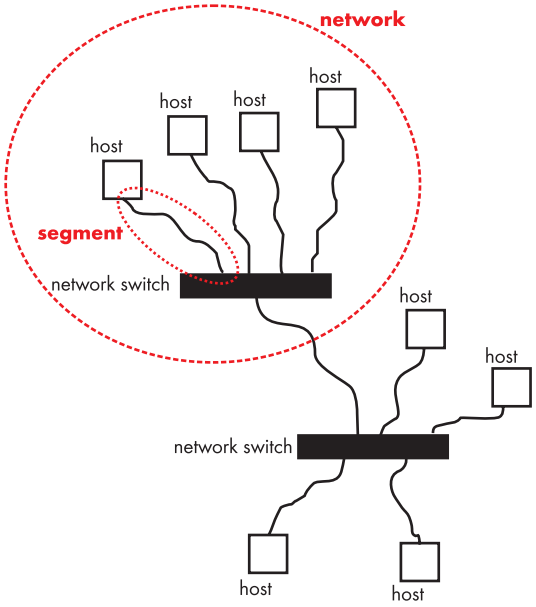
2. Topología de red

Normalmente, las redes basadas en Ethernet incluyen más de dos hosts ('host' es el término técnico para referirse al dispositivo anfitrión habilitado para redes) con una topología de estrella. Esta topología implica que todos los hosts están interconectados mediante uno o más conmutadores o concentradores centrales. A su vez, conmutadores y concentradores también pueden estar interconectados para formar una red mayor. La conexión entre dos hosts se denomina segmento.

Incluso los dispositivos que parece que presentan capacidades para conectarse secuencialmente, porque se suministran con dos conectores y están etiquetados como "entrada" y "salida", en realidad simplemente incorporan un pequeño conmutador de tres puertos con dos puertos visibles desde fuera, mientras que el dispositivo real está conectado al tercer puerto interno.

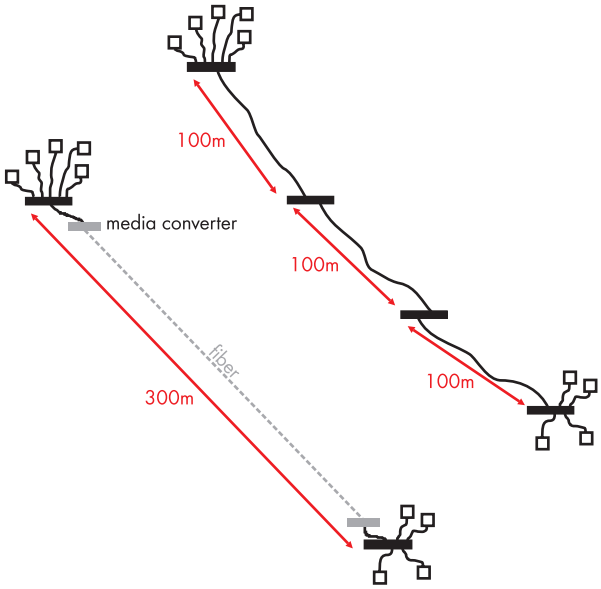
En ninguna circunstancia deben crearse anillos en la red, excepto si se tiene la certeza de que el equipo correspondiente admite esta función y se ha configurado correctamente.

Por otra parte, es una buena idea subdividir físicamente redes mediante varios conmutadores como unidades de distribución. En la ilustración siguiente se muestra un ejemplo típico de dos redes de estrella interconectadas .



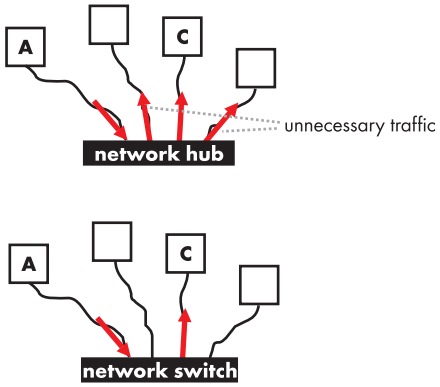
Con segmentos de cobre, la longitud máxima está limitada a unos 100 m, porque varía en función del tipo de cable que se use. Para ampliar la distancia máxima compartida en puente, pueden insertarse conmutadores o concentradores adicionales en todo el recorrido para ganar un segmento adicional de 100 m de longitud cada uno. Otra manera de ampliar la longitud de un segmento de red es utilizar convertidores de soportes y conexiones de fibra óptica. De este modo, se pueden cubrir distancias de decenas de kilómetros.

En la ilustración siguiente se muestran las dos opciones. La distancia que tiene que cubrirse es de unos 300 m. Con segmentos de cobre, se necesitan dos conmutadores o concentradores adicionales a lo largo de la línea lo cual implica otros problemas relacionados: todos tienen que recibir suministro eléctrico y todos representan puntos de fallo. Sin embargo, el uso de convertidores de soportes y cables de fibra óptica permite conectar dos lugares con un cable largo de fibra.



2.1. Conmutadores de red y concentradores de red

Aunque los conmutadores (switchs) son el dispositivo que se utiliza más habitualmente para instalar una red simple, también sigue habiendo bastantes concentradores de red (hubs) en uso. La diferencia esencial entre un conmutador y un concentrador es que el concentrador sólo actúa como un repetidor electrónico. Todos los datos que se reciben en un puerto se transmiten a todos los demás puertos. Esto causa un exceso de tráfico en la red e incluye otros problemas relacionados que, por acumulación, hacen que el funcionamiento de la red sea menos eficaz.



Concentrador y conmutador: Host "A" se comunica con host "C"

Por el contrario, el conmutador "aprende" a qué host (es decir, la dirección MAC) está conectado cualquier otro host de sus puertos y, por tanto, sólo se transmiten datos entre los dos puertos correctos.

3. Identificación y comunicación

Las redes Ethernet contienen hosts de muchos tipos diferentes y de diferentes fabricantes. Para la identificación y la comunicación se utilizan estándares comunes. Aquí se describen los más importantes.

3.1. Dirección MAC

Aunque lo pueda parecer, esto no tiene nada que ver con una popular marca de ordenadores personales. En este caso, la dirección MAC sirve para asignar un identificador exclusivo a un host de red para poder acceder a él directamente.

MAC es la sigla en inglés de **M**edia **A**ccess **C**ontrol (Control de acceso a medios). El fabricante implementa la dirección MAC en el hardware de los hosts de la red (p. ej., una interfaz Ethernet a CAN R70 de d&b, el adaptador de red del equipo informático, un enrutador inalámbrico, etc.) y, además de ser única y exclusiva, no puede cambiarse, al menos en teoría.

En las redes Ethernet, la dirección MAC tiene 48 bits o 6 bytes de longitud y, normalmente, se escribe en notación hexadecimal, por ejemplo:

00:41:80:AD:FC:2C

Un usuario normal de red no suele necesitar acceder a la dirección MAC.

3.2. Dirección IP

Además de la dirección MAC como identificador exclusivo del hardware, los hosts de red deben agruparse para formar redes lógicos. Para ello, se asigna una dirección IP a cada dirección MAC (es decir, al host). A diferencia de la dirección MAC, la dirección IP no es exclusiva de un dispositivo específico de hardware, sino que se asigna por uso según sea necesario.

Actualmente, el protocolo IPv4 es el estándar predominante: las direcciones IP tienen 32 bits de longitud y normalmente se escriben con notación de punto decimal, con cuatro números decimales del intervalo entre 0 y 255. Cada uno de esos cuatro números decimales representa 8 bits, por eso a veces se les llama octetos:

137.152.89.230

La mayoría de las veces es lo que un usuario normal utilizará.

3.2.1. Máscaras de subred IP

En un nivel de mayor complejidad, la dirección IP se subdivide en un prefijo de red y el número de host real (también llamado "la parte del host"), similar a las redes dbCAN, en las que se hace una distinción entre la subred y el ID real, por ejemplo: el ID CAN "5.23" puede separarse en la subred "5" y el ID "23".

En cambio, en una dirección IP no hay un número fijo de dígitos para identificar el prefijo de red o la parte del host. El prefijo de red de la dirección IP se define mediante la máscara subred. Como es un tema bastante complejo, es mejor examinar un ejemplo sencillo y fácil de entender. En este ejemplo, la máscara de subred, cuya notación es muy similar a la notación de la propia dirección IP, tiene este aspecto:

255.255.255.0

Esto significa que los tres primeros octetos definen el prefijo de red y el último octeto es el número de host. Todos los hosts de red que deben comunicarse entre sí sin "ayuda" adicional de la red tienen que tener el mismo prefijo de red.

Con la máscara de subred anterior, una dirección IP de ese tipo tendría este aspecto:

192.168.0.[**x**]

donde [**x**] es el número de host y "192.168.0." debe ser idéntico para todos los hosts, porque indica el prefijo de red. Todos los hosts deberán tener "'255.255.255.0" establecido como máscara de subred en sus preferencias.

De este modo, podrá haber 256 (de 0 a 255) hosts diferentes (= dispositivos). En realidad, los números más bajo y más alto posibles, en este caso 0 y 255, están reservados. Así se reduce el número utilizable de hosts del ejemplo a 254, es decir, en la red pueden haber hasta 254 ordenadores u otros dispositivos habilitados para red. Suele ser más que suficiente para cualquier aplicación estándar.

3.2.2. Redes privadas

De todo el rango de direcciones IP posibles, no todas están libres para el uso. La gran mayoría de direcciones IP las administra centralmente la IANA (sigla de Internet Assigned Numbers Authority, Autoridad para la asignación de números de Internet). No obstante, hay varios rangos de direcciones que están reservadas para redes privadas o "cerradas" sin conexión directa con Internet, que se pueden utilizar dentro de esas redes como se desee. Esos son los rangos de direcciones adecuadas para un entorno de producción. Los dos rangos que se utilizan más habitualmente son:

10.0.0.0 - 10.255.255.254

y

192.168.0.0 - 192.168.255.254

Siempre que se asignan direcciones IP manualmente, deben tomarse de esos rangos indicados más arriba. Con una máscara de subred de 255.255.255.0, las direcciones IP de una red de producción serían como estas:

10.[**x**].[**y**].[**z**] o

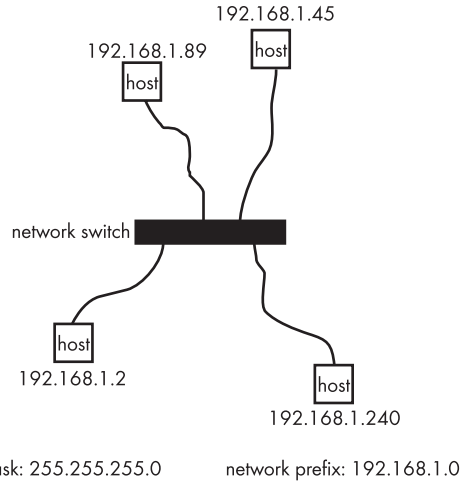
192.168.[**x**].[**z**]

donde [**x**] y [**y**]

son cualquier número entre 0 y 255. Estos números deben ser idénticos para todos los hosts (porque con la máscara de subred actual indican el prefijo de la red)

y [**z**]

es el número de host entre 1 y 254. Este número tiene que ser único y exclusivo para cada host. En la ilustración se muestra un ejemplo de ese tipo de red.



3.2.3. Asignación de direcciones IP automática o manual

Para facilitar las configuraciones rápidas de red, todos los parámetros de red, como la máscara de subred, dirección IP, etc., pueden asignarse automáticamente en una red. Este método se denomina DHCP (Dynamic Host Configuration Protocol, Protocolo de control dinámico de host) y se necesita un servidor DHCP presente en la red. La mayoría de los enrutadores Wi-Fi actuales, si no todos, incorporan funciones de servidor DHCP.

> **Nota:** La red no debe incluir más de **un** servidor DHCP, porque podría causar confusión y pérdida de la comunicación. Por motivos técnicos, esto también puede suceder varias horas o incluso días después de que un segundo servidor DHCP se añadiera accidentalmente a la red. Tenga en cuenta que todos los ordenadores o dispositivos que comparten la conexión de Internet son simultáneamente un servidor DHCP, por lo tanto, hay que proceder con cuidado.

Incluso si se utiliza correctamente, el protocolo DHCP puede tener inconvenientes. En ocasiones, combinaciones especificas de hosts y servidores DHCP no se comunican entre sí debido a mínimas diferencias en la implementación de los estándares respectivos. En estos casos, la asignación automática de direcciones IP no funciona.

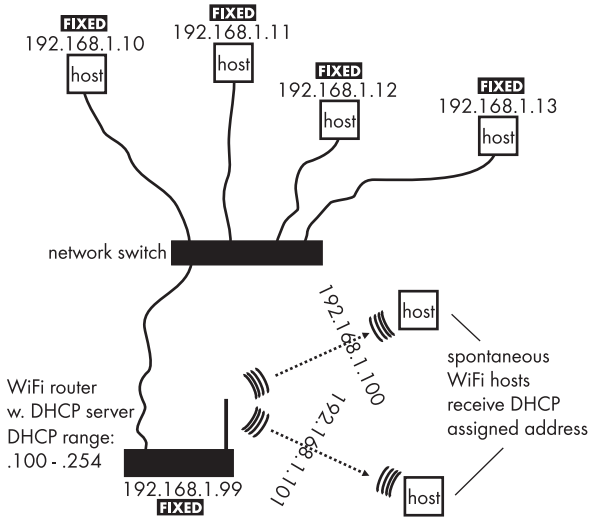
Pueden producirse problemas similares con direcciones IP que se han asignado manualmente, incluso cuando en la red está presente un servidor DHCP. Las direcciones IP duplicadas pueden causar confusión, así como los hosts que supuestamente se han configurado para recuperar de modo automático las direcciones IP a través de DHCP, pero en realidad se configuran manualmente con una dirección IP fija desconocida, potencialmente con un prefijo de red diferente.

Por este motivo, es muy útil comprender cómo restablecer un host para que recupere automáticamente una dirección IP. Si se ha asignado una dirección IP fija, se recomienda etiquetar el dispositivo, p. ej., escribiendo esa dirección en una etiqueta que se adhiera al dispositivo. Este método también se conoce como 'Peg DHCP' porque en muchas redes móviles las direcciones IP se distribuyen manualmente y se escriben en pinzas. Las pinzas se sujetan en el cable que se conecta en el dispositivo respectivo y proporcionan una indicación clara sobre el número de IP determinado que se utiliza.

3.2.4. Esquemas híbridos de asignación de direcciones IP

En aquellas redes que suelen incluir los mismos hosts y sólo adiciones ocasionales, el planteamiento más práctico es una asignación híbrida entre la manual y la automática de las direcciones IP, Muchos servidores DHCP pueden configurarse para que proporcionen direcciones IP de un rango específico, por ejemplo de 192.168.1.**100** a 192.168.1.**254**. De este modo, a todos los hosts normales se les pueden asignar direcciones IP fijas entre 192.168.1.1 y 192.168.1.99. Así, siempre se conocen sus direcciones y se evitan las direcciones duplicadas consecuencia de los hosts que se conectan espontáneamente con las direcciones asignadas por DHCP.

La ilustración siguiente muestra un caso típico: todos los hosts que no se mueven tienen direcciones IP fijas que se han asignado manualmente. El servidor DHCP, que en este caso también es un enrutador WLAN (una disposición muy habitual) tiene un rango de direcciones IP disponibles para que no haya conflictos con las direcciones asignadas manualmente. Aquí, el propio servidor tiene también una dirección IP (asignada manualmente y fija) porque participa activamente en la red. En la ilustración se muestran dos hosts móviles conectados espontáneamente (tabletas, ordenadores portátiles, etc.) que solicitan y reciben una dirección IP asignada automáticamente desde el servidor DHCP en el enrutador WLAN.



3.3. Transmisión de datos mediante TCP y UDP

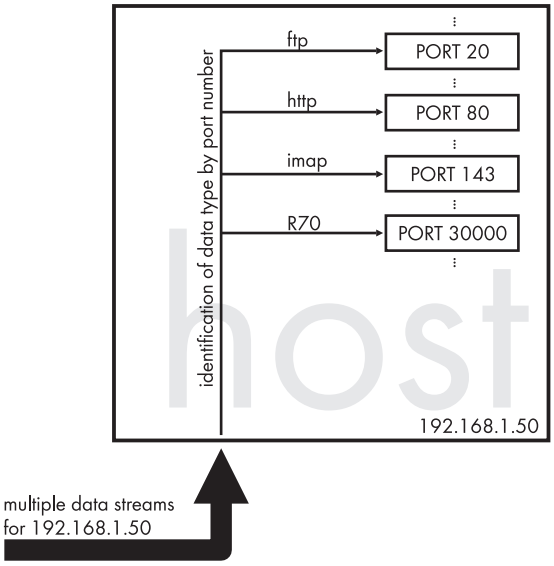
Una conexión de red establecida a través del protocolo de Internet (IP) puede utilizarse para transmitir datos de varias maneras. Para ello, se necesita otra capa de protocolos. Los dos protocolos que se utilizan más habitualmente son TCP (Protocolo de control de transmisión) y UDP (Protocolo de datagrama del usuario).

El más seguro, en cuanto a la entrega garantizada de los datos, es el protocolo TCP. TCP utiliza comunicación entre hosts y comprobación y corrección de errores para garantizar que todos los paquetes se transmiten y reciben correctamente, en el orden adecuado y sin pérdida de datos. Esto significa que el remitente de una secuencia de datos siempre sabe si se ha establecido una conexión y cuál es su estado.

En cambio, UDP envía datagramas a otros hosts sin establecer primero una conexión lógica. Significa que no hay ninguna comunicación previa ni tampoco confirmación de la recepción. Esto hace que las transmisiones por UDP sean menos fiables que las de TCP, pero permite reducir los gastos administrativos generales. En consecuencia, UDP a veces puede ser útil con aplicaciones en tiempo real, en las que un datagrama perdido es preferible a una interrupción más prolongada causada por esperar a los datos retrasados.

3.3.1. Puertos

Para distinguir varias transmisiones de datos simultáneas así como diferentes tipos de transmisión de datos generales, se utiliza un concepto abstracto de software: el "puerto". A cada secuencia de datos entre diferentes hosts se le asigna un número de puerto de 16 bits. Este concepto puede visualizarse como diferentes apartamentos del mismo edificio. Muchos servicios de datos habituales utilizan números de puerto fijos, como se ejemplifica en la ilustración siguiente.



3.4. Firewall y medidas de seguridad

Los firewalls (servidores de seguridad) y sistemas similares de seguridad de red se utilizan para impedir el acceso no autorizado a las redes y bloquear el tráfico de datos malicioso en el interior de las redes. En consecuencia, suelen implementarse y activarse mayoritariamente de forma predeterminada en dispositivos de hardware, como enrutadores WLAN y también en los sistemas operativos más recientes. Estos sistemas de seguridad filtran los datos que se originan en determinadas direcciones IP o intervalos de direcciones o datos dirigidos a puertos específicos, o bien trabajan a la inversa y sólo permiten que pasen datos que se originan en determinadas direcciones MAC o IP o que se envían a un puerto específico.

El motivo principal para que existan los firewalls y otros sistemas de seguridad es la protección de las redes frente al acceso externo malicioso de virus, programas de puerta trasera y similares. La complejidad de las amenazas y del software para defenderse de ellas se incrementa constantemente. Al mismo tiempo, muy pocos usuarios son capaces de configurar el software adecuadamente. Por este motivo, todos los sistemas de seguridad disponibles más habituales funcionan automáticamente. Esto puede causar problemas con otros programas habilitados para redes que se utilizan en aplicaciones de audio profesional, porque esas aplicaciones pueden usar puertos y protocolos que no son habituales en un entorno típico de oficina y algunos firewalls podrían bloquearlos.

Como la red de una producción profesional se supone que **no** se va a conectar a Internet, desactivar las medidas de seguridad adicionales no debe suponer ningún problema, y se garantizará que no se ralentizará la red ni se bloqueará la comunicación deseada.

No obstante, debe procederse con precaución cuando en la red de la producción se usan ordenadores que también se utilizan para acceder a Internet. Es responsabilidad de cada usuario administrar en consecuencia las medidas de seguridad relevantes.

En un entorno de producción profesional, sólo el personal autorizado debe tener acceso físico a los componentes de la red y el acceso mediante Wi-Fi a la red debe protegerse con una contraseña segura (WPA/WPA2, **no** cifrado de Privacidad equivalente por cable (WEP)). Como es imposible lograr que una red sea totalmente segura, cuanto más intervención "manual" exijan las medidas de seguridad que se han descrito más arriba, más eficaces serán para proteger la red, porque hacen que el administrador de la red tenga que pensarlo a fondo.

3.4.1. Instrucciones para la configuración manual

Las preferencias de la red de cualquier dispositivo o sistema operativo incluyen que se especifiquen un gran número de parámetros además de la dirección IP y la máscara de subred. Sin embargo, por lo general, con las redes privadas esos campos son irrelevantes y deben dejarse en blanco, porque se refieren a comunicación de datos con Internet.

A pesar de todo, algunos cuadros de diálogo de configuración de la red exigen que se especifique la entrada de la opción "Gateway" o puerta de enlace, incluso aunque no vaya a tener efectos prácticos en el funcionamiento del dispositivo. En esos casos, se recomienda especificar en este campo la dirección IP del servidor DHCP, incluso si la dirección IP del dispositivo en cuestión se asigna de forma manual.

4. WLAN (“Wi-Fi”)

WLAN es la sigla de Wireless Local Area Network, red inalámbrica de área local, también conocidas como redes Wi-Fi. Las diversas versiones de la norma IEEE 802.11 son muy habituales en entornos de producción, porque las redes Wi-Fi ofrecen movilidad allí donde se necesita. Por este motivo, es buena idea familiarizarse con algunas de sus complejidades.

4.1. Normas y estándares

Se utilizan dos bandas de frecuencia para las diversas implementaciones, tanto en el rango de 2,4 GHz como en el de 5 GHz.

En esas dos bandas de frecuencia, hay varios estándares de transmisión que ofrecen diferentes velocidades máximas y consumen anchos de banda diferentes. No todos esos estándares son igual de habituales.

Norma	Rango frec.	Velocidad máx. de datos sin procesar
802.11a	5 GHz	54 Mbit/s
802.11b	2,4 GHz	11 Mbit/s
802.11g	2,4 GHz	54 Mbit/s
802.11n	2,4 + 5 GHz	150-600 Mbit/s

4.2. Canales y frecuencias

Para habilitar el funcionamiento simultáneo de más de una red WLAN, ambas bandas de frecuencias se subdividen en varios canales.

En la banda de los 2,4 GHz, hay hasta catorce canales anchos de 22 MHz disponibles, en función de la legislación local. Como sus frecuencias centrales están separadas sólo por 5 MHz, cada canal se solapa como mínimo con tres canales adyacentes a cada lado. En consecuencia, sólo hay tres canales en la banda de 2,4 GHz que puedan utilizarse simultáneamente sin interferencias importantes: 1, 6 y 11. Incluso, a pesar de todo, el hecho de que esta banda de frecuencia también se utilice con otros equipos inalámbricos, como intercomunicadores para vigilar a bebés, Bluetooth, teléfonos y micrófonos inalámbricos, que pueden causar que el funcionamiento sea bastante deficiente.

En la banda de los 5 GHz, hay hasta 26 canales disponibles que no se solapan, en función de la legislación local. Además, actualmente hay mucho menos tráfico de otros dispositivos en esa banda de frecuencias, por lo que parece ideal para un funcionamiento de red WLAN sin problemas. Sin embargo, debido a que las longitudes de onda son más cortas, debe tenerse en cuenta que las ondas de radio 5 GHz no atraviesan las paredes u otros obstáculos tan bien como las ondas de 2,4 GHz. Esto podría limitar la banda de frecuencias en determinadas condiciones.

4.3. Cómo buscar un canal WLAN libre

El mejor procedimiento es evitar problemas antes de que surjan y aclarar y coordinar el uso de las radiofrecuencias con todas las partes implicadas.

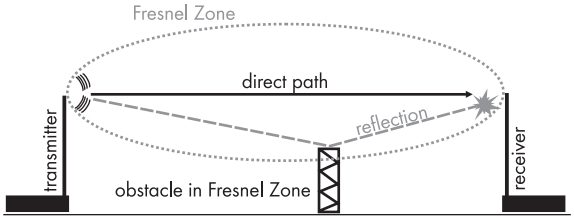
No obstante, las condiciones locales pueden obligar en ocasiones a adaptarse a una situación concreta. En ese caso, puede ser mejor utilizar un escáner de redes inalámbricas para detectar la presencia y la intensidad de la señal de las redes inalámbricas existentes para navegar más fácilmente por ellas.

Una herramienta para hacer ese escaneado, como mínimo para los sistemas basados en Windows, es **'inSSIDer'** de MetaGeek, LLC (metageek.net), que es gratuito. Utiliza el adaptador de red inalámbrica del ordenador para escanear, visualizar y clasificar las redes inalámbricas de los alrededores. No indica otras posibles fuentes de interferencias de radiofrecuencias, como dispositivos Bluetooth o intercomunicadores para vigilar a bebés.

Tenga en cuenta que d&b no es responsable directo ni subsidiario del funcionamiento adecuado de este software de un tercero y tampoco ofrece asistencia técnica al respecto.

4.4. “Línea de visión” y la zona de Fresnel

Toda la comunicación de radio de altas frecuencias depende de la libre propagación directa de las ondas de radio. El concepto "línea de visión" es muy conocido. No es tan conocido el hecho de que la interferencia que causan los reflejos en objetos que no están directamente en la línea de visión, pero sí cerca de ella. La zona en el espacio en la que se producen la mayoría de los reflejos que interfieren la comunicación se llama zona de Frenel, en honor del físico Augustin-Jean Fresnel, y puede describirse como un volumen con forma de cigarro que se extiende desde el transmisor al receptor. Cuanto mayor es la distancia entre esos dos puntos, más grueso será ese "cigarro". Es decir, cuanto mayor es la zona de Fresnel, más atención debe ponerse en procurar que el área de la línea de visión esté libre de obstáculos.



El método más fácil para conseguir como mínimo lo más cercano a las condiciones ideales es montar todo el enrutador WLAN lo más alto posible, o bien utilizar antenas externas que pueden montarse en un punto alto y elevado. La primera solución, elevar el enrutador, puede ser la preferible aunque sea un poco engorrosa, porque cualquier cable entre el enrutador WLAN y la antena parabólica atenuará rápidamente la señal hasta un punto en que puede anular la ventaja que se pretendía obtener. Este efecto es más intenso en la banda de 5 GHz que en la de 2,4 GHz.

4.5. Ser o no ser de la comunicación inalámbrica

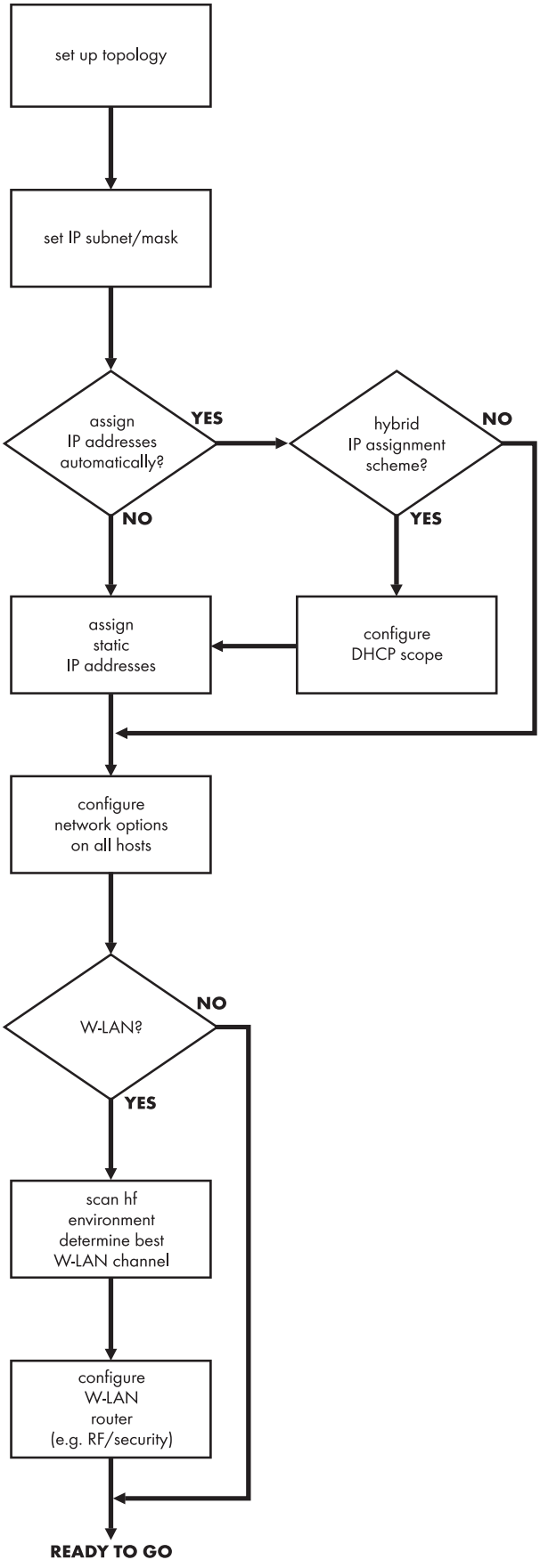
Cualquier cambio en el medio de transmisión añadirá otra capa de incertidumbre al proceso general de comunicación y, dada la complejidad de los sistemas que se utilizan en los espectáculos modernos, ese riesgo debe minimizarse tanto como sea posible.

Por lo que respecta a WLAN, se recomienda que las conexiones inalámbricas sólo deben utilizarse donde sea absolutamente necesario, por ejemplo, el uso de una tableta o un portátil durante la instalación y los ajustes. La conexión para el espectáculo entre un ordenador fijo y el resto del sistema siempre debe hacerse con cable. La conexión con cable facilita mucho localizar los fallos y también libera el máximo de ancho de banda posible para las pocas aplicaciones que tiene que ser inalámbricas.

Otro problema importante que debe tenerse en cuenta es que, durante el espectáculo, es probable que la mayoría del público presente lleve como mínimo un dispositivo con capacidad WLAN (como los smartphones), y muchos tendrán activado WLAN permanentemente. Esto significa que, incluso aunque la red inalámbrica funcione perfectamente en el recinto vacío, puede fallar así que se llene con el público.

5. Inicio rápido

Presuponemos que ha leído y entendido la información que se ofrece en este documento y, a continuación, indicamos el procedimiento paso a paso para configurar rápidamente una red y en el orden lógico.



6. Hardware y cableado de la red

Las redes que se utilicen en un espectáculo, especialmente las que no sólo transmiten datos de control, sino también material audiovisual, exigen una cantidad significativa de ancho de banda. La tecnología Gigabit Ethernet ya está muy extendida y tiene un precio razonable, además de ofrecer todo el ancho de banda que se pueda necesitar. En consecuencia, es mejor no invertir en otras cosas.

Se recomienda encarecidamente el uso exclusivo de hardware de calidad profesional. Aunque hay conmutadores Gigabit baratos que están disponibles para el uso en oficinas domésticas, no ofrecen el mismo rendimiento que un equipo profesional. Por ejemplo, el ancho de banda interna y la latencia de conmutación de un dispositivo doméstico no suele ser adecuada para las secuencias de datos de gran amplitud de banda continua como las que se producen en la red de un espectáculo. Este punto es de especial importancia cuando se transmiten datos de control así como de contenido, por ejemplo, audio o vídeo digital, y esa transmisión se hace por la misma red en un mismo momento, algo que es muy habitual actualmente en el entorno de trabajo de los espectáculos. Por este motivo, lo mejor es invertir en un equipo de calidad.

En la lista siguiente se especifican algunos conmutadores Gigabit Ethernet que han pasado varias pruebas y se han considerado adecuados para el uso profesional. No es una lista exhaustiva, pero incluye varias gamas de precios y funciones auxiliares, como gestión.

- Allied Telesis GS950/8eco
- Allied Telesis GS950/16eco
- Cisco SG300-10
- Cisco SG300-20
- Cisco WS-C2960G-8TC-L
- Dlink DGS-1210-16
- HP 1410-8G
- Luminex Gigaswitch 8
- Teqsas cyberTEQ m

Suele pasarse por alto la calidad de los cables que se utilizan para interconectar los dispositivos de red. En cables de red, puede haber diferencias enormes, especialmente cuando hay que cubrir distancias cercanas a los límites especificados de 100 m y están implicados anchos de banda elevados. Como recomendación general, sólo deben utilizarse cables blindados que se hayan diseñado mecánicamente para resistir los rigores de las aplicaciones móviles.

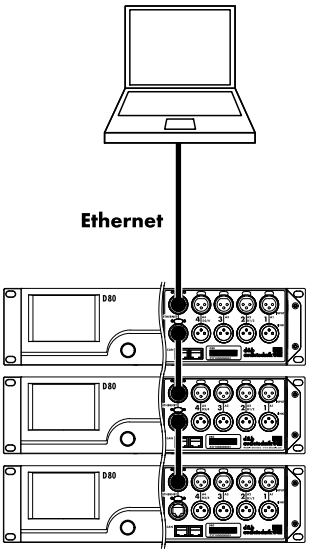
En la lista siguiente se especifican algunas marcas de cables que han pasado varias pruebas y se han considerado adecuados para el uso profesional. No es una lista exhaustiva.

- Klotz RC5SB
- Link LK CAT6STP
- CAE Groupe Giga Audio

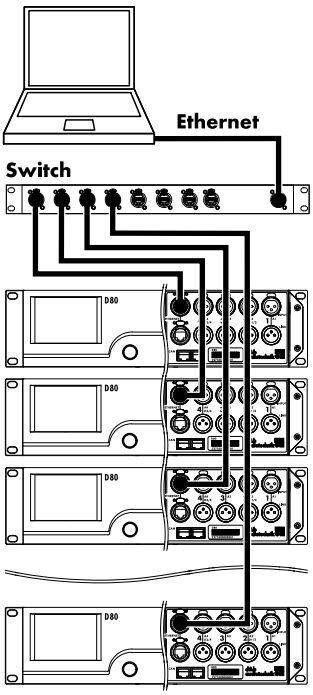
7. Recursos adicionales

Si necesita más información sobre redes, en Internet encontrará abundante documentación adicional. Con sólo una búsqueda en Wikipedia de los términos técnicos que se utilizan en este documento se descubrirá mucha información adicional, que a su vez seguirá abriendo nuevos caminos hacia más detalles.

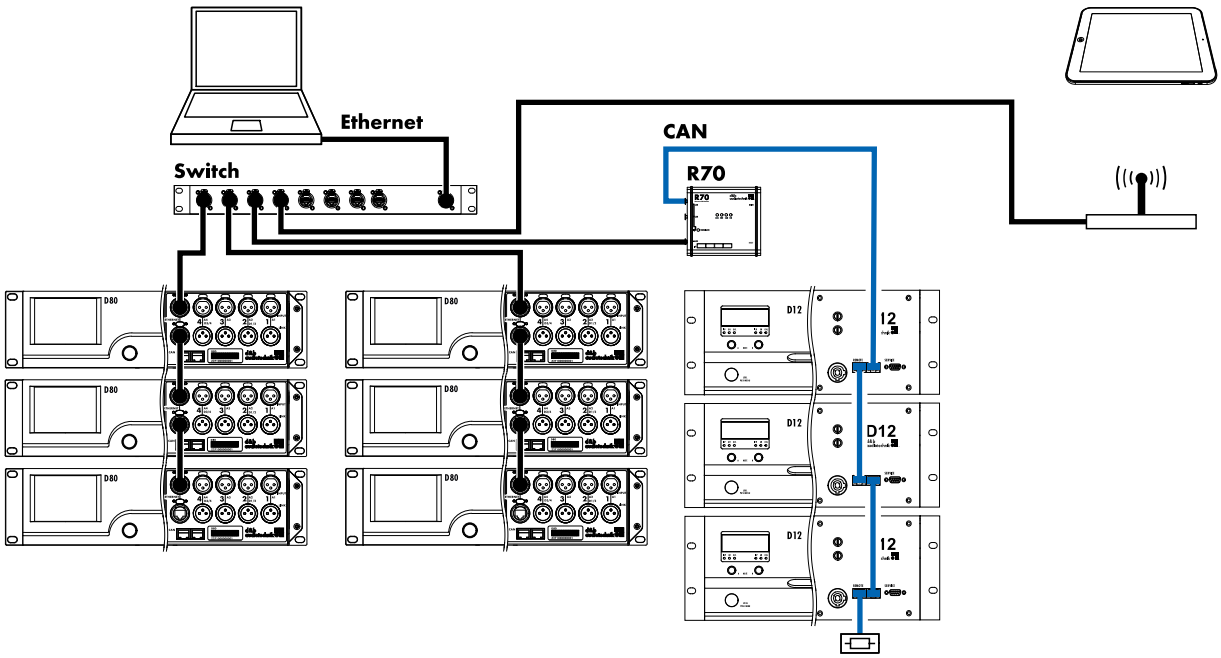
8. Ejemplos de topología en red



Topología en "Daisychain" (en cadena) para un máximo de tres dispositivos



Topología en estrella



Topología combinada

d&b audiotechnik

d&b audiotechnik GmbH, Eugen-Adolff-Str. 134, D-71522 Backnang, Alemania, Teléfono +49-7191-9669-0 Fax +49-7191-95 00 00