TI 310

Ethernet Netzwerke (1.1 DE)

d&b audiotechnik

General information

TI 310 Ethernet Netzwerke

Version 1.1 DE, 12/2014, D5310.DE .01

d&b audiotechnik GmbH
Eugen-Adolff-Strasse 134, D-71522 Backnang, Germany
Telephone: +49-7191-9669-0, Fax: +49-7191-95 00 00
E-mail: support@dbaudio.com, Internet: www.dbaudio.com

Inhalt

1. Einführung

Steuerdaten sowie Audio- und Videodaten werden in der Verantstaltungstechnik zunehmend über Ethernet-Netzwerke übertragen.

Hierbei können Netzwerktopologien und Methoden zum Einsatz kommen, für deren Verständnis und Administration zumindest eine fundierte Fachausbildung notwendig ist. Derartiges Wissen kann und soll diese Informationsschrift nicht vermitteln.

Die überwältigende Mehrheit der Anwendungsfälle betrifft jedoch nicht Großereignisse wie die Olympischen Spiele oder Welttourneen. Vielmehr handelt es sich um Anwendungsgrößen, die mit einem grundlegenden Verständnis der im folgenden aufgeführten Punkte leicht bewältigt werden können:

- Einfache Netzwerktopologien
- MAC-und IP-Adressen sowie IP-Subnetzmasken
- Konfiguration der Netzwerkparameter von Betriebssystemen und Netzwerkgeräten
- Funktionsweise von W-LANs
- Grundlegende Netzwerksicherheit

Dieses Dokument versteht sich als Anleitung für Neulinge und soll relevante Grundlagen praxisorientiert vermitteln. Es ersetzt keinen qualifizierten Netzwerkspezialisten.

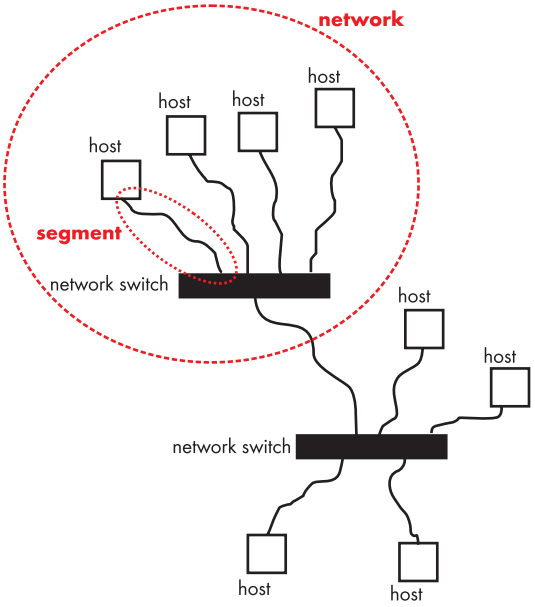
1. Netzwerktopologien

Üblicherweise werden Netzwerke mit mehr als zwei Hosts ('Host' ist die technische Bezeichnung für ein Netzwerkgerät) sternförmig aufgebaut. Alle Hosts sind also nicht direkt, sondern über einen oder mehrere zentrale Knotenpunkte miteinander verbunden. Die einfachste Realisierung eines solchen Knoten- und Verteilpunktes sind sogenannte Hubs oder Switches. Die Verbindung zwischen zwei Hosts beziehungsweise zwischen einem Knotenpunkt und einem Host bezeichnet man als (Netzwerk-)Segment.

Es gibt netzwerkfähige Geräte, die von außen betrachtet eine Reihenschaltung ermöglichen, da sie zwei Anschlüsse mit der Beschriftung "IN" und "OUT" aufweisen. Auch hier handelt es sich in Wirklichkeit um einen eingebauten Switch oder Hub mit wenigstens drei Abgängen oder "Ports", von denen zwei nach außen geführt sind. Der dritte Port ist innenliegend und stellt die tatsächliche Verbindung zum betreffenden Gerät her.

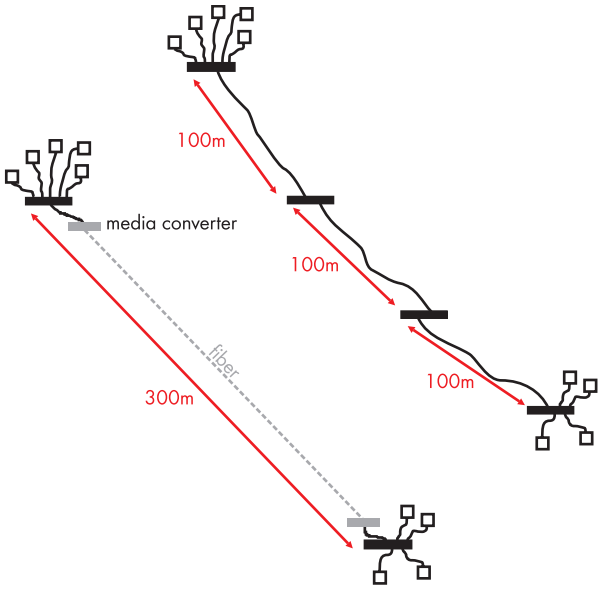
Während Ring- oder Schleifentopologien theoretisch möglich sind, so bedürfen sie spezieller Netzwerkhardware. In Netzwerken ohne besondere Konfiguration führen Ringe oder Schleifen unmittelbar zum Versagen des Netzwerks und sind daher ohne tiefere Kenntnisse unbedingt zu vermeiden.

Nichtsdestotrotz ist es sinnvoll, Netzwerke bei Bedarf nicht nur mit einem, sondern mit mehreren Knotenpunkten strukturiert aufzubauen, wie es die nachfolgende Abbildung zeigt. Dies ist inbesondere dann sinnvoll, wenn es eine Anzahl von Geräten gibt, die untereinander große Datenmengen austauschen und deren Verbindung zum übrigen Netzwerk nur wenig beansprucht wird. Durch die Versorgung dieser Geräte über einen gemeinsamen Unterknoten wird der Rest des Netzwerkes entlastet.



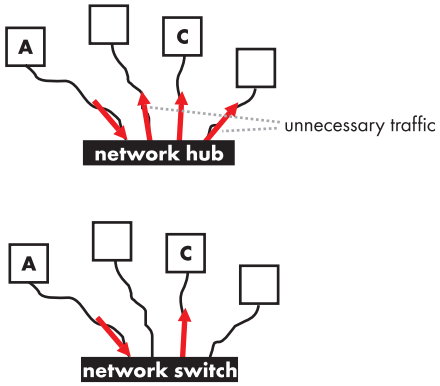
In Abhängigkeit von der Kabelqualität können kupferbasierte Segmente bis zu 100 m lang sein. Um größere Entfernungen zu überbrücken, kann das Segment durch zusätzliche Hubs oder Switches unterteilt werden. Alternativ kann das Segment mittels eines Medienwandlers auf eine Glasfaserverbindung umgesetzt werden. Die dann maximal möglichen Segmentlängen können je nach Art der Glasfaserverbindung auch viele Kilometer betragen.

Die folgende Abbildung zeigt beide Möglichkeiten. Die zu überbrückende Entfernung beträgt ca. 300 m. Mit Kupferkabeln müssen zwei zusätzliche Hubs oder Switches eingesetzt werden, welche jeweils eine weitere Segmentlänge von 100 m ermöglichen. Diese müssen aber mit Strom versorgt werden und stellen zwei zusätzliche Fehlerquellen im Netzwerk dar. Im Gegensatz dazu erlauben Medienwandler den Einsatz einer einzelnen Glasfaser der benötigten Länge ohne weitere technische Hilfsmittel.



1.1. Netzwerkswitch und -hub

Ein Netzwerkknotenpunkt kann entweder mit einem Hub oder einem Switch realisiert werden. Switches werden bedeutend häufiger eingesetzt und sind auch technisch eindeutig zu bevorzugen: Während Hubs alle eingehenden Daten an allen Ports ausgeben und so für jede Kommunikation massiv überflüssigen Datenverkehr erzeugen, erkennen Switches, an welchen Ports bestimmte Hosts angeschlossen sind und leiten die Datenströme gezielt weiter. Dies erhöht die Leistungsfähigkeit des gesamten Netzwerks erheblich.



Hub und Switch: Host 'A' kommuniziert mit Host 'C'

2. Identifikation und Kommunikation

In Datennetzwerken kommen in der Regel Hosts verschiedener Hersteller zum Einsatz. Identifikation und Kommunikation im Netzwerk finden auf der Basis von übergreifenden, offenen Standards statt. Die für den normalen Anwendungsfall relevanten Standards und Begriffe werden im folgenden grundlegend erklärt.

2.1. MAC-Adresse

Die MAC-Adresse hat nichts mit einem bekannten Computer- und Softwarehersteller zu tun. Vielmehr ist **MAC** ein Akronym für "**M**edia **A**ccess **C**ontrol" und dient der eindeutigen Identifikation von Netzwerkgeräten auf Hardwareebene.

Die MAC-Adresse ist in der Hardware jedes Netzwerkgerätes implementiert (d&b R70 Ethernet to CAN Interface, Netzwerkkarte im Computer, W-LAN Router, usw.) und dadurch zumindest theoretisch nicht veränderbar.

In Ethernet-Netzwerken besteht die MAC-Adresse aus 48 Bit oder 6 Byte, die wie im folgenden Beispiel hexadezimal notiert werden:

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

MAC-Adressen sind für den normalen Netzwerknutzer nur selten von Belang, da die benutzerspezifische Konfiguration meist auf höheren Abstraktionsebenen abläuft.

2.2. IP-Adresse

Während MAC-Adressen eine eindeutige Identifikation von Netzwerkhardware erlauben, so ist es in Datennetzwerken von großer Bedeutung, einzelne Gruppen von Hosts logisch zusammenzufassen und abzugrenzen. Dazu wird jedem durch eine MAC-Adresse repräsentierten Netzwerkgerät eine temporäre IP-Adresse zugewiesen.

Im momentan dominierenden Ipv4-Standard haben IP-Adressen eine Länge von 32 Bit und werden üblicherweise als Block aus vier Dezimalzahlen (entsprechend jeweils 8 Bit, daher auch "Oktett") wie folgt notiert:

137.152.89.230

Im Gegensatz zu MAC-Adressen sind IP-Adressen und speziell ihre Vergabe auch für ein normalen Netzwerkanwender oft von Belang.

2.2.1. IP -Subnetze

Zur Bildung von logischen Teilnetzen wird innerhalb von IP-Adressen zwischen Subnetz oder Netzwerkpräfix und Hostadresse unterschieden. Eine grob vergleichbare Unterteilung gibt es auch bei dbCAN-Netzwerken. Die CAN ID 5.23 wird in Subnetz '5' und ID '23' unterteilt.

Bei IP-Adressen besteht aber nicht eine allgemein vorgegebene Unterteilung, vielmehr ergibt sich die Präfixlänge aus der sogenannten Subnetzmaske. Diese wird genau so wie die IP-Adresse notiert. Die Subnetzmaske

255.255.255.0

bedeutet, dass die ersten drei Oktette einer IP-Adresse das Subnetz beschreiben. In einem solchen Netzwerk müssen dementsprechend die ersten drei Oktette der IP-Adressen aller Netzwerkgeräte gleich lauten, wenn diese ohne weitere Hilfe durch das Netzwerk miteinander kommunizieren sollen.

Mit obiger Subnetzmaske könnte eine IP-Adresse wie folgt aussehen:

192.168.0.[**x**]

[**x**] ist dabei die Hostadresse und '192.168.0' der für alle Hosts gleiche Netzwerkpräfix. Bei allen Hosts muss '255.255.255.0' als Subnetzmaske eingestellt sein.

Ein derartiges Netzwerk kann folglich 256 verschiedene Hosts (Hostadresse 0 bis 255) enthalten. Tatsächlich sind aber in allen IP-Adressbereichen die jeweils niedrigste (hier: 192.168.1.0, bezeichnet das Netzwerk selbst) und die höchste IP-Adresse reserviert (hier: 192.168.1.255, die "Broadcastadresse", welche das gesamte Netzwerk anspricht). Es verbleiben zur freien Vergabe noch 254 verschiedene Hostadressen. Diese mögliche Anzahl von Netzwerkgeräten sollte für jede normale Anwendung mehr als ausreichend sein.

2.2.2. Private IP-Adressen (Intranets)

Die Vergabe von IP-Adressen kann nicht völlig wahlfrei erfolgen, sondern unterliegt einigen Regulierungsauflagen. Die meisten IP-Adressbereiche werden von der Internet Assigned Numbers Authority (IANA) verwaltet. Für Intranets, die nicht Teil des Internet sind, wie z.B. Shownetzwerke, sind mehrere 'private' Adressbereiche vorgesehen. Häufig genutzt werden

10.0.0.0 - 10.255.255.254

und

192.168.0.0 - 192.168.255.254

Mit einer Subnetzmaske von 255.255.255.0 haben IP-Adressen innerhalb eines Shownetzwerks folgende Schreibweise:

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

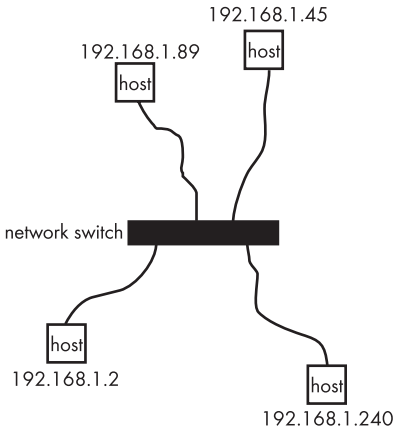
192.168.[**x**].[**z**]

Dabei sind [**x**] und [**y**]

beliebige Zahlen zwischen 0 und 255. Diese bilden nach der oben genannten Subnetzmaske den Netzwerkpräfix und müssen daher für alle Hosts identisch sein.

Die Zahl [**z**]

ist die Hostadresse zwischen 1 und 254. Sie muss für jeden Host eindeutig sein. Die Abbildung zeigt ein Beispiel für ein solches Netzwerk.



subnet mask: 255.255.255.0 network prefix: 192.168.1.0

2.2.3. Automatische und manuelle Zuweisung von IP-Adressen

Zur schnellen Netzwerkkonfiguration können alle relevanten Parameter wie Subnetzmaske, IP-Adresse etc. mittels DHCP (Dynamic Host Configuration Protocol) automatisch zugewiesen werden. Voraussetzung dafür ist das Vorhandensein eines DHCP-Servers im Netzwerk. Diese Funktionalität ist beispielsweise in den meisten W-LAN-Routern enthalten.

Hinweis: Jedes Netzwerk sollte maximal **einen** DHCP-Server beinhalten. Sind versehentlich zwei oder mehr DHCP-Server in einem Netzwerk aktiv, kann dies zu Verbindungsverlusten führen. Aus technischen Gründen kann dies auch erst Stunden oder Tage passieren, nachdem ein zusätzlicher DHCP-Server aktiv war. Besondere Vorsicht ist bei der Verwendung von Mobiltelefonen geboten, die eine Internetverbindung im Netzwerk bereitstellen – auch sie agieren dann als DHCP-Server.

Auch bei korrekter Verwendung können Probleme auftreten. In seltenen Fällen schlägt die Kommunikation mancher Netzwerkgeräte und DHCP-Server fehl, so dass keine IP-Adresse zugewiesen wird.

Verbindungsverluste können auch dann auftreten, wenn IP-Adressen manuell vergeben werden, obwohl ein DHCP-Server im Netzwerk vorhanden ist. Auch der häufige Wechsel zwischen automatischer und manueller Adressvergabe kann zu Schwierigkeiten führen, wenn die entsprechende Funktion bei einzelnen Geräten nicht richtig konfiguriert ist und deren manuell vergebene Adresse auch noch einen unterschiedlichen Netzwerkpräfix aufweist.

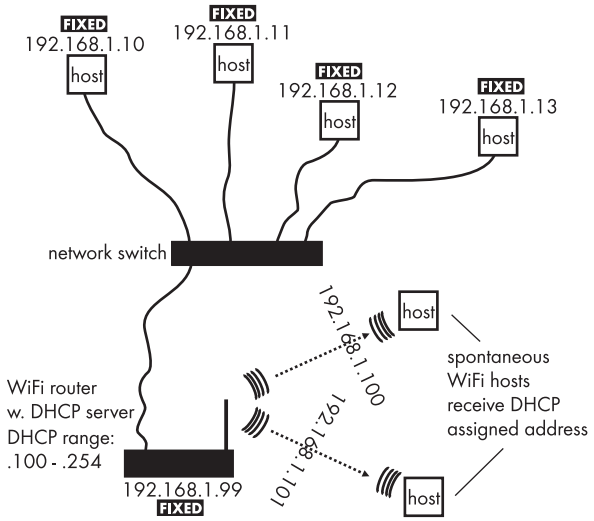
Jeder Anwender sollte daher in der Lage sein, ein Netzwerkgerät auf automatische Adressvergabe (DHCP-Betrieb) zurückzusetzen. Werden IP-Adressen manuell vergeben, so ist es empfehlenswert dies am Gerät durch eine Beschriftung kenntlich zu machen. Ein solches Verfahren ist auch als “Peg DHCP” bekannt und sogar offiziell beschrieben: In temporären Netzwerken werden manuell vergebene IP-Adressen oft auf Wäscheklammern (eng. “cloth peg” = Wäscheklammer) geschrieben und auf das geräteseitige Ende des Netzwerkkabels geklipst.

2.2.4. Hybride IP-Adresszuweisung

Besteht ein Netzwerk größtenteils aus immer den gleichen Hosts, ist es sinnvoll, alle IP-Adressen manuell und permanent zu vergeben. Sollen trotzdem vereinzelt Zusatzgeräte mit geringem Aufwand eingebunden werden können, empfiehlt sich eine Mischform aus manueller und automatischer Adressvergabe.

Bei vielen DHCP-Servern kann der für die automatische Zuweisung verfügbare Adressbereich eingegrenzt werden, beispielsweise auf den Adressraum von 192.168.1.**100** bis 192.168.1.**254**. So können allen dauerhaft im Netzwerk vorhandenen Hosts manuell IP-Adressen von 192.168.1.1 bis 192.168.1.99 zugewiesen werden und es gibt keinen Konflikt mit per DHCP zugewiesenen Adressen von temporären Netzwerkteilnehmern.

Die folgende Darstellung zeigt ein typisches Szenario: Alle festen Hosts haben manuell zugewiesene IP-Adressen. Der DHCP-Server, in diesem Fall der W-LAN-Router, hat ebenfalls eine manuell zugewiesene IP-Adresse und vergibt seinerseits nur Adressen aus einem begrenzten Adressraum an mobile Geräte (Laptops, Tablets, etc.). Diese sind ihrerseits für automatische Adressvergabe konfiguriert und fragen ihre IP-Adresse beim DHCP-Server im W-LAN-Router an.



2.3. Datentransport mittels TCP und UDP

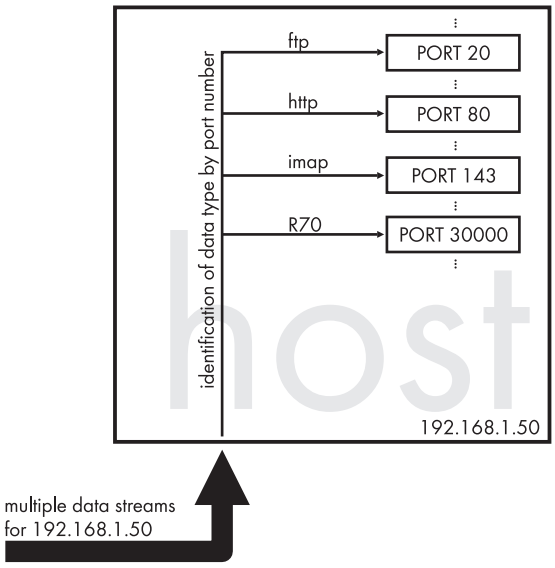
Ist eine Netzwerkverbindung mittels des Internet Protocol (IP) hergestellt, können über diese Verbindung auf verschiedene Art und Weise Daten übertragen werden. Dafür wird eine weitere sogenannte Protokollschicht benötigt. Sehr häufig wird der Datentransport via TCP (Transmission Control Protocol) oder UDP (User Datagram Protocol) abgewickelt.

TCP beinhaltet verschiedene Mechanismen, die unter anderem eine fehlerfreie Datenübertragung sicherstellen und den Sender über den Status der Verbindung informieren.

UDP hingegen ist ein bedeutend simpleres Protokoll. Es beinhaltet weder den Aufbau einer logischen Verbindung zum Empfänger noch jedwege Rückmeldung über den Eingang eines Datenpaketes am Ziel, ist also weitaus unzuverlässiger. Allerdings ist es dadurch schneller und wird daher für viele echtzeitkritische Anwendungen bevorzugt: Ein verlorenes Datenpaket wiegt unter Umständen weniger schwer als eine längere Unterbrechung wegen eines nicht korrekt oder verzögert empfangenen Datenpaketes.

2.3.1. Ports

Netzwerkhosts können nicht nur eine, sondern mehrere Datenverbindungen gleichzeitig aufbauen. Auch können mehrere Ströme gleichartiger Daten gleichzeitig gesendet und empfangen werden. Um diese Datenströme sicher unterscheiden zu können, wird ein logisches Konstrukt genutzt – der 'Port'. Jeder Datenstrom erhält eine 16 Bit lange 'Portnummer' zur Identifikation zugewiesen. Diese kann man sich bildhaft wie die Wohnungsnummer in einem Mehrparteienhaus vorstellen. Häufig vorkommende Datendienste haben in der Regel fest zugeordnete Portnummern. Die folgende Darstellung zeigt einige Beispiele.



2.4. Netzwerksicherheit

Neben Fehlbedienung und Hardwareausfall sind Viren und andere Schadsoftware sowie unbefugter Zugriff das größte Betriebsrisiko eines Netzwerks. Firewalls und ähnliche Sicherheitssysteme sollen dem entgegenwirken und schädlichen Datenverkehr blockieren. Moderne Betriebssysteme, aber auch viele Netzwerkgeräte wie W-LAN-Router besitzen ab Werk aktivierte Firewallfunktionen. Diese blockieren entweder Datenverkehr von bestimmten IP-Adressbereichen oder an bestimmte Ports gerichtete Datenströme oder aber sie erlauben überhaupt nur Kommunikation zwischen bestimmten Netzwerkteilnehmern und -ports.

Die Komplextität derartiger Sicherheitsmechanismen nimmt als Reaktion auf immer ausgefeiltere Bedrohungen stetig zu. Gleichzeitig sind immer weniger Anwender in der Lage, Sicherheitssoftware selbständig richtig zu konfigurieren. Aus diesem Grund versuchen Firewalls und Antivirensoftware, automatisch, schädliche Daten und Programme zu erkennen. Dies führt häufig zu Problemen in Verbindung mit Software aus dem Veranstaltungstechnikbereich, die unter Umständen Protokolle und Ports verwendet, welche in einer Büroumgebung nicht üblich sind.

Schon aus Sicherheitsgründen sollten Steuer- und Datennetzwerke in der Veranstaltungstechnik keine Verbindung zum Internet haben. Ist dies gegeben, können Firewalls und ähnliche Sicherheitssoftware deaktiviert werden, um das Netzwerk nicht unvorgesehen zu behindern oder zu blockieren.

Persönliche Laptops von Technikern werden jedoch oft wechselnd auf Veranstaltungen und für Büroanwendungen mit Internetverbindung genutzt. Hier bedarf es folglich der besonderen Vorsicht jedes einzelnen.

Der kontrollierte physikalische Zugang zu Netzwerkkomponenten ist in der professionellen Anwendung eine wesentliche, weil überprüfbare Maßnahme. Drahtlosnetzwerke bilden prinzipbedingt eine Ausnahme, daher sind die spezifischen Zugangskontrollmaßnahmen wie effektive Verschlüsselung (WPA oder WPA2, **nicht** WEP) und gegebenenfalls MAC-Adressfilterung hier besonders wichtig.

Vollständige Sicherheit kann niemals garantiert werden. Das manuelle Konzipieren und Einrichten von Sicherungsmaßnahmen hat in diesem Zusammenhang zumindest den Vorteil, dass der Netzwerkverantwortliche aktiv die entsprechenden Überlegungen anstellt und sich nicht auf Automatismen verlässt.

2.4.1. Hinweise zur manuellen Netzwerkkonfiguration

Auch wenn dies für geschlossene Netzwerke wie sie im Veranstaltungstechnikbereich verwendet werden, keine Bedeutung hat, so können in den Netzwerkeinstellungen von Betriebssystemen und auch bei vielen vernetzbaren Geräten außer IP-Adresse und Subnetzmaske noch weitere Parameter konfiguriert werden.

In der Regel genügt es, die entsprechenden Felder einfach leer zu lassen. Einzelne Geräte verlangen allerdings zwingend die Angabe einer Gateway-Adresse, auch wenn dies nur für eine mögliche Internetverbindung relevant ist. In diesen Fällen bietet es sich an, die IP-Adresse des DHCP-Servers hier anzugeben, auch wenn das entsprechende Gerät manuell adressiert wird.

3. W-LAN (“Wi-Fi”)

W-LAN ('Wireless Local Area Network') ist der Sammelbegriff für mehrere Implementationen der IEEE Norm 802.11. Im Veranstaltungstechnikbereich ermöglichen richtig konfigurierte drahtlose Verbindungen gerade für Fernsteuerungswendungen eine hohe Mobilität. Im folgenden werden Grundlagen beschrieben, die für ein funktionierendes W-LAN-Netz relevant sind.

3.1. Standards

Die verschiedenen Implementationen der IEEE 802.11 nutzen zwei unterschiedliche Frequenzbänder im Bereich 2.4 Ghz und 5 Ghz.

Nicht alle Technologievarianten werden gleich häufig verwendet.

Standard	Frequenzband	Max. Bruttodatenrate
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

3.2. Kanäle und Frequenzen

Beide Frequenzbänder sind in mehrere Unterbänder, die sogenannten Kanäle, unterteilt. Dies erlaubt in der Regel den gleichzeitigen Betrieb mehrerer unabhängiger W-LAN-Netze. Die Kanalzahl pro Frequenzband ist nicht weltweit einheitlich. Manche Regionen erlauben ein etwas breiteres Frequenzband als andere, so dass dort mehr Kanäle realisiert werden können.

Im 2.4 Ghz Band sind je nach Region bis zu 14 Kanäle mit einer Kanalbandbreite von 22 MHz verfügbar. Die Mittenfrequenzen der einzelnen Kanäle haben jedoch einen Abstand von nur 5 MHz, so dass die Verwendung eines Kanals immer mindestens drei benachbarte Kanäle beeinträchtigt.

Demzufolge können nur drei Kanäle überlappungsfrei gleichzeitig genutzt werden: 1, 6 und 11. Da auch viele andere Geräte wie schnurlose Telefone, Babyphone und neuerdings auch Drahtlosmikrofone dieses Frequenzband nutzen, kann es auch bei umsichtiger Frequenzplanung zu unerwarteten Störungen kommen.

Das 5 GHz Band ermöglicht bis zu 26 nicht überlappende Kanäle. Zusätzlich sind noch relativ wenige Drahtlosgeräte mit diesem Frequenzbereich kompatibel, so dass es als ideal für einen störungsfreien W-LAN-Betrieb erscheint. Allerdings werden die kürzeren Wellenlängen bei 5 GHz leichter von Hindernissen reflektiert oder absorbiert als bei 2.4 GHz, was wiederum zu Empfangsschwierigkeiten führen kann.

3.3. Ermittlung eines geeigneten W-LAN Kanals

Um mögliche Probleme zu minimieren, sollte jegliche Funknutzung bereits im Vorfeld mit allen beteiligten Gewerken koordiniert werden.

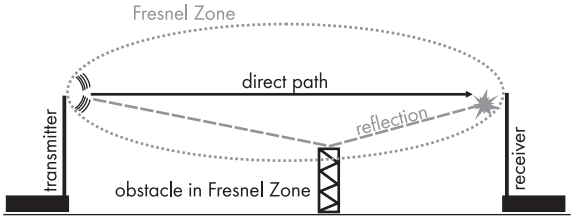
Um trotzdem situationsbedingt reagieren zu können, empfiehlt sich vor Ort die Nutzung eines W-LAN-Scanners, der vorhandene W-LANs und ihre Feldstärke detektieren und anzeigen kann.

Für Windows-Computer ist unter anderem das Programm **'inSSIDer'** von MetaGeek, LLC (metageek.net) zu empfehlen. Es ist kostenlos erhältlich und erfasst und klassifiziert mittels des W-LAN-Adapters des Hostrechners alle W-LAN-Netze in der Umgebung. In der kostenfreien Version werden allerdings nur W-LANs dargestellt. Andere Sender wie Türöffner, drahtlose Telefone etc, welche den gleichen Frequenzbereich nutzen werden nicht erfasst.

Bitte beachten Sie, dass es sich bei inSSIDer nicht um ein Produkt von d&b audiotechnik handelt. d&b audiotechnik übernimmt keine Haftung und leistet keine Unterstützung für Software von Drittanbietern.

3.4. Freie Sichtlinien und die Fresnelsche Zone

Hochfrequenzübertragungen wie W-LAN benötigen eine freie Sichtlinie zwischen Sender und Empfänger. Vielen Funkanwendern ist allerdings weniger geläufig, dass auch Objekte, die sich lediglich in der Nähe der Sichtlinie befinden, das Funksignal durch Reflektion und Interferenz stören können. Der besonders kritische Raumbereich um die Sichtachse ist nach dem Physiker Augustin-Jean Fresnel benannt und hat die Form eines Rotationsellipsoiden. Der maximale Radius des Ellipsoiden ist proportional zur überbrückenden Entfernung. Je länger die Übertragungsstrecke ist, umso wichtiger ist ein freier Bereich um die Sichtlinie.



Die einfachste Methode, um gute Sende- und Empfangsbedingungen zu erreichen, ist eine möglichst hohe Montage entweder des W-LAN-Routers oder seiner Antennen.

Obwohl es merkwürdig anmutet, kann die hohe Montage des gesamten W-LAN-Routers besser sein, denn auch die Kabelführung zu abgesetzten Antennen weist einen nicht unerheblichen Verlust auf. Dieser steigt mit der Frequenz, ist also für 5 GHz stärker ausgeprägt als für 2.4 GHz.

3.5. Praktische Grenzen der drahtlosen Übertragung

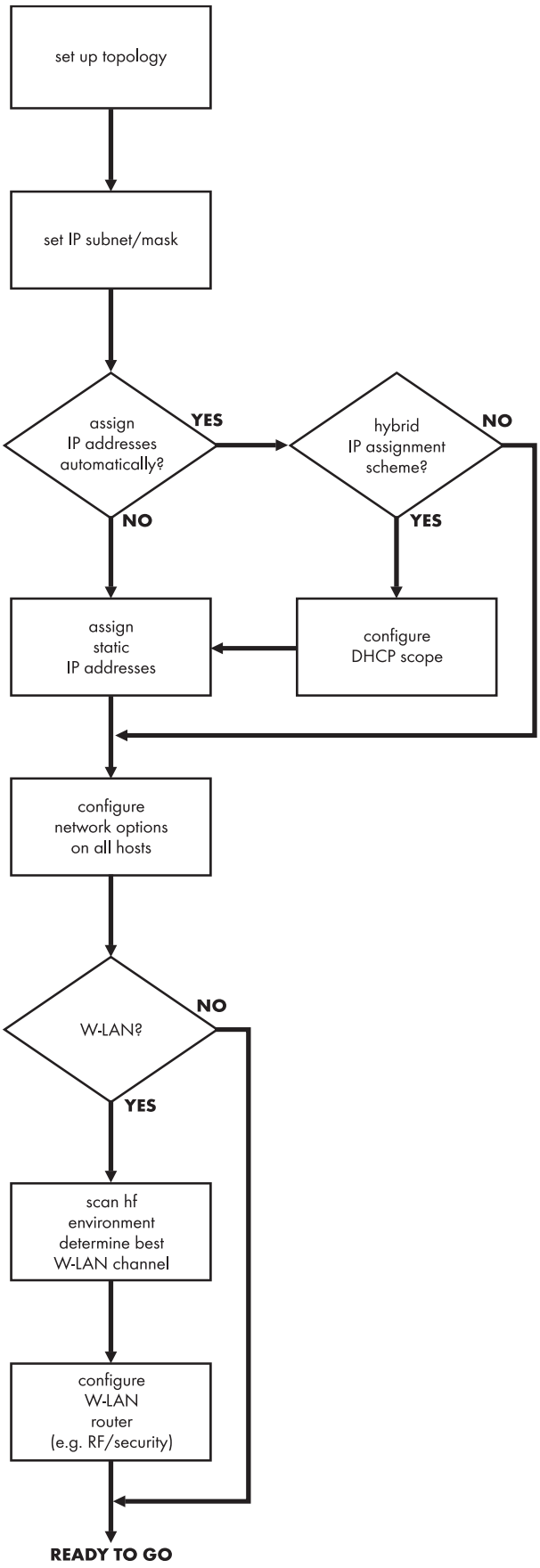
Jeder Medienwechsel erhöht die Fehleranfälligkeit einer Übertragungsstrecke. Diese sollte angesichts der allgemein steigenden Komplexität von Systemen in der Veranstaltungstechnik vermieden werden.

Wir empfehlen, W-LAN-Verbindungen nur dort zu verwenden, wo es absolut notwendig ist. Ein Tablet-PC, welcher zur Inbetriebnahme und Einrichtung einer Beschallungsanlage genutzt wird, profitiert von einer kabellosen Verbindung, da der Systemtechniker von einem beliebigen Zuhörerplatz aus alle Einstellungen vornehmen kann. Während der Vorstellung sollten Steuerdaten aus Gründen der Betriebssicherheit ausschließlich über kabelgebundene Verbindungen übertragen werden. Dies erleichtert nicht nur die Fehlersuche sondern hält auch die größtmögliche Bandbreite für andere Anwendungen frei, welche zwingend drahtlos sein müssen.

Ein nicht unwesentliches Kriterium ist überdies, dass viele Zuschauer Geräte bei sich tragen, die über W-LAN Funktionalitäten verfügen. Viele solcher Geräte mit aktivierter Netzsuche können während einer Vorstellung dafür sorgen, dass für Steuerzwecke installierte W-LANs nicht mehr funktionieren.

4. Kurzanleitung zur Netzwerkeinrichtung

Die folgende Kurzanleitung gibt eine Handreichung zur schnellen Einrichtung einfacher Netzwerke. Voraussetzung dafür ist, dass die in diesem Dokument enthaltenen Informationen verstanden wurden.



5. Netzwerkhardware und -verkabelung

Netzwerke im Veranstaltungsbereich übertragen zunehmend nicht nur Steuerdaten sondern auch Audio- und Videoinhalte. Gerade diese echtzeitkritischen Anwendungen stellen hohe Anforderungen an Verfügbarkeit und Bandbreite des Netzwerkes. Gigabit-Netzwerke stellen große Übertragungskapazitäten zur Verfügung und sind günstig realisierbar.

Auch hier bestehen allerdings große Unterschiede zwischen Hardware für Heimanwender und solcher für den professionellen Gebrauch. Interne Bandbreite und Latenzen von einfachen Geräten sind in der Regel nicht auf die hohen Anforderungen von Shownetzwerken ausgelegt. Dieser Aspekt ist bei Neuinvestitionen dringend zu berücksichtigen.

Als Hilfestellung werden im folgenden Gigabit Ethernet Switche aufgeführt, die für die hohen Datenvolumina im Veranstaltungsbetrieb geeignet sind. Die Liste enhält Geräte verschiedener Preisklassen und mit verschiedenen Zusatzfunktionen. Sie ist nicht vollständig.

- 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

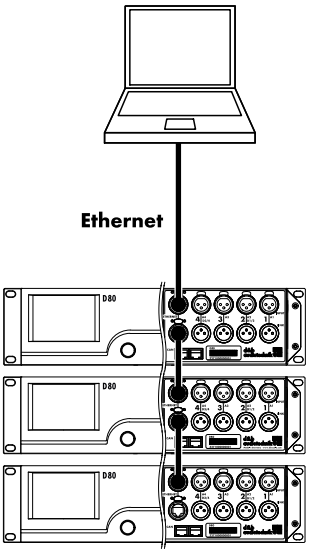
Der Qualität der Verkabelung wird oft nicht genügend Bedeutung beigemessen. Allerdings bewegen sich typische Anwendungen oft sehr nahe an oder auch jenseits der Spezifikationsgrenze von 100 m für ein Netzwerksegment. Dies ist insbesondere dann interessant, wenn auch noch hohe Bandbreiten gefordert werden. Dementsprechend ist die Auswahl des richtigen Kabeltyps kritisch. Die folgende Liste enthält geeignete Kabeltypen. Sie ist nicht vollständig.

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

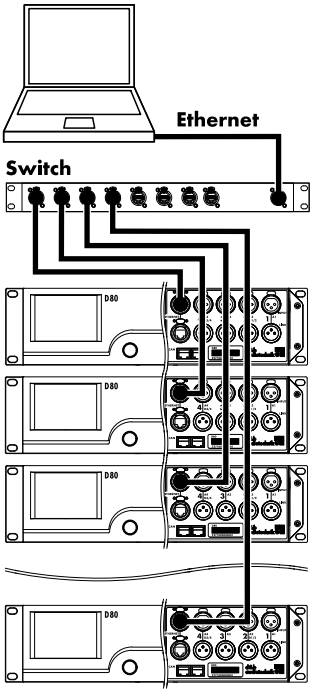
6. Weitere Informationen

Weitere Informationen zu Netzwerken, ihrer Technologie und Verfahren sind mit einer einfachen Internet-Suchanfrage verfügbar. Allein die Wissensplattform Wikipedia bietet einen großen Informationsumfang zu allen in diesem Dokument verwendeten technischen Begriffen und weitreichende zusätzliche Recherchemöglichkeiten.

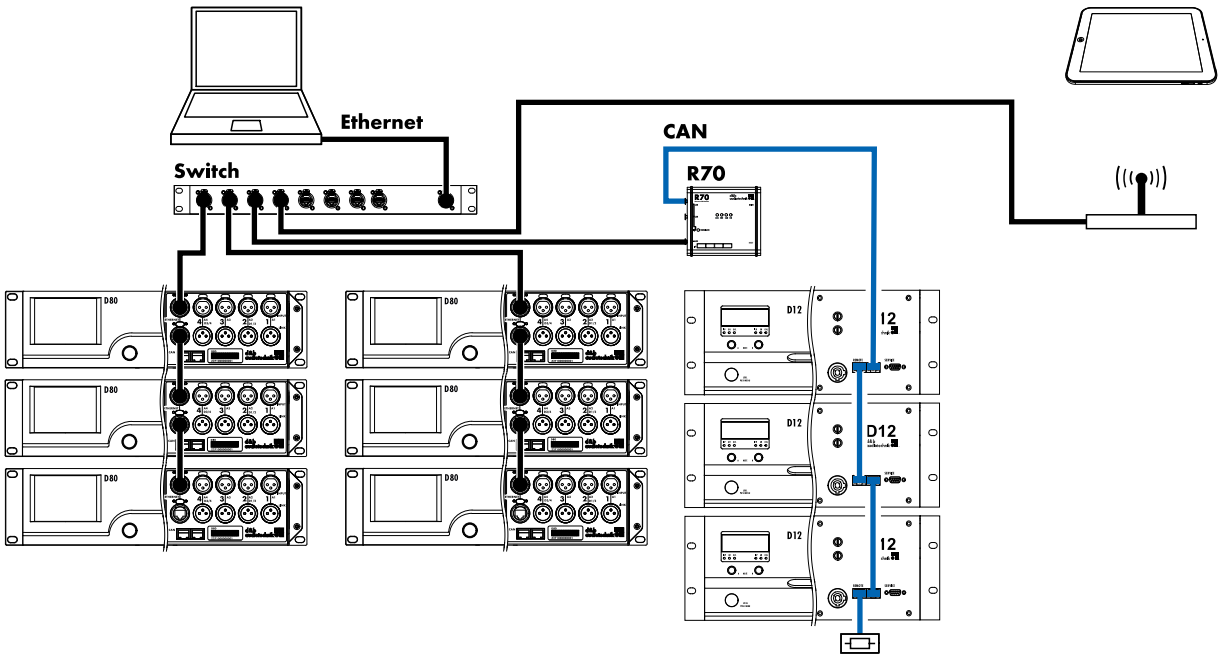
7. Netzwerktopologien



Daisychain-Topologie für maximal drei Geräte



Sternopologie



Gemischte Konfiguration

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