

**REVOX**

## Multuser Netzwerkwissen

### INHALT

#### LAN BETRIEB & MULTICAST

---

Grundlagen	2
IGMP	3
Hardware	3 / 4
VLAN`s	4
Verwendete Ports	4
Multicast Konflikte	4
Beispiele	5 / 6

#### WLAN BETRIEB

---

Grundlagen	7
Störeinflüsse	8
Frequenzen und Kanäle	8 / 9
Latenz und Paketumlaufzeit	9 / 10
Optimierungsmöglichkeiten	10

## Grundsätzliches zu LAN Verbindungen beim Multuser 3.0 System

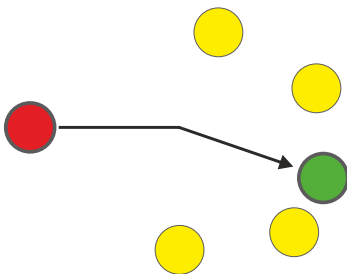
Das Revox Multuser System verwendet die IP-Multicasting Technologie wenn mehrere Komponenten im System per LAN-Kabel verbunden sind!

Mit dieser Technologie ist es möglich, ohne zeitliche Verzögerung Quellen aus unterschiedlichen Räumen abzuspielen. Dazu hat das Multuser System eine Grundlatenz, diese beträgt ca. 75 -90 ms. Um die reibungslose Funktion eines Multicast-Systems wie das Revox Multuser System zu gewährleisten, ist der Aufbau und die richtige Konfiguration der Netzwerkinfrastruktur von höchster Wichtigkeit!

Auf den nachfolgenden Seiten finden Sie Informationen und Darstellungen rund ums Thema Netzwerkaufbau.

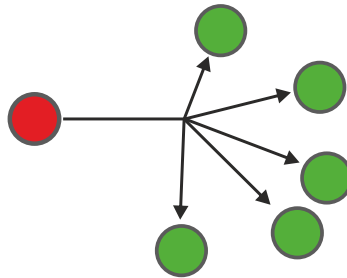
## Netzwerk Kommunikationsarten

### Unicast



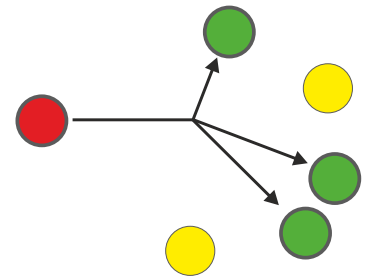
Daten werden von einem Endpunkt über einen Knoten zu genau einem Endpunkt transportiert (eins zu eins).

### Broadcast



Daten werden von einem Endpunkt über einen Knoten zu allen Endpunkten in einem Netzwerk transportiert. Der Knoten übernimmt die Verteilung/Duplizierung und Weiterleitung der Daten an alle Endpunkte.

### Multicast



Daten werden von einem Endpunkt über einen Knoten zu einer beliebigen Anzahl von Endpunkten in einem Netzwerk transportiert. Der Knoten übernimmt die Verteilung/Duplizierung und Weiterleitung der Daten an alle interessierten Endpunkte. Der Knoten kennt die interessierten Empfänger in der Regel anhand der Multicast-Adresse der Endpunkte.

## Netzwerk Grundvoraussetzungen

Da das Revox Multuser System die Multicasting Technologie nutzt, sollten bereits bei der Systemplanung IGMP Snooping und Querier fähige Netzwerk Switches berücksichtigt werden.

Eine Liste mit empfohlener und getesteter Hardware inklusive Konfigurationsanleitung finden Sie auf der Supportseite.

Netzwerk Grundvoraussetzungen für ein Multuser-System:

- Multicast fähiges Netzwerk (IGMP Snooping & Querier Unterstützung)
- Feste 1Gbit Verkabelung – 100 Mbit zu den Clients reicht aus

## IGMP „Internet Group Message Protocol“

Das Internet Group Message Protocol basiert auf dem Internet Protocol (IP) und ermöglicht IPv4-Multicasting (Gruppenkommunikation) im Internet. IP-Multicasting ist die Verteilung von IP-Paketen mit einer Ziel-IP-Adresse an mehrere Stationen gleichzeitig. IGMP bietet die Möglichkeit, dynamisch Gruppen zu verwalten. Die Verwaltung findet nicht in der Sendestation statt, sondern in den Routern, an denen Empfänger einer Multicast-Gruppe direkt angeschlossen sind. IGMP bietet Funktionen, mit denen eine Station einem Router mitteilt, dass sie Multicast-IP-Pakete einer bestimmten Multicast-Gruppe empfangen will. Multicast-Routing-Protokolle (DVMRP, MOSPF, PIM) übernehmen die Koordination der Übertragung zwischen den Routern. Der Sender von Multicast-IP-Paketen weiß dabei nicht, welche und wie viele Stationen seine Pakete empfangen, denn er verschickt nur ein einziges Datenpaket an seinen übergeordneten Router. Dieser dupliziert das IP-Paket bei Bedarf, wenn er mehrere ausgehende Schnittstellen mit Empfängern hat.

## IGMP Snooping

IGMP Snooping ist eine Eigenschaft von Netzwerk Switches. Der Switch belauscht (snoop, schnüffeln) den IGMP-Traffic an seinen Ports zwischen Hosts und Routern. Dabei lernen die Switches beim Empfang von IGMP Membership Requests, welche der angeschlossenen Geräte zu einer Multicast-Gruppe gehören. Wird ein Multicast für eine Gruppe empfangen, wird die Nachricht nur an die entsprechenden Ports, die zu dieser Multicastgruppe gehören weitergeleitet, die anderen Ports sehen diese Nachrichten nicht.

Zusammengefasst: Mittels IGMP Snooping kann verhindert werden, dass Multicast-Traffic an alle Switchports geflutet wird. So wird die Netzwerklast reduziert.

## IGMP Querier

Damit das IP-Multicasting im Netzwerk über alle Komponenten funktioniert, wird ein zentrales Gerät benötigt, der allen Netzwerk Komponenten deren Multicast Gruppen Zugehörigkeit verwaltet, der sogenannte IGMP Querier. Die Antworten auf Querier-Anfragen veranlassen die Switches ihre Membership Listen entsprechend zu aktualisieren.

**Die Querier Funktion wird nur von Router oder Layer 3 Switches unterstützt, nicht aber von Layer 2 Switches.**

## Router

Revox empfiehlt die Netzwerkanforderungen (IGMP Querier und Snooping) mit Layer 3 und ggf. Layer 2 Switches abzudecken und verzichtet auf die Empfehlung von Router.

Oft sind Router Provider seitig bereits vorhanden und decken die gewünschten Anforderungen nicht ab oder verlieren diese bei Softwareaktualisierungen.

## Firewall

Wenn die eingesetzte Firewall im Multicasting Bereich das IGMP Snooping und das IGMP Querier abdeckt, können nachfolgende Netzwerk Switches als Layer 2 Ausführung eingesetzt werden. Wenn auf der Firewall keine Multicast Einstellungen vorgenommen werden können oder die Funktionen fraglich sind, wird der zusätzliche Einsatz eines Layer 3 Switch empfohlen. Die Firma Revox verzichtet auf eine Firewall Hardware Empfehlung.

## Layer 2 Switch

Ein Layer 2 Switch kann LAN-Segmente miteinander verbinden und die zur Verfügung stehende Bandbreite effizient auf die Nutzer verteilen. Ein Layer 2 Switch hat keine Vermittlungs- und Routingfunktionen. In der Regel beschränken sich Layer 2 Switches im Bereich Multicasting auf das IGMP Snooping und bieten kein IGMP Querier. Aus diesem Grund eignen sich Layer 2 Switches als Erweiterung im Zusammenspiel mit einem Layer 3 Switch. Beachten Sie dazu die Praxis Beispiele auf den folgenden Seiten und unsere Hardwareempfehlungsliste.

## Layer 3 Switch

Ein Layer 3 Switch ist eine Kombination aus Router und Switch und hat somit Vermittlungs- und Routingfunktionen. Gegenüber einem Layer 2 Switch bietet er im Bereich Multicasting ein **IGMP Snooping** und eine **IGMP Querier Funktion**. Aus diesem Grund empfiehlt es sich in einem Multicast-System **mindestens einen Layer 3 Switch** einzusetzen. Beachten Sie dazu die Praxis Beispiele auf den folgenden Seiten und unsere Hardwareempfehlung sowie die Konfigurationsanleitung.

## VLAN`s

Wenn die Netzwerkkumgebung von einem Multiuser System den Multicast Anforderungen entspricht, besteht kein Bedarf für eine VLAN Topologie. Sollte trotzdem eine VLAN Struktur gewünscht sein, sollten die nachstehenden Hinweise beachtet werden. Die Multicast Anforderungen (IGMP Snooping und Querier) gelten auch für das erstellte VLAN. Des Weiteren ist darauf zu achten, dass **Bonjourdienste weitergeleitet werden** damit die Funktionen von z.B. Spotify Connect oder Airplay1 gewährleistet sind. Beachten Sie bitte auch die Multicast- und Portadressweiterleitungen bei VLAN übergreifender Kommunikation.

## Multiusler Port- und Multicastadressen

Das Multiuser System verfügt über ein Text Protokoll, welches zur Steuerung interner Abläufe ebenso verwendet werden kann wie für Steuerungseingaben von externen Systemen (z.B. Gebäudeautomations-Server). Die Action Server Kommunikation (Eingabe/Rückmeldung) findet via Telnet auf die IP des Servers über den **Port 11244** statt.

### Verwendete Multicast Adressen:

Audio Streaming: 236.240.xx.xx (Port:11248)

Multiusler Text: 236.013.08.66 (Port:11246)

### Kommunikation Ports:

Menu Server Port: 11224

Action Server Port: 11244

Internet (http) : 80 / 8080

Internet (https) : 443

Revox update Server: DNS: revox-update.com (Port: 54321)

Revox Remote Server: DNS: revox-remote.com

### Airplay, Spotify und Airable (iRadio):

Airplay (Bonjour) Ports: 5010 bis 5020

Spotify (Zero Conf) Ports: 10740 bis 10830

Spotify (Bonjour) Ports: 4070 und 5353

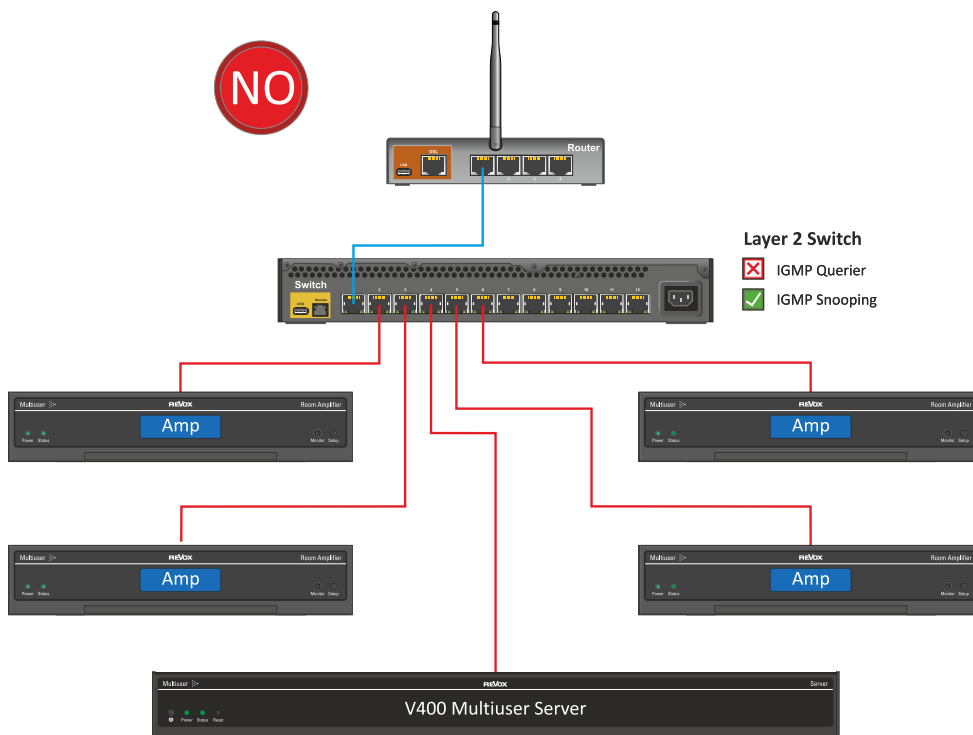
Airable Internetradio Ports : dynamisch\*

\* die verwendeten Ports werden von den Radiostationen festgelegt und sind daher nicht eingrenzbare

## Multicast Versionen / Konflikte

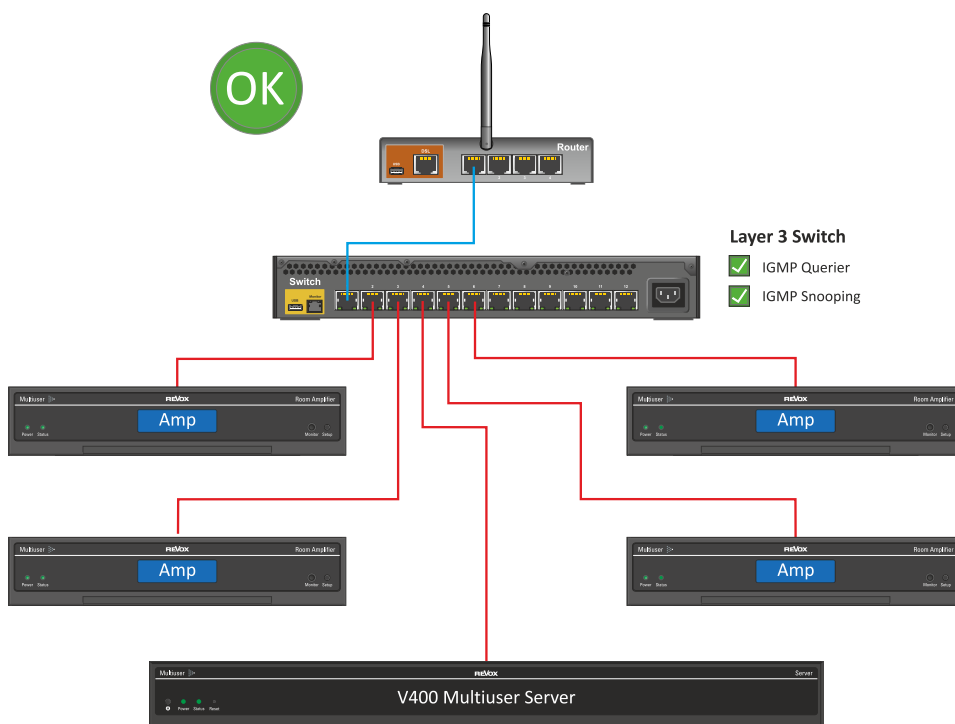
Das Multiuser-System basiert auf dem IGMPv2 Standard und kommuniziert auf IPv4 Basis. Wenn weitere Multicast Produkte von anderen Herstellern im Netzwerk eingesetzt werden, ist Vorsicht geboten. Immer häufiger anzutreffen sind IPTV Lösungen dessen Multicast Standard auf IGMPv3 basieren. Ohne weitere Konfiguration an den managed Switches im Netzwerk kann es schnell zu IGMP Konflikten oder einem totalen Ausfall der Kommunikation kommen. Deshalb sollten sämtliche Multicast Anforderungen aller Produkte bei der Planung und Konfiguration beachtet werden. Im Zweifelsfall können unterschiedliche Multicast Produkte über separate Leitungen und Switches geführt werden.

## Situation 1: Router mit Layer 2 Switch



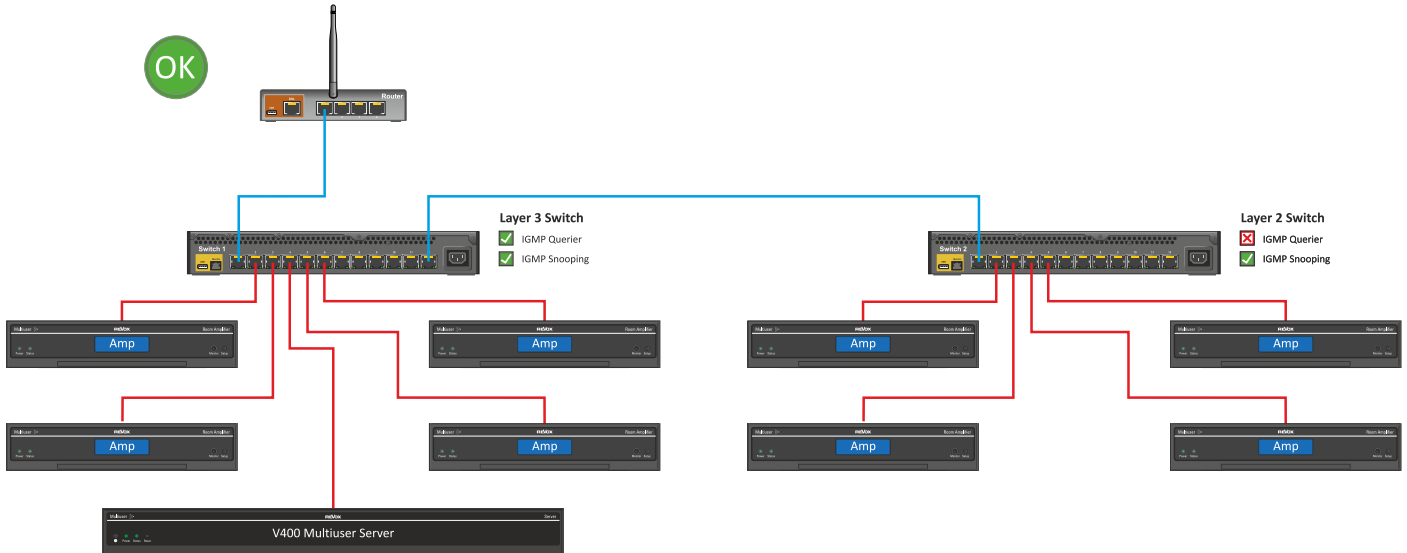
Ein Netzwerk ohne Querier erfüllt die Multuser System Anforderungen nicht

## Situation 2: Router mit Layer 3 Switch



Durch einen Layer 3 Switch können IGMP Snooping und Querier Anforderungen abgedeckt werden

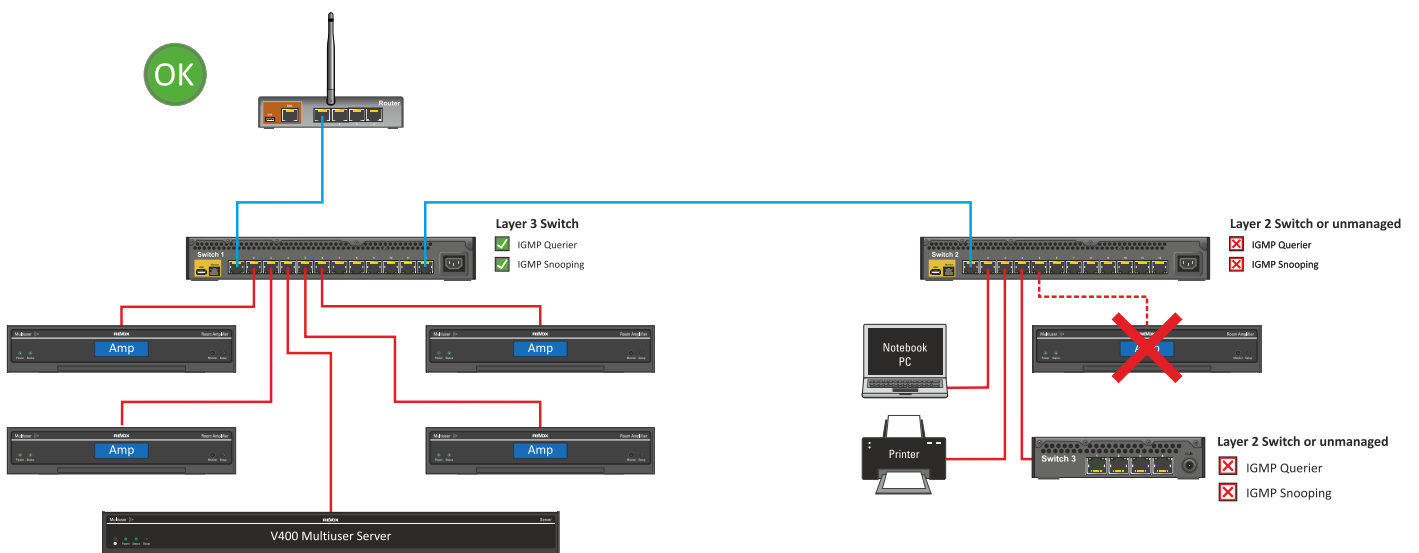
### Situation 3: Router mit mehreren managed Switches



Wenn die Revox Multiuser Komponenten über mehrere Switches verteilt werden, sollte der erste Switch nach dem Router ein Layer 3 Switch mit aktiviertem IGMP Querier und Snooping sein. Die nachfolgenden Switches sollten mindestens Layer 2 mit aktiviertem IGMP Snooping sein.

Anmerkung: anstelle des abgebildeten V400 Servers könnte auch ein STUDIOMASTER M300 oder M500 sein

### Situation 4: Router mit Kombination Layer 3 und unmanaged Switches



Wenn sämtliche Revox Multiuser Komponenten am Layer 3 Switch angeschlossen werden, können nachfolgende Switches als "unmanaged" ausgeführt werden.

### Grundsätzliches zu WLAN Verbindungen im Multiuser 3.0 System

Wenn ein Multiuser 3.0 Server (**STUDIOMASTER M300 / M500**) per WLAN mit dem Netzwerk verbunden ist, erfolgt die Kommunikation mit sämtlichen Nebenraumverstärkern per Unicast, egal ob diese per Netzwerkkabel oder WLAN verbunden sind. Somit ist Multicast und die dadurch vorausgesetzten Filter (Snooping und Querrier) kein Thema.

Wenn der Multiuser 3.0 Server (**STUDIOMASTER M300 / M500 oder V400**) per Kabel mit dem Netzwerk verbunden ist und alle Nebenraumverstärker per WLAN im Netzwerk teilnehmen, so erfolgt die Kommunikation ebenfalls per Unicast. Auch in diesem Fall gibt es keine Multicast Anforderungen zu berücksichtigen.

Sobald mindestens zwei Multiuser 3.0 Komponenten per Kabel mit dem Netzwerk verbunden sind, sind die Multicast Vorschriften zu beachten!

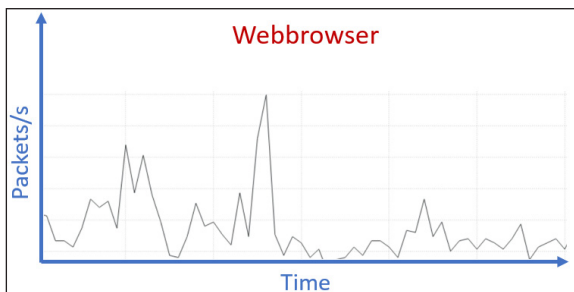
Bitte beachten Sie zum Thema Multiuser 3.0 und WLAN auch unbedingt unser Dokument Leistungsumfang und Limitierungen, da ein WLAN-Betrieb keinen unbegrenzten Systemausbau zulässt.

### System Stabilität

Damit ein Revox Multiuser System oder Verstärker auch mit einer WLAN-Verbindung zuverlässig funktioniert, braucht es eine gute WLAN-Abdeckung. Was unter einer «guten» WLAN-Abdeckung zu verstehen ist, muss selbstverständlich genauer definiert werden. Dazu gilt es ein paar wichtige Eckpunkte bei der kabellosen Datenübertragung zu beachten, welche in den nachfolgenden Kapiteln erklärt werden.

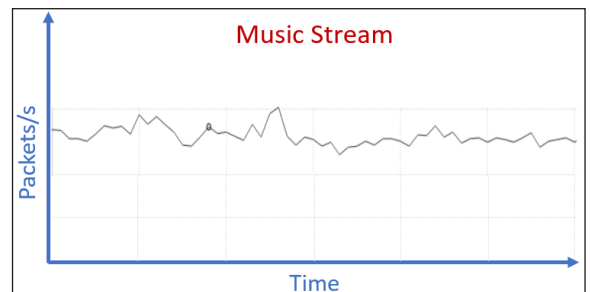
### Konstanter Datenfluss

Gegenüber z.B. einem Webbrowser, welcher bloss gezielt und in zeitlichen Abständen Inhalte aus dem Netzwerk oder Internet aufruft, ist ein Musik Streamer auf einen konstanten und stabilen Datenfluss angewiesen. Was damit genau gemeint ist, zeigen die beiden Darstellungen:



#### Beispiel Webbrowser:

Der Inhalt einer aufgerufenen Seite wird «portionenweise» abgerufen und aufgebaut. Kommt ein Teil nicht an, wird er in einem nächsten Paketaufruf wieder angefordert.



#### Beispiel Musik Stream:

Der Musik Stream basiert auf einer fortlaufenden Datenübertragung. Zusätzlich werden weitere Daten für die Steuerung und Anzeige übertragen. Dies führt zu einem permanenten Datenverkehr. Wird dieser konstante Datenfluss gestört, gibt es zwar einen Buffer (also Daten im Zwischenspeicher vom Multiuser Verstärker), ist dieser jedoch aufgebraucht, kommt es zu Musik Unterbrüchen.

### Information



Wer nun denkt, sein WLAN sei gut, weil sein Indikator auf dem Mobilien Gerät oder dem Rechner vollen Empfang anzeigt, der irrt. Erstens sind diese Empfangsanzeigen ungenau und zweitens sagen sie nichts darüber aus, wie konstant und stabil der Datenfluss im WLAN ist.

Um sicherzustellen, dass die Qualität von einem WLAN-Netzwerk tatsächlich gut ist, gilt es ein paar Punkte zu verstehen und ggf. zu optimieren. Doch zuerst muss man verstehen, woher Störeinflüsse kommen können und was man dagegen tun kann.

## Störeinflüsse

Ein WLAN basiert auf einem Funknetz und dieses Funknetz kann jederzeit gestört und beeinflusst werden. Darunter leidet dann nicht nur die Signalstärke, sondern auch die Datenübertragungsrate und es führt dazu, dass die Paketlaufzeiten stark schwanken. Letzteres ist für ein Multiroom System ganz schlecht hinsichtlich Synchronität und Wiedergabe.

Welche Faktoren beeinflussen ein WLAN-Funknetz am stärksten?

### 1. sind das Geräte, welche ebenfalls Funksignale erzeugen:

- Andere WLAN-Netzwerke
- Mobiltelefone
- DECT-Funktelefone (Festnetz)
- Bluetooth-Geräte
- Babyfon
- Mikrowellen Geräte
- Zigbee oder Kleernet Komponenten (Funktaster und ähnliches)

### 2. sind das Materialien, die es für das Funksignal zu durchdringen gilt.

Jedes Objekt, jede Wand, besonders Glas, mit Stahl armierte Betonwände und Wasser- sowie Stromleitungen stellen für das WLAN-Funknetz ein Hindernis dar und schwächt es ab.

### 3. sind das weitere WLAN-Teilnehmer, welche im eigenen Netzwerk angemeldet sind.

Diese beziehen ebenfalls Daten und nehmen somit einen Teil der verfügbaren Bandbreite in Anspruch oder haben selbst einen schwachen Empfang und veranlassen den Sender zu einer Drosselung der Datenübertragungsgeschwindigkeit aller Teilnehmer! Wer sein WLAN mit Repeatern erweitert, verstärkt damit zwar das WLAN-Signal, mindert jedoch die Datenübertragungsmenge und Geschwindigkeit.

## Abdeckung und Frequenzen

Viele der oben genannten Störeinflüsse lassen sich nicht oder nur teilweise vermeiden.

Deshalb ist es ratsam ein WLAN mit mehreren Access Points aufzubauen um eine gute Abdeckung zu erreichen. Zusätzlich sollte man darauf achten, dass die Sender über einen neuen WLAN-Standard mit hoher Datenübertragungsrate verfügen.

Die WLAN-Signalstärke sollte beim Multiuser Server oder Verstärker zwischen **-30dBm und -55dBm** sein (ablesbar in der Multiuser App – Tools – Room Debug). Übrigens: Je näher die Zahl bei null liegt, desto stärker und besser ist die Signalstärke.

Heutige WLAN-Sender können auf zwei Frequenzen senden: 2,4 Gigahertz und 5 Gigahertz.

Ein 2,4GHz Funknetz hat zwar einen etwas tieferen Speed, jedoch oft den grösseren Abdeckungsradius.

Beim 5 Gigahertz Funknetz ist es genau umgekehrt.

Welche Frequenz sie nutzen, sollte nebst dem Abdeckungsradius hauptsächlich von den freien Kanälen abhängen.

## Kanäle

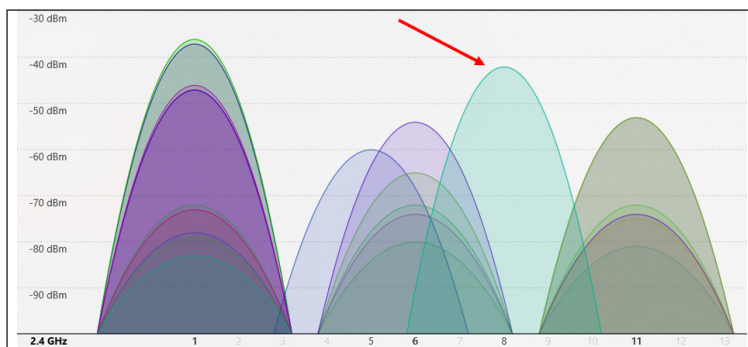
Innerhalb der 2,4 und 5 Gigahertz Frequenzen gibt es Kanäle, auf denen Ihr WLAN-Sender das Signal übertragen kann. Konfigurieren Sie Ihr WLAN immer auf einen freien Kanal oder suchen Sie sich einen Kanal, auf dem wenig los ist.

Es gibt zwar viele Router, welche über eine Kanalsuchfunktion verfügen und somit den optimalen Kanal automatisch einstellen, aber eine Kontrolle/Konfiguration kann nie schaden. Je weniger Überschneidungen von anderen WLAN umso besser (siehe Störeinflüsse)!

Überprüfen lässt sich Ihre WLAN-Umgebung ganz einfach mit diversen kostenlosen Wifi Analyse Apps fürs Mobiltelefon oder gratis Software für Ihren Rechner (WLAN-Empfang vorausgesetzt).

In unserem Beispiel verwenden wir folgenden kostenlosen Wifi Analyzer: <https://matthafner.com/wifi-analyzer>





*In diesem Beispiel ermittelte der Wifi-Scan 20 weitere WLAN in der Umgebung!  
Die meisten senden auf Kanal 1, 6 und 11. Deshalb wurde das eigene WLAN auf Kanal 8 konfiguriert, wo es die geringsten Kanalüberschneidungen gibt.*

## Kanalbündelung

Eine weitere Möglichkeit ist die Konfigurationsoption der Kanalbündelung. In diesem Fall kann man sein WLAN über zwei Kanäle mit jeweils 20 MHz Bandbreite legen, was dann dazu führt, dass insgesamt 40 MHz zur Verfügung stehen.

Problematisch ist die doppelte Kanalbelegung bei 2,4-Ghz jedoch in dichter besiedelten Regionen. Denn hier genügen bereits zwei solcher 40-MHz-WLANs in unmittelbarer Nachbarschaft, um die gesamte Bandbreite von insgesamt 80 MHz zu belegen.

Kommen ein dritter, vierter oder noch mehr WLAN-Router hinzu, kommt es zwangsläufig zu massiven Übertragungsstörungen, da alle Geräte über dieselben Übertragungskanäle funken.

**In diesem Fall ist eine stabile 20-MHz-Verbindung über einen Kanal deutlich effektiver als eine massiv gestörte 40-MHz-Verbindung über zwei Kanäle.**

## Latenz und Paketumlaufzeiten

Wie bereits in den Kapiteln *Konstanter Datenfluss* und *Störeinflüsse* erwähnt, ist ein stabiler und konstanter Datenfluss im Netzwerk die Grundvoraussetzung für ein stabiles Multiuser System. Eine gute WLAN-Abdeckung und die richtige Frequenz- und Kanalwahl bilden die Basis dafür.

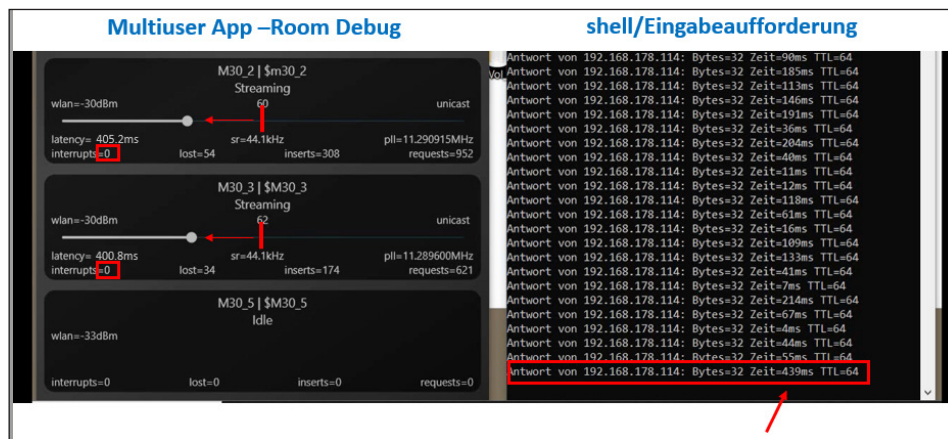
Der letzte und entscheidende Faktor ist nun ein Datenfluss mit möglichst gleichmässiger Übertragung.

Das Multiuser System ist ab Werk im WLAN-Betrieb auf eine **Latenzzeit von 400ms** eingestellt. Dieser Wert lässt sich anpassen, dazu jedoch später mehr. Sollten also die Pakete im Netzwerk zwischen Multiuser Server und Multiuser Verstärker länger als 400ms brauchen bis sie ankommen, kommt das System in einen Bereich, in welchem der Buffer irgendwann die ausbleibenden Pakete nicht mehr kompensieren kann. Ab diesem Zeitpunkt kann es zu Unterbrüchen bei der Musikwiedergabe kommen.

Sollte also die generelle Paketumlaufzeit in einem (WLAN) Netzwerk trotz aller erfüllten WLAN-Kriterien langsam sein oder stark schwanken, kann dies weitere Gründe haben. Zum Beispiel temporäre Störeinflüsse von anderen Funknetzen, schlechte Kabelverbindungen von Routern oder Switches, Prozesse im Router und vieles mehr...

Wie man eine Paketumlaufzeit Diagnose mit Bezug auf das Multiuser System macht, zeigen wir auf der nächsten Seite auf. Die benötigten Tools dazu sind einfach...

1. Öffnen Sie auf Ihrem Rechner die Multiuser PC App und navigieren sie zum Room Debug (Werkzeuge)
2. Öffnen Sie auf Ihrem Rechner die shell/Eingabeaufforderung (cmd) und positionieren dieses Fenster direkt neben der Multiuser App
3. Starten Sie nun in der shell/Eingabeaufforderung einen wiederholenden Ping auf einen Multiuser Server oder Verstärker, welcher per WLAN verbunden ist.  
Der Start Befehl lautet: `ping -t 192.168.1.100` (Beispiel IP)  
Der Stopp Befehl lautet: `Strg + c` (dann erscheint ein Summary aller Laufzeiten)  
Die IP-Adresse des gewünschten Multiuser Servers oder Verstärkers finden Sie ebenfalls in der Multiuser App unter Raum- oder Userinformation
4. Beobachten Sie nun die Latenzzeiten in der Shell. Liegen Sie konstant oder oft über 400ms zeigt sich dies unmittelbar auch im Room Debug des angepingten Raums in der Multiuser App...



In dem Moment wo die Paktumlaufzeit (TTL) 439ms anzeigt, sackt der Buffer unmittelbar zusammen im Room Debug (verlässt die Mittelposition). Noch haben keine Unterbrechungen (Interrupts) stattgefunden...

Zeigt diese Messung auf, dass die Multiuser Latenz von 400ms regelmässig überschritten wird, kann in der Multiuser App unter Einstellungen – Multiuser Einstellungen – Experten Einstellungen die WLAN-Raumlatenz erhöht werden. Besser wäre es jedoch, den Grund für die hohe Paketumlaufzeit zu finden und diesen Fehler zu beheben. Alle anderen Netzwerkteilnehmer profitieren schliesslich auch davon...

## Zusammenfassung der Diagnose- und Optimierungsmöglichkeiten

1. Stellen Sie sicher, dass die WLAN-Abdeckung gut ist. Infos zur Signalstärke erhalten Sie in der Multiuser App unter dem Room Debug. Positionieren Sie den WLAN-Sender richtig oder erweitern Sie Ihr WLAN-System mit Access Points.
2. Suchen Sie sich einen freien oder gering ausgelasteten Funkkanal. Hier hilft ein Analyse Tool und eine WLAN-Konfiguration.
3. Überprüfen Sie bei Bedarf die Paketumlaufzeiten im Netzwerk und sorgen Sie für stabile und geringe Paketumlaufzeiten. Passen Sie falls nötig die Raumlatenz im Multiuser System an