REVOX
Multiuser network knowledge

CONTENT

LAN OPERATION & MULTICAST

Basics	2
IGMP	3
Hardware	3 / 4
VLAN`s	4
Used Ports	4
Multicast conflicts	4
Examples	5 / 6

WLAN OPERATION

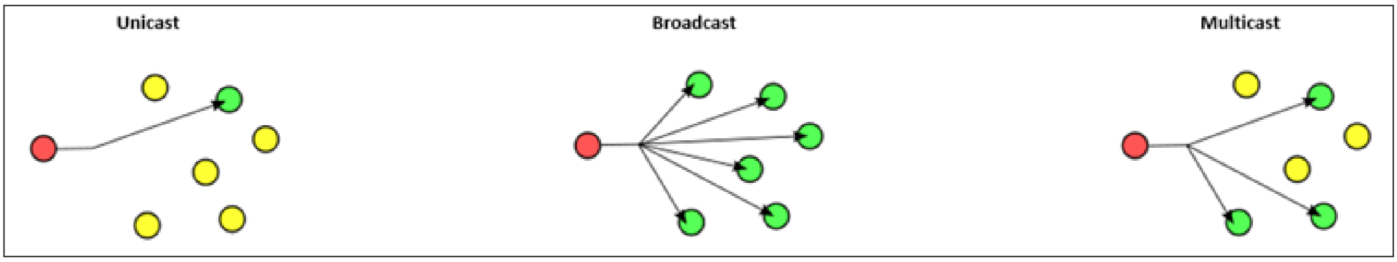
Basics	7
interferences	8
Frequencies and channels	8 / 9
Latency and packet turnaround time	9 / 10
Optimization options	10

Basic information on LAN connections for the Multiuser 3.0 system

The Revox Multiuser System uses the IP multicasting technology when several components in the system are connected via LAN cable!

With this technology it is possible to play sources from different rooms without any time delay. For this purpose, the Multiuser System has a basic latency, this is approx. 75 -90 ms. In order to ensure the smooth functioning of a multicast system such as the Revox Multiuser System, the setup and correct configuration of the network infrastructure is very important!
On the following pages, you will find information and illustrations on the subject of network construction.

Network communication types



Data is transported from an endpoint via a hub to exactly one endpoint (one-to-one).

Data is transported from an endpoint via a hub to all endpoints in a network. The hub handles the distribution/duplication and forwarding of the data to all endpoints.

Data is transported from an endpoint via a hub to any number of endpoints in a network. The hub handles the distribution/duplication and forwarding of the data to all interested endpoints. The hub knows the interested recipients by the multicast address of the endpoints.

Network basic requirements

Because the Revox Multiuser System uses multicasting technology, every system should be planned with multicast-capable switches.
A list of recommended and tested switches including configuration instructions can be found on the support page.

Network Basic requirements for a Multiuser System:

- Multicast capable network (IGMP snooping & querier support)
- 1Gbit cabling - 100 Mbit to the clients is sufficient

IGMP „Internet Group Message Protocol“

The Internet Group Message Protocol is based on the Internet Protocol (IP) and enables IPv4 multicasting (group communication) on the Internet. IP multicasting is the distribution of IP packets with a destination IP address to multiple stations simultaneously. IGMP offers the possibility to manage groups dynamically. The management does not take place in the sending station, but in the routers to which receivers of a multicast group are directly connected. IGMP provides functions with which a station informs a router that it wants to receive multicast IP packets of a specific multicast group. Multicast routing protocols (DVMRP, MOSPF, PIM) handle the coordination of transmission between routers. The sender of multicast IP packets does not know which and how many stations receive its packets, because it only sends a single data packet to its higher-level router. This duplicates the IP packet as required if it has several outgoing interfaces with receivers.

IGMP Snooping

IGMP snooping is a feature of network switches. The switch snoops the IGMP traffic on its ports between hosts and routers. In doing so, the switches learn which of the connected devices belong to a multicast group when receiving IGMP membership requests. When a multicast is received for a group, the message is forwarded only to the corresponding ports that belong to that multicast group; the other ports do not see these messages.
In summary: IGMP snooping can be used to prevent multicast traffic from flooding all switch ports. This reduces the network load.

IGMP Querier

In order for IP multicasting to work across all components in the network, a central device is required to manage the multicast group membership of all network components, the so-called IGMP Querier. The responses to querier requests cause the switches to update their membership lists accordingly.
The Querier function is only supported by routers or Layer 3 switches, but not by Layer 2 switches.

Router

Revox recommends to cover the network requirements (IGMP Querier and Snooping) with Layer 3 and if necessary Layer 2 Switches and does not recommend routers.
Often routers are already available on the provider side and do not cover the desired requirements or lose them with software updates.

Firewall

If the firewall used covers IGMP snooping and IGMP querier in the multicasting area, subsequent network switches can be used as layer 2 versions. If no multicast settings can be made on the firewall or the functions are questionable, the additional use of a Layer 3 switch is recommended. The Revox company does not make a firewall hardware recommendation.

Layer 2 Switch

A Layer 2 Switch can interconnect LAN segments and efficiently distribute the available bandwidth to users.
A Layer 2 switch has no switching or routing functions. As a rule, Layer 2 switches are limited to IGMP snooping in the area of multicasting and do not offer IGMP querier. For this reason, Layer 2 switches are suitable as an extension in conjunction with a Layer 3 switch. Please refer to the practical examples on the following pages and our hardware recommendation list.

Layer 3 Switch

A Layer 3 switch is a combination of router and switch and thus has switching and routing functions. Compared to a layer 2 switch, it offers IGMP snooping and an IGMP querier function in the area of multicasting. For this reason, it is recommended to use at least one Layer 3 switch in a multicast system. Please refer to the practical examples on the following pages and our hardware recommendation as well as the configuration guide.

VLAN`s

If the network environment of a multi-user system meets the multicast requirements, there is no need for a VLAN topology. If a VLAN structure is nevertheless required, the following notes should be observed. The multicast requirements (IGMP snooping and querier) also apply to the VLAN created. Furthermore, it must be ensured that Bonjour services are forwarded so that the functions of Spotify Connect or Airplay1, for example, are guaranteed. Please also note the multicast and port address forwarding for cross-VLAN communication.

Multiuser Port- und Multicast addresses

The multiuser system has a text protocol that can be used to control internal processes as well as for control inputs from external systems (e.g. building automation server). The action server communication (input/feedback) takes place via Telnet to the IP of the server via **port 11244**.

Multicast addresses:

Audio Streaming:	236.240.xx.xx (Port:11248)
Multiuser Text:	236.013.08.66 (Port:11246)

Communication 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):

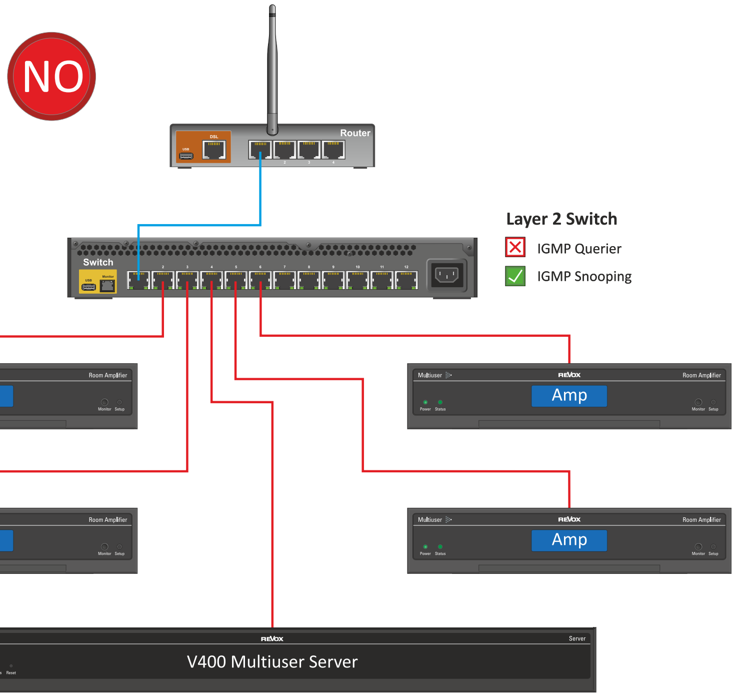
Airplay (Bonjour) Ports:	5010 bis 5020
Spotify (Zero Conf) Ports:	10740 bis 10830
Spotify (Bonjour) Ports:	4070 und 5353
Airable Internetradio Ports :	dynamic*

* the ports used are defined by the radio stations and are therefore not restrictable

Multicast Versions / Conflicts

The multiuser system is based on the IGMPv2 standard and communicates on an IPv4 basis. If other multicast products from other manufacturers are used in the network, caution is advised. IPTV solutions whose multicast standard is based on IGMPv3 are becoming increasingly common. Without further configuration on the managed switches in the network, this can quickly lead to IGMP conflicts or a total failure of the communication. Therefore, all multicast requirements of all products should be considered during planning and configuration. If in doubt, different multicast products can be routed over separate lines and switches.

Situation 1: Router with Layer 2 Switch



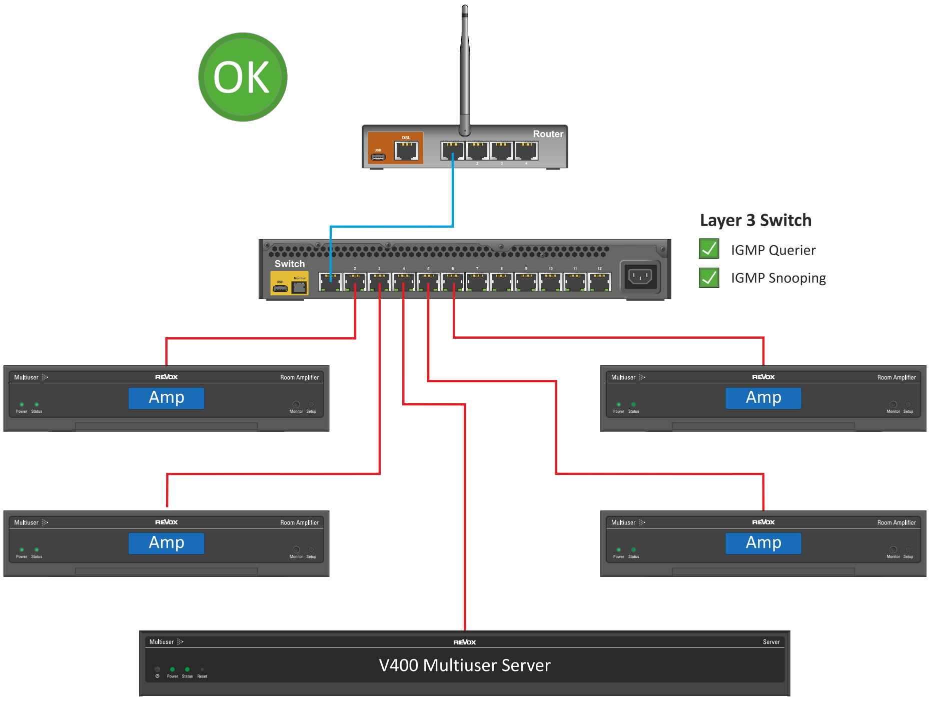
Layer 2 Switch

☒ IGMP Querier

☑ IGMP Snooping

A network without querier does not meet the multiuser system requirements

Situation 2: Router with Layer 3 Switch



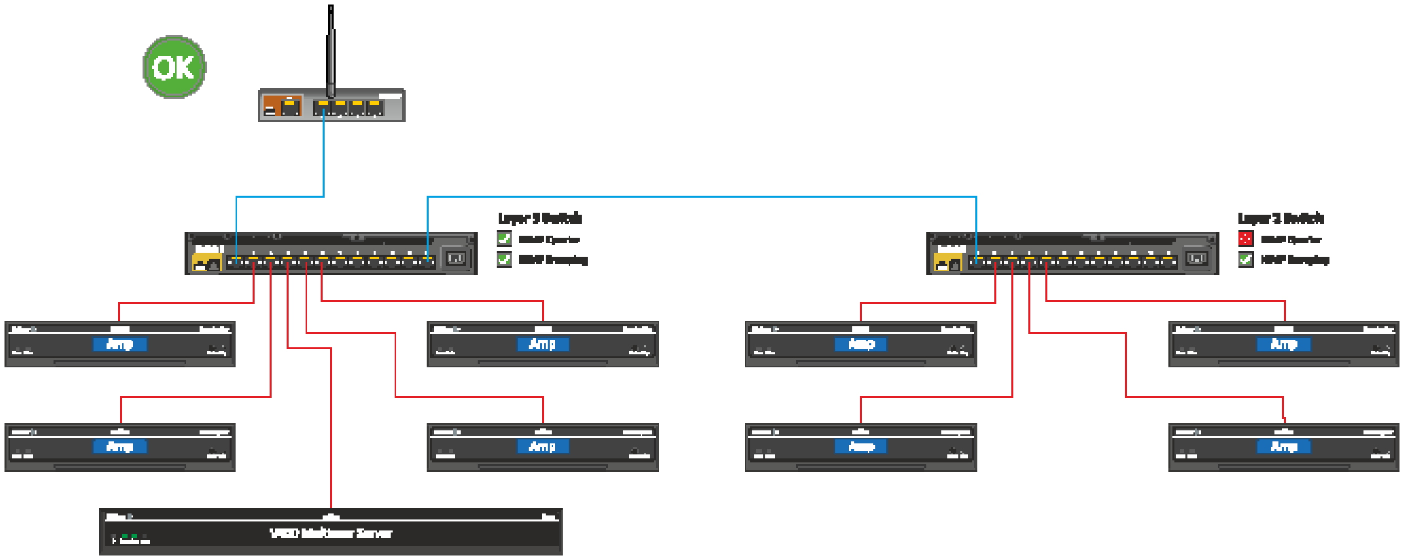
Layer 3 Switch

☑ IGMP Querier

☑ IGMP Snooping

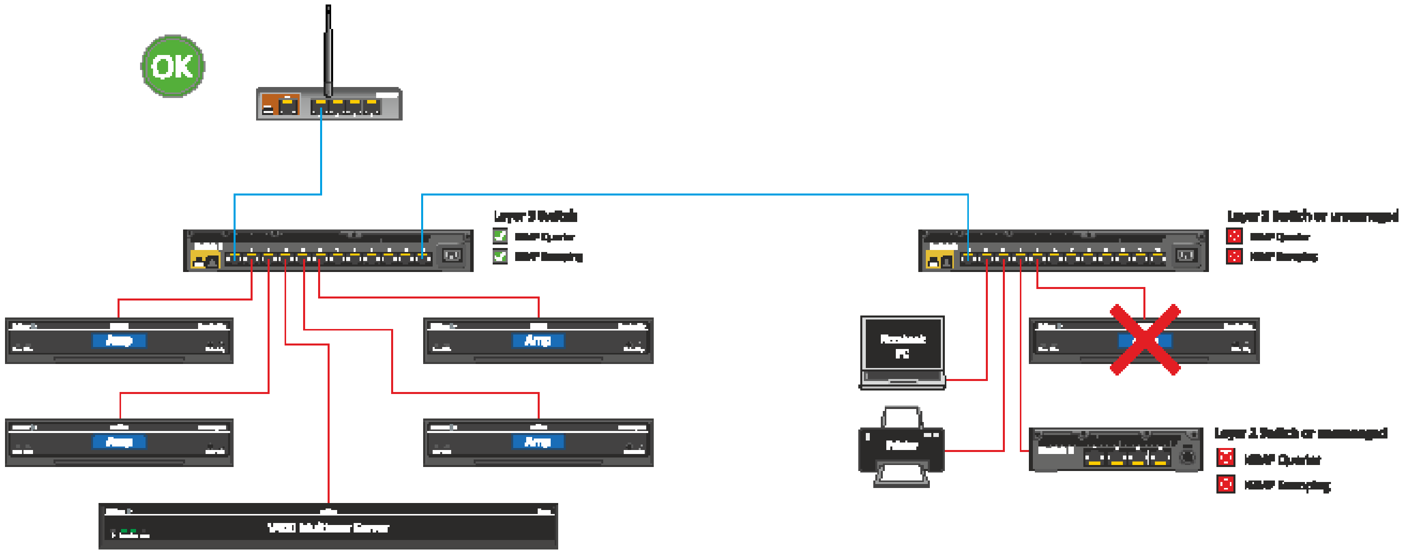
IGMP snooping and querier requirements can be covered by a layer 3 switch

Situation 3: Router with several managed switches



If the Revox Multiuser components are distributed over several switches, the first switch after the router should be a Layer 3 switch with activated IGMP Querier and Snooping. The subsequent switches should be at least Layer 2 with activated IGMP Snooping.
Note: instead of the V400 server shown, it could also be a STUDIOMASTER M300 or M500.

Situation 4: Router combination with Layer 3 and unmanaged switches



If all Revox Multiuser components are connected to the Layer 3 Switch, subsequent Switches can be designed as „unmanaged“.

Basic information on WLAN connections for the Multiuser 3.0 system

If a Multiuser 3.0 server (**STUDIO**MASTER M300 / M500) is connected to the network via WLAN, communication with all room amplifiers takes place via unicast, regardless of whether they are connected via network cable or WLAN. This means that multicast and the filters it requires (snooping and querrier) are not needed.

If the Multiuser 3.0 Server (**STUDIO**MASTER M300 / M500 or V400) is connected to the network via cable and all room amplifiers connected in the network via WLAN, communication is also carried out via unicast. In this case, there are no multicast requirements needed.

As soon as at least two Multiuser 3.0 components are connected to the network by cable, the multicast regulations must be observed!

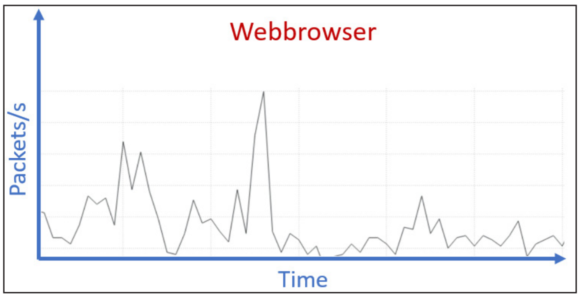
Please also refer to our document *Scope of services and limitations* on the subject of Multiuser 3.0 and WLAN, as WLAN operation does not allow unlimited system expansion.

System stability

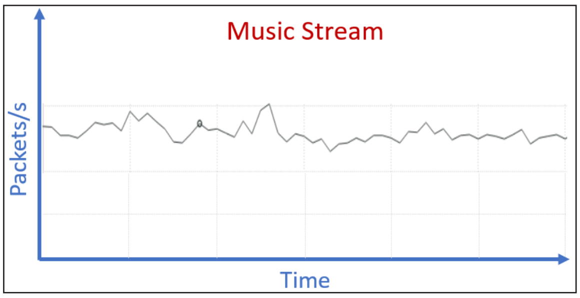
In order for a Revox Multiuser System or amplifier to also function reliably with a WLAN connection, it needs good WLAN coverage. What is meant by „good" WLAN coverage must of course be defined more precisely. For this purpose, a few important key points must be observed for the wireless data transmission, which are explained in the following chapters.

Constant flow of data

In contrast to a web browser, for example, which only calls up content from the network or Internet at specific intervals, a music streamer is dependent on a constant and stable data flow. The two illustrations show exactly what is meant by this:



Example web rowser:
The content of a requested page is retrieved and built up „in portions". If a package does not arrive, it is requested again in a next packet call.



Example music stream:
The music stream is based on a continuous data transmission. In addition, further data is transmitted for control and display. This leads to a constant data traffic. If this constant data flow is disturbed, there is a buffer (i.e. data in the intermediate memory of the multiuser amplifier), but if this is used up, music interruptions occur.

Conclusion

If you think your WLAN is good because the indicator on your mobile device or computer shows full reception, you are mistaken. First, these reception indicators are inaccurate, and second, they say nothing about how constant and stable the data flow is in the WLAN.

To ensure that the quality of a WLAN network is actually good, a few points need to be understood and optimized if necessary. But first you need to understand where interference can come from and what you can do about it.

Interferences

A WLAN is based on a radio network and this radio network can be disturbed and influenced at any time. Not only the signal strength suffers, but also the data transfer rate and the packet turnaround times fluctuate strongly. The last item is quite bad for a multiroom system in terms of synchronicity and playback.
Which factors influence a WLAN wireless network the most?

1. These are devices which also generate radio signals:

- Other WLAN networks
- Cell phones
- DECT wireless phones (landline)
- Bluetooth devices
- Baby monitors
- Microwave devices
- Zigbee or Kleernet components (wireless switches and similar)

2. These are materials that weaken the radio signal:
Every object, every wall, especially glass, concrete walls reinforced with steel and water- as well as power -lines are an obstacle for the WLAN radio network and weaken it.

3. Other additional WLAN participants, which weaken the network:
Other WLAn devices also draw data and thus take up part of the available bandwidth or have weak reception themselves and cause the transmitter to throttle the data transfer speed of all subscribers! If you expand your WLAN with repeaters, you strengthen the WLAN signal, but reduce the data transfer volume and speed.

Coverage and frequencies

Many of the above-mentioned interferences can not or only partially be avoided.
It is therefore advisable to set up a WLAN with several access points to achieve good coverage. In addition, you should make sure that the transmitters have a new WLAN standard with a high data transmission rate.
The WLAN signal strength should be between **-30dBm and -55dBm** for the multiuser server or amplifier (readable in the Multiuser App - Tools - Room Debug). By the way: The closer the number is to zero, the stronger and better the signal strength is.

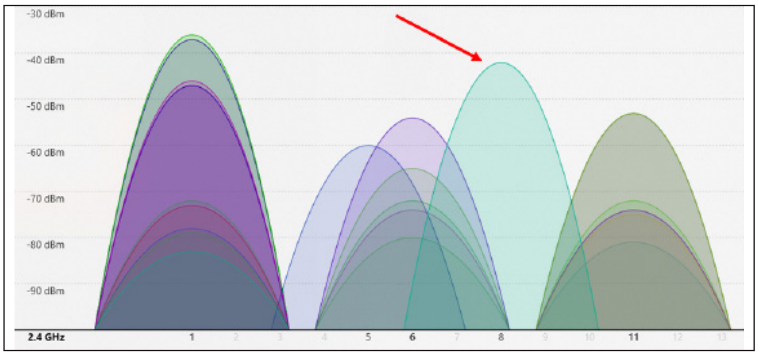
Today's WLAN transmitters can transmit on two frequencies: 2.4 gigahertz and 5 gigahertz.
A 2.4 GHz radio network has a lower speed, but often the larger coverage radius.
With the 5 gigahertz radio network, it is exactly the opposite.
Which frequency you use should mainly depend on the free channels in addition to the coverage radius.

Channels

Within the 2.4 and 5 gigahertz frequencies, there are channels on which your WLAN transmitter can transmit the signal. Always configure your WLAN to a free channel or find a channel where there is little traffic.

There are many routers that have a channel search function and thus automatically set the optimal channel, but a control / configuration is always better. The less overlaps from other WLAN the better (see interference)!

You can easily check your WLAN environment with various free Wifi analysis apps for your cell phone or free software for your computer (assuming WLAN reception).
In our example we use the following free Wifi Analyzer: https://matthafner.com/wifi-analyzer



In this example, the Wifi scan detected 20 other WLAN in the environment!
Most of them transmit on channel 1, 6 and 11, so the own WLAN was configured on channel 8, where there is the least channel overlap.

Channel bundling

Another option is the configuration option of channel bundling. In this case, you can place your WLAN over two channels with 20 MHz bandwidth each, which then leads to a total of 40 MHz being available.
However, double channel assignment at 2.4 GHz is problematic in more densely populated regions. Here, two such 40 MHz WLANs in the immediate environment are sufficient to occupy the entire bandwidth of 80 MHz.
If a third, fourth or even more WLAN routers are added, massive transmission interference is inevitable because all devices transmit via the same transmission channels.
In this case, a stable 20 MHz connection over one channel is much more effective than a massively disturbed 40 MHz connection over two channels.

Latency and packet turnaround times

As already mentioned in the chapters Constant data flow and Interference, a stable and constant data flow in the network is the basic prerequisite for a stable multiuser system. Good WLAN coverage and the right frequency and channel selection form the basis for this.

The final and decisive factor is now a data flow with the smoothest possible transmission.
The Multiuser system is set to **a default latency of 400ms** in WLAN mode. This value can be adjusted, but more on this later. If the packets in the network between the multiuser server and the multiuser amplifier take longer than 400ms to arrive, the system will reach a point where the buffer can no longer compensate for the missing packets.
From this point on, music playback may be interrupted.

So if the general packet turnaround time in a (WLAN) network is slow or fluctuates strongly despite all fulfilled WLAN criteria, this can have further reasons. For example, temporary interference from other wireless networks, poor cable connections from routers or switches, processes in the router and much more...

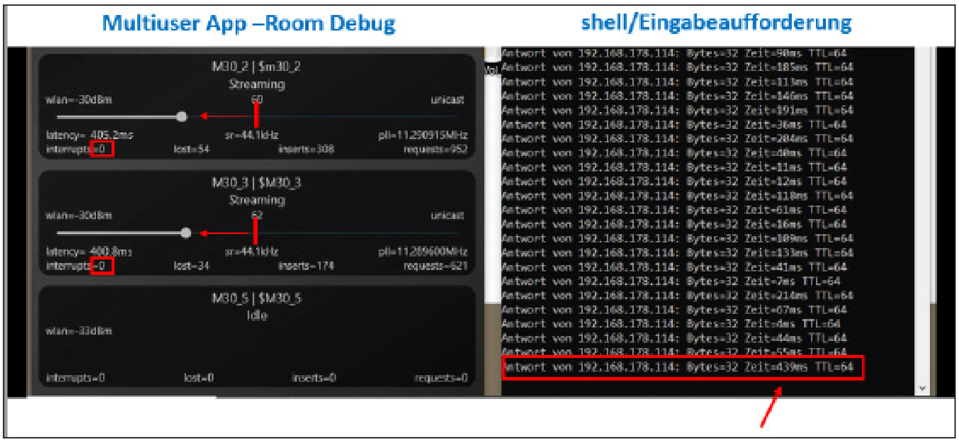
How to make a packet turnaround time diagnosis with respect to the multiuser system is shown on the next page. The tools needed for this are simple...

1. open the Multiuser PC app on your computer and navigate to the Debug room (Tools).

2. open the shell/command prompt (cmd) on your computer and position this window directly next to the Multiuser App.

3. in the shell/command prompt, start a repetitive ping to a multiuser server or amplifier that is connected via WLAN.
   The start command is: *ping -t 192.168.1.100* (Beispiel IP)
   The stop command is: *Strg + c* (dann erscheint ein Summary aller Laufzeiten)
   The IP address of the desired multiuser server or amplifier can also be found in the Multiuser App under Room or User information

4. Now observe the latency times in the shell. If they are constantly or often above 400ms, this is immediately reflected in the Room Debug of the pinged room in the Multiuser App...



Multiuser App –Room Debug

```
M30_2 | $m30_2
Streaming
wlan=-30dBm                 60                  unicast
latency= 405.2ms         sr=44.1kHz       pll=11.290915MHz
interrupts=0     lost=54      inserts=308      requests=952

M30_3 | $M30_3
Streaming
wlan=-30dBm                 62                  unicast
latency= 400.8ms         sr=44.1kHz       pll=11.289600MHz
interrupts=0     lost=34      inserts=174      requests=621

M30_5 | $M30_5
Idle
wlan=-33dBm
interrupts=0     lost=0       inserts=0        requests=0
```

shell/Eingabeaufforderung

```
Antwort von 192.168.178.114: Bytes=32 Zeit=90ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=185ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=113ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=146ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=191ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=36ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=284ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=40ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=11ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=12ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=118ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=61ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=16ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=109ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=133ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=41ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=7ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=214ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=67ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=4ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=44ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=55ms TTL=64
Antwort von 192.168.178.114: Bytes=32 Zeit=439ms TTL=64
```

At the moment when the TTL shows 439ms, the buffer immediately collapses in the Room Debug (leaves the center position). No interrupts have taken place until yet...

If this measurement shows that the multiuser latency of 400ms is regularly exceeded, the WLAN room latency can be increased in the Multiuser app under Settings - Multiuser settings - Expert settings. However, it would be better to find the reason for the high packet turnaround time and fix this error. After all, all other network users benefit from it as well...

Summary of diagnostic and optimization options

1. Make sure that the Wi-Fi coverage is good. You can obtain information on the signal strength in the Multiuser app under the Room Debug. Position the WLAN transmitter correctly or expand your WLAN system with access points.

2. Look for a free or low used radio channel. An analysis tool and subsequent WLAN configuration will help here.

3. If necessary, check the packet turnaround times in the network and ensure stable and low packet turnaround times. Adjust latency in the multiuser system if necessary.