Network Configuration for Listen Everywhere

Overview:

The purpose of this tech note is to provide guidance when configuring, optimizing, or troubleshooting a network where the Listen Everywhere (LE) system is deployed to stream audio to participants.

How It Works:

The LE system takes an audio input and streams it over Wi-Fi to connected Android and iOS mobile devices. This process has two phases: Discovery and streaming. In the discovery phase the LE app on the mobile device seeks out the LE server on the Wi-Fi network via multicast (mDNS). It then moves to the streaming phase, where audio is streamed unicast via the User Datagram Protocol (UDP) from the LE server to the LE app on the connected mobile device.

Network Requirements:

The network requirements can vary based on the number of simultaneous users the LE system will need to support. The most basic requirements are:

- Enterprise-Grade Wireless Access Point(s) (WAP), 802.11n or better (802.11ac wave 2 or better is recommended).*
- The data load is approximately 125 kbps per connected user. It is recommended that LE traffic only account for 20% of the total network bandwidth.
- Internet connectivity to the LE server is required for initial customization and for some features to be available (see *Internet Connectivity*).

**The amount of WAPs needed will be determined on your venue's needs. For assistance with this you may need to seek assistance from an IT/Network Administrator or from the manufacturer of the products you are interested in utilizing.*

Recommended Configuration:

Though not required for the LE system to function, here are several recommendations and optimizations that can improve performance:

- Enterprise-Grade Router or Switch.*
- Enable Multicast UDP (i.e. mDNS, Bonjour, Avahi) (see *Enabling Multicast UDP*).
- Use an open network (no encryption). Using encryption can lower the number of users that can connect to the WAP and add latency to the LE system. TKIP encryption should not be used.
- Enable Quality of Service (QoS) on the network to prioritize LE traffic (see *Enabling QoS*).
- Set the WAP(s) to static channels (see *Wireless Access Point Channel Optimization*).

- For optimum latency and performance, avoid using range extenders, mesh networks, or multi-hop networks. Doing so may add latency, cause audio stuttering, or dropouts.

**Consumer-grade and business-grade routers and switches do not always have the required features, configuration options, or necessary compute power to handle basic needs of the LE server. Please refer to the Wireless Access Point Optimization tech note for some suggested networking hardware.*

Internet Connectivity:

An Internet connection is not required for the LE system to function. However, the LE server must be able to reach Cloud Services (see *Ports and Services*) for the initial setup and for some features to function.

The following features **do not require** a persistent connection to Cloud Services:

- Audio Streaming
- App Theme Settings (title and colors)*
- Channel Settings (names, images, gain, and delay)*
- Welcome Ad (image or video)*

The following features **require** a persistent connection to Cloud Services:

- Banner Ads
- Offers
- Documents
- Firmware Updates
- Downloading Log Files

**Requires an Internet connection for initial setup and if changes are needed.*

Stand-Alone Networks:

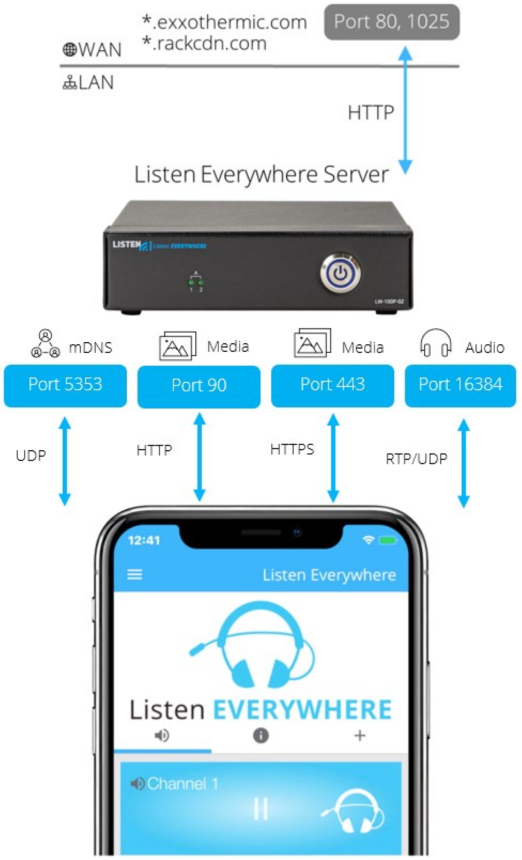
When a stand-alone network is desired, the LE server can function as the DHCP server. This setup requires at least one WAP to be used. No internet connectivity is available when in this mode. To enable the DHCP server mode on the LE server, please refer to the Server Admin Interface manual for instructions.*

The default network settings set by the LE server when in DHCP mode are:

- Gateway: 172.30.0.1
- Netmask: 255.255.0.0
- DHCP Range: 172.30.0.2 – 172.30.0.254
- Lease Time: 24 Hours

Ports and Services:

LAN Ports and Services:



- LE App Discovery & Server Data:
  - The LE server listens for mDNS traffic over port 5353 to allow the mobile app and additional LE servers to advertise the server's IP address (see *Enabling Multicast*).
  - The LE Server exposes an HTTPS web server over port 443 (or HTTP port 8000 on LE Servers running firmware version 4.1 or older) to download any text and customization details (e.g., channel names, background colors, server settings, etc.).
  - The LE Server exposes an HTTP file server over port 90 to download any media (e.g., welcome ads, banner ads, channel images, etc.).
- Audio Streaming:
  - The LE Server sends RTP packets via UDP to the app over a range of dynamic ephemeral ports. This may vary by network and should be examined by a network administrator.
  - The mobile app listens to and communicates with the LE Server via UDP over port 16384.

WAN Ports and Services:

- Cloud Services communicates via HTTP with the LE server through *.exxothermic.com over port 1025, with updates communicating over port 80. Additionally, ubuntu.com, launchpad.net, odroid.in are also used for updates via port 80.
- Media files are stored on and transferred via HTTP through *.rackcdn.com over port 1025.

Enabling Multicast (mDNS / Avahi / Bonjour):

Multicast (mDNS) is used in the discovery process for the app and the server to connect via a network scan, which allows automatic connection when the app is opened.
To enable mDNS, perform the following:

- Add the following case-sensitive services to the allowed list in the Gateway/WAP mDNS settings:
  - _ExXothermic._tcp *
  - _AsClient_ExXothermic._tcp *
- Open Port 5353.
- Add the mDNS IP address to the allowed subnets list. 224.0.0.251 is the most common mDNS IP address, but it could be any of the 224.0.0.0/24 range.

**For Cisco controllers: ".local." may need to be added to the end of each service name (e.g. _ExXothermic._tcp.local.)*

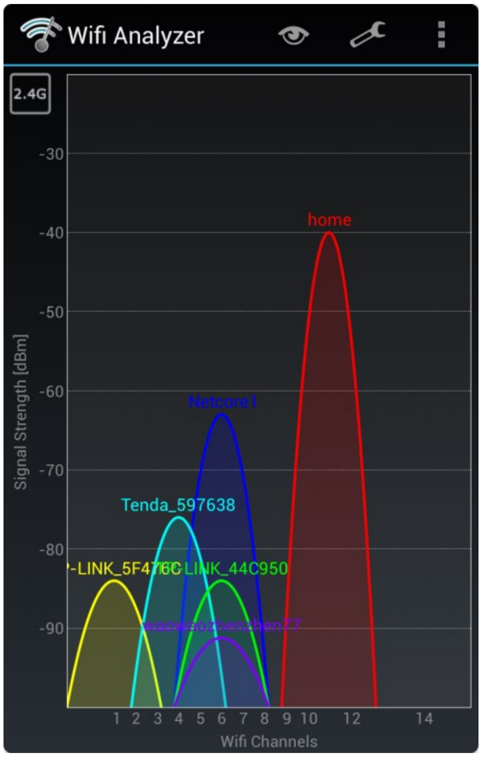
Note: mDNS discovery may not be desired. In those cases, mDNS can be disabled on the network and the LE server can be connected to via the IP address text field or QR code (*Please refer to the Mobile App Connection Methods tech note for more details*).

Wireless Access Point Channel Optimization:

Many WAPs can automatically change channels to try and find one with the least interference. This feature can cause audio drops each time the channel changes, as often as every 20 seconds. If it does not settle on a channel after 30-60 minutes, it may be best to choose a channel manually.

When manually setting channels, you should use a Wi-Fi signal analyzer. A Wi-Fi signal analyzer will provide a clear picture of the signal congestion in your space.*

Channel width is very important to consider. 2.4GHz networks may improve when set to a width of 20MHz. 5GHz networks may improve when set to a width of 40MHz. Wider channels are more susceptible to interference.



**Many Access Points have this functionality built in. For Android and Windows devices, we suggest the 'WiFi Analyzer' app. No comparable app is available for iOS.*

Enabling Quality of Service (QoS):

By default, the LE server uses Type of Service/Differentiated Services (ToS/DS) tags so that audio data can be prioritized over other data traffic on the network. This priority allows the latency to be as low as possible while travelling over the network. For this to function with other data, QoS must be enabled on the network.

- Enable QoS on the Router or Managed Switch.
- Enable Wireless Multimedia Extensions (WMM) in the WAP.

By default, the LE Sever is set to the ToS/DS tag of 0xB8 (Critical, low delay, high throughput, and normal reliability). Other tags can be used depending on existing networking configurations.

To change the ToS/DS of the LE Server:

1. Ensure the LE server is connected to the Internet
2. Login to Cloud Services (The LE server must be registered)
3. Select the **Menu** in the top-left corner
4. Select **Venue Servers & Labels**
5. Select **Venue Servers List**
6. Select the Sever ID or Edit pencil icon
7. Change the TOS/DS field
8. Select the **Save** button within the Edit your Venue Server section

Guest Networks and VLANs:

Most network controllers or WAPs have a 'Guest Network' option. This creates a network with tighter security settings. The settings can vary by manufacturer but will usually include Client Isolation, which prevents connected wireless devices from communicating with other devices on the network (such as iOS/Android devices communicating with the LE server) and disables mDNS.

To bypass Client Isolation and allow wireless clients to connect to the LE server, you must add the LE server(s) to the allowed address list (Whitelist) for the Guest Network/VLAN in the Router and/or WAP configuration. Some routers require that this be done by IP address, and some by MAC address. The IP and MAC addresses of the LE server can be found in Cloud Services, and the DHCP lease table. The MAC address can also be found on the Server ID label on the bottom of the unit. The IP address for mDNS must also be enabled or whitelisted (see *Enabling Multicast*).

In some network configurations a VLAN is desired to isolate the LE server and/or iOS/Android devices from other network traffic. For the LE server to function as expected, the LE server will need to be able to access the intended iOS/Android devices and vice versa. In most cases they will be required to be on the same VLAN with the ability for the VLAN tag to be sent to and from the switch port connected to the LE server through the WAPs configured to connect to the iOS/Android devices.

Mesh Networking:

A mesh network is a type of network topology where each node (e.g. WAP) in the network is wirelessly connected to every other node. This network type can cause mDNS discovery issues, increased latency, and audio dropouts. The use of mesh networks is not recommended.

System Security:

Listen Technologies' Listen Everywhere servers present only a very limited HTTPS endpoint structure to un-validated endpoints. The attributes supplied by clients in this way are used only to retrieve visual and auditory assets from the Listen Everywhere server and to start and stop unidirectional UDP streams. Other interactions with the Listen Everywhere server will require authentication. This authentication has been reviewed to use encryption that is up to date with modern security requirements in technique and bit-depth. Because of these development efforts, users can be assured that most known forms of attack against these network servers will fail and the network in which users are connected will remain uncompromised.

For additional security, venue networks can be configured to prevent access to or from the Listen Everywhere server to both WAN and non-Listen Everywhere client devices. The Listen Everywhere server will continue to operate without WAN or general network access. This can be accomplished through subnets and/or VLANs with appropriate directional policies. In the very unlikely event that a Listen Everywhere server is compromised, this would dramatically limit exposure to the rest of the venue network.

Should you have any further questions or concerns, please contact Listen Technologies' Technical Services team at 1-800-330-0891 or support@listentech.com for assistance.