Listen Everywhere Network Configuration Guide

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:

Listen Everywhere from Listen Technologies is a seamless solution for streaming audio over Wi-Fi to Android and iOS devices, enhancing how we experience sound in public spaces. Designed for simple integration into existing wireless networks, audio over Wi-Fi solutions from Listen Technologies simplify audio delivery through a two-phase process: (1) discovery, where the listening devices discover and connect to the Wi-Fi Audio Servers on the network and (2) streaming, where live audio is streamed from the server(s) to listening devices, providing hearing assistance to users. Often times, to unlock its full potential, specific network configurations are essential.

The backbone of Listen Everywhere functionality is dependent on a well-designed network with proper configuration.

Here are the top 3 things to consider for a successful network implementation:

1. Ensure that your network supports one of the following protocols:
    a. Multicast discovery (mDNS) – an automatic discovery mechanism required for devices to discover a service or device on a network.
    b. DNS (domain name service) – a professional discovery protocol that allows devices to find a service on the network. This requires IT to implement a specific record in their DNS server, allowing the discovery to take place.
2. Proper communication ports will need to be opened if blocked, allowing proper data to flow between the Wi-Fi audio servers and listening devices on your network. This guide should be reviewed by your IT staff to ensure these requirements can be met.
3. Ensure that your Wi-Fi network is operating on a good channel with no interference or overlap from other channels. Networks that have been deemed acceptable for daily data transfer (emails, videos, etc.) can become unacceptable once streaming low latency real-time audio across them. A clean Wi-Fi channel, in addition to network priority given to Wi-Fi audio is paramount in the success of any audio over Wi-Fi hearing assistance solution.

Ultimately, setting up an audio over Wi-Fi system might require initial assistance from IT professionals.

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:

- Wireless router or a managed DHCP server with wireless access point(s) running WiFi 4 (802.11n) or better.
    - Enterprise-grade equipment running 802.11ax or better is recommended.
- The data load is approximately 125 kbps per connected user. It is recommended that LE traffic only accounts for 20% of the total network bandwidth.

Recommended Configuration:

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

- Enterprise-Grade networking equipment. Consumer-grade and business-grade routers and switches do not always have the required features, configuration options, or necessary computing power to handle basic needs of the Enable Multicast UDP or set up a DNS record on the network using the alias **listenwifi-audio**.
- Enable Quality of Service (QoS) on the network to prioritize LE traffic (see *Enabling QoS*).
- Avoid using range extenders, mesh networks, or multi-hop networks. Doing so may add latency, cause audio stuttering, or cause audio dropouts.
- If utilizing the DNS-SD connection method, the Listen Everywhere server should be placed on the same network/subnet as connected users. If this is not possible and/or DNS-SD connectivity is not desired, the DNS connection method can be utilized.

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:

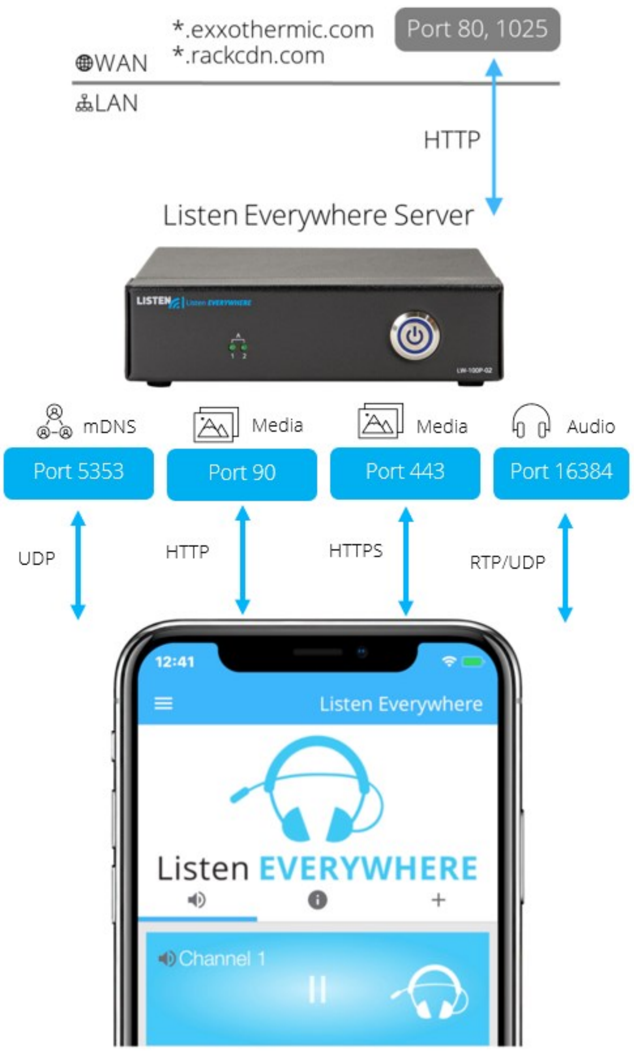
- Banner Ads
- Offers
- Documents
- Firmware Updates
- Downloading Log Files

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

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.

Connection Method #1: Venue Scan (mDNS)

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.)*

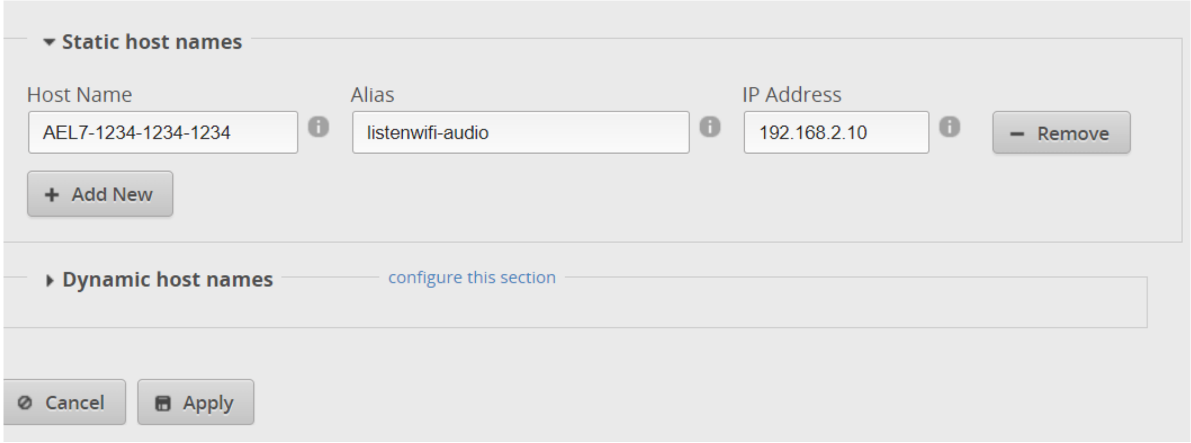
Connection Method #2: Venue Scan (DNS Record)

This method requires setting a static IP address for the LE server, and then creating a DNS record for the server with the alias listenwifi-audio. When performing a venue scan, the LE server will automatically search for a device with alias listenwifi-audio and try to connect.

How it works:

1. Set a static IP address for the LE server. This is performed through the [Server Admin interface](#) (i.e. local GUI).
2. Create a DNS entry for the LE server using alias listenwifi-audio.
3. Reboot your networking equipment, then reboot your LE server.

Included below is a screenshot of what this configuration looks like when logging into a Ubiquiti EdgeRouter X (ER-X) admin interface. The configuration screen will vary between network interfaces.



Static host names

Host Name	Alias	IP Address
AEL7-1234-1234-1234	listenwifi-audio	192.168.2.10

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. This setting can be changed through the Cloud Services interface.

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.

System Security Statement:

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.