ListenWIFI Network Configuration Guide

Overview

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

How It Works

ListenWIFI from Listen Technologies is a seamless solution for streaming audio over Wi-Fi to dedicated ListenWIFI receivers, as well as 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, to unlock its full potential, specific network configurations are essential.

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

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

1. Ensure that your network supports one of the following protocols:
    a. DNS-SD/mDNS discovery – 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.

Commented [BC1]: Per Irene: fix spacing. Long blue line for short titles, short blue line for long titles.

Minimum Networking Requirements

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

- Wireless router or a managed DHCP server with wireless access point(s) running Wi-Fi 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.

Recommended Configuration

Though not required for the LW 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 LW server.
- Enable DNS-SD/MDNS services or set up a DNS record using the alias **listenwifi-audio**.
- Enable Quality of Service (QoS) on the network to prioritize traffic.
- Avoid using range extenders or mesh networks. Doing so may add latency, cause audio stuttering, or cause audio dropouts.
- If utilizing the DNS-SD/MDNS connection method, the ListenWIFI server should be placed on the same network/subnet as connected users. If this is not possible and/or DNS-SD/MDNS connectivity is not desired, the DNS connection method can be utilized.

Internet Connectivity

An Internet connection is not required for the LW system to function or to take advantage of the features offered in the ListenWIFI Manager. However, an internet connection would be required to perform updates through the ListenWIFI Manager from FTP site ftp://ftp.listentech.com/ through port 20 and 21.

Regarding LA-490 Beacons

The LA-490 beacons are utilized to connect the mobile app and/or LWR-1050 receivers to a specific audio channel, as designated in the ListenWIFI Manager. The beacon will *not* automatically connect a user to the wireless network, and it will *not* initiate the initial connection to the LW server. The Wi-Fi connection and the LW server discovery need to be established prior to beacon deployment to allow a guest to connect to an audio channel.

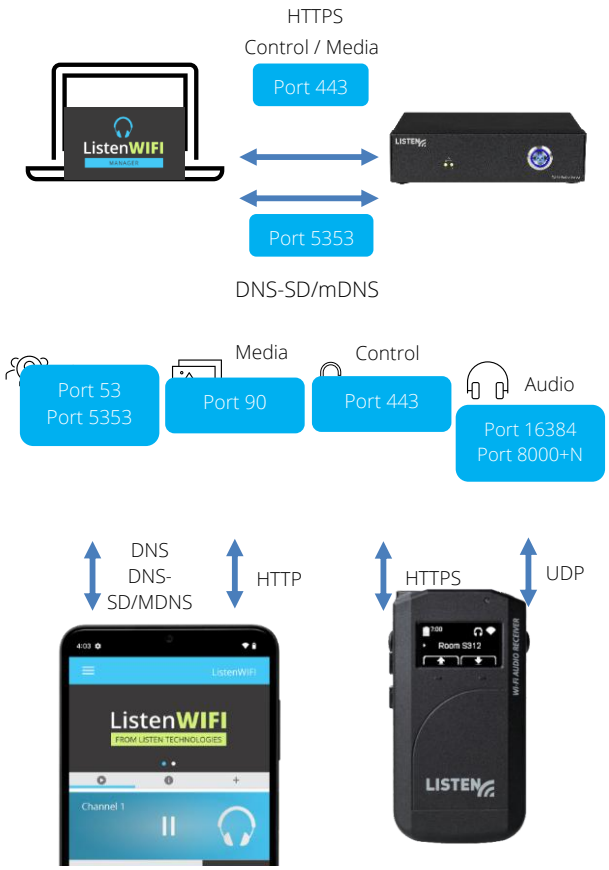
Ports and Services (LAN)

Discovery

- LW Clients (Mobile Apps and LWR-1050) may use several connection methods to discover one or more LW Servers.
- For no dedicated network configuration (Zeroconf), DNS-SD/MDNS (RFC 6763) relies on Multicast DNS (RFC 6763) which uses **destination port 5353**.
- For a configured DNS setup, DNS (RFC 1035) uses **destination port 53**.
- For venues which only use QR Codes, discovery happens "out of band" and does not require any network interaction.

Control

- LW Clients make HTTPS (RFC 2818) requests to learn about available streams after discovery and start/stop streams during runtime. This uses the standard HTTPS **destination port 443**.



Media

- LW Mobile Apps make HTTP (RFC 2616) requests for static assets (Banners, Offers, Etc.) at discovery time. This uses a non-standard **destination port 90**.

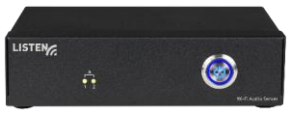
Audio

- LW Clients use UDP Hole Punching (RFC 5128 section 3.3) to initiate solicited audio streams across networks with NAT and/or Firewalls.
- This uses **destination port 16384**. Then, LW Servers use RTP (RFC3550) to send audio to the clients. This uses a **variable destination port** determined by the source port of the Hole Punching packet.
- The LWR-1050 receivers listen to and communicate with the LW server via UDP over destination port 8000+N, where N is the numbered server designated by the network (e.g. 8001 would be the destination port for a single-server venue. If a second server is added, the second server would communicate via port 8002).

Firmware Updates: Firmware files are sent over **destination port 443** to the LW server. Firmware files are sent over **destination port 4242** (not shown) to the LWR-1050 receiver when updates are initiated from a Listen docking station

***Note**: All ListenWIFI traffic is designed such that it will appear as solicited to any stateful firewalls in the network*

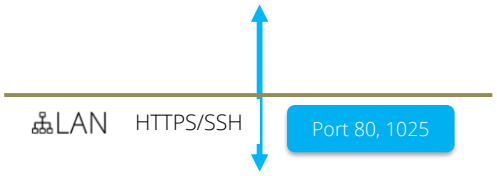
WAN



Ports and Services (WAN)

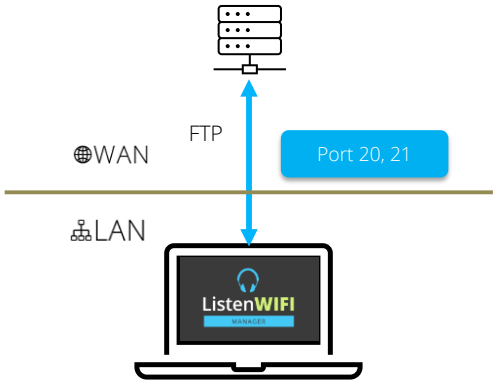
Listen Technologies Technical Support Visibility:

- In rare cases, Listen Technologies support can communicate with the server remotely through the Cloud Services portal if needed. This is not currently available to users.
- Cloud Services communicates via HTTP with the LW server through *.exxothermic.com (IP address: 108.166.110.178) over **port 1025**, with updates communicating over **port 80**. Additionally, ubuntu.com, launchpad.net, odroid.in are also used for updates via **port 80**.



Firmware Updates via LWM:

- ListenWIFI Manager utilizes protocol FTP through **port 20** and **port 21** for server, beacon, and receiver firmware update files.
- If these ports are disabled on the network, you will need to contact Listen Technical Support for the firmware files. They need to be placed into the local firmware folder for ListenWIFI. By default, the location path is C:\Users\USERNAME\AppData\Local\Listen Technologies\ListenWIFI\LE User Data\Firmware.



Server Discovery Method#1: DNS-SD/mDNS

DNS-SD/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 DNS-SD/MDNS, perform the following:

- Add the following case-sensitive services to the allowed list in the Gateway/WAP DNS-SD/MDNS settings:
  - **_lw-server._tcp**
  - **_lw-receiver._tcp**
  - **_lw-mobile._tcp**
- Open **Port 5353**.
- Add the DNS-SD/MDNS IP address to the allowed subnets list. **224.0.0.251** is the most common DNS-SD/MDNS IP address, but it could be any of the **224.0.0.0/24** range.

Note: *For some Cisco controllers: ".local." or ".local" may need to be added to the end of each service name (e.g. _lw-server._tcp.local.)*

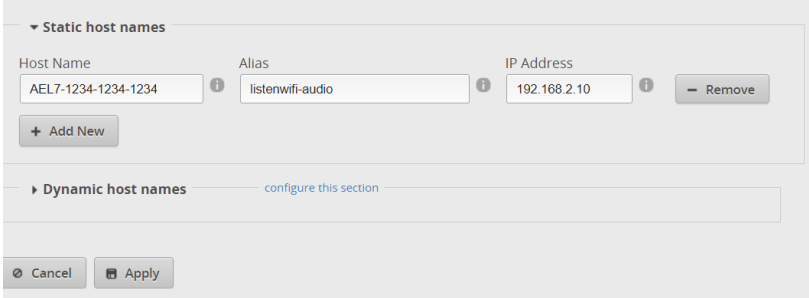
Server Discovery Method#2: DNS Record

This method requires setting a static IP address for the LW server and then creating a DNS record for the server with the alias **listenwifi-audio**. When performing a venue scan, the LW 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 LW server through the ListenWIFI Manager software.
2. Create a DNS entry for the LW server using alias **listenwifi-audio**.
3. Reboot your networking equipment, then reboot your LW server.

Included 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.



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 LW server) and disables DNS-S /mDNS services.

To bypass Client Isolation and allow wireless clients to connect to the LW server, you must add the LW 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 LW server can be found in the networks' DHCP lease table or with a network scan. The MAC address can also be found on the Server ID label on the bottom of the unit. The IP address for DNS-SD/MDNS services must also be enabled or whitelisted.

In some network configurations a VLAN is desired to isolate the LW server and/or iOS/Android devices from other network traffic. For the LW server to function as expected, the LW 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 LW server through the WAPs configured to connect to the iOS/Android devices.

Enabling Quality of Service (QoS)

By default, the LW 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 LW Server is set to the ToS/DS tag of B8 (Critical, low delay, high throughput, and normal reliability). Other tags can be used depending on existing networking configurations. This setting can be changed in the ListenWIFI Manager

System Security Statement

Security is of utmost importance for any device that resides on your network. A single vulnerable device can compromise the security of your entire network, leading to data breaches, malware infections, and other cybersecurity threats. The ListenWIFI products, including Wi-Fi audio servers, receivers, mobile apps, and management software, have been hardened against security threats and vulnerabilities to ensure that the risk of unauthorized access is minimized and your network remains protected.

Maintaining network security is an ongoing process that requires regular monitoring, updates, and proactive measures to stay ahead of evolving threats. We are continually monitoring and identifying potential threats and vulnerabilities, subsequently pushing out software updates and patches to address those that could impact ListenWIFI. Therefore, we highly recommend keeping your software up to date on your ListenWIFI servers and products deployed on your network.

System hardening is a continuous effort on ListenWIFI to reduce the attack surface of system components, providing significantly improved security, functionality, and product performance. The following highlights some of the system hardening efforts that have been implemented on the ListenWIFI product platform to ensure our system remains both secure and reliable:

- Software and operating systems are updated and patched when vulnerabilities are discovered.
- All data in transit is encrypted using **TLS 1.2 or higher**, and stored data uses **AES-256 encryption**.
- Data transmission is contained to the Local Area Network (LAN) and never sent over the internet.
- Only very low-sensitivity data is stored on the ListenWIFI servers and is encrypted.
- HTTPS endpoint communications between servers and listening devices is limited to basic data transmittal to start/stop UDP audio streams and exchange basic visual assets.
- Access controls implemented allowing only authorized accounts access to management software and controls, following strong password management practices as outlined in the **Password Policy** section.
- Independent third-party security audits and penetration testing are conducted to ensure threats are addressed.

Network Protection and Resilience

ListenWIFI products are designed to:

- Avoid harming network functionality or misusing network resources.
- Prevent unauthorized access and protect against traffic manipulation or overload.
- Be resilient against denial-of-service (DoS) attacks and other common network-based threats.

These measures align with EN 18031 / ETSI EN 303 645 and EU Cyber Resilience Act requirements for secure-by-design products.

Update Notifications

Users are notified of available updates via **email alerts**, as well as **upon launching the ListenWIFI Manager software**. Updates may include security patches, firmware upgrades, and feature enhancements.

The security of ListenWIFI will also be dependent on your network architecture and implementation. For the best security and performance on your network, we recommend placing your Wi-Fi audio server on the same network that your listening devices will connect to and whitelisting communication to the server with client isolation implemented as applicable. This deployment will typically allow the required communication to occur between devices without having to modify your router or firewall rules and prohibits any unnecessary communications between client devices. Alternatively, the server and listening devices can be placed on separate networks; however, the proper ports must be opened and the ListenWIFI traffic must be routable, which can increase network vulnerabilities. Please reference our Network Configuration Guide for more details.

If you have questions or would like to review your deployment of ListenWIFI on your network, please reach out to one of our team members at Listen Technologies Corporation.