ListenTech-Note

LISTEN TECHNOLOGIES

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 and 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 ListenWIFI 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. DNS-SD 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.

ListenTech-Note

Minimum Network 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 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 LW traffic only accounts for 20% of the total network bandwidth.
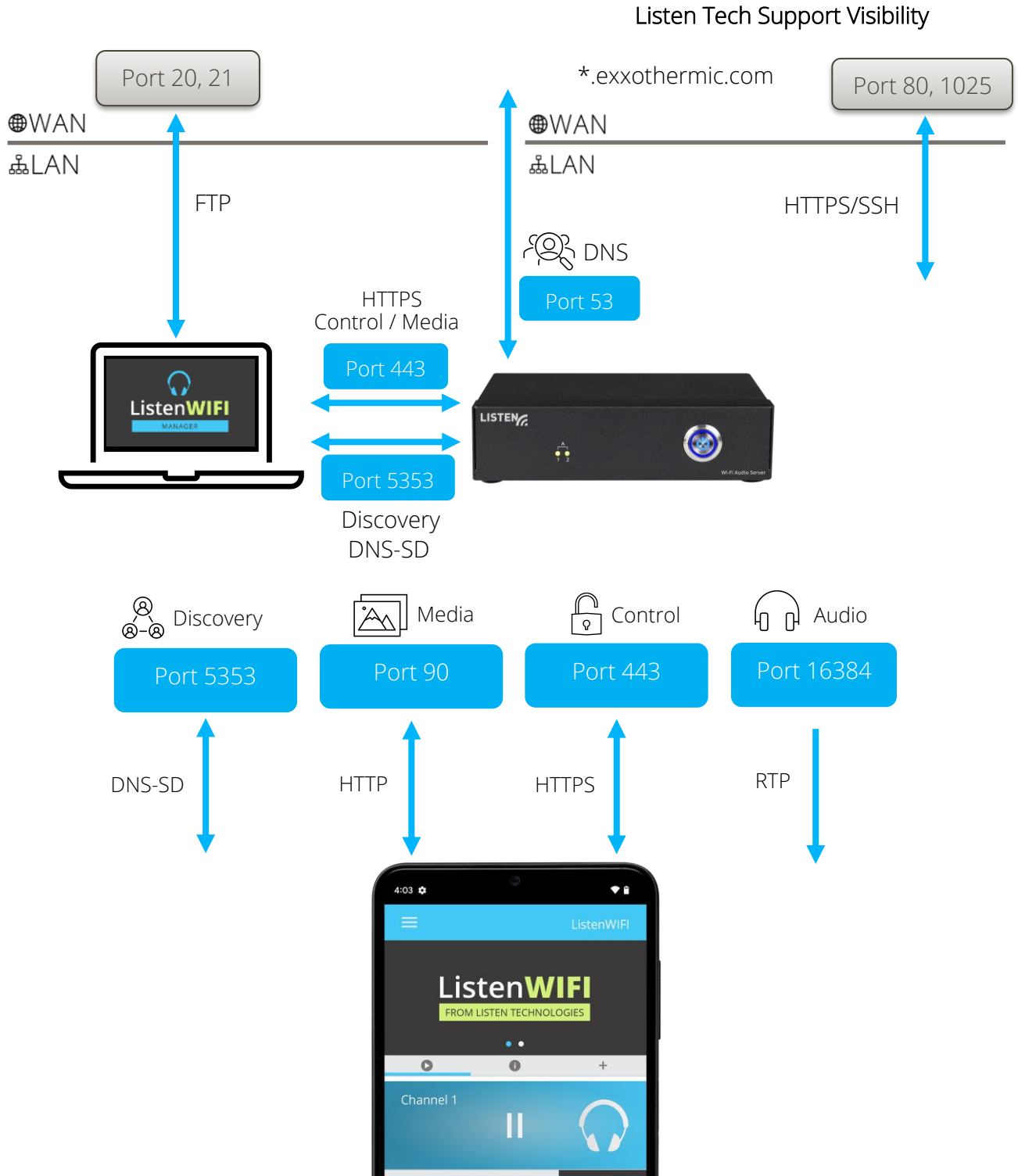
Recommended Configuration:
Though not required for the LW system to function, here are several recommendations and optimizations that can improve performance:

- 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 services or set up a DNS record on the network using the alias **listenwifi-audio**.
- Enable Quality of Service (QoS) on the network to prioritize LW traffic (see *Enabling Quality of Service*).
- 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 ListenWIFI 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 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/ (IP address 50.205.4.21) through port 20 and 21.

ListenTech-Note

LISTEN TECHNOLOGIES

Ports and Services:

Listen Tech Support Visibility

Port 20, 21

*.exxothermic.com

Port 80, 1025

🌐 WAN
🔗 LAN

🌐 WAN
🔗 LAN

FTP

HTTPS/SSH

👥 DNS

Port 53

HTTPS
Control / Media

Port 443

Port 5353

Discovery
DNS-SD

ListenWIFI MANAGER

Wi-Fi Audio Server

Discovery	Media	Control	Audio
Port 5353	Port 90	Port 443	Port 16384

DNS-SD

HTTP

HTTPS

RTP

4:03 ⚙

ListenWIFI

☰   ListenWIFI

ListenWIFI
FROM LISTEN TECHNOLOGIES

▶   ⓘ   +

Channel 1

⏸   🎧

Connection Method #1: Venue Scan (DNS-SD)

DNS-SD 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, perform the following:

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

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

Connection Method #2: Venue Scan (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. This is performed 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 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.

ListenTech-Note
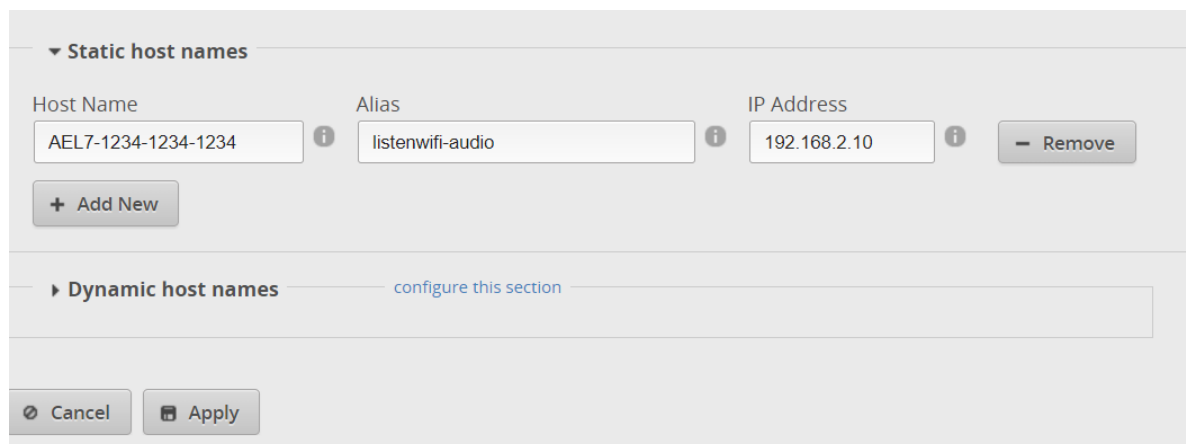
QR Codes and Hyperlinks

A QR code or hyperlink can be used to make it easy for guests to connect to a ListenWIFI channel after they have the ListenWIFI app installed on their mobile device and are connected to the same wireless network as the ListenWIFI server.

How to create QR code/Hyperlink in ListenWIFI Manager (LWM)*:*
1. Open the ListenWIFI Manager
2. Select **Mobile Apps**
3. Select **Channels**
4. Select the channel you want the guest to connect to when scanning QR code (Guest can still swap channels manually after scanning QR code)
5. Select **Print Channel QR Code**, and you will see a popup for the QR code.

Note: Please make sure to always use ListenWIFI Manager in full screen mode; certain options will not appear if ListenWIFI manager is not opened in full screen. (such as the "Print Channel QR Code" option).

You must be connected to the same network as your ListenWIFI server, and the ListenWIFI server needs to be online/connected in LWM when creating a QR code.

How the QR code works:
1. Install the ListenWIFI app.
2. Connect to the Wi-Fi network.
3. Open the ListenWIFI app and select the QR code icon at the bottom right of the screen.
4. Scan the QR code using the ListenWIFI app's QR option, automatically connecting a guest to the desired Channel.

How the Hyperlink works:
1. Install the ListenWIFI app.
2. Connect to the Wi-Fi network.
3. Select the hyperlink from a mobile device or select an image that the link is embedded into.
5. The link / image will automatically open the ListenWiFi app, connecting the guest to the desired Channel.

ListenTech-Note

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-SD 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 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

ListenTech-Note

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.
- Encryption of all data at all times, regardless of configuration.
- User 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.
- 3rd party security audits are completed to ensure threats are addressed.

The security of ListenWIFI will also be dependent on your network architecture and implementation. For the best security and performance on your network, we do recommend that you place your Wi-Fi audio server on the same network that your listening devices will connect to, and simply whitelist 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.

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.