WI-FI DEPLOYMENT GUIDELINES FOR WAVE PTX™

WHAT YOU NEED TO KNOW TO OPTIMIZE WAVE PTX BROADBAND PTT PERFORMANCE OVER WI-FI

MOTOROLA SOLUTIONS

ENHANCING CONNECTIVITY

A unique feature of the WAVE PTX™ broadband push-to-talk (PTT) service is the ability to use Wi-Fi networks to extend PTT communication into areas with weak or non-existent cellular coverage, such as factories, warehouses, and underground work areas. Compatible Wi-Fi networks include public Wi-Fi hotspots, home networks, and corporate Wi-Fi networks.

To use WAVE PTX broadband PTT over a Wi-Fi network, customers need to have 802.11g/n/r/ac access points with Internet access, and the WAVE PTX mobile application loaded on a device with Wi-Fi support. The WAVE PTX mobile application uses standard HTTPS and TLS connections over TCP when connected to Wi-Fi.

The WAVE PTX mobile application automatically performs a handoff from the cellular network to the Wi-Fi network whenever the phone connects to Wi-Fi. The WAVE PTX mobile application then switches back to cellular data as soon as the Wi-Fi connection is lost.

Typical WAVE PTX broadband PTT communication over Wi-Fi does not require any special configuration of the Wi-Fi network, assuming the network meets the basic set of requirements. If WAVE PTX broadband PTT is expected to be used in larger Wi-Fi coverage areas involving multiple access points or high Wi-Fi usage density, a higher grade of reliability and performance can be provided by fine tuning Wi-Fi networks for best PTT performance.

BASIC REQUIREMENTS

The WAVE PTX mobile application requires Internet access to provide service over a Wi-Fi network. In addition, because the service uses Voice over IP technology, it requires continuous, uninterrupted media streams to ensure that the voice packets are delivered on-time, without interruptions or errors. The basic requirements for the WAVE PTX broadband PTT over Wi-Fi solution to work seamlessly are listed below.

BACKEND NETWORK REQUIREMENTS

- The backend network to which the APs connect should provide access to the internet
  - This includes DHCP allocation of IP addresses, DNS servers and default gateways that provide full access to all broadband PTT server IP addresses / FQDNs

FIREWALL REQUIREMENTS

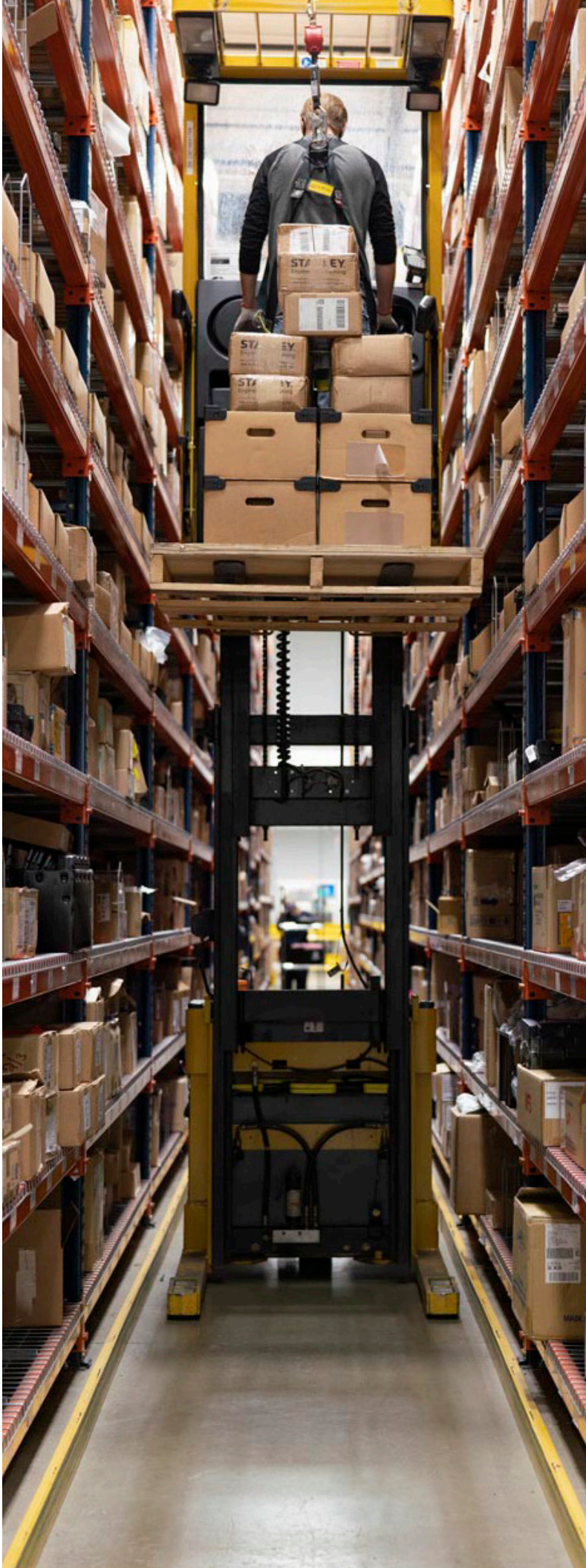
- Wi-Fi networks should allow devices to access standard TLS ports [TCP Port 443] towards the broadband PTT server's IP address/FQDNs.

WI-FI ACCESS POINT REQUIREMENTS

- Access points should support either 802.11g/n/r/ac

INTERNET CONNECTION REQUIREMENTS

- Maximum Round Trip Time (RTT) to server - 100 ms
- Maximum jitter between packets - 50ms
- Maximum packet loss rate - 0.5 %
- Minimum Wi-Fi signal strength - -69dbm



FINE TUNING THE WI-FI NETWORK

Most corporate Wi-Fi networks will not have an issue supporting the basic requirements to use WAVE PTX. Wi-Fi environments, such as public hotspots, university campuses, or factories, may have difficulty meeting these minimum requirements due to the unpredictable data traffic generated by the large number of connected devices or the large coverage area. These Wi-Fi networks, however, can be tuned to provide the needed level of service by following the guidelines for Voice over WLAN (VoWLAN), with a few key differences.

1. WI-FI STANDARD AND EQUIPMENT

a. IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands. While there are several modulation standards for IEEE 802.11, only the following should be used for optimal WAVE PTX performance.
   i. 802.11g
   ii. 802.11n
   iii. 802.11e (for QoS support)
   iv. 802.11k (for AP signal strength)
   v. 802.11r (Roaming)
   vi. 802.11x (Enterprise-level authentication)

b. Functionalities required in Wi-Fi equipment are:
   i. Support Wi-Fi Power Saving Mode (Wi-Fi PSM)
   ii. Support WMM QoS
   iii. Support DTIM period tuning
   iv. Support higher QoS settings for voice
   v. Support Wi-Fi power level tuning

2. OPTIMIZE CHANNELS, POWER, AND DATA RATES

a. If you use 1.4 GHz channel:
   i. Use Channels 1, 6 and 11, as the spectrum used for these channels does not overlap.

b. If you use 5GHz channel:
   i. Use channels from UNII-1 (36-48), UNII-2 (52-64), UNII-2 Extended (100-140), and/or UNII-3 (149-161 but not 165)
   ii. If radar detection is frequent, avoid the DFS channels (UNII-2, UNII-2 extended)

c. Data rates:
   i. Set 6Mbps as the lowest mandatory rate, be sure that 12 and 24Mbps are enabled
   ii. Remember to make any changes on all WLCs in the Wi-Fi Network Group

3. AUTHENTICATION AND ROAMING

a. Enterprise-level authentication using Extensible Authentication Protocol (EAP) is recommended, but an alternate Wi-Fi Security mechanism such as WPA2 or WPA can be used (all devices must be using same pre-shared key).

b. All access points must be configured with the same SSID and use the same security mechanism. This ensures that the user experiences smooth broadband PTT service when changing Wi-Fi access points. Access points with overlapping signals must use different channels to minimize interference. There should be Wi-Fi usage site planning tools to optimize the Wi-Fi wireless channel allocations and analyze the data over time to allocate the bandwidth in order to avoid congestion.

c. To minimize frequent Wi-Fi transitions or connect/disconnects, the access points must be placed at all the points where users are expected to move or transition frequently (e.g. break rooms). The device IP address should remain unchanged when it roams across multiple access points, with roaming across wireless controller and access points seamless for large coverage areas. Access point-to-access point roaming latency should be less than 100ms and ensure no packet loss while transitioning between access points.

4. ENABLE WI-FI POWER SAVING MODE (WI-FI PSM)

a. PSM is a power conservation technique defined in WMM 802.11. The methodology is for the mobile device to suspend periods of inactivity, and then wake up periodically (usually about 3 beacon frames, 100 ms approximately) to see if the infrastructure has queued any traffic for it.

b. Wi-Fi Power Saving Mode allows broadband PTT devices to receive calls even while the devices are sleeping. PSM supports U-APSD (Unscheduled Automatic Power Save Delivery), which is an enhanced power-save mode for IEEE 802.11e networks. If UAPSD is enabled, the wireless client is allowed to enter Power Save mode.

c. The delivery traffic indication message period (DTIM) indicates how often clients serviced by the access point should check for buffered data awaiting pickup on the access point. The DTIM period should be set to 200ms (typical default).

5. ENABLE WMM QOS (IEEE 802.11E)

a. A router with good quality of service (QoS) technology can prevent unequal distribution of precious resources. For this analogy, it is like one should be able to dip only one straw into the Internet at a time and QoS ensures that each client gets its chance for a sip, and it also takes each client's specific needs into account.

b. Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM), is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. To improve the reliability of voice transmissions in this nondeterministic environment, it is recommended to use any device that supports the industry-standard IEEE 802.11e and is Wi-Fi Multimedia (WMM)-certified. WMM enables differentiated services for voice, video, best-effort data, and other traffic. In order for these differentiated services to provide sufficient QoS for voice packets, however, only a certain amount of voice bandwidth can be serviced or admitted on a channel at any one time. If the network can handle N voice calls with reserved bandwidth, when the amount of voice traffic is increased beyond this limit (the N+1 call), the quality of all calls suffers

6. ACCESS POINTS, WIRELESS CONTROLLERS AND DEVICES

a. Access points and wireless controllers (used to connect more than one access point smoothly while moving between them) need to be upgraded with the latest firmware.

b. Wi-Fi devices need to be updated with latest firmware version (mostly supplied by device hardware vendor/operator) and latest client software version

7. QOS AND VLANS

a. It is recommended that VLANs are used to separate voice traffic from data traffic. This technique enables security and isolation of higher-priority voice traffic so that it can be dealt with using maximum resources.

b. Separating voice from data requires a minimum of two VLANs, and an assigned SSID on the WLAN for each VLAN. Using separate general purpose and broadband PTT or voice VLANs enables specific QoS settings on all traffic on the broadband PTT/voice VLAN, to give it a higher QoS profile. Standard network designs support four levels of QoS over the air: platinum for voice, gold for video, silver for best effort (the default), and bronze for background. You can configure the broadband PTT/voice traffic WLAN to use platinum QoS, assign the low-bandwidth WLAN to use bronze QoS, and assign all other traffic between the remaining QoS levels. Separating traffic by VLAN and using the QoS profiles for VLAN traffic reduces the chance of data clients crowding the broadband PTT/voice WLAN and causing unnecessary traffic overhead and delays.

8. WI-FI RADIO UPSTREAM/DOWNSTREAM QOS

The WLAN must also allow you to maintain a QoS profile for Layer 2 and Layer 3 over wireless and wired networks. All WLAN traffic that passes between the access point and the wireless LAN controller is encapsulated. This encapsulation maintains the Layer 3 marking in the original packet. Once the packet is de-encapsulated at the access point or wireless LAN controller, the original Layer 3 marking is again used by QoS mechanisms in the network infrastructure. With this capability, the network can achieve end-to-end QoS for voice traffic, over the air and across the wired network.

9. FIREWALL REQUIREMENTS

The firewall connecting to the Internet should be configured with a timeout of 30 minutes for TCP port 443 (HTTPS port 443) for any communication with the broadband PTT server FQDN/IP address.

10. VOICE SERVICES RF ENVIRONMENT

a. The IEEE 802.11 standards use the 2.4-GHz (802.11b and 802.11g) and the 5GHz (802.11a) bands. In the 2.4-GHz band, there are up to 11 channels available (14 channels are available in Japan). Each channel offers 11 or 54Mbps over-the-air data rates for 802.11b and 802.11g, respectively. Because the wireless medium is continuous and shared, all clients that are associated with access points on the same channel will share the bandwidth available in that channel, with reception power (and therefore data rates) diminishing with distance.

b. Adding capacity to the network is accomplished by using more access points on non-overlapping channels. In the 2.4-GHz band, there are three non-overlapping channels. On the 5 GHz (802.11a) band, however, all 23 channels (depending on geographic area) are non-overlapping channels, which results in increased network capacity, improved scalability, and the ability to deploy without interference from adjacent cells.

c. At the edge of each voice cell, the received signal strength indication (RSSI) measurement should be -67 dBm. It is recommended that you have an RSSI signal strength above 35 at the edge of the cell, which is equivalent to -67dBm, for optimum performance on the PTT device.

d. Each cell in the network should overlap with the adjacent cells in order to facilitate uninterrupted handoff as a client moves between cells, and to provide a minimum service even in case of access point failure. For a typical PTT/voice deployment, it is recommended to maintain a 15 to 20 percent overlap of a given access point's cell from each of the adjoining cells.

11. FAST SECURE ROAMING

a. To minimize the delay introduced by authenticating roaming clients, it is recommended to use the Extensible Authentication Protocol-Flexible Authentication via Secured Tunnel (EAP-FAST).

b. EAP-FAST is an 802.1x EAP framework for authentication that encrypts EAP transactions with a Transport Layer Security (TLS) tunnel. While similar to Protected Extensible Authentication Protocol (PEAP) in this respect, it differs significantly in that EAP-FAST tunnel establishment is based upon strong secrets that are unique to clients. These secrets are called Protected Access Credentials (PACs), which the infrastructure generates using a master key.

c. During roaming, re-authentication time back to the RADIUS server alone can take 500 ms or more. Use centralized key management to achieve access-point-to-access-point roaming latency of less than 100 ms.

d. Centralized key management permits the negotiation of a session key from a cached master key and avoids the need to go back to the authentication, authorization, and accounting (AAA) server during a roam. When the client roams, it informs the infrastructure that it has roamed and the infrastructure forwards the keying material to the new access point. The efficiency of EAP-FAST with centralized key management helps ensure maximum protection with minimum transaction time.

USER EXPERIENCE

Users will experience seamless service as they transition between cellular and Wi-Fi networks. The table below provides details on what the user will experience during the transitions from cellular service to Wi-Fi, Wi-Fi-to-cellular, and Wi-Fi-to-Wi-Fi.

TRANSITION TYPE	USER EXPERIENCE
Cellular – to- Wi-Fi	• Automatic transition within 6-12 seconds • No indication if the PTT application is in the background • "Reconnecting" message is displayed to the user during the transition if the PTT application is in the foreground
Wi-Fi-to-Cellular	Same behavior as cellular-to-Wi-Fi transition Note: The transition could take longer as some devices require complete W-Fi signal loss before disconnecting from Wi-Fi.
Wi-Fi-to-Wi-Fi (AP-to-AP with same SSID)(AP-to-AP roaming)	Seamless, assuming: • The Wi-Fi network is designed according to Motorola Solutions guidelines • No signal "dead zone" exists between the access points (AP) used for AP-to-AP roaming
Wi-Fi-to-Wi-Fi (AP-to-AP with different SSID)	Same behavior as cellular-to-Wi-Fi transition Note: The transition could take longer as some devices require complete Wi-Fi signal loss (with previous AP/SSID) before transitioning to another Wi-Fi AP

In rare cases when a broadband PTT user does not want to use Wi-Fi networks, the Android WAVE PTX mobile application provides a setting which allows that user to turn off the transition to Wi-Fi.

SUMMARY

The WAVE PTX ability to seamlessly transition between cellular and Wi-Fi networks allows users to enjoy continuous service whatever their location, whatever their network.

MOTOROLA SOLUTIONS

Motorola Solutions Inc., 500 West Monroe St, Chicago, IL 60661 U.S.A. motorolasolutions.com