Zebra Wi-Fi 6E Connectivity and Performance in the Enterprise WLAN

ZEBRA

White Paper

MN-004795-01EN Rev A

Terms of Use

Proprietary Statement

This manual contains proprietary information of Zebra Technologies Corporation and its subsidiaries (“Zebra Technologies”). It is intended solely for the information and use of parties operating and maintaining the equipment described herein. Such proprietary information may not be used, reproduced, or disclosed to any other parties for any other purpose without the express, written permission of Zebra Technologies.

Product Improvements

Continuous improvement of products is a policy of Zebra Technologies. All specifications and designs are subject to change without notice.

Liability Disclaimer

Zebra Technologies takes steps to ensure that its published Engineering specifications and manuals are correct; however, errors do occur. Zebra Technologies reserves the right to correct any such errors and disclaims liability resulting therefrom.

Limitation of Liability

In no event shall Zebra Technologies or anyone else involved in the creation, production, or delivery of the accompanying product (including hardware and software) be liable for any damages whatsoever (including, without limitation, consequential damages including loss of business profits, business interruption, or loss of business information) arising out of the use of, the results of use of, or inability to use such product, even if Zebra Technologies has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Introduction

This white paper describes the benefits of deploying Zebra Wi-Fi 6E devices in various challenging enterprise environments. It details the technology and enhancements available in Zebra devices to handle various use case requirements which are important for Zebra customers.

The document includes sections highlighting the capabilities and advantages related to connectivity in all three WLAN bands of the ecosystem; 6GHz, 5GHz, and 2.4GHz, or even if the WLAN does not support the 6GHz. Where applicable, sub-sections further enhance how the user benefits in a 6GHz-enabled deployment.

This white paper applies to the following devices:

- TC53
- TC58
- TC73
- TC78
- TC22 with Zebra's MDNA license
- TC27 with Zebra's MDNA license

Zebra’s 6GHz Best Practices documents with Cisco and Aruba WLAN 6E Deployments, with Configuration Recommendations, can be found on the Wireless Fusion product support pages.

Faster Connection to Available Wi-Fi Network

This section describes scenarios in which a properly configured device, complete with network profile and security parameters, attempts to connect or re-connect to Wi-Fi after being disconnected, or when the device's Wi-Fi is turned off for any period of time and for any reason.

Use Cases and Ecosystems of Applications

Examples of the scenarios mentioned above:

- User is in an area completely out of WLAN coverage and then enters into coverage.
- User roams in an area of spotty coverage, where it is expected that the device does not get continuous coverage for an extended period of time.
- User with a cell carrier-capable device is outdoors and then switches to Wi-Fi indoor coverage.
- User has to put the device in airplane mode and then toggle back.
- User has to restart the device and reconnect for maintenance and configuration reasons.

These scenarios are affected by the location and the motion of the device with respect to the coverage upon the initial connection attempt. The density level of the AP layout can be an additional factor.

The Zebra device connects to the network within a short time in those scenarios, optimized by faster and aggressive scans, doing so in a wider range of coverage. Overall, the goal is to provide the fastest connection possible to serve application connectivity and traffic. For example, it allows the user to immediately receive a new phone call in urgent situations entering the indoor environment.

Immediate Action When Network is Visible

The timing of searching for the network is especially important when the device is disconnected outside the coverage for any amount of time, or while moving across coverage gaps, (for example, between buildings of same network), and then needing to connect quickly upon entering back into coverage. In these cases, it is likely that the user makes multiple attempts to find while out of range of coverage, and at some point, the user moves progressively closer to coverage.

The Zebra device includes optimization of scan timing, and has a tuned-up receiver sensitivity, which allows it to hear the Wi-Fi coverage at a significant distance from the perimeter of the coverage. This occurs once the device has minimally reasonable signal strength, thus it is able to yield successful scan results of a suitable AP.

Once the AP yields successful scan results at the greater distance, it is meaningful not only because of the range of the connectivity, but also contributes to application readiness at a further edge of the perimeter.

Consider an example of a user moving towards the coverage at a normal walking-speed. An optimized Zebra device finds the network and immediately completes the connection within 1-3 seconds, all without any delay with respect to the available coverage. Conversely, a device without such optimizations does not act immediately which adds a very noticeable connection delay, commonly in the range of 30 seconds to 3 minutes with respect to the available coverage.

Length of Scan Cycle

In both scenarios, whether the connection has a weak signal or a strong signal (for example, toggling Airplane mode), there is an additional distinct factor of how long it takes for each cycle of the search to complete in either coverage scenario. In a generic sense, the search of the coverage is a full scan cycle process that could be very lengthy, depending on the number of WLAN bands and number of channels in each band configured in the venue.

The most impactful factors on scan length are when Dynamic Frequency Selection (DFS) channels are enabled in the 5GHz band, which is the typical case in Enterprise WLAN.

In WLAN deployments of APs with 2.4GHz and 5GHz Bands, only (WLAN supporting up to Wi-Fi6) or including 6GHz Bands (WLAN supporting Wi-Fi6E), the Zebra device utilizes Dual Band Simultaneous (DBS) mechanisms in specific enhanced ways during the scanning.

NOTE: Refer to Advantages of Dual Band Simultaneous for details on DBS concept and time-saving ratios of scan times.

Regarding WLAN which includes 6GHz Band, the Zebra device uses Reduced Neighbor Report (RNR) information from the APs, in which the WLAN advertises its 6GHz channels in the 2.4GHz and 5GHz beacons of the same APs.

The immediate action when Network is Visible, together with the Length of Scan Cycle, accomplishes the previously described application use cases. For example, when a user needs to make an urgent call upon entering a coverage area, accomplishing the connection in one second by a Zebra device is transparent to the user and the call can be made immediately. However, with another device without optimizations, a connection can take 30 seconds or more to occur, which leads to user frustration.

Connectivity Consistency and Resiliency

This section details device features and optimizations for keeping the consistency and resiliency of the connection while the user travels the Wi-Fi network, providing stable connection while roaming in different network conditions.

Stable Connectivity

Stable network connectivity is important for the application that is running on the device. A user expects a flawless experience when using an application on the device, even when the device roams across multiple Access Points with different RF conditions.

When a device moves across the area, it might go through situations like:

- Walking through open spaces of the Wi-Fi coverage environment in varying speeds.
- Walking between good coverage to almost no coverage, and then back to good coverage.
- Walking through corridors and turning corners.
- Entering an elevator, riding the elevator, and then exiting the elevator.
- Entering and standing in isolated staircases.
- Entering, standing, and exiting shield areas like walk-in refrigerators or basements.

During these scenarios, a device will face varying degrees of abrupt changes in Wi-Fi coverage. Zebra devices maintain connectivity and support traffic in all these use cases so that user applications work smoothly.

It is also important that a device handles situations like hearing issues between the AP and device or rejections from the AP for connection attempts due to various reasons. There may be dynamic changes in RF environment in deployments caused due to other equipment or due to physical changes in the area (for example, new racks/shelfs) which increases instances of handover failures. Zebra devices handle such failure instances seamlessly by switching to another AP so that network connectivity is not impacted.

Zebra devices are optimized for scanning and roaming, ensuring proper timing of the scans and selection of best APs, and ensuring a faster handoff to the new AP. The optimization yields traffic performance of minimal or no packet loss, and negligible or no packet delays/latencies, even in challenging RF conditions.

- The Zebra device scanning performance, prior to the handoff to the new AP, ensures that during scans the device and the connected AP packets sent to each other suffer zero loss. During these short scan periods, individual packets might be delayed by 50-60ms in most instances, even if also scanning DFS channels. The worst case scenario is a packet delay of up to 100ms in some DFS cases. Conversely, a device without optimizations operating within the same WLAN will have packet delays of ~150ms in many more scanning instances, and not only in specific conditions.

- The Zebra device handoff performance, once switching to the new AP channel, ensures that the handoff offline period is ~50ms with a variation of ±10ms depending on which fast-roam method used. When performed during Voice or Video traffic, typically in ~20ms or 30ms intervals, this performance also ensures that the system path rerouting and forwarding of traffic (between the old and new AP) may drop up to 2 packets. Conversely, a device without optimizations operating within the same WLAN will have handoff offline period of ~100ms or more. When performed during Voice or Video traffic, this can result in a drop of ~5 packets or more.

The previously mentioned Zebra Device performance provides suitable support for any application-level traffic transmit & receive needs, in any user roaming mentioned earlier in this section. When those scenarios also include using Latency Sensitive Applications such as Voice, the performance ensures that audio continuity remains intact, keeping the expected quality consistent throughout the call.

Devices without optimization demonstrate lesser performance which affects different types of application traffic and user experience. For example, if running latency-sensitive applications such as Voice, the audio continuity is interrupted with noticeable choppiness and breaks missing syllables/words.

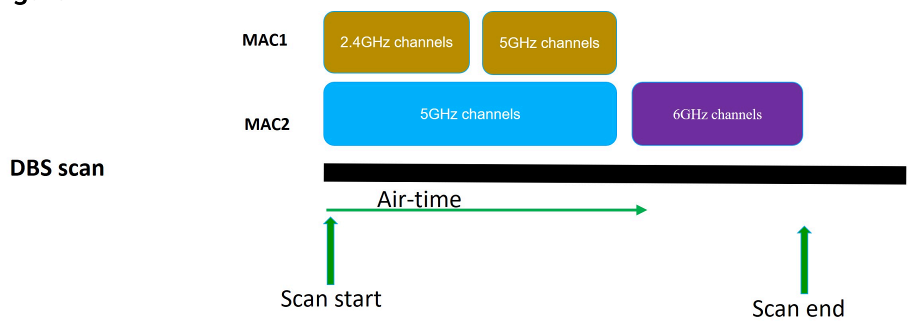
Advantages of Dual Band Simultaneous (DBS)

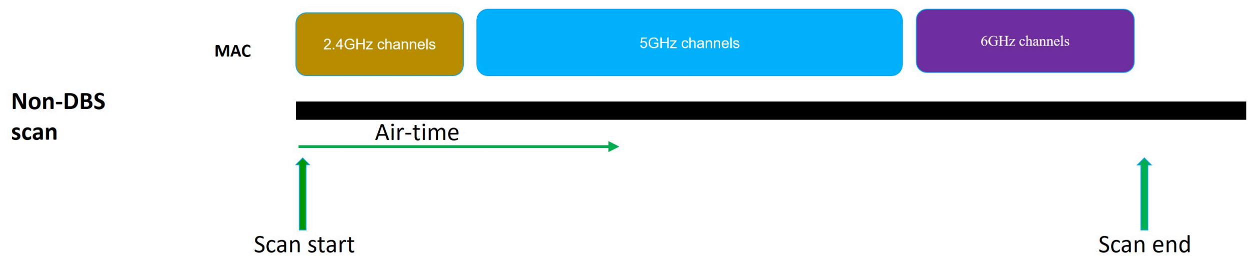
Zebra Wi-Fi 6E devices support Dual Band Simultaneous (DBS) feature, which helps in completing Wi-Fi scans faster. Wi-Fi scanning can happen in multiple use cases.

- When device user launches Wi-Fi settings UI in device, it initiates Wi-Fi scanning to discover all surrounding networks. Users may configure the device to connect to one such network found during a scan. Using DBS, devices can scan for Wi-Fi networks in 2.4GHz and 5/6GHz in parallel, thereby reducing overall scan time by up to 40% compared to a device that does not have DBS capability. This allows users to connect to network quicker.
- When a user moves around carrying the device, it will need to roam from one AP to another when coverage deteriorates for the currently connected AP. In order to discover a better AP to connect to, the device will initiate a roaming scan. Using DBS, the device can scan in both 2.4GHz and 5/6GHz bands at the same air time in parallel, thereby reducing the total scan time during roaming by up to 37% compared to a device that does not have DBS capability. Taking a longer time to complete the scan will delay roaming and it will impact the applications that are running on the device. In voice use cases, delayed roams and more off-channel scanning instances may impact audio quality and the overall user experience.
- When a device goes through areas where Wi-Fi coverage is not present for a short time, such as moving between buildings, there will be disconnection and reconnection. In use cases where a device goes through quick disconnect/reconnect situations, reconnection can be faster by up to 26% when DBS is used, compared to a device that does not have DBS.

Devices that do not support DBS will have to scan all channels sequentially, resulting in increased total scan time and delayed connection/roam. In use cases where the current connection is no longer good for smooth flow of application traffic, lack of DBS will cause delays in moving to next AP and affecting the application that is being used at that time. For example, a VoIP application may experience breaks in audio during such instances.

Figure 1





Zebra devices intelligently use 802.11k, 802.11v and Reduced Neighbor Report (RNR) information to find out best candidate APs faster so that roaming can be completed faster. Using this information, a device can quickly detect all neighboring APs and find best candidate for roaming. With optimized use of 802.11k, 802.11v and RNR, total roam scan time will be less. Reducing the total scan time is critical when there is an active stream of traffic, as the device does not need to stay away from a connected channel for longer time. In a typical deployment where 802.11k/v is supported, a device can complete a roam scan in 75% less time compared to when 802.11k/v is not supported.

Zebra devices support Fast BSS Transition (802.11r) using Over-the-Air and Over-the-DS methods. With FT Over-the-DS roam, roam time improves by 5% which results in a better user experience, especially in use cases such as Voice.

Band Preference in 2.4-GHz and 5GHz Ecosystems

Wi-Fi networks are typically deployed in 2.4GHz and 5GHz when legacy Wi-Fi infrastructure is used. Some deployments use a 2.4GHz band for a better range or for supporting older Wi-Fi client devices that support only 2.4GHz. Wi-Fi in the 2.4GHz band can have interferences due to guest networks and from other technologies like Bluetooth. Also, there are only three non-overlapping channels in 2.4GHz resulting in co-channel interferences in the deployment. Wi-Fi performance will be constrained in 2.4GHz due to all these factors.

If an Enterprise network is available in both 2.4GHz and 5GHz bands, client devices should use the 5GHz network for performance reasons. The 5GHz band is less noisy and supports higher data rates. The 2.4GHz network may appear stronger compared to 5GHz network due to factors such as frequency band and transmit power differences. However, even if 2.4GHz shows better signal strength, client devices should prefer 5GHz if 5GHz network quality is good, as it can provide better network performance. Zebra devices support a Band Preference feature, which allows the device to choose the 5GHz band during initial connection and roam. The decision to select a band occurs by evaluating multiple parameters so that the device chooses a better network with less congestion. Zebra devices make intelligent decisions with the goal of improving the network traffic conditions.

This is based on multiple Wi-Fi parameters to remain or move to 5GHz networks in areas where 2.4GHz network may seem like the stronger available network , but is not necessarily the right network to which to connect.

When comparing a 2.4GHz deployment with 20MHz bandwidth to a 5GHz deployment with 40MHz bandwidth, the 5GHz network can yield almost 125% more throughput compared to the 2.4GHz. Considering a use case where the signal seen by the device in 5GHz is -62dBm and that in 2.4GHz is -52dBm, devices that do not have the band preference optimizations will select the 2.4GHz band resulting in a significantly lower performance.

Zebra devices use the optimized band preference feature that allows it to be on 5GHz band as much as possible when quality criteria are met. Similarly, for other use cases such as voice, Zebra devices with this optimization have lower jitter and packet loss compared to devices that do not have this optimization.

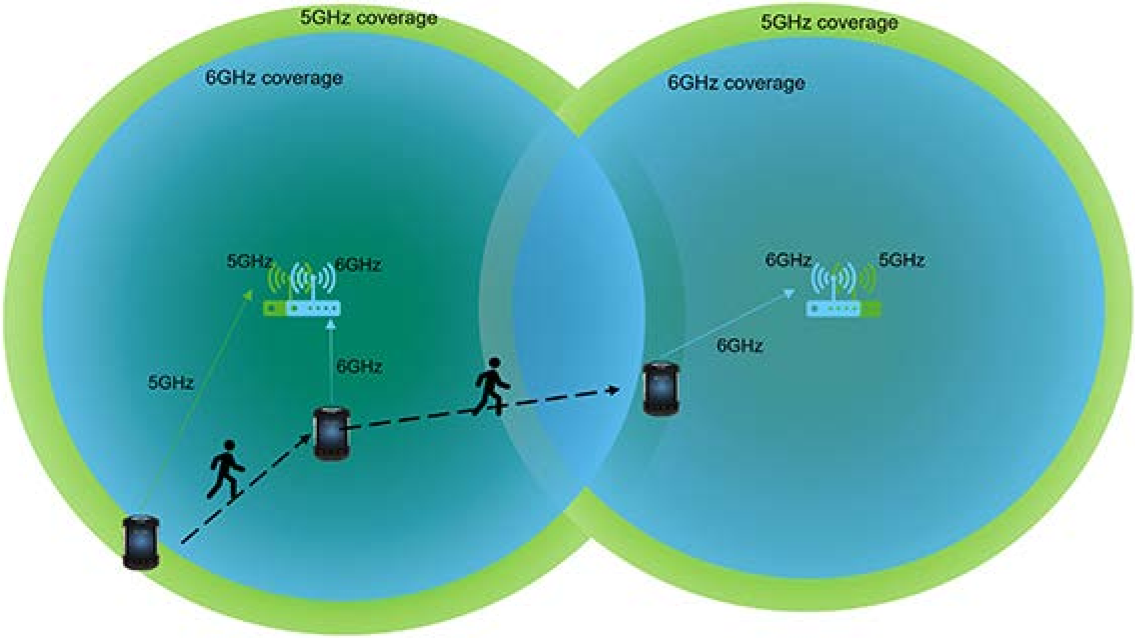
Band Preferences in Wi-Fi 6E Ecosystem

In co-located multiband deployments, 2.4GHz and 5GHz networks may show better RSSI compared to 6GHz band in some places due to factors such as differences in transmit power. RSSI for a 6GHz network may appear lower compared to 2.4/5GHz network as AP in 6GHz may be transmitting beacons and probe responses in a lower transmit power in 20MHz bandwidth. Despite that, 6GHz supported client devices should ideally prefer the 6GHz band since it has cleaner channels and can support higher bandwidth for enhanced performance. By default, Zebra devices will prefer 6GHz over 2.4/5GHz up to a certain coverage level.

When a device moves from one area to another, signal strength for the connection degrades and the device will have to search for a better AP to which to roam. In some cases, legacy band APs might show better RSSI than 6GHz band AP due to frequency and transmit power differences. Even if the 6GHz AP RSSI is slightly lower than legacy band APs, it can still be a better candidate for roam if all parameters for a stable connection are considered. Zebra devices evaluate the candidate APs based on RSSI and other parameters so that device always stays in 6GHz band.

With the arrival of Wi-Fi 6E, it is expected that enterprises will modify network layout such that corporate network is present in both 2.4/5GHz and 6GHz bands. Legacy clients will use 2.4/5GHz band for connectivity and Wi-Fi 6E clients can utilize the 6GHz band for an improved connectivity experience. When a client device enters a coverage area, band preference capability of Zebra devices makes sure that 6GHz-capable devices get connected in the 6GHz band and continue to stay in the same band when the device moves around within the coverage area.

Figure 2



Device entering coverage area of 5GHz/6GHz network, and then roaming to another AP. This is for illustrating the 6GHz band preference feature. In real deployments, actual coverage area may not be circular.

When comparing a 5GHz deployment with 20MHz bandwidth to a 6GHz deployment with 80MHz bandwidth, the 6GHz network yields almost 275% more throughput compared to the 5GHz. Regarding a use case where the signal seen by the device in 6GHz is -62dBm, and when in 5GHz is -52dBm, devices that do not have the band preference optimizations will select 5GHz band resulting in a significantly lower performance. Zebra devices use the optimized band preference feature that allows it to be on 6GHz band as much as possible when quality criteria are met. Similarly, for other use cases such as Voice, Zebra devices with this optimization will have lower jitter and packet loss compared to devices that do not have this optimization.

Additional Benefits of Wi-Fi 6E

Wi-Fi 6E is an extension of Wi-Fi 6, enabling the operation of Wi-Fi features in the 6GHz band in addition to the existing 2.4GHz and 5GHz bands. The 6GHz frequency band provides additional spectrum to increase the efficiency and performance for the growing density needs of Wi-Fi devices.

The 6GHz radio band provides greater capacity and better performance, coupled with higher data rates and low delays, to create a better overall user experience. In addition to the existing features available under Wi-Fi 6 standard (such as Uplink/Downlink MU-MIMO, OFDMA and TWT), Wi-Fi 6E supports multiple BSSID functionality, Reduced Neighbor Report (RNR), a greater number of channels, and wider channels.

The combined benefits of the Wi-Fi 6E features, used in the additional spectrum, boost an application's performance and quality in enterprise use-cases. This occurs while the connected device is roaming around in dynamic Wi-Fi environments, such as Retail, Healthcare, Education, Manufacturing and Warehousing.

Channel Width

The 6GHz band provides additional spectrum (1200MHz in US), which can be used for deploying high quality Enterprise Wi-Fi networks. Spectrum availability may vary across regulatory domains. For the list of countries that have enabled the 6GHz band and the specific approved sub-bands, please go to wi-fi.org/countries-enabling-wi-fi-6e.

In the United States, the 6GHz band can support the following channels:

- 59 20MHz channels
- 29 40MHz channels
- 14 80MHz channels
- 7 160MHz channels

Due to the availability of a larger number of wider channels (80MHz and 160MHz bandwidths) in 6GHz band, administrators can deploy Enterprise WLAN networks in the 6GHz band that use the wider channels for better user experience. The larger number of channels in 6GHz gives flexibility to the network administrators to design the network layout without constraints.

Preferred Scanning Channels (PSC)

The 6GHz band supports 59 20MHz channels. It is time-consuming for client devices to scan all these channels to discover APs for connection. To speed up the discovery process, every fourth channel in the 6GHz band is classified as Preferred Scanning Channel (PSC). WLAN APs are expected to beacon in PSC channels for faster discovery. As part of discovery during initial connection or roam, client devices scan in all PSC channels, which is also known as in-band discovery.

When enabled, Fast Initial Link Setup (FILS) announcements and Unsolicited Probe Responses transmit mini-beacons every 20ms. Client devices can wait for 20ms to receive these frames from all APs to decide whether any of the APs are suitable for connection.

Networks can also be discovered using out-of-band discovery, mainly by looking at the Reduced Neighbor Report Information Element sent by multiband APs as part of its beacon in legacy bands.

Zebra devices use both in-band and out-of-band discovery methods to find out the suitable AP for connection, as well to increase roaming speed.

6E Multi-BSSID

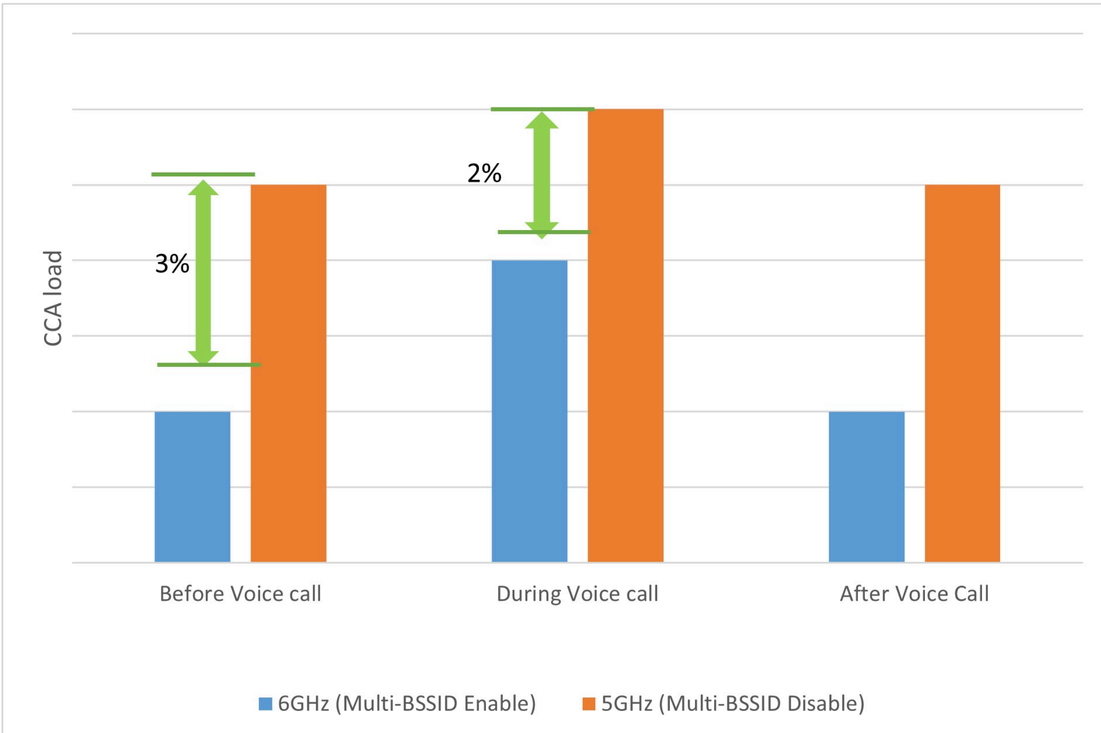
Multi-BSSID (MBSSID) was originally specified in the IEEE 802.11v and is a mandatory 802.11ax feature for Wi-Fi 6E-capable APs. This feature broadcasts information for multiple BSSIDs within a single beacon or probe response frame, instead of multiple beacons or probe response frames, for each corresponding single BSSID. This reduces the RF interference and overhead on air as the APs broadcast fewer beacons and probe responses. While the feature aims to reduce RF utilization and interference, this does not necessarily mean that the WLAN vendor configuration allows a higher number of SSIDs in the deployment.

A big factor to consider regarding MBSSID is Clear Channel Assessment (CCA). CCA is a physical carrier-sensing technique used in wireless networks for channel sensing as part of their medium access mechanism. When a Wi-Fi station performs a physical carrier sense, it listens to the channel to identify if the channel is occupied with any other RF transmissions.

While CCA itself is implemented at the PHY layer, the primary impact of its performance is on MAC metrics such as throughput, latency, and power efficiency. Higher CCA increases Wi-Fi clients channel contention time to send and receive data on the negotiated channels which affects Wi-Fi Clients performance in terms of lower throughput, high latency, packet loss, and more power consumption. Therefore, Zebra recommends using Multi-BSSIDs in the WLAN.

Figure 3 depicts the Air Medium Consumption Level measured by CCA load and affected by Multi-BSSID Beacons that are enabled in the 6GHz network, compared to the 5GHz network which does not support this feature. Furthermore, it compares the levels in different traffic scenarios of before, during, and after voice calls. In the following example, the 6GHz and 5GHz networks are configured with 6 BSSIDs.

Figure 3 CCA Load Level Multi-BSSID Enable vs. Disable in Different Traffic Scenarios



Stable Quality for Voice and Latency-Sensitive Applications

This section depicts the ways that device Wi-Fi technologies and features specifically contribute to quality of Latency-Sensitive (a.k.a. Delay-sensitive) Applications over the Wi-Fi connection.

Use Cases and Ecosystems of Wi-Fi Applications

A flawless user experience of latency-sensitive applications, such as Voice and Video Streaming and Conferencing over the Wi-Fi, is a primary expectation in most enterprise network venues. In almost any deployment there is at least one application which users frequently interact with for purposes of live communication with other staff members, remote customer support, productivity, and urgent communication tasks.

At a mass scale of highly mobile ecosystems, the expectation of a flawless experience is contextualized in two levels: First, in the individual context of how any user might need to roam around while using the application. Second, in the high-capacity context of how multiple users might need to use applications at the same place and time, expecting the individual experience to remain intact.

Some examples as depicted by Voice Applications scenarios:

- User (retail associate, healthcare nurse) is in a call with a remote peer or customer/patient, and during the call the user is:
  - Roaming, normally between different areas and hallways of the building.
  - Needing to run quickly between patient rooms.
  - Asked to take the elevator or staircases to get something from the basement floor.
  - Walking between high metal shelves of store or warehouse to locate merchandise.
  - Walking outside to a garden center or backyard.
  - Walking to the parking lot to get something from the car.
  - Helping another customer to load or unload merchandise to the truck.
  - Entering and exiting secluded back-rooms or refrigerator areas
- 10-20 users sitting inside a room, each talking on the phone individually and using headsets (separate call or conferencing).
- 10-20 users moving around sporadically while in individual calls, and temporarily cross each other path or congregate in the same area (for example, same patient room, same elevator, or same store aisle corner).

Orthogonal Frequency-division Multiple Access (OFDMA)

The OFDMA is the main contributing technology to achieve consistent quality in the above scenarios.

Latency-sensitive traffic takes advantage of the OFDMA Uplink and Downlink technologies of the 802.11ax, which is supported with Wi-Fi6 standard on 2.4GHz & 5GHz bands, and with Wi-Fi6E on the 6GHz. In most deployments where 6GHz is supported, the channel serving the connected devices of the latency-sensitive apps is using 80MHz channel width. On the 2.4GHz & 5GHz bands, most deployments use 20MHz width to support latency-sensitive apps.

Given that streaming traffic uses a relatively small Resource Unit (RU) Tones of the OFDMA, there is a likelihood that multiple separate subcarriers are utilized in accessing the medium without any contention, able to efficiently fill vacancies of the spectrum.

The efficiency of the OFDMA allows the ecosystem to support a larger capacity of such applications, while keeping the traffic performance intact and maintaining the stable performance with lower jitter, latency, and packet loss for all the connected devices. Without OFDMA, a lower density of connected devices can maintain good quality.

Benefits of Wi-Fi 6E

In addition to the benefits of having OFDMA versus not having it, the application benefits greatly from connectivity with OFDMA over Wi-Fi6E WLAN supporting the 6GHz, compared to connectivity with OFDMA over Wi-Fi6 WLAN without 6GHz. Using Wi-Fi6E/6GHz improves the user experience in any scenario and especially in ecosystems which include higher density and large number of users and application sessions.

Channel Width Wi-Fi 6E

For examples of latency-sensitive deployments, consider the following voice scenarios:

In one scenario, multiple Zebra Wi-Fi6E-capable devices are connected to a 6GHz channel, and while most of those devices handle ongoing voice calls, some others handle background traffic of data applications. In this situation, the advantage of the default deployment of 6GHz using 80MHz bandwidth allows for significantly more ongoing voice calls to maintain consistently lower jitter and latency, and a consistently high level of MOS values overall, without degradation across all devices, compared to a bandwidth of 20MHz.

Figure 4 depicts an 80MHz width with packet jitter remaining consistently low with an increasing number of voice clients.

Figure 4

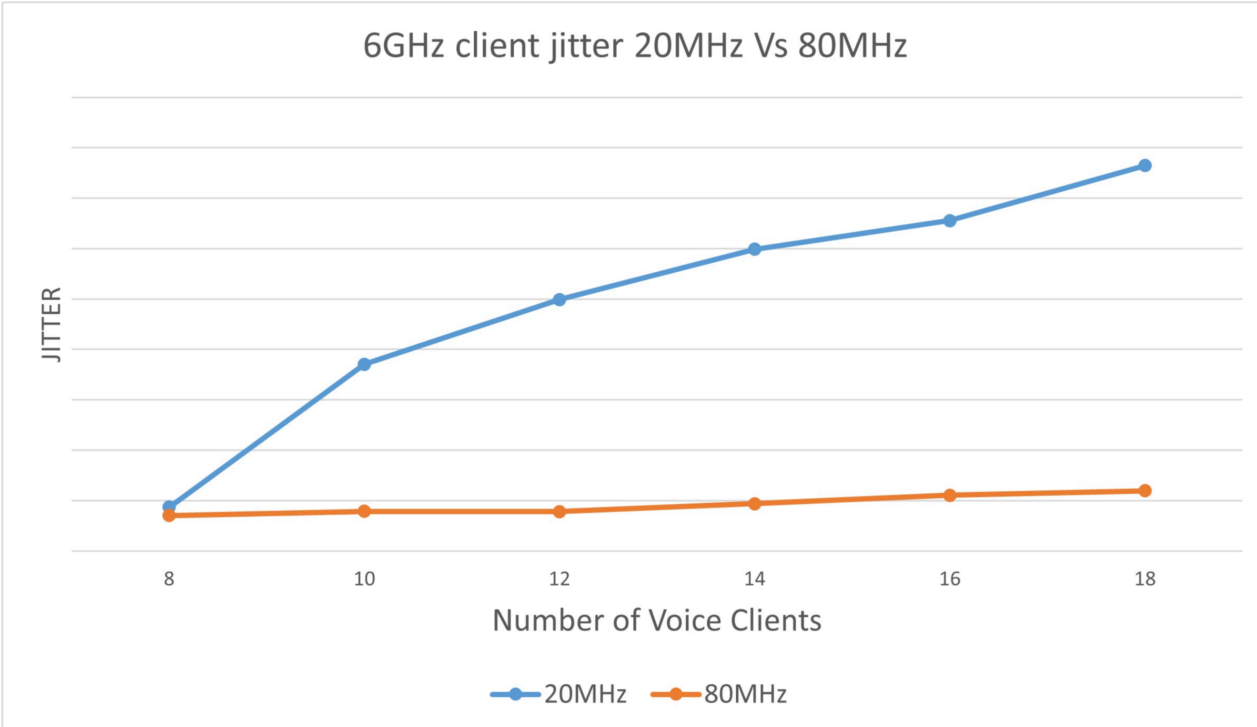
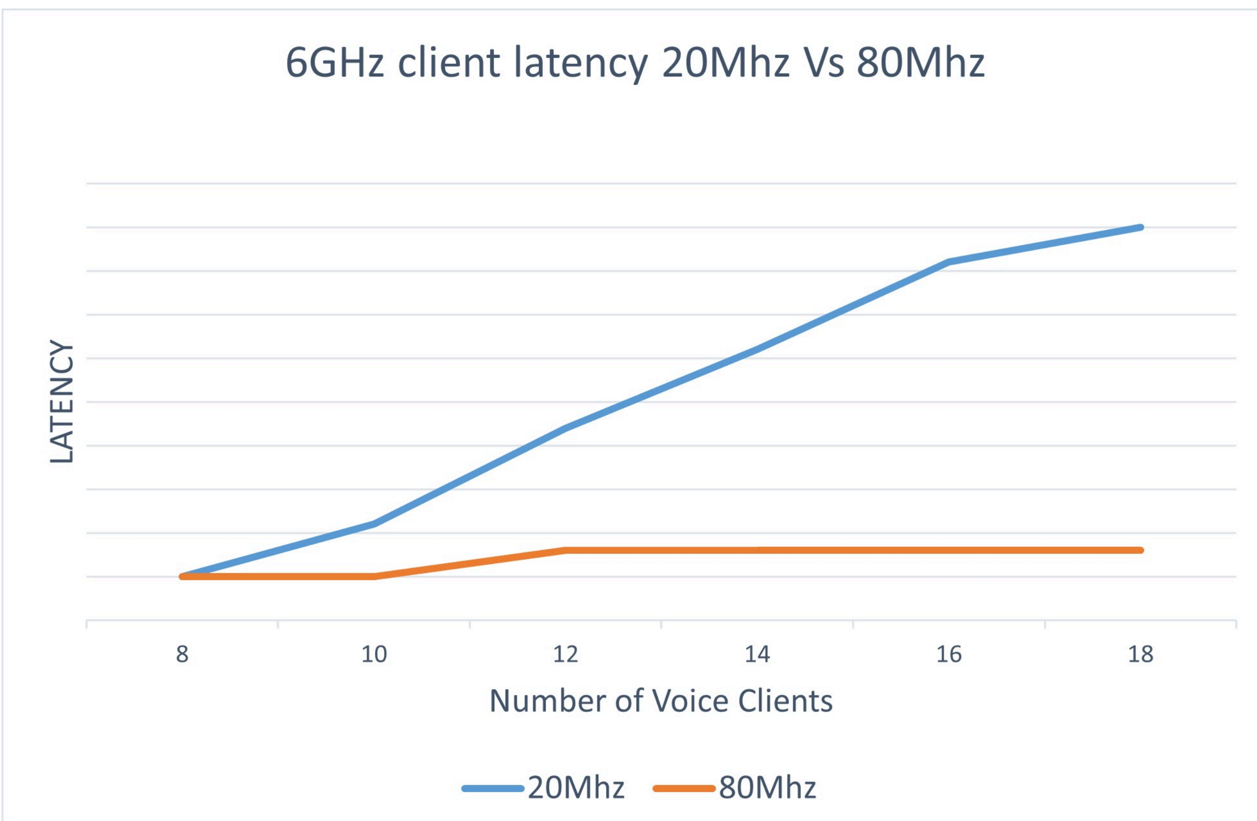


Figure 5 depicts 80MHz width with packet latency remaining consistently low, with an increasing number of Voice Clients.

Figure 5

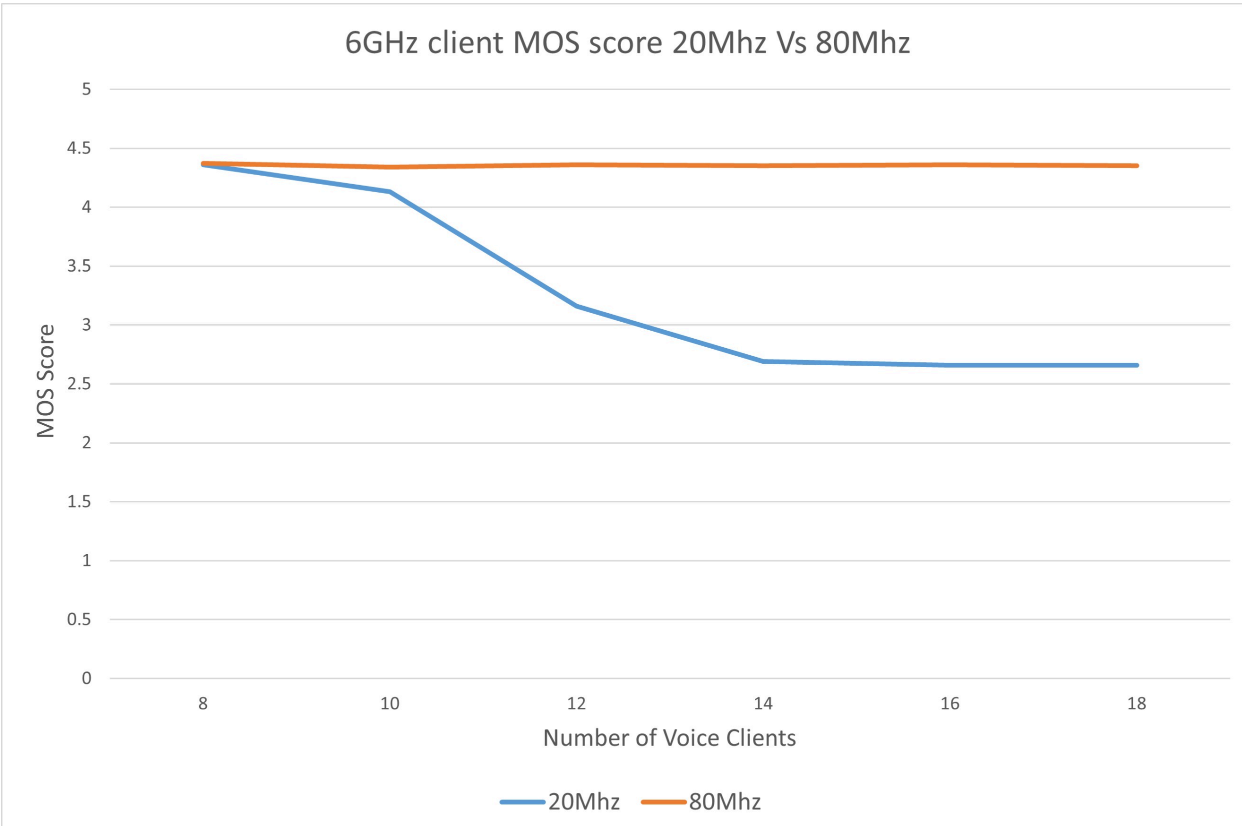


The following chart depicts 80MHz width with Mean Opinion Score (MOS) values remaining consistently high with an increasing number of voice clients

NOTE: In most Voice Application MOS scales, a value of 4.3 and above is considered Excellent, between 4 and 4.3 is Good, and anything below 4 yields noticeable impact to the user experience and is considered Fair, Poor, or Bad.

As shown in Figure 6, in the 80MHz plot the average MOS value for each given number of voice calls remains consistently Excellent as the number of calls increase. Conversely, in the 20MHz plot, the average MOS value is Excellent in up to eight calls before decreasing to Good over ten calls, and further degrading to “Poor” and “Bad” when the number of calls exceeds ten.

Figure 6



In another deployment scenario, a voice solution is deployed on a mixed fleet of device types at the same venue; some are Zebra’s Wi-Fi6E-capable devices and others are Wi-Fi5-capable or older, which do not support Wi-Fi6/6E and therefore are not OFDMA-capable.

At certain times and places in the venue, where the 6GHz coverage is either insufficient or not supported by the WLAN at all, the Zebra Wi-Fi6E-capable devices are connected to the 5GHz coverage that is also used by the Wi-Fi5 devices. Those Wi-Fi5 devices either run Voice Calls at the same time or any data application. Overall, all traffic over 5GHz of all connected devices with same AP is used over a 20MHz width of the channel.

At other times, if 6GHz is supported by the WLAN and its coverage is sufficient, the Zebra Wi-Fi6E-capable devices are connected to the 6GHz coverage. In this scenario, the Wi-Fi6E-capable devices facilitate their voice calls on the 6GHz/80MHz while the Wi-Fi5-capable devices facilitate their voice calls or data applications on the 5GHz/20MHz.

In this mixed fleet scenario, it is expected that if and where 6GHz WLAN is supported, the Zebra Wi-Fi6E-capable devices will maintain performance as depicted in the previous charts 80MHz orange plot.

Performance for High Throughput Applications

This section depicts the ways that device Wi-Fi technologies and features specifically contribute to the performance of High Throughput Applications over the Wi-Fi connection.

Use Cases and Ecosystems of Applications for Wi-Fi 6E

Enterprise WLAN deployments strive to provide a readily available network bandwidth for as many connected devices as possible, some of which are used for high throughput congesting applications. It is important to keep in mind that bandwidth and throughput are strongly related but are not the same thing. The relationship between them is commonly depicted as an analogy of relationship between a pipe (bandwidth) and water (throughput) flowing through the pipe: the larger the pipe, the more water can flow through it at one time. What matters for the pipe is how large it can be so it is ready to accommodate as much water at a given time, whereas what matters for the water is how quickly it can flow (speed) until it reaches its destination, given that the pipe can be unpredictably saturated.

At a mass scale, the expectation of high throughput is contextualized at two levels: First, in the individual context of a given application data-pumping task (in any traffic direction or both), it needs to finish as soon as possible. This is pure speed and time lapse expectation. Second, in the high capacity context of multiple devices which might need to use the same data-pumping applications at the same place and time. This is an expectation of how the aggregated traffic in the network can be used over the multiple devices connections.

Examples of use cases:

- Video is evolving into Virtual and Augmented Reality (VR and AR) and Imaging Overlays. Some AR and VR applications which need to render video in High Definition (HD) need to be served by effective throughput of 100-400 Mbps on a specific connected device.
- Retail associates and healthcare staff send and receive large files during customer support face-to-face sessions (for example, shopper records, how-to clips, and medical records).
- The above cases are performed in congregation in the help desk area, same shopping aisle, etc.
- Devices in maintenance period, going through Over The Air (OTA) OS Upgrade, which is a download of approximately 1.5G file. Customers expect the start-to-finish OS Upgrade time to be as short as possible.

Data Rate Speeds

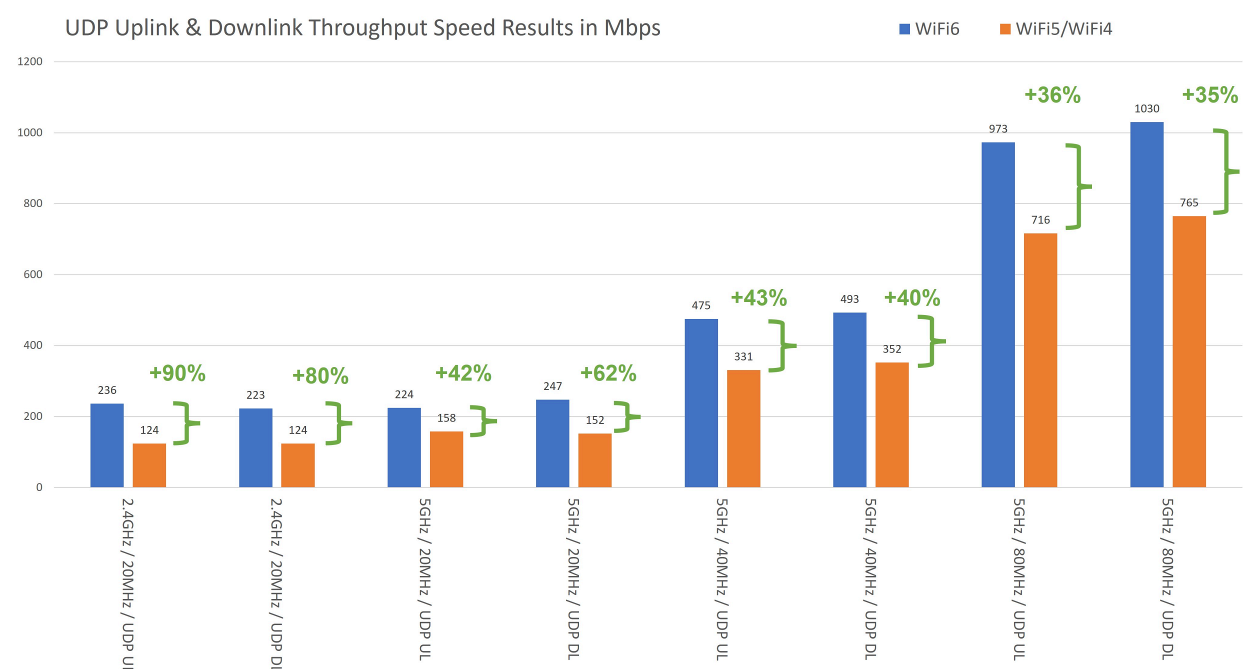
Since the introduction of 802.11ax specifications, ecosystems with connectivity over Wi-Fi6 or Wi-Fi6E benefit from the following major technology improvements related to Data Rates:

- **Longer Symbol:** The increased number of OFDM subcarriers is expected to contribute ~20% efficiency boost to throughput in all bands and channel width combinations, compared to respective deployments prior to 802.11ax.
- **QAM:** Adding 1024 QAM in 802.11ax in code-rate 3/4 (MCS10) and 5/6 (MCS11), together with utilizing the OFDM longer symbol efficiency boost, is expected to yield an overall improvement of ~35-60% higher speed compared to 256 QAM of 802.11ac/Wi-Fi5 (5GHz) , and almost double the speed compared to 64 QAM of 11n/Wi-Fi4 (2.4GHz). It is expected that in reasonably good RF conditions of the deployment, the 1024 QAM will be used for transmission of most of the traffic.
- The larger the amount of modulated bits is in the constellation of the QAM quadrants, as in the 1024 compared to 256 QAM, the more it is susceptible to interfering noise which might suppress the modulation. For this reason, it is expected that 1024 QAM is more successful and consistent in the cleaner 6GHz band.

The data rate technology improvements described above are main contributors to fulfilling the use case examples in Use Cases and Ecosystems of Applications for Wi-Fi 6E on page 13, providing larger bandwidth and higher speed in the more throughput-thirsty applications.

To demonstrate the expected improvements, Figure 7 depicts speed (Mbps) results in 5GHz and 2.4GHz channel width combinations, where the 802.11ax/Wi-Fi6 and pre-802.11ax/Wi-Fi6 are side-by-side in the same setting. Note that the same settings comparison cannot be depicted for 6GHz as it is not backwards compatible to 11ac/11n.

Figure 7



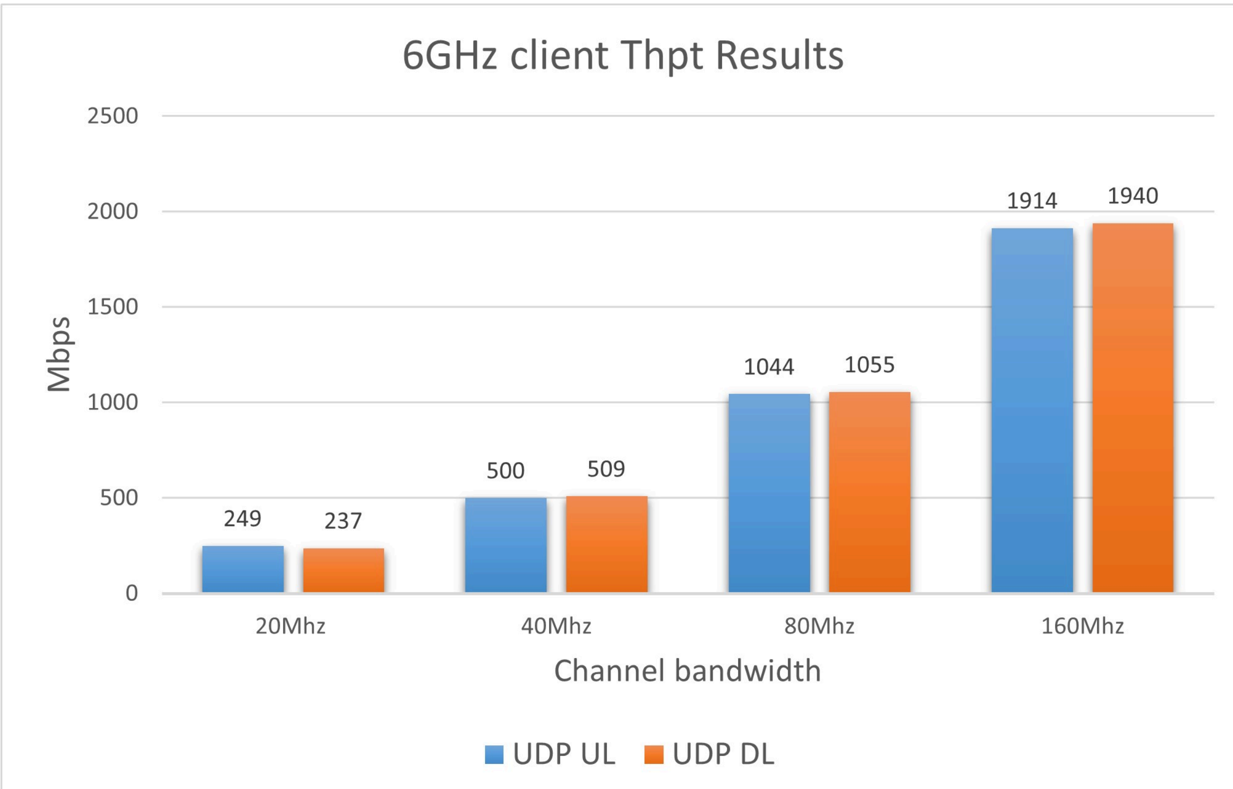
Additional Benefits of Wi-Fi 6E

Channel Width for Wi-Fi 6E

The common practice in the industry, as well as Zebra's recommendation, is to deploy 6GHz with 80MHz, as it is best suited for all the variations of Enterprise Application types, use cases, and wide, well-balanced coverage.

Figure 8 depicts an example of throughput results over 6GHz in different channel widths. The differences reflect the ways that the 802.11ax takes advantage of the width, while the sub-technologies in effect are identical. As shown, with each one step of doubling the width size, the speed (Mbps) doubles.

Figure 8



MU-MIMO

This section describes how Multiuser (MU) MIMO allows an AP to transmit and receive traffic with multiple connected devices simultaneously.

MU-MIMO lets the AP manage the multiuser traffic in separate simultaneous lanes, where each is dedicated to a connected device at any given time, not logically separated to traffic timing and sizes. Unlike OFDMA, the MU-MIMO does not split the channel into independent subcarriers of the spectrum in which each does not contend with others, thus able to fill unused vacancies in the spectrum. Rather, MU-MIMO is very effective in scenarios where multiple users/devices all need to receive and transmit full buffers of traffic with all connected devices without any time-gaps in between, such as during high throughput applications by all the participating users.

The MU-MIMO's relative gain and effectiveness during high throughput of multiuser traffic, compared to without MU-MIMO, largely depends on the following factors:

- How far apart devices are from each other during the time that high-throughput traffic is in effect with all of them. The farther apart they are, the more MU-MIMO efficiency can be accomplished within the given bandwidth.
- The AP execution of the Multiuser connections. This is a combination of AP's hardware dependencies, such as MIMO capabilities (4x4, 8x8), and the AP's concurrency of the connections over the MIMO. For example:
    - AP with 8x8 MIMO can have peak MU-efficiency supporting four concurrent devices with 2x2 MIMO.
    - AP with 4x4 MIMO can have peak MU-eficiency supporting two concurrent devices with 2x2 MIMO.

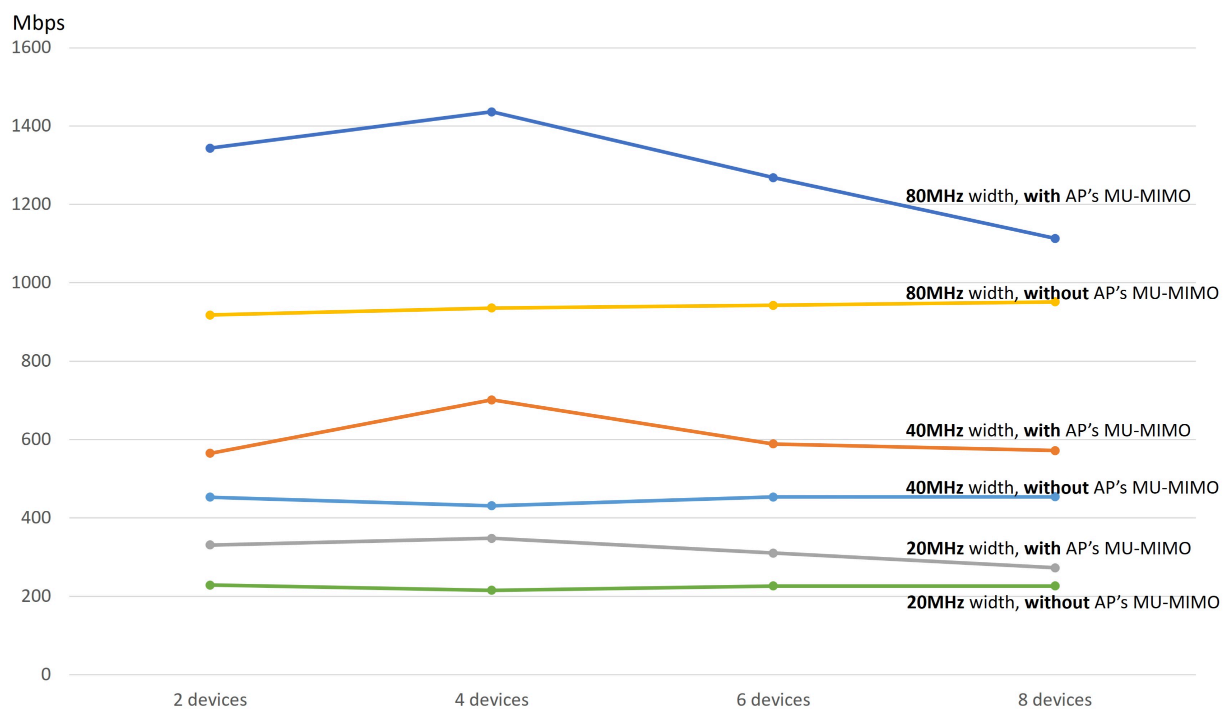
If larger number of devices participate in full buffers scenario beyond the peak-efficiency, the pure relative gain may diminish.

The MU-MIMO effectiveness improvements described above are main contributors to fulfilling the use case examples in Use Cases and Ecosystems of Applications for Wi-Fi 6E on page 13.

MU-MIMO in the 6GHz ecosystem greatly benefits from the recommended channel widths of 80MHz, in the sense that the 80MHz is efficient for both the MU-MIMO type of multiuser applications as well as OFDMA type of multiuser applications. Compare this to ecosystems of the 2.4GHz band, which typically is 20MHz only for all applications, and 5GHz band, which typically is 20MHz if it needs to support latency-sensitive applications.

Figure 9 depicts test results of multiuser aggregated downlink speed in Mbps unit for given number of participating devices. The tests are conducted in single AP environment, during either AP's MU-MIMO operations or AP's non MU-MIMO operations, for each of the three AP channel widths settings: 20MHz, 40MHz and 80MHz. The relative gain of speed of AP's MU-MIMO operations is ~50% in each of the three different channel widths.

Figure 9



Security

This section details the recent Wi-Fi Security technologies of WPA3 and Enhanced-Open (EO).

Deployment Use Cases

Zebra Wi-Fi6E-capable devices might be deployed in non-6E WLAN systems with WPA3 and/or Enhanced Open, in which case the WLAN system is likely enabling WPA3 and/or Enhanced Open Transition mode of the respective connectivity, Enterprise, Personal, or Open. This is so the SSID can support WPA3-capable and WPA2-capable devices at the same time. Non-6E WLAN systems may also choose to enable specifically dedicated SSIDs with WPA3 or Enhanced Open only mode, to not allow WPA2 and open connections.

In Wi-Fi6E WLAN, connection on the 6GHz band must use WPA3 or Enhanced Open only. 6GHz does not support WPA2 and open connections. Therefore, it is expected that the Wi-Fi6E WLAN system which enables co-located SSID, for example, SSID on 5GHz+6GHz or 2.4GHz+6GHz or 2.4GHz+5GHz+6GHz, the same SSID will have properties of: WPA3 or Enhanced Open only mode on the 6GHz, and WPA3 or Enhanced Open transition mode on the other bands, where the respective security configuration of the SSID/WPA3 is the same across all bands. In such cases, the Zebra Wi-Fi6E-capable devices will normally connect and roam with WPA3 across all the enabled bands.

WPA3 Enterprise

WPA3-Enterprise is based on WPA2-Enterprise with the additional requirement of using Protected Management Frames (PMF) for WPA3 connections. It also adds support for stronger hash algorithm SHA-256 for deriving the keys while using the 802.1X authentication and the AES-CCMP-128 cipher. WPA3 Enterprise 192-bit mode offers increased security in enterprise networks. It uses EAP-TLS (certificate-based authentication) with elliptic curve certificates, SHA-384 hash algorithm for key derivation, and GCMP-256 cipher, which is a more efficient AES algorithm and uses longer key size than AES-CCMP-128.

Radius server and certificate requirements for WPA3 192Bit mode:

- WPA3-Enterprise 192-bit Mode requires a supported EAP servers like Cisco ISE (Identity service Engine) and Aruba CPPM (Clearpass policy manager) which requires 802.1X Authentication type as TLS EAP (EAP-TLS).
- Supported 192bit cipher suites:
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

- The current certificate generation mechanisms (Windows 2019 CA) support RSA key sizes of 512, 1024, 2048, 4096, 8192 and 16384. 192-bit requires the use of RSA certificates with the key size >= 3072 bits. Therefore, while generating the certs use 4096 key size certs.

WPA3 Personal

WPA3 Personal uses the Simultaneous Authentication of Equals (SAE) protocol with PMF required, replacing WPA2 Personal with Pre-shared Key (PSK). WPA3 SAE provides more reliable password-based authentication and is resistant to offline dictionary attacks. SAE authentication uses both H2E and HnP methods to obtain the PWE (password element) from passwords. Zebra clients supports both H2E and HnP, however in 6GHz networks, HnP is disallowed and only H2E is allowed. H2E is mandatory for WPA3 certification in 6 GHz band. SAE and SAE FT AKM's are supported by Zebra client.

Enhanced Open

Prior to the introduction of the Enhanced Open security method, network ecosystems that had challenges supporting Passphrase Management architecture, such as Captive-Portal systems, had to choose between either staying open and completely unsecure, or minimally enabling WPA2-PSK, which could de-stabilize the system. Since the introduction of Enhanced Open based on the Opportunistic Wireless Encryption (OWE) standard, those systems can choose to use Enhanced Open, which has more robust security than publicly sharing passphrase for WPA2-PSK. It is a better fit for architecture lacking Passphrase-Management. This mode uses OWE protocol, which is defined in the IETF document RFC 8110. OWE provides AES(CCMP128) encryption for data privacy, and PMF is required.

Supported WPA3 Combinations in Priority Order

Zebra devices support various security methods and roaming protocols. Preference is always given to stronger security and faster roam performance. For example, stronger cipher such as GCMP-256 is preferred over AES-CCMP-128, SuiteB-192-bit protocol is preferred over 802.1X or SAE, and Fast BSS Transition is preferred over PMK Caching or OKC. The following table illustrates the Zebra recommendation for selecting the security and roaming settings for a secure and high performance wireless network.

Protocol	AKM	Encryption	Default Config	Supported Config	Recommended for Co-located Environment
WPA3 Enterprise	SuiteB-192 FT	GCMP 256	Enabled	FT	FT
WPA3 Enterprise	FT 802.1x	AES-CCMP 128	Enabled	FT	FT
WPA3 Personal	SAE FT	AES-CCMP 128	Enabled	SAE H2E	SAE H2E
WPA3 Enterprise	SuiteB-192	GCMP 256	Enabled	PMKID	PMKID
WPA3 Enterprise	802.1x-SHA256	AES-CCMP 128	Enabled	OKC	OKC
WPA3 Personal	SAE	AES-CCMP 128	Enabled	SAE H2E	SAE H2E

Protocol	AKM	Encryption	Default Config	Supported Config	Recommended for Co-located Environment
Enhanced Open	OWE	AES-CCMP 128	Enabled	OWE	As default

Devices which do not support FT (802.11r) protocol for faster roam performance, but must keep same level or increase security, are impacting and degrading the performance of application traffic and user experience during roams.

Zebra devices support FT over the Air and FT over the DS authentication mechanisms for both WPA3 personal and WPA3 enterprise modes. FT Over DS provides 5% faster roam times which benefits user experience, especially for media applications such as voice and video. Zebra devices will automatically prioritize Over DS.

Wi-Fi Locationing: 802-11mc Fine Time Measurements (FTM)

This section depicts Wi-Fi FTM Locationing enterprise use cases and the Zebra device capabilities fulfilling them.

Locationing Use Cases

In many cases, Enterprise Applications strive to support use cases of Indoor Navigation, Device Tracking, Asset Tracking, and other Location Based Services (LBS) on their Mobile Devices. For example:

- Navigation to Merchandise on a shelf in the store, show the real time path over a map.
- Find closest associate to a specific location**:** Dispatch an associate to quickly help a shopper that rings from a 'help' station in a big store. The system needs precise location of all associates and decide who is the closest.
- Track Device which is forgotten/lost by an associate on high shelves, fork lifts, etc.
- Record exactly where an application has an issue of service/connectivity

Using Wi-Fi FTM Locationing for those use cases delivers on two major standardized points:

- Sub-meter accuracy based on time of flight Round Trip Time (RTT) protocol, which yields precise distance between two involved FTM-capable entries (for example, Device and AP), and replacing older sensory-based technologies like RSSI.
- Leveraging on the ubiquity of Wi-Fi networks; does not require a separate infrastructure.

Ecosystem of FTM-capable Devices

Since Zebra's Wi-Fi6E devices are all FTM-capable, the native Android offers to applications to integrate the 802.11mc RTT technology, which is accessible through the Google Wi-Fi RTT Service APIs. The application utilizes these base APIs to manage the flows of distance measuring, then computes positioning and implements deployment techniques of correlating the real time positioning with global or local ground references.

Zebra's Wi-Fi Locationing Provider service allows Zebra devices a simple way to the enable locationing use-cases. Benefits of this service are further explained in the next section.

Applications may also choose to use the native Android Location Manager and Fused Location Services beyond the native Wi-Fi RTT Service. These additional location and fuse managers provide to applications the computed global positioning updates by incorporating Wi-Fi RSSI and other physical sensors data computations, as well as combining location data from exchanges with remote providers, including network addressing and cellular. However, those global positioning techniques do not incorporate RTT distance measuring.

Zebra Wi-Fi Locationing Provider Solution

Zebra Wi-Fi Locationing Provider is a proprietary solution, based on a proprietary API service that is an extension to the Android native APIs.

An application that integrates this solution can benefit from the following:

- The service provides computed live Location Updates, as Global or Local 3-dimentional positioning data. Applications using the service do not need to compute the positioning themselves from raw RTT distance measures. The service does this for them.
- The outcome of positioning data is within 1-meter accuracy.
- Registering with the service is via an extension to the Android Location Manager, and the Location Updates of the computed position are provided to the application in a standard position format.

Additionally, the service ensures the following device performance during FTM and Location Updates activities:

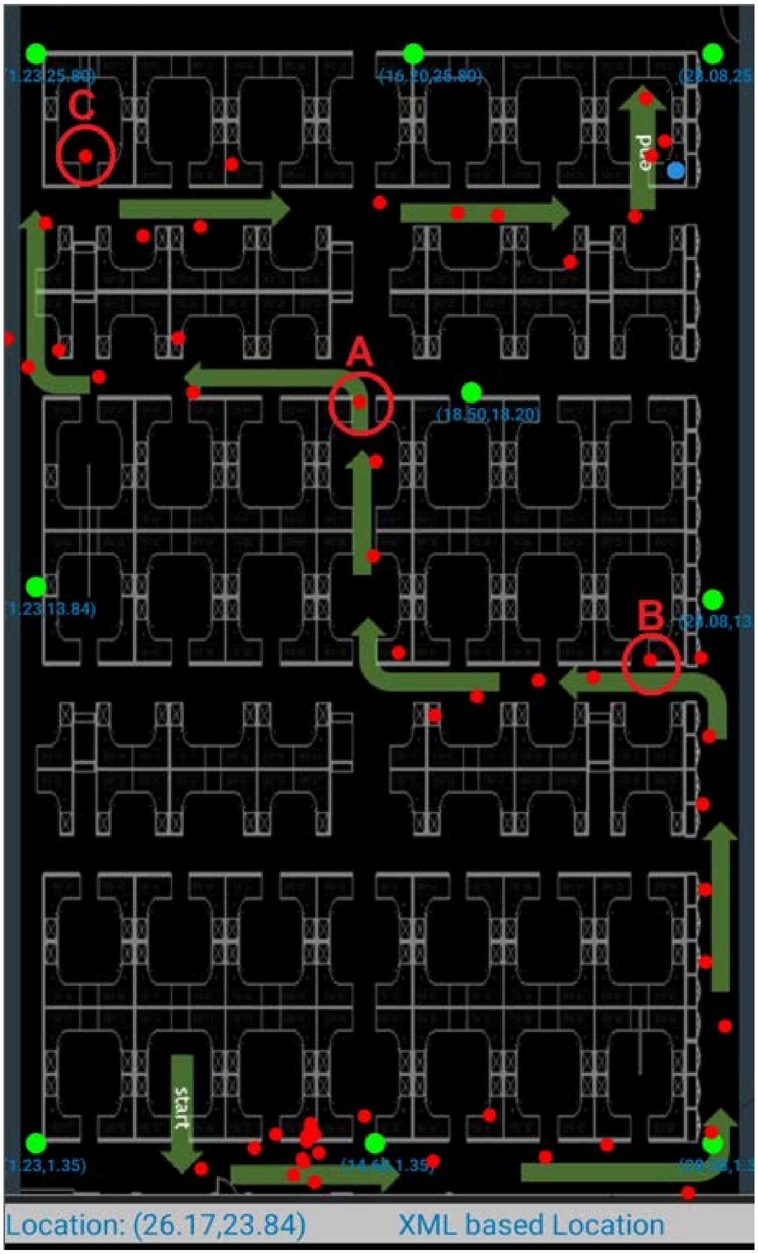
- Latency-sensitive traffic, such as Voice and Video, is not interrupted.
- High Throughput Application's Speed (Mbps) is impacted only negligibly.
- Net battery draining is negligible.

The following table depicts performance metrics of deploying FTM with using the Zebra Locationing Provider, compared to deploying FTM with using other solutions.

FTM Activities and Location Updates	Solutions using Zebra Locationing Provider	Other FTM Solutions Not Using Zebra Locationing Provider
During Voice and Video	User Experience of Audio and/or Video is not interrupted	Inconsistent. Sometimes interrupted leading to choppiness.
During High Throughput	Average reduction of speed: 1-5% Rare worst-case reduction: 10%	Average reduction of speed: 10-15% Frequent dips reductions: 20-25%
Battery Consumption	Net consumption: ~5% in 12-hours	Net consumption: ~12% in 12-hours

Figure 10 depicts an example of real-time indoor navigation Application using the Zebra location provider service.

Figure 10



The figure shows an office floor map where:

- Green dots are the 11mc-capable APs.
- Green arrows are the user's physical walking path.
- Red dots are the real-time location updates data that the Zebra location provider service provides to the application along the path.

- Circles around the red dots are drawn to highlight a few examples of deviations:
  - A is location data which deviates between 0 to 0.2 meters from the physical location.
  - B is location data which deviates between 0.3 to 0.5 meters from the physical location.
  - C is location data which deviates between 0.8 to 1 meters from the physical location.

As shown, most of the red dots deviate from the physical path similarly to A and B.

Wi-Fi and Bluetooth Analytics

This section depicts Wi-Fi and Bluetooth Analytics solutions available with Zebra devices.

Wireless Analyzer

Customers' admins can use a Wireless Analyzer (WA) application, built into the Zebra SW, to analyze the Wi-Fi and troubleshoot connectivity scenarios and issues.

The application can be at the tip of the admin's fingers or used remotely, for multiple use cases mentioned below. Overall, the WA facilitation and the analyzed data saves cumbersome and expensive handling of external tools, and with WA guaranteeing that the data is the result of the connected/deployed device experiencing the use case or issue, not an external interpretation.

Figure 11 and Figure 12 depict examples of live Roaming and Voice Analysis data of the Wireless Analyzer application, while the device is roaming around during ongoing real voice call.

Figure 11

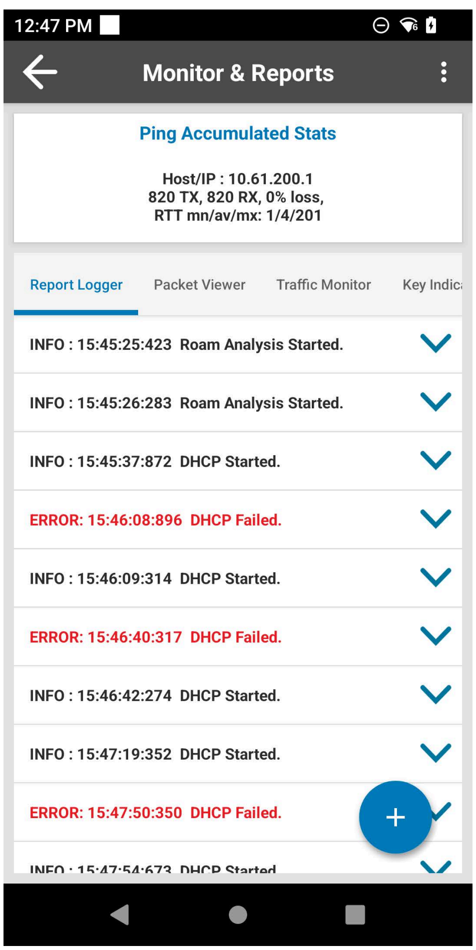
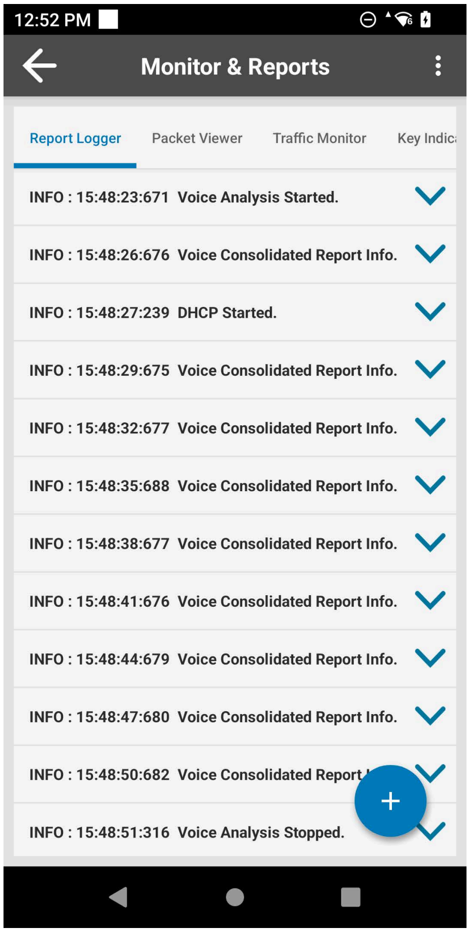


Figure 12



More screenshots and User Guide of the Wireless Analyzer product available at: zebra.com/us/en/support-downloads/software/productivity-apps/wireless-analyzer.html

Unique Use Cases and Features

Imagine that a customer WLAN deployment needs to be validated in advance for its readiness for an upcoming deployed device connectivity and for performance of prospect Voice Application installed on that same device type. In traditional practices of network validations, this effort normally entails facilitation by experts; using multiple tools, accessing restricted information, making sure the tests are conducted properly, and performing offline analysis methods for each separate networking sub-technology.

Overall, since the variables of readiness can relate to many different sub-technologies, it forces involvement of multiple technical tools & subdomain-expertise, and additional time to making sure the conclusions are 'agreeable' by all experts.   After all, it is not easy to 'agree' about readiness of 'everything'; configuration, WLAN/AP behavior, device behavior, environmental RF conditions, End-to-End parameters of the Application, etc.

In those traditional practices, the most lacking aspects of validation are the deployed-device’s internal Views, Data, and runtime Analysis. Validation might also require post-installed apparatus/tools to simulate specific Network Traffic performance such as the Voice.

This is where the Wireless Analyzer comes in. It provides several features that can be administered in the UI of the device without technical expertise for the purpose of most of the network readiness testing needs. For example, data provided by the Analysis of the Voice is viewable directly in the UI and assists in deriving immediate mitigation action if needed, without dependencies on other tools.

The following is a breakdown of additional use-cases, or granular tasks of live-network troubleshooting or network-readiness validations, mapped to Wireless Analyzer features.

- The Admin looks for immediate visibility of APs configured capabilities.
    - WA provides a Scan List feature which shows the AP's capabilities directly from 802.11 beacons.
    - Without WA, external sniffers or network tools must be facilitated and interpreted by experts.
- The Admin looks for immediate ways to view the entire WLAN Network (SSID) Coverage and the device's connectivity interactions with that environment.
    - WA provides a Coverage View feature which shows the coverage and connectivity from the device view.
    - Without WA, external Sniffers or Network tools must be facilitated and interpreted by experts, and in any case, it does not reflect a first-hand experience of the connected device.
- The Admin looks to quickly validate initial network connectivity to configured network profile.
    - WA provides a Connection Analysis feature which analyzes the underlying sub-layers of the Wi-Fi connection, IP connection, and Reachability to a designated remote IP address.
    - Without WA, external tools needed, as well as RF and Wi-Fi protocol expertise, to produce the analysis manually.
- The Admin looks to view and collect in the background the real-time data about the roaming performance, issues, and provided reasons for any failures or degradation of traffic quality.
    - WA provides a Roaming Analysis feature which detects and analyzes in the background the real-time issues, causes, and RF environmental parameters. It can be used in Passive mode without any consumption of resources, or in Active mode with additional synthetic data traffic.
    - Without WA: external tools needed, as well as RF and Wi-Fi protocol expertise, to produce the analysis manually.
- Admin looks to view and collect in the background the real-time data about voice performance, issues, and provided reasons for any failures or degradation to voice metrics (MoS, Jitter, Pkt Loss, Latency).
    - WA provides a Voice Analysis feature which detects and analyzes in the background the real-time issues and performance of voice traffic, combined with Roaming data of the Roaming Analysis feature (inclusive). In Passive mode, it detects SIP calls in runtime of the Device’s Voice applications, produces periodic quality reports about the voice traffic, and analyzes voice traffic issues such as Jitter, Packet Loss, and Latencies. In Active mode, it generates synthetic voice traffic, produces periodic quality reports about that traffic, and analyzes issues.
    - Without WA: external tools needed, as well as RF and Wi-Fi protocol expertise, to produce the analysis manually.

- The Admin looks to view and collect in the background wireless packets for troubleshooting and analysis of customer environment and configuration.
  - WA provides a Packet Capture feature which includes all 802.11 Mgmt & Data packets belong to the connected device with their local-radio parameters.
  - Without WA: external Sniffers needed with multiple Wi-Fi adapters for all desired channels, and even with that the external capture does not reflect an exact reception and transmission of the device.
- The Admin looks for immediate ways to simulate multiple Application concurrency of reachability & performance to far network segments.
  - WA provides Ping and Traceroute features. There can be 2 Pings executions, each one to different IP destination and independently configuration of ICMP parameters.
  - Without WA: one or more 3rd-party Ping-tool instances must be installed & permitted on the device to accomplish basic reachability or concurrency simulations.
- The Admin looks to control and save data during the troubleshooting session.
  - WA Analysis provides Analysis 'sessions' database management, automatic saving, and options to re-play and export sessions on the capturing device or any other Zebra device with WA.
  - Without WA, on-device basic networking applications do not provide rich data management options.

Wireless Insights

Zebra devices allow customers to write applications or use existing solutions of Zebra Partners cloud systems, to retrieve Zebra's Wi-Fi Analytics by using Zebra Wireless Insights APIs.

With a Zebra Partners Cloud Solutions, such as with HPE/Aruba UXI, Juniper/Mist Marvis, and Extreme Networks Intuitive Insights, the Wireless Insights data is further processed by the partner and enriches the dashboard by providing Zebra's Roaming and Voice Analysis data and on-demand packet capture. This gives customer admins holistic insights, which helps them expedite addressing the Wi-Fi ecosystem challenges through proactive identification of issues across locations and uncover the root cause to maintain network stability and worker productivity.

- Actionable Insights with rich telemetry data from the network and Zebra client across the fleet.
- Correlation of network and client events to easily identify root cause.
- Pinpoint the exact location of performance degradation.

Zebra Partnerships Examples Using Wireless Insights Data

Figure 13 is an example of a specific drilled down device view from HPE/Aruba UXI Dashboard.

In this example, the user is in Voice Call on the Zebra device while walking (roaming). The UXI view depicts a period in which the device went through 5 Roam failed instances, all of them RESOLVED. The view can be further drilled down to see the Reason Code root cause information of each of the Roam failed instances, and they can get correlated to the ROAM COMPLETED WITH RETRY view.

During the same viewing period, but after all the roam failed instances, there were 26 voice call warning events, each of them can be further drilled down to see the granular metrics; MOS, Packet-Loss, Latency and Jitter, as well as the Reason Code root cause information leading to the indicated metrics.

In this situation, the system was further correlating the voice-specific metrics with periods in which the Wi-Fi had no degradation at all. Therefore, the actionable item for the administrator in this case was to focus on other non-Wi-Fi components of the network.

Figure 13

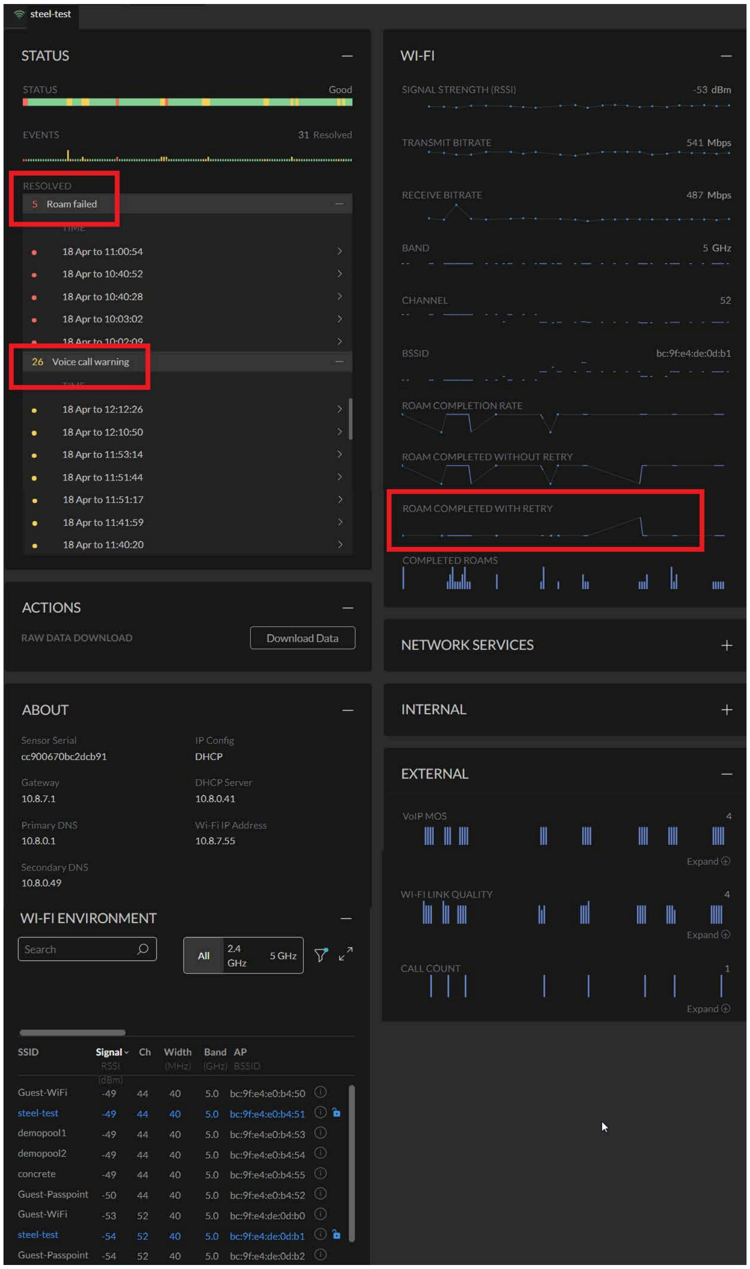


Figure 14 is an example is of specific drilled down device view from Extreme Networks Intuitive Insights (EII) Dashboard.

In this example the User is in Voice Call on the Zebra device while walking (roaming). The EII view depicts a period in which the device's Wi-Fi roaming performance, shown in the zoomed-in righthand black rectangle, looks normal without warnings or failures of concern. But at the same time the voice traffic indicators, shown in the zoomed-in lefthand black rectangle, do not look normal: AVG Packet Loss (%) is 3.5 and VOIP Link Quality (MOS) is 3.77. In this scenario, the Wireless Insights data from the device will include additional Reason Codes root cause information.

Much like in the previous example of UXI, in this EII example the system further correlates the voice-specific metrics with periods in which the Wi-Fi had no degradation at all. Therefore, the actionable item for the administrator in this case was also to focus on other non-Wi-Fi components of the network.

Figure 14

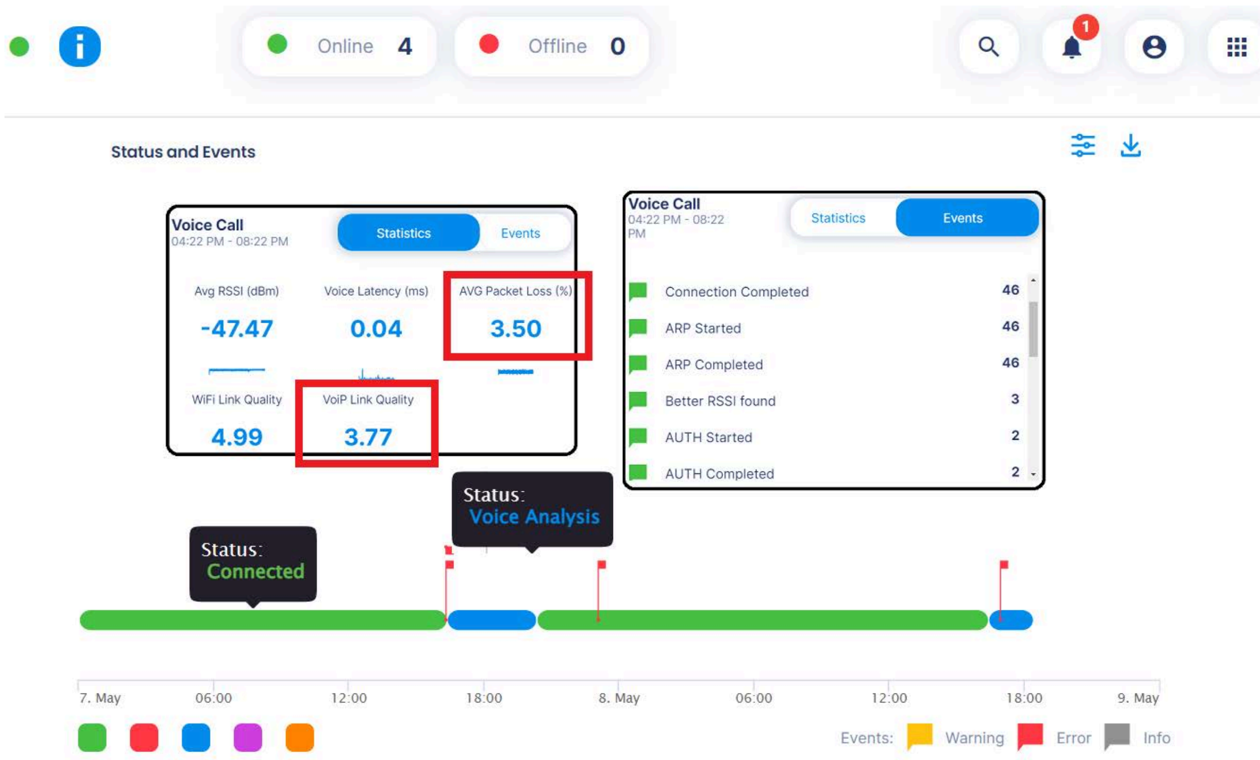
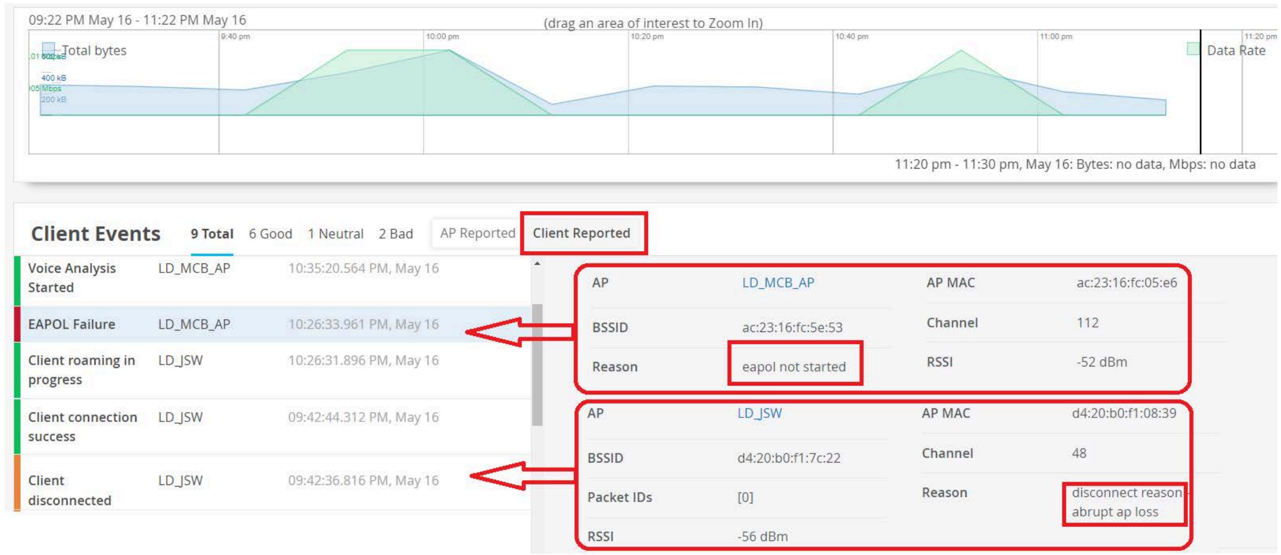


Figure 15 depicts a specific drilled down device view from Juniper/Mist Marvis Dashboard.

In this example, the user is just walking (roaming) with the Zebra Device, without using any application. The Marvis view depicts a Client Events pane which includes the individual Client Reported and AP Reported events correlated with all the Client Events in the zoomed-in period. In this screenshot, the Client Reported Tab is shown and zoomed into two roam issues: in the earlier issue, the Client Disconnected and is reporting a root cause of abrupt AP loss.

This instance was further correlated to a location where the user abruptly exited the intended coverage, therefore there is no actionable item. Then, ~45 minutes later, the user came back to the coverage to attempt re-connection, but had an EAPOL Failure with root cause of eapol not started, and the device connected successfully a short time later. That problem was further correlated to the specific area (AP) where the User came into the coverage, being too weak of a signal, and the device could not hear the AP's EAPOL packet. The actionable item for the Administrator was to consider increasing the AP power in that specific area.

Figure 15



Zebra information about the Wireless Insights product can be found here: zebra.com/us/en/support-downloads/software/productivity-apps/wireless-insights.html

The following links are of pre-established Zebra-Partners' cloud Solutions using the APIs:

- HPE/Aruba UXI: arubanetworks.com/products/network-management-operations/analytics-monitoring/user-experience-insight-agent-for-zebra/
- Extreme Intuitive Insights: extremenetworks.com/extreme-intuitive-insights/
- Juniper Mist Marvis: mist.com/partners/zebra/

Unique Use Cases and Features for Wi-Fi 6E

Traditional WLAN monitoring systems attempt to alert the backend administrator about network health issues or potential issues impacting connected devices, and further, how the impact might propagate at scale, affecting multiple devices, areas, APs, stores/buildings, etc.

The health assessed by traditional systems typically does not include the aggregated connected devices' views and analyzed data. The Administrator, therefore, does not have high confidence in applying corrective actions. The Wireless Insights data is a perfect fit for health monitoring. Not only does it provide the sought after devices' view of the network health, but the data includes granular metrics and issue root causes as applicable, and is unified across all the enabled devices. This enables trusted conclusions of the scale of the performance or issues.

With Wireless Insight APIs servicing an application (agent), either of a Zebra Partner Agent of a pre-established cloud system or customer-written agent, the following systematic features and capabilities are possible, compared to generic application/agent which is not serviced by Zebra APIs:

Features/Capabilities	Zebra Wireless Insights	Generic Agent
Basic Current Connection information and Synthetic Testing		
Real Voice Application Performance monitoring (not only synthetic) and Root Cause analysis of issues		X

Features/Capabilities	Zebra Wireless Insights	Generic Agent
Roaming performance and Root Cause Analysis directly from packet analysis (not available from Android OS)		X
Location-Issue tracking using 802.11mc		X
Access to persistent device identifiers (Hidden by Android OS A11+)		X
Service does not alter device performance*		X
Packet Capture		X

*Generic agents may impact device roaming behavior and battery performance.

Bluetooth Insights

Zebra's Bluetooth Insight API allows customer applications/user agents to register and receive important events related to Bluetooth peripherals for cloud/localized analytics purposes.

Bluetooth Insight API helps customers to better understand the usage patterns of Bluetooth peripherals such as headsets and ring scanners associated with Zebra mobile devices. This provides greater visibility into the activities of Bluetooth peripherals, easing management and helping to improve accountability for peripheral loss.

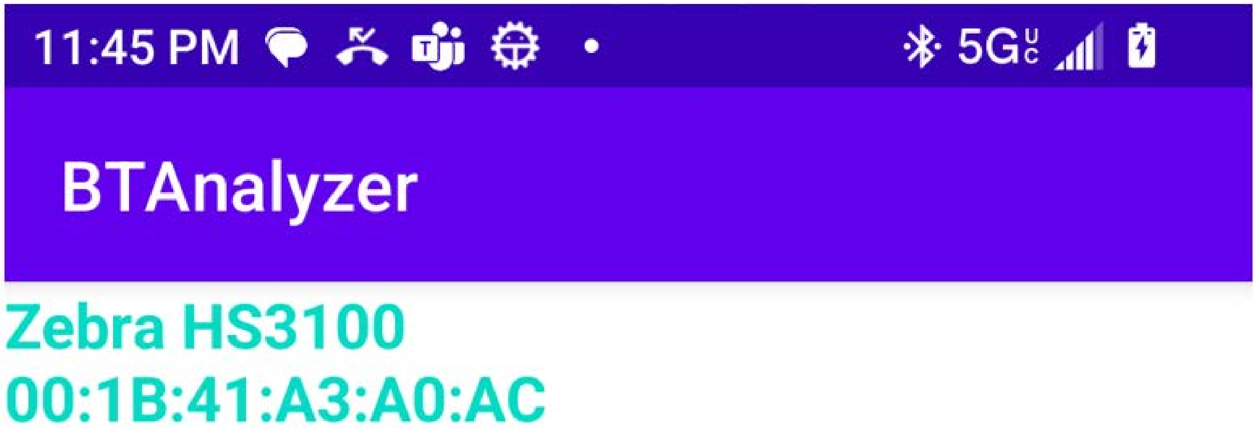
Any of Zebra's Enterprise customers whose workflow involves using small form-factor Bluetooth peripherals, such as ring scanners, may have experienced associates losing/leaving behind these peripherals. These customers would benefit from the ability to know specific information such as when these peripherals were last bonded/unbonded, or last connected/disconnected, along with reason for disconnection. This information combines with other Zebra mobile device specific attributes to track when, where and who used these peripherals and when they were last used.

Zebra provides integrators of the APIs a sample application/agent which demonstrates how the features and operations of the APIs can be integrated and facilitated, as preparation for a production-level agent.

See more information about the Bluetooth Insights at: techdocs.zebra.com/bti/1-0/about/

The following screenshot examples are from a sample application, depicting the usage of the Zebra Bluetooth Insights API data. Zebra HS3100 Bluetooth Headset is shown paired with the Zebra mobile device. The device Name/ID and MAC address is shown.

Figure 16



The screen in Figure 17 displays when pressing on the device entry to view the additional details.

As shown, the device is in bonded and connected states, with additional respective details about last connected/disconnected timestamp, along with the last reason for the disconnect.

Figure 17

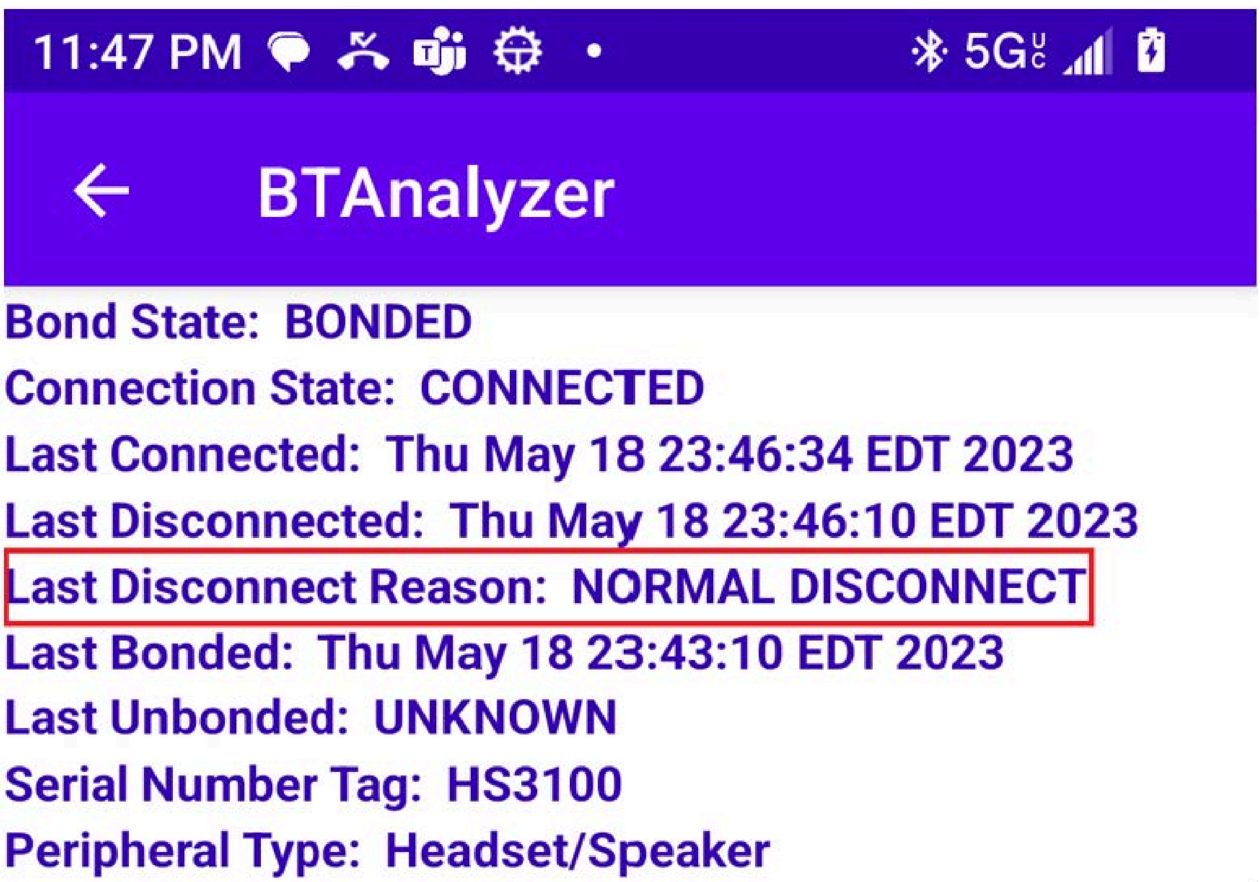
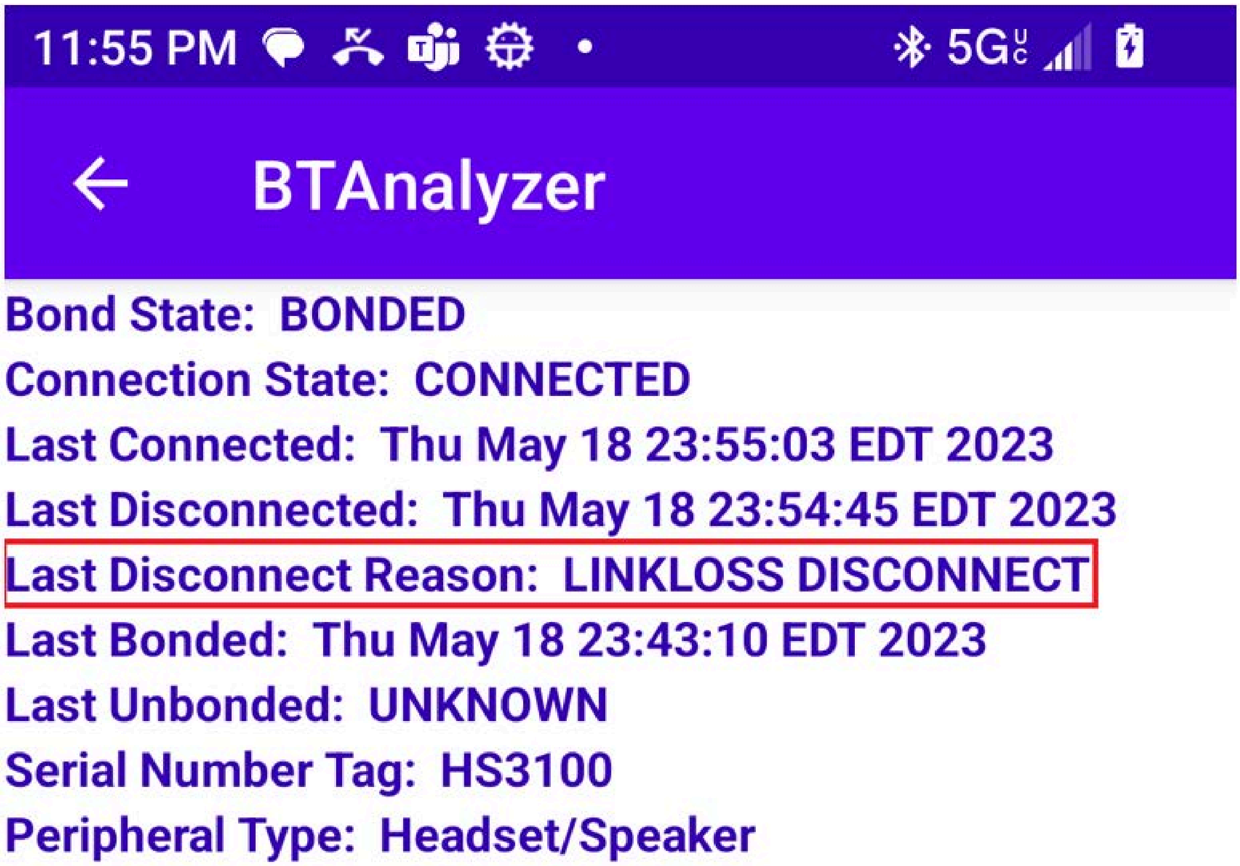


Figure 18 shows an example of that same device, but with a different disconnect reason type of linkloss disconnect. Linkloss disconnect would be shown as a reason if a user walked away from an accessory, or if there was sudden disconnect such as forcibly removing the battery from a remote peripheral.

Figure 18



Abbreviations

AP	Access Point
BSS	Basic Service Set
BSSID	BSS Identifier
CCA	Clear Channel Assessment
DBS	Dual Band Simultaneous
DFS	Dynamic Frequency Selection
FT	Fast Transition (802.11r)
FTM	Fine Time Measurement
H2E	Hash to Element (SAE)
HnP	Hunting and Pecking (SAE)
MBSSID	Multi-BSSID
MIMO	Multiple Input Multiple Output
MOS	Mean Opinion Score
MU-MIMO	Multiuser MIMO
OFDM	Orthogonal Frequency-Division Multiplexing
OFDMA	Orthogonal Frequency-Division Multiple Access
OWE	Opportunistic Wireless Encryption
PSC	Preferred Scan Channel
QAM	Quadrature Amplitude Modulation
RNR	Reduced Neighbor Report
RTT	Round Trip Time
SAE	Simultaneous Authentication of Equals
SNR	Signal to Noise Ratio
TWT	Target Wake Time
WPA	Wi-Fi Protected Access
WPA2	WPA version 2
WPA3	WPA version 2