Zebra Enterprise Wi-Fi 7 Android Devices

Best Practices for Cisco WLAN Infrastructure

MN-005596-01EN Rev. A

ZEBRA

Zebra Technologies | 3 Overlook Point | Lincolnshire, IL 60069 USA
zebra.com

Copyright

2026/03/10

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.

Contents

About This Guide **5**

Notational Conventions 5

Icon Conventions 6

Service Information 6

Wi-Fi 7 Devices Capabilities and Features **7**

Multi-Link Operation 7

4096 Quadrature Amplitude Modulation 10

320 MHz Channels 11

Multiple Resource Units and Preamble Puncturing 12

512 Compressed Block Ack 13

Triggered Uplink Access Optimization 13

802.11az 14

Wi-Fi Aware 14

Device Settings **15**

802.11k Lite 17

802.11k Full 17

Band Selection 18

Channel Width 18

Band Preference 18

Country-Specific Allowed Preferred Scanning Channels 18

Common Infrastructure Setting Recommendations **20**

Contents

Data Rates 20

Cisco Infrastructure Setting Recommendations 21

Security Recommendations for Zebra Devices on Wi-Fi 7 Networks 22

WPA3 Enterprise 22

WPA3 Personal 22

Enhanced Open 23

Beacon Protection 23

Supported WPA3 Combinations 23

WLAN Security Considerations in Deployment Modes 24

Zebra Client Devices Deployed in Wi-Fi 7 Infrastructure 24

Zebra Wi-Fi 7 Client Devices Deployed in Wi-Fi 6/6E Infrastructure 25

Zebra-Recommended WLC and AP Models by Vendor 27

List of Acronyms 28

About This Guide

This guide provides recommendations for deploying Zebra's Enterprise Wi-Fi 7 Android devices listed in the following table on a WLAN network that includes a Cisco AP hardware access point.

Table 1 Supported Wi-Fi 7 Devices

Device Type	Supported Devices
Tablet	ET401 Premium and ET401 Standard
Handheld	TC501 and TC701

NOTE: This guide does not address the deployment cases of:

- Devices not listed in the table (Wi-Fi 5, Wi-Fi 6, Wi-Fi 6E) when deployed in a WLAN network using APs that support and enable Wi-Fi 7 or any earlier WLAN Wi-Fi generations.
- Devices listed in the table, but were deployed in earlier WLAN Wi-Fi generations, or are using Wi-Fi 7 hardware that does not enable Wi-Fi 7.

In these deployment cases, refer to the appropriate Best Practices guides on the Zebra Wireless Fusion Support page for configuration information.

Wi-Fi 7 (also known as IEEE 802.11be) delivers unprecedented speed, efficiency, and reliability. Building upon the advancements of Wi-Fi 6 and Wi-Fi 6E, Wi-Fi 7 aims to support demanding applications that need high throughput, deterministic latency, and greater reliability.

Wi-Fi 7 introduces a range of features, including Multi-Link Operation (MLO) for simultaneous connections across multiple frequency bands, a 320 MHz channel width, 4K-QAM (Quadrature Amplitude Modulation) for higher data rates, and Multiple Resource Units (MRU) for increased capacity. With increased speed and efficient spectrum usage, Wi-Fi 7 enables seamless experiences in enterprise environments. Its backward compatibility ensures smooth integration with existing Wi-Fi networks while providing a future-proof foundation for next-generation devices and applications.

Notational Conventions

The following notational conventions make the content of this document easy to navigate.

- **Bold** text is used to highlight the following:
  - Dialog box, window, and screen names
  - Dropdown list and list box names
  - Checkbox and radio button names

  - Icons on a screen
  - Key names on a keypad
  - Button names on a screen
- Bullets (•) indicate:
  - Action items
  - List of alternatives
  - Lists of required steps that are not necessarily sequential
- Sequential lists (for example, those that describe step-by-step procedures) appear as numbered lists.

Icon Conventions

The documentation set is designed to give the reader more visual clues. The following visual indicators are used throughout the documentation set.

NOTE: The text here indicates information that is supplemental for you to know and that is not required to complete a task.

IMPORTANT: The text here indicates information that is important for you to know.

CAUTION: If the precaution is not heeded, you could receive a minor or moderate injury.

WARNING: If danger is not avoided, you CAN be seriously injured or killed.

DANGER: If danger is not avoided, you WILL be seriously injured or killed.

Service Information

If you have a problem with your equipment, contact Zebra Global Customer Support for your region. Contact information is available at: zebra.com/support.

When contacting support, please have the following information available:

- Serial number of the unit
- Model number or product name
- Software/firmware type and version number

Zebra responds to calls by email, telephone, or fax within the time limits set forth in support agreements.

If your problem cannot be solved by Zebra Customer Support, you may need to return your equipment for servicing and will be given specific directions. Zebra is not responsible for any damages incurred during shipment if the approved shipping container is not used. Shipping the units improperly can possibly void the warranty.

If you purchased your Zebra business product from a Zebra business partner, contact that business partner for support.

Wi-Fi 7 Devices Capabilities and Features

This section describes the Wi-Fi-related features supported by Zebra Wi-Fi 7 devices.

Multi-Link Operation

Multi-Link Operation (MLO) enables Wi-Fi 7 devices to simultaneously connect to and transmit data across multiple frequency bands or channels, such as 2.4 GHz, 5 GHz, and 6 GHz. By leveraging multiple links concurrently, MLO introduces a new paradigm of multi-band communication that enhances throughput, reduces latency, and ensures a more resilient connection in various networking environments.

Key benefits of MLO include:

- Increased throughput
- Reduced latency
- Enhanced reliability
- Optimized Spectrum utilization

The table below explains the different ways multi-link devices can operate. It compares them based on their radio setup and whether they can send and receive data simultaneously. This will affect their speed and reliability.

Table 2 Operating Modes

Transmit/ Receive Capability	Radio	Description and Purpose	Relative Performance
NSTR (non-simultaneous)	Multi-Link Single-Radio (MLSR)	A single radio switching between different links (for example, 5 GHz and 6 GHz). The radio cannot transmit and receive simultaneously. This mode is used for load balancing and reducing latency compared to non-MLO, but does not aggregate speed and is sub-par to other MLO modes.	High
	Enhanced MLSR (eMLSR)	While MLSR can listen to only one link at a time, the enhancement of eMLSR provides the ability to listen to multiple in parallel. Hence, eMLSR yields faster overall switching between links if one of them degrades in quality.	

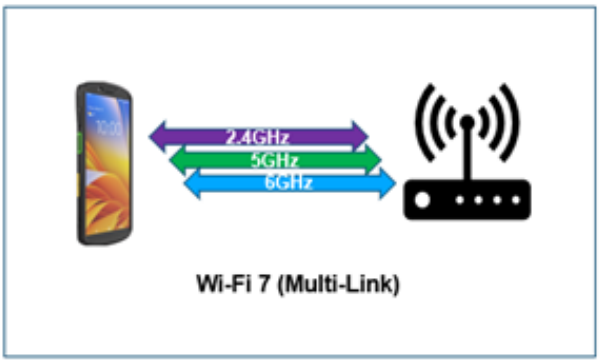
Table 2 Operating Modes (Continued)

Transmit/ Receive Capability	Radio	Description and Purpose	Relative Performance
	Multi-Link Multi-Radio (MLMR)	Multiple radios are synchronized to either transmit or receive at any given moment. This allows for link aggregation to achieve higher throughput by combining the bandwidth of multiple links for transmission or reception.	Higher
	Enhanced MLMR (eMLMR)	In this NSTR mode, the eMLMR enhancement also enables dynamic link reconfiguration. This finer control of NSTR operations typically yields tangible improvements in throughput for traffic in a congested environment.	
STR (simultaneous)	Multi-Link Multi-Radio (MLMR)	Multiple radios operate independently, allowing the device to transmit on one link while simultaneously receiving data on another. This is the highest-performing mode, offering the preferred throughput, lowest latency, and preferred reliability by enabling full-duplex communication across bands.	Highest
	Enhanced MLMR (eMLMR)	In STR of Multi-Radio, the output performance and benefits can be achieved using either MLMR or eMLMR. The theoretical difference between them is eMLMR's ability to dynamically reconfigure links. However, given the STR nature, this enhancement may inherently introduce complexity and overhead, largely diminishing the need for it even in a congested environment and, in some cases, even degrading performance compared to the STR-MLMR.	

Zebra Wi-Fi 7 devices listed in the Table 1 Supported Wi-Fi 7 Devices, support STR-MLMR, as shown in the third row in the Table 2 Operating Modes. When a Wi-Fi 7 network is configured in any Multi Link dual- or tri-band configuration, with all APs in STR-MLMR mode, the Zebra device's MLO automatically interoperates with STR-MLMR.

The Zebra device STR-MLMR capability further ensures that the following very critical points are accomplished, beyond standard STR-MLMR operations and beyond the generic performance expectation mentioned in the above table:

- The Zebra device constantly listens across multiple links to evaluate their quality. For each packet, it selects the best link for transmission. This dynamic selection process replaces complex link reconfiguration methods, such as STR-eMLMR. By dynamically selecting the best link, the device efficiently improves throughput and reduces latency in congested environments.
- At the interoperability level between Wi-Fi 7 APs and Wi-Fi 7 devices, Zebra ensures that the AP's implementation of STR-MLMR and the device's STR-MLMR fully interoperates and is further stabilized in collaboration with Enterprise WLAN network vendors. Most Wi-Fi 7 APs have the aforementioned considerations to avoid the complexities of STR-eMLMR; thereby, this interoperability stabilization goes a long way.
- Zebra's STR-MLMR support does not require any change in the device's battery preservation or charging practices.



The Zebra's MLO is supported when the WLAN network uses either tri-band or dual-band MLO in the following configuration combinations:

- 2.4 GHz + 5 GHz
- 2.4 GHz + 6 GHz
- 5 GHz + 5 GHz
- 5 GHz + 6 GHz
- 2.4 GHz + 5 GHz + 6 GHz[1]
- 5 GHz + 5 GHz + 6 GHz[2]

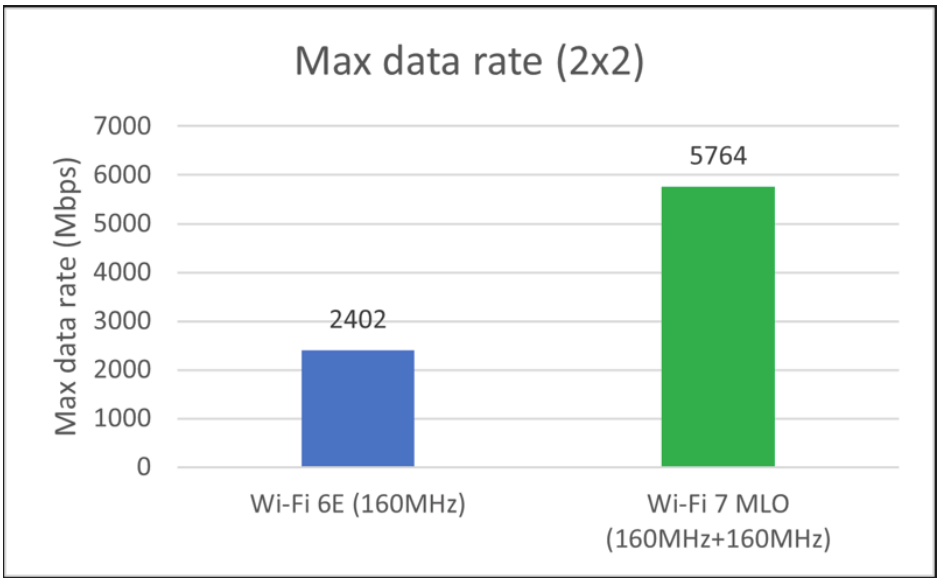
When operating in MLO, the maximum bandwidth supported for each link is as follows:

- 2.4 GHz can support 20 MHz
- 5 GHz can support up to 160 MHz
- 6 GHz can support up to 160 MHz

The following charts compare the performance between Wi-Fi 6E (Single Link) and Wi-Fi 7 (Multi-Link) at 80 MHz and 160 MHz.

[1] Up to two links can be active at any point in time.

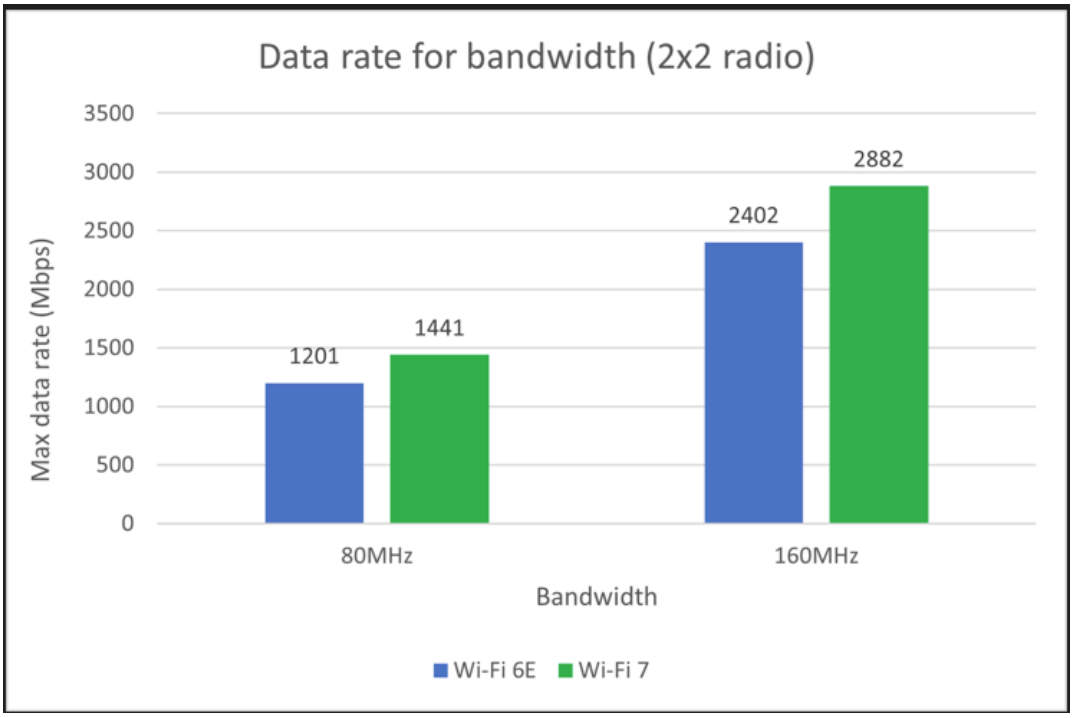
[2] Up to two links can be active at any point in time.



4096 Quadrature Amplitude Modulation

4096 Quadrature Amplitude Modulation (4096-QAM or 4K-QAM) is the latest modulation scheme used in Wi-Fi 7. This modulation scheme allows for the transmission of higher data rates by encoding more bits per symbol compared to its predecessors. Zebra Wi-Fi 7 devices support 4K-QAM, enabling a 20 % higher data rate compared to Wi-Fi 6. This enhancement allows Wi-Fi 7 to deliver ultra-fast speeds, making it ideal for bandwidth-intensive applications.

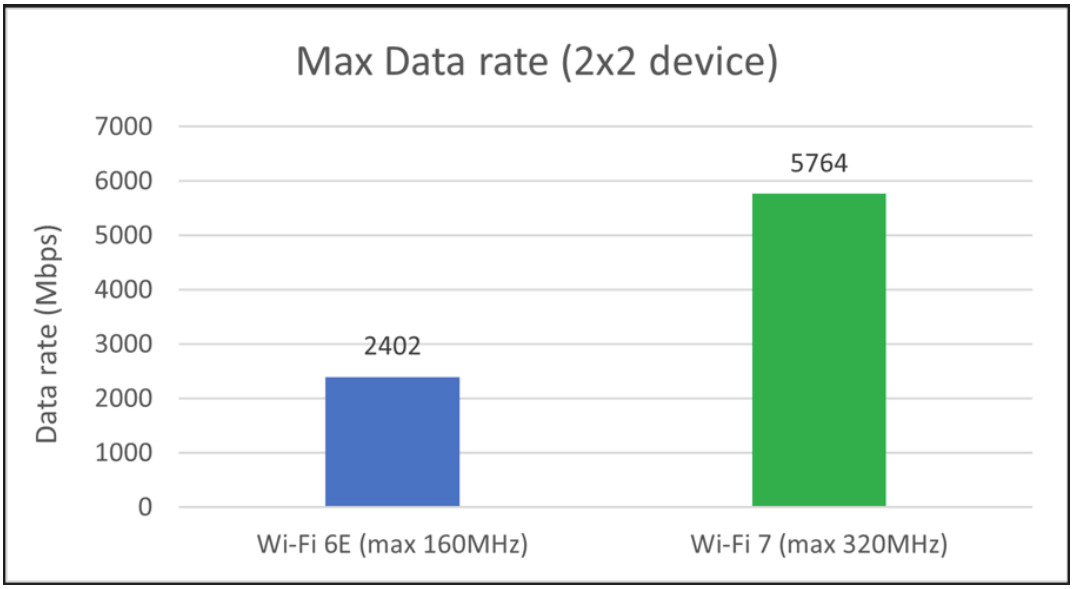
The following chart compares the performance of the data rate for bandwidth (2x2 radio) between Wi-Fi 6E and Wi-Fi 7.



320 MHz Channels

Wi-Fi 7 extends channel width to 320 MHz in the 6 GHz frequency band. This increase in channel width doubles the throughput in Wi-Fi 7 compared to Wi-Fi 6E devices. Zebra devices support a 320 MHz channel width when operating in the 6 GHz frequency band in single link mode.

The following chart compares the performance between Wi-Fi 6E and Wi-Fi 7 throughput.

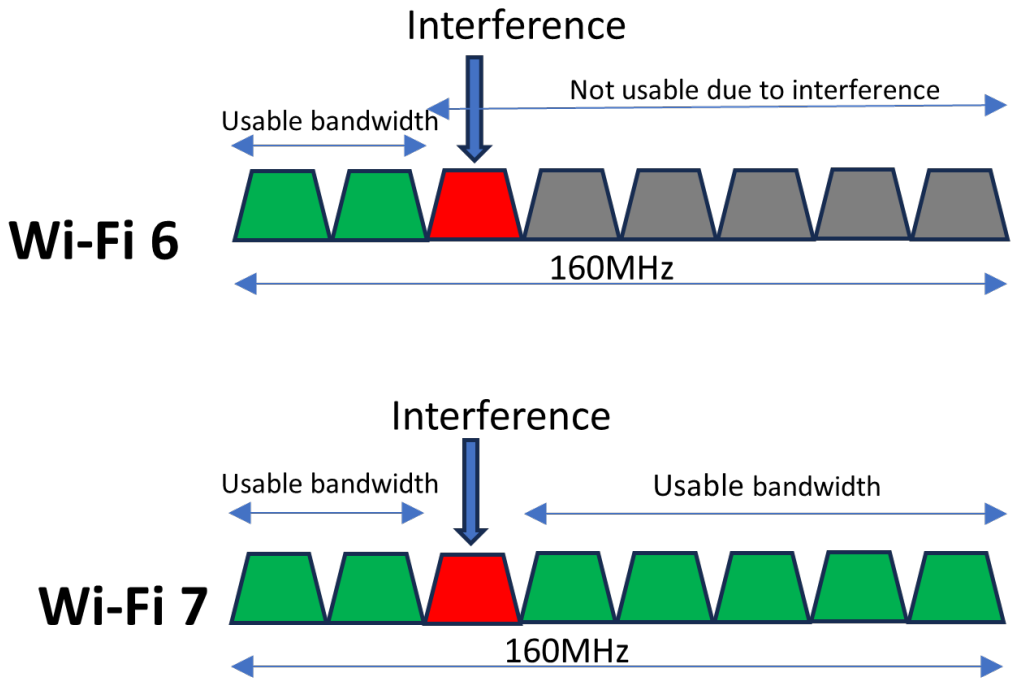


Multiple Resource Units and Preamble Puncturing

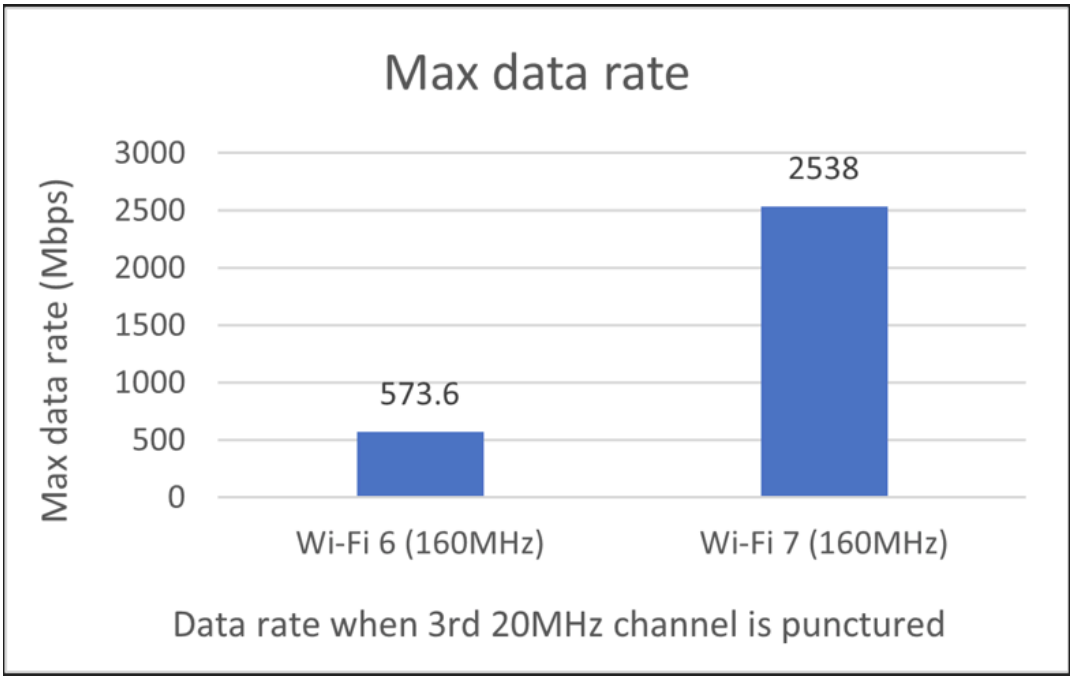
Multiple Resource Units (MRU) is a feature of Wi-Fi 7 that optimizes spectrum use by enabling flexible, interference-aware RU allocation.

With the introduction of Orthogonal Frequency-Division Multiple Access (OFDMA) in Wi-Fi 6, the available channel bandwidth is divided into smaller units called Resource Units (RU). Each RU can be allocated to multiple devices, allowing them to transmit or receive data simultaneously on the same channel. This improves spectral efficiency and reduces latency compared to traditional single-user transmissions. Wi-Fi 7 builds on this concept by introducing MRUs, allowing devices to use combinations of RUs within a channel for greater flexibility and performance. MRU enhances the network's ability to deliver high throughput, low latency, and consistent performance.

Preamble Puncturing helps devices to utilize portions of a wide channel by puncturing or excluding the parts of the channel that are affected by interference, while still transmitting over the remaining interference-free portions. Preamble Puncturing enables devices to achieve higher throughput and maintain reliable connections, even when the entire channel cannot be used. This feature is particularly valuable in congested or crowded environments. With MRU and Preamble puncturing, Wi-Fi 7 devices can reduce bandwidth interference losses.



The following chart compares the performance of the maximum data rate between Wi-fi 6 and Wi-Fi 7 throughput.



The benefits of MRU and Preamble Puncturing:

- Improved spectrum efficiency
- Enhanced Performance in congested environments
- Higher throughput
- Reduced latency

512 Compressed Block Ack

With the Block Ack feature, a transmitter can aggregate multiple MAC Protocol Data Units (MPDU) into a single frame, and the receiver can acknowledge these in a single Block Ack frame. Wi-Fi 7 can support a Block Ack size of 512 MPDUs.

NOTE: Zebra Wi-Fi 7 devices support up to 512 Block Ack size.

Triggered Uplink Access Optimization

Triggered Uplink Access Optimization is a Wi-Fi 7 feature designed to improve the efficiency of uplink transmissions, particularly in multi-user environments. This feature enables devices running latency-sensitive applications, such as voice and video, to communicate their Quality of Service (QoS) requirements to the WLAN, allowing APs to optimize their scheduling to improve network efficiency and user experience.

NOTE: Zebra Wi-Fi 7 devices support Triggered Uplink Access Optimization.

802.11az

The 802.11az standard introduces advanced location capabilities to Wi-Fi networks. It significantly improves the accuracy, reliability, and scalability of positioning compared to its predecessor (802.11mc). 802.11az enables precise indoor and outdoor location tracking with sub-meter accuracy, supporting secure, authenticated, and private positioning.

The benefits of 802.11az:

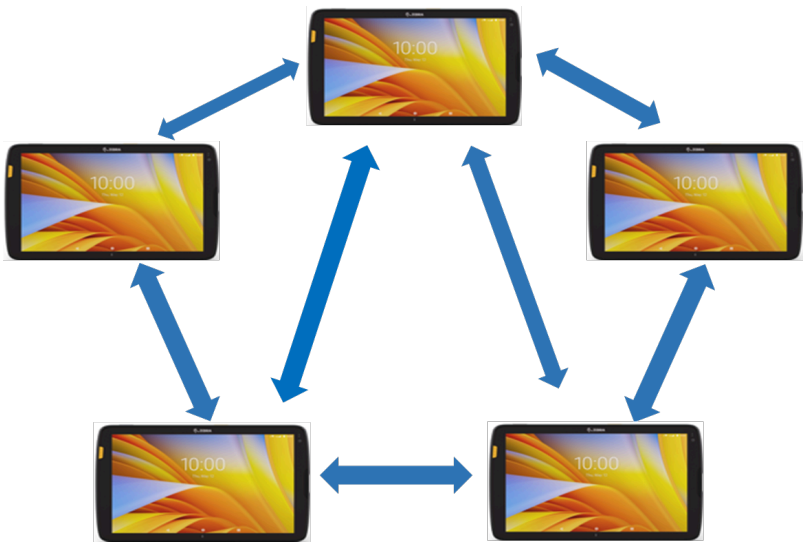
- Less than 1 m accuracy
- Security
- Scalable to a large number of client devices

Zebra Wi-Fi 7 devices support the 802.11az Wi-Fi location feature.

NOTE: In the ET401 devices, this feature is supported either by the factory-installed ET401 Enterprise model or by upgrading the ET401 Professional model with an Enterprise license, but it is not available in the standalone ET401 Professional model.

Wi-Fi Aware

Wi-Fi Aware, also known as Neighbor Awareness Networking (NAN), is a technology that enables devices to discover and communicate directly with each other without requiring traditional network infrastructure (such as Wi-Fi APs). It facilitates seamless peer-to-peer communication by using proximity-based discovery, allowing devices to detect and exchange information with nearby devices or services in real-time.



Device Settings

This section describes important settings to understand when deploying Zebra Wi-Fi 7 devices.

For detailed settings, refer to the Zebra Wi-Fi Manager.

NOTE: In the ET401 devices, some settings are included by default in the ET401 Enterprise model, or can be enabled by upgrading the ET401 Professional model with an Enterprise license, but they are not available in the standalone ET401 Professional model.

Table 3 Device Settings

Feature	Default Configuration	Supported Configuration	Recommended Configuration
2.4 GHz Channels	1-13	1-13	Default
5.0 GHz Channels	(36-48), (52-64), (100-144), (149-165)	(36-48), (52-64), (100-144), (149-165)	Default

Table 3 Device Settings (Continued)

Feature	Default Configuration	Supported Configuration	Recommended Configuration
6.0 GHz Channels	(1-93), (97-113), (117-181), (185), (189-233)	(1-93), (97-113), (117-181), (185), (189-233)	As per the country-specific allowed PSC Channels
Radio Frequency Band Selection	Auto/all bands	• Auto/all bands • 2.4 GHz • 5 GHz • 6 GHz • 2.4 GHz and 5 GHz • 2.4 GHz and 6 GHz • 5 GHz and 6 GHz	Default
Band Preference	Prefer 6 GHz or 5 GHz	• Prefer 5 GHz • Prefer 2.4 GHz • Prefer 6 GHz or 5 GHz • Prefer 5 GHz band over 6 GHz • Disable	Default
Power Save Mode	NDP	• Always active (CAM) • WMM-PS • Null Data Power Save (NDP) • PS-POLL • TWT	Default
802.11k	Enable 802.11k Lite	• Disable • Enable 802.11k Lite • Enable 802.11k Full	Default
802.11w	Capable	• Optional (Capable) • Disable	Default
802.11v	Enabled	• Enable • Disable	Default

Table 3 Device Settings (Continued)

Feature	Default Configuration	Supported Configuration	Recommended Configuration
PMKID	Disabled	• Enable • Disable	Default
OKC	Enabled	• Enable • Disable	Default
Fast Transition (FT)	Enabled	• Enable • Disable	Default
FT Over DS	Enabled	• Enable • Disable	Default
Channel Width	20/40/80/160/320	20/40/80/160/320	Not configurable
Call Admission Control	Enabled	• Enable • Disable	Default
FTM Enable	Enabled	• Enable • Disable	Default

802.11k Lite

802.11k Lite configuration allows the disabling of the 802.11k measurement features (Link Measurement, Beacon Measurement, and others), while keeping only the Neighbor Report feature and Beacon Table Report features enabled. Zebra devices advertise only Neighbor Report and Beacon Table Report during initial connection and while roaming across the APs.

802.11k Full

802.11k Full configuration enables all the 802.11k features supported by a Zebra device. Zebra devices support the following 802.11k features, which are used by APs to identify traffic or environment conditions of a client device.

- Link Measurement
- Neighbor Report
- Beacon Passive Measurement
- Beacon Active Measurement
- Beacon Table Measurement

Band Selection

Zebra devices support all three bands, and all are enabled by default. Band selection features can be used to turn off one or more bands.

Zebra Wi-Fi 7 devices support tri-link MLO. If all three bands are enabled, it can connect to the network in 2.4 GHz + 5 GHz + 6 GHz MLO mode. The Zebra Wi-Fi 7 device will choose the ideal one or two links for traffic at any point in time.

If the infrastructure supports only two frequency bands, then select the same frequency bands for device configuration as well. The Zebra device can support the following MLO combinations:

- 2.4 GHz + 5 GHz + 6 GHz
- 5 GHz + 5 GHz + 5 GHz
- 5 GHz + 5 GHz
- 5 GHz + 6 GHz
- 2.4 GHz + 5 GHz
- 2.4 GHz + 6 GHz

Channel Width

Zebra devices are versatile and support various channel widths for connectivity, including 20, 40, 80, 160, and 320 MHz.

- 2.4 GHz supports up to 20 MHz
- 5 GHz supports up to 160 MHz
- 6 GHz supports up to 320 MHz

Band Preference

The Zebra devices select and move between available bands or channels based on Received Signal Strength Indicator (RSSI), channel conditions, and other factors. By default, Zebra devices use the Prefer 6 GHz or 5 GHz configuration. When connecting to Wi-Fi 7 networks, Zebra Wi-Fi 7 devices will prefer the 6 GHz frequency band for establishing a connection (primary link).

NOTE: In the ET401 devices, this feature is supported either by the factory-installed ET401 Enterprise model or by upgrading the ET401 Professional model with an Enterprise license, but it is not available in the standalone ET401 Professional model.

Country-Specific Allowed Preferred Scanning Channels

The channel mask configuration (if configured) on the device should always match the actual channel deployment at the site. For the 6 GHz band, it is recommended to deploy only Preferred Scanning Channels (PSC). There are 15 PSC channels across the entire 6 GHz band, but the actual number varies by country of operation.

For a list of countries that have enabled the 6 GHz band and the approved sub-bands, go to wi-fi.org/countries-enabling-wi-fi-6e.

The device UI configuration for the 6 GHz channel mask marks the PSC channels with an asterisk next to their channel numbers for easier identification. For example, channel 5 is a PSC channel and is shown as *Ch.5 (5975 MHz) to indicate that it is a PSC channel.

Common Infrastructure Setting Recommendations

This section provides the recommended common (non-AP-vendor-specific) infrastructure settings and configuration considerations for Zebra devices that an Admin user must consider when deploying Wi-Fi 7 networks.

Table 4 Common Infrastructure Settings Parameter

Configuration Parameter	Recommended Settings for Wi-Fi 7 Networks
Channel Width for 2.4 GHz	20 MHz
Channel Width for 5 GHz	40 MHz
Channel Width for 6 GHz	80 MHz
Beacon Protection	Enable
Target Wake Time (TWT)	Enable
Broadcast Target Waketime	Enable
Multiple BSSID	Enable
802.11k	✓
RNR	✓
802.11v	✓
Data Rates (Mbps) (for Data Only Deployment)	6(B), 9, 12(B), 18, 24(B), 36, 48, 54 MCS 0-13
Data Rates (Mbps) (for Voice Deployment)	12(B), 18, 24(B), 36, 48, 54 MCS 0-13

Data Rates

To provide reliable coverage, Wi-Fi networks should be configured to deliver adequate signal strength in all areas where the Wi-Fi stations will be used. The required minimum signal strength for all Zebra devices depends on the frequency band it is operating in, data rates enabled on the AP, and data rate used by the Zebra device while operational.

Zebra devices use automatic rate-switching capabilities so that the Wi-Fi radio adapts and uses lower rates for data transmissions as the device moves away from the AP. This results in increased range when operating at lower transmission data rates.

NOTE: Rate settings may need to change according to environmental characteristics to accomplish balanced AP Minimum Coverage.

Cisco Infrastructure Setting Recommendations

The table below provides Zebra's recommendations for deploying Wi-Fi 7 within a Cisco infrastructure. For each recommendation, it is important to verify the Cisco configuration documentation to ensure that the parameters are set correctly, whether they are defaults or require explicit adjustments.

Table 5 Cisco Infrastructure Settings Parameter

Configuration Parameter	Recommended Settings for Wi-Fi 7 Networks
MLO Group	2 + 5 5 + 6 2 + 5 + 6 5 + 5 (9176 and 9178 AP's)
OFDMA Multi-RU	✓
Downlink OFDMA	✓
Uplink OFDMA	✓
Downlink MU-MIMO	✓
Uplink MU-MIMO	✓
Enable FTM Responder (SSID Configuration)	✓
Enable AP Geolocation (AP Global Configuration)	✓
Enable FTM (AP Join Profile)	✓

Security Recommendations for Zebra Devices on Wi-Fi 7 Networks

Wi-Fi 7 does not allow open security and WPA2 security combinations. To provide more robust security, Wi-Fi 7 enforces the use of WPA3 Enterprise, WPA3 Personal, and Enhanced Open security combinations.

By default, WPA3 uses PMF (802.11w), and it is a mandatory requirement for both devices and APs, which helps to prevent deauthentication attacks. Zebra devices support all three security combinations: WPA3 Enterprise, WPA3 Personal, and Enhanced Open.

WPA3 Enterprise

WPA3-Enterprise security is based on WPA2-Enterprise with the additional requirement of using Protected Management Frames (PMF) for WPA3 connections. CCMP-128 and GCMP 256 cipher suites are used for data encryption, and the BIP (GMAC-256) cipher suite is used to protect Group Management frames. WPA3 Enterprise 192-bit mode is an optional mode of operation that provides enhanced security for enterprise networks and uses EAP-TLS (certificate-based authentication) and strong cryptographic algorithms. WPA3-Enterprise 192-bit Mode requires support of GCMP-256 for encryption and Signature hash algorithm ECDSA_SHA384 for key derivation.

Radius server and Certificate requirements for WPA3 192-bit mode:

- WPA3 Enterprise 192-bit Mode requires a supported EAP server such as Cisco Identify Service Engine (ISE) and Aruba Clearpass Policy Manager (CPPM), which require 802.1X Authentication type as TLS EAP (EAP-TLS)
- Supported 192-bit 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, 2,048, 4,096, 8,192, and 16,384. The 192-bit Mode mandates the use of RSA certificates with a key size greater than or equal to 3,072 bits. Therefore, when generating the certs, be sure to use 4096-bit 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. In Wi-Fi 7, SAE authentication must use the H2E (Hash-to-Element) method to obtain the Password Element (PWE) from passwords. Wi-Fi 7 devices cannot use HnP (Hunting and Pecking) for SAE.

Wi-Fi 7 connections use FT SAE, using a group-dependent hash of 00-0F-AC:25 (FT SAE-EXT), or SAE authentication, using a group-dependent hash of 00-0F-AC:24 (SAE-EXT).

Enhanced Open

Prior to the introduction of the Enhanced Open (EO) 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. With the introduction of EO based on the Opportunistic Wireless Encryption (OWE) standard, those systems can choose to use EO, which is more robust security than the WPA2-PSK, and with a better fit to the no-Passphrase-Management architecture. 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.

Beacon Protection

Wi-Fi 7 introduces Beacon Protection as a mandatory requirement for both APs and devices. When this feature is enabled, an AP provisions its devices with the AP's Beacon Integrity Key during initial authentication setup and adds a Message Integrity Check (MIC) element to its Beacon frames. This allows devices associated with the AP to verify the integrity of Beacon frames and detect active attacks that forge or modify them.

Both the AP and the device announce their capability to support Beacon Protection in their Extended Capabilities field. Beacon Protection can be enabled for any of the WPA3 Authentication Key Management (AKM) modes such as OWE, SAE, SAE-FT, SAE-EXT, SAE-EXT-FT, SUITEB192-1x, 802.1x-SHA256, and FT-802.1x.

Supported WPA3 Combinations

This section details supported WPA3 combinations.

Table 6 Supported WPA3 Combinations

Protocal	Encryption	AKM	Default Config	Supported Config
WPA3 Personal	GCMP 256	SAE EXT- FT	Enabled	SAE-EXT-FT-H2E
WPA3 Personal	GCMP 256	SAE -EXT	Enabled	SAE-EXT-H2E
WPA3 Enterprise	GCMP 256	SuiteB-192 FT	Enabled	FT
WPA3 Enterprise	GCMP 256	SuiteB-192	Enabled	PMKID
WPA3 Enterprise	AES-GCMP 256	802.1X-SHA256	Enabled	OKC
Enhanced Open	GCMP 256	OWE	Enabled	OWE
WPA3 Enterprise	AES-CCMP 128	802.1X-SHA256	Enabled	FT
WPA3 Enterprise	AES-CCMP 128	802.1X-SHA256	Enabled	OKC
WPA3 Enterprise	AES-CCMP 128	FT 802.1X	Enabled	FT
WPA3 Enterprise	AES-CCMP 128	802.1X	Enabled	OKC
Enhanced Open	AES-CCMP 128	OWE	Enabled	OWE

WLAN Security Considerations in Deployment Modes

This section outlines the Single SSID recommendations for Zebra Client devices when deployed in Wi-Fi 6/6E and Wi-Fi 7 infrastructure.

Zebra Client Devices Deployed in Wi-Fi 7 Infrastructure

This section describes the Single SSID design recommendations when Zebra Wi-Fi 6, Wi-Fi 6E, and Wi-Fi 7 client devices are deployed in Wi-Fi 7-capable infrastructure.

WPA3 Configuration

Zebra recommends using WPA3 Enterprise security when deploying either only Zebra Wi-Fi 7 clients or a mixed generation of Zebra Wi-Fi 6, Wi-Fi 6E, and Wi-Fi 7 clients in Wi-Fi 7-capable infrastructure.

The following are the configuration guidelines.

- Set the security to **WPA3** with Beacon Protection and configure AKM as **FT over IEEE 802.1X**.

```
Security
    FT Support                                  : Enabled
    Security-2.4GHz/5GHz
        802.11 Authentication                       : Open System
        Wi-Fi Protected Access (WPA/WPA2/WPA3)      : Enabled
            WPA3 (WPA3 IE)                          : Enabled
                AES Cipher                          : Enabled
            Auth Key Management
                FT dot1x                            : Enabled
                Dot1x-SHA256                        : Enabled
        PMF Support                                 : Required
        Beacon Protection                           : Enabled
    Security-6GHz
            WPA3 (WPA3 IE)                          : Enabled
                AES Cipher                          : Enabled
            Auth Key Management
                FT dot1x                            : Enabled
                Dot1x-SHA256                        : Enabled
        PMF Support                                 : Required
       Beacon Protection                            : Enabled
```

If the SSID is WPA3 Personal, then Zebra recommends the following configuration guidelines.

- Set the security to **WPA3** with Beacon Protection and configure AKM as **SAE-FT, SAE-EXT-FT**.

```
Security
    FT Support                                  : Enabled
    Security-2.4GHz/5GHz
        802.11 Authentication                       : Open System
        Wi-Fi Protected Access (WPA/WPA2/WPA3)      : Enabled
            WPA3 (WPA3 IE)                          : Enabled
                AES Cipher                          : Enabled
                GCMP256 Cipher                      : Enabled
            Auth Key Management
                FT SAE                              : Enabled
                FT SAE-EXT-KEY                      : Enabled
        SAE PWE Method                              : Hash to Element, Hunting and Pecking(H2E-HNP)
        PMF Support                                 : Required
        Beacon Protection                           : Enabled
    Security-6GHz
            WPA3 (WPA3 IE)                          : Enabled
                AES Cipher                          : Enabled
                GCMP256 Cipher                      : Enabled
            Auth Key Management
                FT SAE                              : Enabled
                FT SAE-EXT-KEY                      : Enabled
        SAE PWE Method                              : Hash to Element(H2E)
        PMF Support                                 : Required
       Beacon Protection                            : Enabled
```

Zebra Wi-Fi 7 Client Devices Deployed in Wi-Fi 6/6E Infrastructure

This section describes the Single SSID design recommendations when Zebra Wi-Fi 7 client devices are deployed in Wi-Fi 6 or Wi-Fi 6E-capable infrastructure.

WPA3 Configuration

Zebra recommends using WPA3 Enterprise security when deploying Wi-Fi 7 clients in Wi-Fi 6 or Wi-Fi 6E-capable infrastructure.

The following are the configuration guidelines.

- Set the security to **WPA3** and configure AKM as **FT over IEEE 802.1X**.

```
Security
    FT Support                                  : Enabled
    Security-2.4GHz/5GHz
        802.11 Authentication                       : Open System
        Wi-Fi Protected Access (WPA/WPA2/WPA3)      : Enabled
            WPA3 (WPA3 IE)                          : Enabled
                AES Cipher                          : Enabled
            Auth Key Management
                FT dot1x                            : Enabled
                Dot1x-SHA256                        : Enabled
        PMF Support                                 : Required
        Beacon Protection                           : Enabled
    Security-6GHz
            WPA3 (WPA3 IE)                          : Enabled
                AES Cipher                          : Enabled
            Auth Key Management
                FT dot1x                            : Enabled
                Dot1x-SHA256                        : Enabled
        PMF Support                                 : Required
       Beacon Protection                            : Enabled
```

If the SSID is WPA3 Personal, then Zebra recommends the following configuration guidelines.

- Set the security to **WPA3** and configure AKM as **SAE-FT**.

```
Security
    FT Support                                  : Enabled
    Security-2.4GHz/5GHz
        802.11 Authentication                       : Open System
        Wi-Fi Protected Access (WPA/WPA2/WPA3)      : Enabled
            WPA3 (WPA3 IE)                          : Enabled
                AES Cipher                          : Enabled
            Auth Key Management
                FT SAE                              : Enabled
        SAE PWE Method                              : Hash to Element, Hunting and Pecking(H2E-HNP)
        PMF Support                                 : Required
     Security-6GHz
            WPA3 (WPA3 IE)                          : Enabled
                AES Cipher                          : Enabled
            Auth Key Management
                FT SAE                              : Enabled
        SAE PWE Method                              : Hash to Element(H2E)
        PMF Support                                 : Required
```

Zebra-Recommended WLC and AP Models by Vendor

The following list shows the recommended Wi-Fi 7 WLC and AP models from Zebra for Cisco systems:

- WLC 9800 series (software versions 17.15.3, 17.18.1)
- AP models: 9172, 9176, 9178, 9136, 9166, 9164, 9130, 9115

List of Acronyms

This section provides a list of acronyms used in this guide for reference.

Table 7 List of Acronyms

Acronyms	Definition
AFC	Automated Frequency Coordination
AP	Access Point
BSS	Basic Service Set
CCA	Clear Channel Assessment
DFS	Dynamic Frequency Selection
EIRP	Equivalent Isotropically Radiated Power
FCC	Federal Communications Commission
HE	High Efficiency
H2E	Hash-to-Element
HnP	Hunting and Pecking
LPI	Low Power Indoor
MIMO	Multiple Input Multiple Output
MU-MIMO	Multiuser MIMO
OFDM	Orthogonal Frequency-Division Multiplexing
OFDMA	Orthogonal Frequency-Division Multiple Access
OWE	Opportunistic Wireless Encryption
PSC	Preferred Scan Channel
PSD	Power Spectral Density
QBSS	QoS BSS
RNR	Reduced Neighbor Report
SAE	Simultaneous Authentication of Equals
SNR	Signal to Noise Ratio
SP	Standard Power

Table 7 List of Acronyms (Continued)

Acronyms	Definition
STA	Station (client device)
TWT	Target Wake Time
U-NII	Unlicensed National Information Infrastructure
VLP	Very Low Power
WPA	Wi-Fi Protected Access
WPA3	WPA Version 3