Voice Deployment with Cisco WLAN Infrastructure

Best Practices Guide

ZEBRA

MN-004338-02EN Rev A

Copyright

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

This guide is jointly authored by Zebra Technologies and Cisco Systems Inc.

This guide provides recommendations for voice deployment using the following mobile computers and their accessories.

- TC52 and TC52-HC
- TC52x and TC52x-HC
- TC52ax and TC52ax-HC
- TC57
- TC57x
- TC72
- TC77
- PC20
- MC93
- EC30
- TC21 and TC21-HC (with Zebra mDNA license)
- TC26 and TC26-HC (with Zebra mDNA license).

Notational Conventions

The following conventions are used in this document:

- **Bold** text is used to highlight the following:
  - Dialog box, window, and screen names
  - Drop-down 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 graphic icons are used throughout the documentation set. These icons and their associated meanings are described below.

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

Related Documents

For the latest version of this guide and all documentation sets for the respective devices, go to: zebra.com/support.

Refer to specific vendor documentation for detailed infrastructure information.

Device Settings

This chapter includes device settings for default, supported, and voice traffic recommendations.

Default, Supported, and Recommended for Voice Device Settings

Note the following:

- Pairwise master key identifier (PMKID) is disabled on the device by default. If your infrastructure configuration is configured for PMKID, enable PMKID and disable the opportunistic key caching (OKC) configuration.
- The Subnet Roam feature allows you to change the network IP of the WLAN interface when the network is configured for a different subnet on the same extended service set identification (ESSID).
- In execution of default fast transition (FT) (also known as FT Over-the-Air), in case that other non-FT Fast Roaming Methods might be available on the same SSID, see Fast Roam Methods in Table 4 and relevant notes in General WLAN Recommendations on page 17.
- Use mobile device management (MDM) agents to change settings. Use the user interface (UI) to change parameter subsets.
- For voice applications, and for any highly-dependent client-server communication apps, it is not recommended to use the Android battery optimization feature (also known as Doze Mode) in device management tools. Battery optimization interrupts communication between dependent endpoints and servers.
- Media access control (MAC) randomization:
  - From Android Oreo onwards, Zebra devices support the MAC randomization feature, which is enabled by default. Disable or enable this via MDM or via Android privacy setting Use Device MAC:
    - When enabled in Android 10 versions and earlier, the randomized MAC value is used only for Wi-Fi scanning of new networks prior to association with the intended network (prior to new connection), however, it is not used as the associated device MAC address. The associated MAC address is always the physical MAC address.
    - When enabled in Android 11 onwards, the randomized MAC value is also used for association with the intended network. The randomized value is specific for each network name (SSID). It remains the same when the device roams from one AP of the connected network to different AP(s) of the same network, and/or when it has to fully re-connect to the specific network after being out of coverage.
  - The MAC randomization feature does not affect voice performance and it is not necessary to disable this feature for general troubleshooting purposes. However, in some specific situations, disabling it may be helpful during the troubleshooting data collection.

NOTE: The TC21, TC21-HC, TC26, and TC26-HC are assumed to be provisioned with Zebra's mDNA software license in the voice deployment. Table 1 does not apply to the these devices if they do not have that license.

The following table lists the default, supported configuration, and recommended voice settings.

The default value is recommended in the Recommended for Voice column, which is also the default value populated in recent Product Releases. Observe the notes in the Default Configuration columns. If a prior release is applicable in the deployment and the Recommended for Voice setting is the default, then it

is recommended to reconfigure the respective item in the older release to match the noted value in the newer release.

Table 1 Default, Supported, and Recommended Voice Device Settings

Feature	Default Configuration	Supported Configuration	Recommended for Voice
State11d	Country selection set to Auto	• Country selection set to Auto • Country selection set to Manual	Default
ChannelMask_2.4 GHz	All channels enabled, subject to local regulatory rules.	Any individual channel can be enabled or disabled, subject to local regulatory rules.	Device Mask matches the exact set of network side operating channels configuration. It is recommended to configure both the device and the network to a reduced set of channels 1, 6, and 11, if WLAN SSID is enabled on 2.4 GHz.
ChannelMask_5.0 GHz	• Up to Android Oreo Build Number 01.13.20, all non-dynamic frequency selection (DFS) channels are enabled. • From Android Oreo Build Number 01.18.02 onwards, Android 9 and, Android 10, all channels are enabled, including DFS. All the above are subjected to regulatory.	Any individual channel can be enabled or disabled, subjected to regulatory	Device Mask matches the exact set of network side operating channels configuration. It is recommended to configure both the device and the network to a reduced set of only non-DFS channels. For example, in North America, configure the network channels to 36, 40, 44, 48, 149, 153, 157, 161, 165.
Band Selection	Auto (both 2.4 GHz and 5 GHz bands enabled)	• Auto (both bands enabled) • 2.4 GHz • 5 GHz	5 GHz

Table 1 Default, Supported, and Recommended Voice Device Settings (Continued)

Feature	Default Configuration	Supported Configuration	Recommended for Voice
Band Preference	Disabled	• Enable for 5 GHz • Enable for 2.4 GHz • Disable	Enable for 5 GHz, if WLAN SSID is on both bands.
Open Network Notification	• Enabled in Android 10 onwards • The default is disabled in Android 10 versions and earlier.	• Enable • Disable	Default
Advanced Logging	Disabled	• Enable • Disable	Default
User Type	Non-Restricted	• Enable • Disable	Default
Cisco Centralized Key Management (CCKM)	All other models: Enabled if this is the only key management method in the SSID configuration. This is not used if 11r is also enabled on SSID. TC52ax: Disabled. Requires staging change to enable if this is the only key management method in the SSID configuration.	• Enable • Disable	Default TC52ax: Not recommend to enable for voice centric deployments, except forced by SSID configuration.
FT	Enabled	• Enable • Disable	Default
OKC	Enabled	• Enable • Disable	Default
PMKID	Disabled	• Enable • Disable	Default

Table 1 Default, Supported, and Recommended Voice Device Settings (Continued)

Feature	Default Configuration	Supported Configuration	Recommended for Voice
Power Save	NDP (Null data power save)	• NDP • Power save polling (PS-POLL) • Wi-Fi multimedia power save (WMM-PS)	Default
11k	Enabled	• Enable • Disable	Default
11v	TC52ax: Enabled from build 11.16.05 with U120 onwards All other models: Enabled from build 11.20.18 onwards	• Enable • Disable	Use the default for each build version.
Subnet Roam	Disabled	• Enable • Disable	Default
11w	After Android 10: Enable / Optional Before Android 10: Disable	• Enable / Mandatory • Enable / Optional • Disable	Default
Channel Width	2.4 GHz - 20 MHz 5 GHz - 20 MHz, 40 MHz and 80 MHz	Not configurable	Default
11n	Enabled	• Enable • Disable Note: Disabling this also disables 11ac.	Default
11ac	Enabled	• Enable • Disable	Default

Device Wi-Fi Quality of Service (QoS) Tagging and Mapping

This section describes device QoS tagging and mapping of packets from the device to the AP (such as outgoing packets in the uplink direction).

The tagging and mapping of traffic in the downlink direction from the AP to the device is determined by the AP or controller vendor implementation or configuration, which is not in the scope of this document.

For the uplink direction, an application on the device sets Differentiated Service Code Point (DSCP) or Type of Service (ToS) values for its sourced packets, based on the application's specifications. Prior to the transmission of each packet over Wi-Fi, the DSCP or ToS values determine the device's further 802.11 Tagging ID assigned to the packet, and the mapping of the packet to 802.11 Access Category.

The 802.11 tagging and mapping columns are provided for reference and are not configurable. The IP DSCP or ToS values may or may not be configurable, depending on the app.

NOTE: Table 2 describes the tagging and mapping values for outgoing packets when no other dynamic protocols affect them by standard specifications. For example, if the WLAN infrastructure mandates the Call Admission Control (CAC) protocol for certain traffic types (such as voice and/or signaling), tagging and mapping obey the dynamic states of the CAC specifications. This means that there could be CAC configuration or sub-periods in which the tagging and mapping apply different values than mentioned in the table, even though the DSCP value is the same.

Table 2 Device Wi-Fi QoS Tagging and Mapping for Outgoing Traffic

IP DSCP Class Name	IP DSCP Value	ToS Hexa	Tagging of 802.11 TID (Traffic ID) and UP (802.1d UserPriority)	Mapping to 802.11 Access Category (same as Wi-Fi WMM AC spec)
none	0	0	0	AC_BE
cs1	8	20	1	AC_BK
af11	10	28	1	AC_BK
af12	12	30	1	AC_BK
af13	14	38	1	AC_BK
cs2	16	40	2	AC_BK
af21	18	48	2	AC_BK
af22	20	50	2	AC_BK
af23	22	58	2	AC_BK
cs3	24	60	4	AC_VI
af31	26	68	4	AC_VI
af32	28	70	3	AC_BE
af33	30	78	3	AC_BE
cs4	32	80	4	AC_VI
af41	34	88	5	AC_VI
af42	36	90	4	AC_VI
af43	38	98	4	AC_VI
cs5	40	A0	5	AC_VI
ef	46	B8	6	AC_VO
cs6	48	C0	6	AC_VO
cs7	56	E0	6	AC_VO

Network Settings and Device RF Characteristics

This section describes device settings for the recommended environment and device RF characteristics.

Recommended Environment

- Perform a Voice Grade Site Survey to ensure the requirements in Table 3 are met.
- Signal to Noise Ratio (SNR), measured in dB, is the delta between the noise in dBm and the coverage RSSI in dBm. The minimum SNR value is shown in Table 3. Ideally, the raw noise floor should be -90 dBm or lower.
- In floor level, Same-Channel Separation refers to two or more APs with the same channel are in RF sight of a scanning device in a given location. Table 3 specifies the minimum received signal strength indicator (RSSI) delta between these APs.

Table 3 Network Recommendations

Setting	Value
Latency	< 100 msec end-to-end
Jitter	< 100 msec
Packet Loss	< 1%
Minimum AP Coverage	-65 dBm
Minimum SNR	25 dB
Minimum Same-Channel Separation	19 dB
Radio Channel Utilization	< 50%
Coverage Overlap	20% in critical environments

Table 3 Network Recommendations (Continued)

Setting	Value
Channel Plan	2.4 GHz: 1, 6, 11 • No adjacent channels (overlapping) • Overlapping APs must be on different channels 5 GHz: 36, 40, 44, 48, 149, 153, 157, 161, 165 • If you are using DFS channels, broadcast the SSID in beacons. • Unlicensed National Information Infrastructure-2 (U-NII-2) (DFS channels 52 to 140) and U-NII-3 (channels 149 to 165) are subject to local regulatory rules.

Device RF Capabilities

The device model capabilities supported by the Zebra device are not configurable and are listed as follows:

- 2x2 MU-MIMO is a two antennas solution.
  - Wi-Fi 6 without Dual Band Simultaneous (DBS) - TC52ax and TC52ax-HC
  - Wi-Fi 5 with DBS - TC52, TC52-HC, TC52x, TC52x-HC, TC57, TC57x, TC72, TC77, PS20, EC30, and MC93.
- 1x1 MU-MIMO is a single antenna solution with the ability to participate in the downlink MU-MIMO environment of the AP.
  - Wi-Fi 5 without DBS - TC21, TC21-HC, TC26, and TC26-HC.

DBS Advantages in 2x2 MU-MIMO Devices

2x2 devices with DBS use several functionalities which allow one antenna to be on a specific band (5 GHz or 2.4 GHz), while the other antenna can be on another band at the same air time.

Important DBS Performance Considerations

Stable network connectivity and streaming traffic during roaming are important to time-sensitive applications such as voice. The availability of DBS on the devices results in better performance concerning the following parameters:

- DBS devices do not spend much time on off-channel scanning compared to non-DBS devices. Packet loss typically happens when devices are performing off-channel scanning. Therefore, the ongoing traffic between the DBS devices and the APs has lower packet loss. This reduces the jitter and delays of the traffic.
  - The off-channel scanning time depends on the distributions or layouts of deployments and the WLAN configurations such as 11k. On average, DBS devices spend about half the time non-DBS do on off-channel scanning.
- DBS devices complete scanning cycles in a shorter time than the non-DBS to search for the best AP. DBS devices scan and connect to the next stronger AP before the current AP connection deteriorates and impacts the traffic or disconnects during roaming. By doing this quicker than non-

DBS, the connectivity is less likely to be interrupted, and the data transmission traffic keeps going in an expected stable quality without packet retries. In addition to that, when DBS devices move from a poor network coverage area which is not covered at all or spotty to a better one, the devices can connect to the new network quicker than the non-DBS.

- The switching speed from one AP to another by DBS devices depends on the distributions or layouts of deployments and the WLAN configuration such as 11k. On average, DBS devices are 50% faster than non-DBS.

Relevant Use Cases and Environments

The WLAN deployment eco-system and the quality requirements of applications impose different dynamic characteristics that probably impact the connectivity and the quality. The use cases and environments relevant to the capabilities of DBS are as follows:

- When the deployment includes time-sensitive applications using Wi-Fi, such as voice and video calls, which need to maintain active registration and connectivity parameters with the backend servers.
- When users are using time-sensitive applications, such as voice calls, moving across a building for a continuous duration while roaming.
- When users are using applications that need to have good connection quality while moving within a building that does not have continuous Wi-Fi network coverage. The building layout, obstruction, and other use cases may impact the Wi-Fi network coverage.
- When the infrastructure channel plan has many channels (such as more than 15 channels).

The higher the level of those characteristics is, the more critical DBS is.

Devices with Wi-Fi 6 Advantages

Devices that support Wi-Fi 6 (802.11ax) can use the unique capabilities when connected to WLAN or APs infrastructure that also supports Wi-Fi 6 or 802.11ax. Orthogonal frequency-division multiple access (OFDMA) is a Wi-Fi 6 feature that increases the efficiency of handling the application traffic and is useful for time-sensitive applications such as voice.

OFDMA allows the APs to subdivide the serving channel into sub-channels and to allocate smaller frequencies to each, such that the AP can handle the simultaneous data transmission on the channel to multiple connected devices (OFDMA downlink transmissions), and simultaneous data reception on the channel from multiple connected devices (OFDMA uplink transmissions).

The efficiency of the OFDMA allows the ecosystem to support a much larger capacity of time-sensitive applications that are used by multiple devices simultaneously on the channel, while keeping the traffic performance intact and maintaining the stable performance with negligible jitter, latency, and packet loss for all the connected devices. Without OFDMA, a lower number of connected devices can receive good quality service from the given APs.

2x2 MU-MIMO and 1x1 MU-MIMO Devices Antenna Configuration

Device RF Capabilities on page 13 shows that most devices covered in this guide are 2x2 MU-MIMO and some are 1x1 MU-MIMO. Most APs of the WLAN infrastructure in enterprise deployments support 2x2 MU-MIMO. The key aspects of the 2x2 or 1x1 devices in Device RF Capabilities on page 13 fitting into a 2x2 WLAN environment are different, especially when stable network connectivity is required and time-sensitive applications such as voice are used.

Air Medium and Time Sharing

In the WLAN infrastructure that supports Wi-Fi 5 (802.11ac) or earlier and regardless of the Wi-Fi generation of the wireless devices, the AP and devices must wait for the air medium to be free before each and next data transmission can occur. If the AP and the device are both 2x2, the transmission speed can be at the maximum rate of the 2x2 communication capability between them. Meaning, the airtime for each transmission between the AP and the device is shorter and the medium is free in a shorter time for the next potential transmission. However, if the device is 1x1, the maximum rate of communication between the AP and the device is determined by the 1x1 modulation scheme which has a lower speed. This leads to longer airtime for each transmission and longer wait time for each and next potential transmission.

When the Wi-Fi 6-enabled devices are connected to a WLAN infrastructure that also supports Wi-Fi 6 (802.11ax), there is no contention in airtime. The OFDMA technology in Wi-Fi 6 mitigates the airtime contention challenge to some degree by allowing simultaneous data transmission to multiple devices. However, the maximum rate is still determined by the maximum modulation scheme of 2x2 or 1x1.

Even though a 1x1 is capable of carrying the traffic of time-sensitive application in terms of speed and pace, the main aspects that need attention are the nearby congregation and potential amount of the 1x1 links between the APs and devices in the network ecosystem. This may dynamically impact the air medium, and then may impact the traffic utilization and capacity, potentially leading to latency to or from one or more of the applications.

For example, when many devices are likely to be connected to the same strong AP and each of these devices are sending and receiving time-senstitive application data at the same time, the 2x2 devices are less likely to be suffering air medium contention, whereas the data streaming speed for the 1x1 devices might be impacted. In another example, in the networks which must serve high-throughput applications next to the ongoing operating voice, regardless of the number of users, utilization of the high-throughput applications has lesser impact on the voice in the network ecosystem of 2x2 links as compared to the 1x1.

No formula can be used to compute the exact capacity and performance of the 1x1. When 1x1 devices are considered for time-sensitive application deployments, running pre-tests in the deployed WLAN of the respective use-cases or in the heaviest RF conditions and capacity is important to evaluate the performance.

Multipath and Interference

Multipath, caused by RF signals reflected from the surfaces of physical obstructions, and external RF signals are two factors that potentially distort the original transmission of any 802.11 wireless network. In such conditions, a 1x1 device may struggle to decode a large amount of distorted signals, which results in the network having to retransmit the signals. A high retransmission rate in the ecosystem causes latency, packet loss, and medium congestion, which can then become a self-inflicting factor that impacts the air medium and capacity. However, the 2x2 devices are capable of taking advantage of the elevated gains of the multipath signals and using the maximum ratio combined (MRC) method to decode the distorted signals. Therefore, retransmission is not required.

No network environment is free of multipath, and no formula can predict the exact level of multipath impacting the 1x1 which may lead to retry and poor data transmission quality. It is recommended that users run pre-tests on the 1x1 models to evaluate the RF signal performance. In addition, users can use some RF spectrum survey tools and sniffers to detect the noise level and RF interference in the environment.

Coverage and Range

For the WLAN deployments that take place in uneven network coverage areas due to low RSSI, weak spots where individual AP range does not overlap, and/or the devices are at a farther distance outside the

network perimeter or in transitions between two separate areas or buildings, the following aspects need to be fulfilled:

- The devices need to hear APs beacons at a larger distance to maintain the connectivity.
- The devices need to hear the AP downlink of time-sensitive packets at that same distance.
- The AP needs to hear the device uplink of time-sensitive packets at that same distance.

There are several mechanisms that give a 2x2 device more advantages than a 1x1 device to accomplish the three aspects above.

- When a 2x2 device hears the AP beacons or AP-downlink from a far distance that have weak signals, the ability to use the maximum ratio combined (MRC) from the two spatial streams improves the chances to decode the signal as valid and distinguish it from the local noise. A 1x1 device is unlikely to be able to decode weak signals.
- The 2-antenna design and placement in the 2x2 device help MRC receive signals and reduce the chances that the dynamic positioning of the device (such as the device orientation and the way that the users hold the device) in the 3-dimensional space might impact the ability to hear weak signals.
- A 2x2 uses the cyclic delay diversity (CDD) mechanism to achieve full diversity by turning spatial diversity into frequency diversity when transmitting data to an AP as in any 2x2 MU-MIMO transmission. Using CDD increases the chances for the AP to hear the 2 spatial streams of the device that is from a far distance.

When the coverage expectations are known, the potential challenges may be surveyed and corrected by using WLAN coverage survey tools.

It is important to consider that time-sensitive applications in 1x1 devices require a close to ideal WLAN coverage to operate, where the deployed AP power or channels are overlapped and no error in other network criteria. In such deployments, it is recommended to re-survey and re-check the coverage more frequently, especially when the infrastructure-related configuration parameters have changes.

Infrastructure and Vendor Model Recommendations

This section includes recommendations for Cisco infrastructure settings, including WLAN practices for enabling voice as well as more specific recommendations to manage voice traffic and maintain expected voice quality.

This section does not include a full list of WLAN configurations, but only those required verification to accomplish successful interoperability between Zebra devices and the Cisco network.

The listed items may or may not be default settings of the given Cisco release version. Verification is advised.

General WLAN Recommendations

This section lists recommendations to optimize WLAN to support voice deployment.

- For best results, use Wi-Fi Certified (voice enterprise certification from Wi-Fi Alliance) AP models.
- If SSID for voice is enabled on 2.4G band, do not enable the 11b-legacy data rates on that band unless specifically required by some restricted coverage planning or older legacy devices must be supported.
- The device chooses to roam or connect to an AP depending on the infrastructure settings in effect and the underlying dynamics of the RF ecosystem. Generally, the device scans for other available APs at certain trigger points (for example, if the connected AP is weaker than -65 dBm) and connects to a stronger AP if available.
- 802.11r: Zebra strongly recommends that the WLAN network supports 11r FT as a fast-roaming method to achieve the best WLAN and device performance and user experience.
    - 11r is recommended above other fast-roaming methods, including any vendor-proprietary methods, such as Cisco centralized key management (CCKM).
    - When the 11r is enabled on the network, either with pre-shared-key (PSK) security (such as FT-PSK) or with an authentication server (such as FT-802.1x), the Zebra device automatically facilitates 11r, even if other parallel non-11r methods co-exist on the same SSID network. No configuration is needed.
- Disable unused Fast Roam Methods from the SSID if possible. However, if older devices on the same SSID support a different method, that two or more methods may remain enabled if they can coexist. The device automatically prioritizes its selection per the Fast Roaming Method in Table 4.
- It is a general best practice to limit the amount of SSID per AP to only those required. There is no specific recommendation on the number of SSIDs per AP as this depends on multiple RF environmental factors which are specific to each deployment. A high number of SSIDs impacts channel utilization which comprises not only users and application traffic, but also beacons traffic of all SSIDs on the channel, even those not in use.

- Call Admission Control (CAC):
  - The network's CAC feature is designed to facilitate VoIP deployments, but uses algorithmic complexities to determine whether to accept or reject new calls based on network resources in runtime.
  - Do not enable (set to mandatory) CAC on the controller without testing and validating the stability of admissions (calls) in the environment under stress and plurality conditions.
  - Be aware of devices that do not support CAC which are using the same SSID as Zebra devices support CAC. This scenario requires testing to determine how the network CAC impacts the entire eco-system.
- If WPA3 is required for the deployment, refer to the Zebra WPA3 Integrator Guide for guidance on device models that support WPA3 and configuration guidance.

WLAN Infrastructure Recommendations for Voice Support

Table 4 WLAN Infrastructure Recommendations for Voice Support

Setting	Value
Infra type	Controller based
Security	WPA2 or WPA3
Voice WLAN	5 GHz only
Encryption	AES Note: Do not use Wired Equivalent Privacy (WEP) or Temporal Key Integrity Protocol (TKIP).
Authentication: Server Based (Radius)	802.1X EAP-TLS/PEAP-MSCHAPv2
Authentication: Pre-Shared Key (PSK) Based	Enable both PSK and FT-PSK. Note: Device automatically selects FT-PSK. PSK is necessary to support legacy/non-11r devices on same SSID.
Operational Data Rates	2.4 GHz: • G: 12, 18, 24, 36, 48, 54 (disable all lower rates, including 11b-legacy) • N: MCS 0 -15 5 GHz: • A:12, 18, 24, 36, 48, 54 (disable all lower rates) • AN: MCS 0 - 15 • AC: MCS 0 - 7, 8 • AX: MCS 0 - 7, 8, 9, 10, 11 Note: Adjust rate settings according to environmental characteristics. See Recommended Environment on page 12 to accomplish balanced AP minimum coverage.

Table 4 WLAN Infrastructure Recommendations for Voice Support (Continued)

Setting	Value
Fast Roam Methods (See General WLAN Recommendations on page 17)	If supported by infrastructure in priority order: • FT (802.11R) • CCKM • OKC or PMK Cache. Do not enable both.
DTIM Interval	1
Beacon Interval	100
Channel Width	2.4 GHz: 20 MHz 5 GHz: 20 MHz
WMM	Enable
802.11k	Enable only Neighbor Report. Do not enable any 11k measurements.
802.11w	Enable as optional (not mandatory)
802.11v	Enable
AMPDU	Enable Note: Local environmental/RF situations (such as high interference level, collisions, obstructions) may yield local high retries ratio, delays, and packet-drops. The AMPDU feature can degrade voice performance in addition to the challenging RF. In such cases, it is recommended to disable the AMPDU.

Cisco Infrastructure Recommendations for Voice Quality

This section lists more specific Cisco infrastructure recommendations to handle voice traffic and maintain expected voice Quality.

Table 5 Cisco Infrastructure Recommendations for Voice Quality

Recommendation	Required	Recommended But Not Required
Configure voice WLAN to use the 802.11a band.		✓
Set EAP Retry Timeout to default.	✓	
Disable DHCP address assignment required option.	✓	
Disable Session Timeout or set to shift duration + one hour.	✓	
Disable Client Exclusions.	✓	
Set the User Idle Timeout to Session Timeout definition (above).	✓	
Enable Fast SSID change.	✓	
Disable Cisco client extensions (CCX) Radio Measurements.	✓	
Allow WMM for the voice WLAN.	✓	

Table 5 Cisco Infrastructure Recommendations for Voice Quality (Continued)

Recommendation	Required	Recommended But Not Required
Mark Voice WLAN with Platinum QoS.	✓	
For Platinum QoS profile set 802.1p bits to 6.	✓	
Trust DSCP markings end to end.		✓
Validate that the mobility status shows as UP between all controllers in the same mobility group.	✓	
Set EAP-Identity-Request Timeout (seconds) to 3 (see note below table.)		✓
Set EAP-Identity-Request Max Retries to 2.	✓	
Set EAP-Request Timeout (seconds) to 3.	✓	
Set EAP-Request Max Retries to 2.	✓	
Disable MAC protocol data unit (MPDU) aggregation for voice.	✓	
Disable Optimized Roaming.	✓	
Ensure FT (11r) is set to Enable, not Adaptive.	✓	
Verify that the EDCA profile on the controller is set to Voice Optimized.		✓
Verify that Aggressive Load Balancing is disabled.	✓	
Verify that DTPC is disabled. See Recommendations for DTPC (Dynamic Transmit Power Control) in Notes on page 20.		✓
Verify the Beacon Interval is set to 100 msec.	✓	
Verify that Client MFP is disabled.		✓
Verify that peer-to-peer blocking is disabled.	✓	
Validate the virtual interface address is the same across all controllers in the same mobility group.	✓	

Notes

- Inspect Cisco software versions to determine if they are marked DF (deferred release) by Cisco. If so, avoid these version.
- Cisco ecosystems typically use features which attempt to dynamically learn and improve the RF environment. While beneficial, these features, such as Radio Resource Management (RRM), Dynamic Channel Assignment (DCA), Auto Transmit Power, Coverage Hole Detection (CHD), and Off-Channel-Scan-Defer, engage in constant processing that can negatively impact the RF stability necessary for voice applications.
    - Zebra strongly recommends carefully analyzing the usage of these features throughout the deployment, during the enabling phases and after reconfiguration, as well as using wireless survey, RF tools, and frequent monitoring of the health and impact of these features. If such precautions are not possible, Zebra recommends disabling them completely in voice deployments.

- Following are best practices for RRM, DCA, CHD, and related features. Consider the particular deployment to determine if they are applicable.
  - Recommendations for DCA when set to Automatic:
    - The DCA Channel List is used to assign a channel to each radio/band of APs.
    - Set Sensitivity Threshold to Low.
    - Set Interval of DCA to 24 hours.
    - For several other DCA parameters that use the Avoid … terminology, follow Cisco guidelines.
  - Recommendations for RRM, CHD, and Auto Transmit Power:
    - Set the monitoring interval and frequency values to maximum (lowest frequency) where possible, respective to tasks, such as AP channel scans and neighbor-packets-scans.
    - Set the Transmit Power minimum and maximum within a range of 6 dB. For example, min = 12, max = 18. Note: This is a command-line interface (CLI) only parameter.
  - Recommendations for Off Channel Scan Defer:
    - For Scan Defer Priority selection for voice (platinum, UP = 6), set the Scan Defer Time to the maximum value supported (lowest frequency of the scan).
- Take care when setting the mandatory and supported rates:
  - Set Beacons to the lowest mandatory rate (Cisco default).
  - Disable rates below lowest-mandatory, unless there is specific reason to make the cell sizes appear smaller than the range (distance) that data/voice packets can travel. This is typically not the case.
- Recommendations for Aironet IEs:
  - In typical voice deployments, enabling Aironet IEs in the controller is required when CCKM is used for fast roaming. Otherwise, Aironet IEs sub-features are ineffective for voice enterprise and have been replaced by other standards.
  - If CCKM is not used for fast roaming, disable Aironet IE.
- Recommendations for DTPC (Dynamic Transmit Power Control):
  - DTPC is a mechanism in which the AP requests CCX-enabled clients to set their transmit power to a specific value determined by dynamic algorithms of the RRM. In a voice deployment with the careful configuration of RRM parameters with respect to the environment, the DTPC may help resolve corner cases of localized imbalance issues (for example, the AP not hearing the device), and otherwise cause no harm.
  - Disable the DTPC in the following situation: In a complex RF environment, DTPC changes may be excessive system-wide, reflecting the AP-side RRM changes. As a result, because a device moves faster than the RRM relearns and rebalances in surrounding areas, the device may remain the DTPC value of the prior RF area, rather than adjusting to the value of the new RF area. In this way, the DTPC may possibly create the imbalance that it is designed to resolve. The AP RRM indexes from the new RF area would continually loopback and make more power changes to resolve the issues created by DTPC. This recursive loop could negatively impact voice quality.
- Set the EAP-Request-Identity Timeout to 30 seconds, if connected devices on the relevant SSID are not only mobile devices. For example, laptops in which the EAP identity exchange (user/password) with the EAP server may involve human interaction via typed-in credentials.

Zebra Recommended WLC, AP Models, and Firmware versions

NOTE: Model versioning recommendations in this section are based on satisfactory interop test plan results. Zebra recommends that when using other software versions not listed below, consult the WLC/AP in the Release Notes to verify that a particular version is stable and preferred by the vendor.

- WLC 5508:
  - Software Version: 8.5.171.0 in Local Mode
- WLC 3504 and WLC 5520:
  - Software Versions: 8.10.151.x, 8.10.162.x, 8.10.171.x
- WLC 9800:
  - Software Version: 17.3.4, 17.6.3
- Tested AP Models: 1242,1262, 1852, 2600, 2802, 3602, 3708, 3800, 9115, 9120, 9130

Additional WLC and AP Resources and Notes

- Go to the following Cisco pages for versioning recommendations per controller type, compatibility matrices of software and hardware, EOL announcements, and additional information:
  - cisco.com/c/en/us/support/wireless/index.html
  - cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html
- Go to Cisco support cisco.com/c/en/us/support/index.html to open a case if Cisco support is needed.
- Go to the following pages for Catalyst 9800 Wireless Controller recommendations and configurations:
  - cisco.com/c/en/us/td/docs/wireless/controller/9800/17-3/config-guide/b_wl_17_3_cg.html
  - cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/guide-c07-743627.html
  - cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214863-voice-deployment-on-catalyst-9800-wirele.html
  - Go to cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810.html for AireOS Wireless Controller recommendations and configurations.
- FlexConnect vs Local Mode:
  - FlexConnect is a wireless solution that enables customers to configure and control access points (APs) in a branch or remote office from the corporate office through a wide area network (WAN) link without requiring a controller in each office. FlexConnect APs switch client data traffic and perform client authentication locally when the connection to the controller is lost. When connected to the controller, APs can send traffic back to the controller as well as perform local authentication.
  - In Local Mode, APs associate directly to an on-site wireless controller via control and provisioning of wireless APs (CAPWAP) (or lightweight access point protocol (LWAPP) depending on the IOS

version) tunnel. Traffic goes directly to the wireless controller to be centrally switched. If an app loses connectivity to the controller, it stops forwarding traffic and starts looking for the controller.

- Cisco and Zebra recommend using Local Mode for Zebra and Cisco deployments due to additional features it offers, but encourage using the mode best suited for the specific deployment.
- Go to the following pages for more information on FlexConnect and Local Mode for Cisco Wireless Deployments:
  - cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213945-understand-flexconnect-on-9800-wireless.html
  - cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/flexconnect.html.