ZEBRA

cisco
The bridge to possible

Best Practices Guide
Voice Deployment Optimization with Cisco Infrastructure

Zebra TC51, TC56, TC70x, TC75x, MC33

Contents

© 2021 Cisco and/or its affiliates. All rights reserved.
© 2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

The bridge to possible

Contents

© 2021 Cisco and/or its affiliates. All rights reserved.
© 2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

About this guide

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

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

- TC51
- TC51-HC
- TC56
- TC70x
- TC75x
- MC33.

Icon conventions

The documentation set is designed to give the reader helpful 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 the specific vendor documentation for detailed infrastructure information.

ZEBRA

CISCO
The bridge to possible

Contents

© 2021 Cisco and/or its affiliates. All rights reserved.
© 2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

Device settings

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

Default, supported, and recommended voice device settings

This section includes specific recommendations for voice that are not set as the default out-of-the-box configuration. It is generally advised to examine those specific settings in alignment with the WLAN network needs and compatibilities. In some cases, changing the defaults could harm generic connectivity performance.

Besides these specific recommendations, which need careful examination, most of the device's default settings are already optimized for voice connectivity. For that reason, it is recommended that you keep the defaults and let the device dynamically adjust the WLAN's dynamic feature-selection levels. Device configuration should change only if there are WLAN (Wireless LAN Controller [WLC] or Access Point [AP]) features that mandate respective changes on the device side to allow proper interoperation.

Note the following:

- The 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 Identifier (ESSID).
- In execution of default Fast Transition (FT) (also known as FT Over-the-Air), if other non-FT fast roaming methods might be available on the same SSID, see Fast Roam Methods in Table 5 and relevant notes in General WLAN Recommendations on page 11.
- 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, we recommended not using the Android battery optimization feature (also known as Doze mode) in device management tools. Battery optimization interrupts communication between dependent endpoints and servers.

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

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 the network-side operating channels' configuration. We recommend configuring 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	All non-Dynamic Frequency Selection (DFS) 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 the network-side operating channels' configuration. We recommend configuring 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, and 165.
Band Selection	Auto (both 2.4 GHz and 5 GHz bands enabled)	• Auto (both bands enabled) • 2.4 GHz • 5 GHz	5 GHz
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	Disabled	• Enable • Disable	Default

© 2021 Cisco and/or its affiliates. All rights reserved.
© 2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

ZEBRA

CISCO
The bridge to possible

Feature	Default configuration	Supported configuration	Recommended for voice
Advanced Logging	Disabled	• Enable • Disable	Default
User Type	Nonrestricted	• Enable • Disable	Default
Cisco Centralized Key Management (CCKM)	Enabled	• Enable • Disable	Default
Fast Transition (FT)	Enabled	• Enable • Disable	Default
Opportunistic Key Caching (OKC)	Enabled	• Enable • Disable	Default
Pairwise Master Key Identifier (PMKID)	Disabled	• Enable • Disable	Default
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
Subnet Roam	Disabled	• Enable • Disable	Default
11w	Disabled	• Enable/Mandatory • Enable/Optional • Disable	Default or Enable/Optional

© 2021 Cisco and/or its affiliates. All rights reserved.
© 2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

Feature	Default configuration	Supported configuration	Recommended for voice
Channel Width	2.4 GHz: 20 MHz 5 GHz: 20 MHz, 40 MHz, and 80 MHz	Not configurable	Default
FT Over The DS	Enabled	• Enable • Disable	Default
11n	Enabled	• Enable • Disable **Note:** Disabling this also disables 11ac.	Default
11ac	Enabled	• Enable • Disable	Default
11v	Disabled	• Enable • Disable	Enable

© 2021 Cisco and/or its affiliates. All rights reserved.
© 2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

ZEBRA

cisco
The bridge to possible

Contents

© 2021 Cisco and/or its affiliates. All rights reserved.
© 2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

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 Services 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 an 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 under the 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 there could be a CAC configuration or subperiods 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 user priority)	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

ZEBRA

CISCO
The bridge to possible

Contents

IP DSCP class name	IP DSCP value	ToS hexa	Tagging of 802.11 TID (traffic ID) and UP (802.1d user priority)	Mapping to 802.11 access category (same as Wi-Fi WMM AC spec)
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

© 2021 Cisco and/or its affiliates. All rights reserved.
© 2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

ZEBRA

cisco
The bridge to possible

Contents

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 that the requirements in Table 3 are met.
- The Signal-to-Noise Ratio (SNR), measured in dB, is the delta between the noise in dBm and the coverage received Signal Strength Indication (RSSI) in dBm. The minimum SNR value is shown in Table 3. Ideally, the raw noise floor should be -90 dBm or lower.
- At the floor level, same-channel separation refers to two or more APs with the same channel that are in RF sight of a scanning device in a given location. Table 3 specifies the minimum RSSI delta between these APs.

Table 3. Network environment recommendations

Setting	Value
Latency	< 100 ms end-to-end
Jitter	< 100 ms
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
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. ▪ **Note:** Unlicensed National Information Infrastructure-2 (U-NII-2) (DFS channels 52 to 140) and U-NII-3 (channels 149 to 165) are subject to the local regulatory rules

© 2021 Cisco and/or its affiliates. All rights reserved.
© 2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

The bridge to possible

Contents

© 2021 Cisco and/or its affiliates. All rights reserved.
© 2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

Device RF capabilities

Table 4 lists the RF capabilities supported by the Zebra device. These are not configurable.

Table 4. RF capabilities

Setting	Value
Dynamic Transmit Power Control (DTPC)	Supported (as per Cisco Client Extensions v4)
Roam Threshold	-65 dBm (cannot be modified)
Device-specific Antenna Configuration	• TC51: 2x2 Multiple Input, Multiple Output (MIMO) • TC51-HC: 2x2 MIMO • TC56: 1x1 Single Input, Single Output (SISO) • TC70x: 2x2 MIMO • TC75x: 2x2 MIMO • MC33: 2x2 MIMO
11n Capabilities	A-MPDU Tx/Rx, A-MSDU Rx, STBC, SGI 20/40, etc.
11ac Capabilities	Rx MCS 8-9 (256-QAM) and Rx A-MPDU of A-MSDU

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 that require 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.

ZEBRA

cisco
The bridge to possible

Contents

© 2021 Cisco and/or its affiliates. All rights reserved.
© 2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

General WLAN recommendations

This section lists recommendations to optimize the 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 the 2.4-GHz band, do not enable the 802.11b legacy data rates on that band unless specifically required by some restricted coverage planning or older legacy devices that 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 support 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.
  - When 11r is enabled on the network, either with Preshared 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 roaming methods from the SSID if possible. However, if older devices on the same SSID support a different method, two or more methods may remain enabled if they can coexist. The device automatically prioritizes its selection per the Fast Roam Methods setting in Table 5.
- It is a general best practice to limit the number 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 that are specific to each deployment. A high number of SSIDs impacts channel utilization, which comprises not only user and application traffic, but also the beacon 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.

ZEBRA

cisco
The bridge to possible

Contents

© 2021 Cisco and/or its affiliates. All rights reserved.
© 2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

WLAN infrastructure recommendations for voice support

Table 5. WLAN infrastructure recommendations for voice support

Setting	Value
Infra Type	Controller based
Security	WPA2
Voice WLAN	5 GHz only
Encryption	Advanced Encryption Standard (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 or non-11r devices on the 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 to15 5 GHz: • A:12, 18, 24, 36, 48, 54 (disable all lower rates) • AN: MCS 0 to 15 • AC: MCS 0 to 7, 8 **Note:** Adjust rate settings according to environmental characteristics. See Recommended Environment on page 9 to accomplish balanced AP minimum coverage.

ZEBRA

cisco
The bridge to possible

Contents

Setting	Value
Fast Roam Methods (see General WLAN Recommendations on page 11)	If supported by infrastructure in priority order: • FT (802.11R) • CCKM • OKC or PMK Cache (do not enable both)
Delivery Traffic Indication Message (DTIM) Interval	1
Beacon Interval	100
Channel Width	2.4 GHz: 20 MHz 5 GHz: 20 MHz
Wireless Multimedia Extensions (WMM)	Enable
802.11k	Enable only Neighbor Report. Do not enable any 11k measurements.
802.11w	Enable as optional (not mandatory)
802.11v	Enable
Aggregated MAC Protocol Data Unit	Disable for voice

© 2021 Cisco and/or its affiliates. All rights reserved.
© 2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

ZEBRA

cisco
The bridge to possible

Contents

© 2021 Cisco and/or its affiliates. All rights reserved.
© 2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

Cisco infrastructure recommendations for voice quality

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

Table 6. 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 the Dynamic Host Configuration Protocol (DHCP) Address Assignment Required option.	✔	
Disable Session Timeout or set to shift duration + 1 hour.	✔	
Disable Client Exclusions.	✔	
Set the User Idle Timeout to Session Timeout definition (above).	✔	
Enable Fast SSID Change.	✔	
Disable Cisco Client Extensions Radio Measurements.	✔	
Allow WMM for the voice WLAN.	✔	
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.	✔	

ZEBRA

cisco
The bridge to possible

Contents

Recommendation	Required	Recommended but not required
Set EAP-Request Timeout (seconds) to 3.	✔	
Set EAP-Request Max Retries to 2.	✔	
Disable MPDU aggregation for voice.	✔	
Disable Optimized Roaming.	✔	
Ensure that FT (11r) is set to Enable, not Adaptive.	✔	
Verify that the Enhanced Distributed Channel Access (EDCA) profile on the controller is set to Voice Optimized.		✔
Verify that Aggressive Load Balancing is disabled.	✔	
Verify that Dynamic Transmit Power Control (DTPC) is disabled. See Recommendations for DTPC in the Notes at the end of this table.		✔
Verify that the Beacon Interval is set to 100 ms.	✔	
Verify that Client Management Frame Protection (MFP) is disabled.		✔
Verify that peer-to-peer blocking is disabled.	✔	
Validate that the virtual interface address is the same across all controllers in the same mobility group.	✔	

Notes:

- Inspect Cisco software versions to determine whether they are marked DF (deferred release) by Cisco. If so, avoid these versions.
- Cisco ecosystems typically use features that 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.

© 2021 Cisco and/or its affiliates. All rights reserved.
© 2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

ZEBRA

cisco
The bridge to possible

Contents

© 2021 Cisco and/or its affiliates. All rights reserved.
© 2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

  - 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 whether 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 the maximum (lowest frequency) where possible, respective to tasks, such as AP channel scans and scans of neighbor packets.
    - 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 the Scan Defer Priority for voice (Platinum, UP = 6), set the Scan Defer Time to the maximum value supported (the 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 rate unless there is a 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 Cisco Centralized Key Management (CCKM) is used for fast roaming. Otherwise, Aironet IEs' subfeatures are ineffective for voice enterprise and have been replaced by other standards.
  - If Cisco Centralized Key Management is not used for fast roaming, disable Aironet IEs.

ZEBRA

CISCO
The bridge to possible

Contents

© 2021 Cisco and/or its affiliates. All rights reserved.
© 2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

- Recommendations for DTPC:
  - DTPC is a mechanism in which the AP requests Cisco Client Extensions-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 DTPC in the following situation: In a complex RF environment, DTPC changes may be excessive systemwide, 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 retain 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 create the type of imbalance that it is designed to resolve. The AP RRM indexes from the new RF area would continually loop back and make more power changes to resolve the issues created by DTPC. This recursive loop could negatively affect 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 and AP 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, you consult the release notes for the WLC or AP to verify that a particular version is stable and preferred by the vendor.

- Cisco 5508 Wireless Controller:
  - Software version: 8.5.171.0 in Local mode
- Cisco 3504 and 5520 Wireless Controllers:
  - Software versions: 8.10.151.x or 8.10.162.x
- Cisco Catalyst® 9800 Series Wireless Controllers:
  - Software version: 17.3.4
- Tested Cisco AP models: Cisco Aironet 1242,1262, 1852, 2600 Series, 2802, 3602, 3708, and 3800 Series and Cisco Catalyst 9115AX, 9120AX, and 9130AX Series.

ZEBRA

cisco
The bridge to possible

Contents

© 2021 Cisco and/or its affiliates. All rights reserved.
© 2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

Additional WLC and AP resources and notes

- Go to the following Cisco pages for versioning recommendations for each controller type, compatibility matrices of software and hardware, end-of-life 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 at 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 Series 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.
- Cisco FlexConnect® vs. Local mode:
  - Cisco FlexConnect is a wireless solution that enables customers to configure and control access points in a branch or remote office from the corporate office through a 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) tunnel, depending on the operating system. 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 we 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.

ZEBRA

cisco
The bridge to possible

Contents

Copyright

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corporation, registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. ©2021 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

For further information regarding legal and proprietary statements, please go to:

Software: zebra.com/linkoslegal
Copyrights: zebra.com/copyright
Warranty: zebra.com/warranty
End User License Agreement: zebra.com/eula.

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.

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C07-745010-00 11/21