User's Guide

CC33xx WLAN Features

ABSTRACT

This document provides information about CC33xx family of devices and Wi-Fi® features, as well as TI proprietary enhancements. The document does not provide the complete application programming interface (API) set, but a high-level overview of the features. The CC33xx Linux® software package is based on the open source mac802.11 implementation; the complete API can be found in: https://elixir.bootlin.com/linux/latest/source/net/mac80211.

Table of Contents

List of Figures

List of Tables

Trademarks

Wi-Fi® is a registered trademark of Wi-Fi Alliance.
Linux® is a registered trademark of Linus Torvalds in the U.S. and other countries.
All trademarks are the property of their respective owners.

1 Introduction

1.1 Scope

This document covers the entire CC33xx family, as shown in the CC33xx Family Table.

Table 1-1. CC33xx Family

CC33xx	Description
CC3300	Single Band 2.4 GHz Wi-Fi 6
CC3301	Single Band 2.4 GHz Wi-Fi 6 and Bluetooth Low Energy

1.2 Acronyms Used in This Document

Table 1-2. Acronyms Table

Acronyms	Description
AC	Access Category
ACK	Acknowledge
ACS	Automatic Channel Selection
ADDBA	Add Block Acknowledgment
AES	Advanced Encryption Standard
AIFSN	Arbitration Interframe Space Number
A-MPDU	Aggregate MAC Protocol Data Unit
A-MSDU	Aggregate MAC Service Data Unit
AP	Wi-Fi Access Point
BA	Block Acknowledgment
BLE	Bluetooth Low Energy
BPSK	Binary Phase-Shift Keying
BT	Bluetooth
CCK	Complementary Code Keying
COEX	Co-Existence
CW	Contention Window
DELBA	Delete Block Acknowledgment
EAP	Extensible Authentication Protocol
EDCA	Enhanced Distributed Channel Access
ELP	Extreme Low Power
GI	Guard Interval
LAN	Local Area Network
LGI	Long Guard Interval
MAC	Media Access Control
MCS	Modulation Coding Scheme
MIMO	Multiple Input, Multiple Output
MR	Multi Role
MRMC	Multi-Role Multi-Channel
OFDMA	Orthogonal Frequency-Division Multiplexing Access

Table 1-2. Acronyms Table (continued)

Acronyms	Description
P2P	Wi-Fi Peer-to-Peer
PBC	Push-button Configuration
PHY	Physical (layer)
PS	Power Save
PTA	Packet Traffic Arbitration
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RADIUS	Remote Authentication Dial-In Service
RSN	Robust Security Network
RSSI	Receive Signal Strength Indicator
RX	Receive
SGI	Short Guard Interval
SSID	Service Set IDentifier (Wi-Fi Network Name)
STA	Wi-Fi Station
TID	Transmission ID
TIM	Traffic Indication Map
TSF	Timing Synchronization Function
TWT	Target Wake Time
TX	Transmit
TXOP	Transmit Opportunity
U-APSD	Unscheduled Automatic Power Save Delivery
UPSD	Unscheduled Power Save Delivery
WoW	Wake on WLAN
WLAN	Wireless Local Area Network
WMM	Wireless Multi-Media
WPS	Wi-Fi Protected Setup

1.3 CC33xx Specification

Table 1-3. CC33xx Specification

Role	Feature	Description
Station (STA)	Wi-Fi 6 / 802.11ax	OFDMA Trigger Frames TWT
	Filtering	Multicast
	Preferred Networks	Supported (WPA Supplicant)
	Wake on WLAN	Supported
	Wi-Fi Power Management Modes	**Standard Features** U-APSD Target Wake Time (TWT) **TI Specific Features** Auto Power-Save Mode Keep Alive Long Sleep Interval
Access Point (AP)	Hidden SSID	Supported
	Maximum Connected Stations	Up to 16 station connections *Dependent on if QoS is enabled
	Aging	Supported

Table 1-3. CC33xx Specification (continued)

Role	Feature	Description
General (STA or AP)	802.11b/g	Supported
	802.11a	Supported (Platform Dependent)
	802.11n	Supported
	A-MSDU and A-MPDU	Supported with exceptions
	BA Sessions	TX: 4 / RX: 8 *Per link
	Keep Alive	Supported
	QoS (WMM)	Supported
	Wi-Fi Protected Setup (WPS)	Supported
	Antenna Diversity	Supported
	Channel Switch	Supported
	Wi-Fi Power Management Modes	**Power Modes** Active **Standard Features** Legacy Power Save
	Security	**STA and AP** Personal: WPA3; WPA2-PSK; WPS PBC + PIN; Open **STA Mode Only** Enterprise: WPA3 GCMP support + 192-bit keys, EAP Methods (TLS, TTLS, TTLS-MSCHAP, PEAPv0-MSCHAP, and PEAPv1-TLS)
Multirole Multichannel	AP-STA	Supported
	STA-STA	Supported
All Roles	Wi-Fi Bluetooth Coexistence	Supported

2 General Features

2.1 Supported Rates

CC33xx devices support SISO20 PHY rates. The expected RF performance (TX and RX) for the different rates are documented in CC330x SimpleLink™ Wi-Fi 6 and Bluetooth® Low Energy. For transmission, rates and TX power are selected by the link adaptation algorithm of the device to maximize the data transmission rate and minimize the power consumption of the device.

The different rates and their modulations are detailed in the following subsections.

2.1.1 11ax Rates

MCS Index	Modulation	Code Rate	Data Rate (Mb/s)		
			0.8 µs GI	1.6 µs GI	3.2 µs GI
0	BPSK	1/2	4.3	4.0	3.6
		1/2	8.6	8.1	7.3
1	QPSK	1/2	8.6	8.1	7.3
		1/2	17.2	16.3	14.6
2		3/4	25.8	24.4	21.9
3	16-QAM	1/2	17.2	16.3	14.6
		1/2	34.4	32.5	29.3
4		3/4	25.8	24.4	21.9
		3/4	51.6	48.8	43.9

MCS Index	Modulation	Code Rate	Data Rate (Mb/s)		
			0.8 µs GI	1.6 µs GI	3.2 µs GI
5	64-QAM	2/3	68.8	65.0	58.5
6		3/4	77.4	73.1	65.8
7		5/6	86.0	81.3	73.1

2.1.2 11n Rates

MCS Index	Modulation	Code Rate	Data Rate [Mb/s]	
			0.4 µs GI	0.8 µs GI
0	BPSK	1/2	7.2	6.5
1	QPSK	1/2	14.4	13
2	QPSK	3/4	21.7	19.5
3	16-QAM	1/2	28.9	26
4	16-QAM	3/4	43.3	39
5	64-QAM	2/3	57.8	52
6	64-QAM	3/4	65	58.5
7	64-QAM	5/6	72.2	65

2.1.3 11a/g Rates

Table 2-1. CC33xx 802.11a/g Supported PHY Rates

Data Rate [Mb/s]	Modulation	Code rate
6	BPSK	½
9	BPSK	¾
12	QPSK	½
18	QPSK	¾
24	QAM-16	½
36	QAM-16	¾
48	QAM-64	½
54	QAM-64	¾

2.1.4 11b Rates

Table 2-2. CC33xx 802.11b Supported PHY Rates

Modulation	Data Rate (Mb/s)	Defined in
DBPSK	1	802.11
DQPSK	2	
CCK	5.5	802.11b
CCK	11	

2.2 A-MPDU and A-MSDU

Frame aggregation reduces overhead of the 802.11 protocol and increases data throughput by using a single PHY or MAC header to send multiple frames of data. There are primarily two methods available to accomplish frame aggregation: aggregate MAC service data unit (A-MSDU) and aggregate MAC protocol data unit (A-MPDU).

The main distinction between MSDU and MPDU is how information transmitted through the respective layers.

- MSDUs transmit information between the upper part of the MAC layer to higher layers.
- MPDUs transmit information between the lower part of the MAC layer to the PHY layer.

Beyond the difference in transmission between layers, there is also a difference in the frame structure when the units are aggregated.

- Individual MSDUs each receive an MSDU subframe header to create MSDU subframes. Two or more of these subframes are then inserted into an 802.11 MAC frame with a header and trailer. Once inserted the combined frames are considered an A-MSDU and transmitted using a single MAC header.
- Unlike MSDUs, MPDUs each have their own 802.11 MAC header and trailer that are then transmitted under the same PHY header.

In frame aggregation these techniques are combined so that multiple MSDUs can be concatenated into a single MPDU and transmitted. These aggregate exchange sequences are implemented through a protocol that acknowledges (ACKs) multiple MPDUs with a single block ACK. For more information on block ACK sessions, see Section 2.3. The CC33x can both transmit and receive data in the A-MPDU format and is able to receive data in the A-MSDU format.

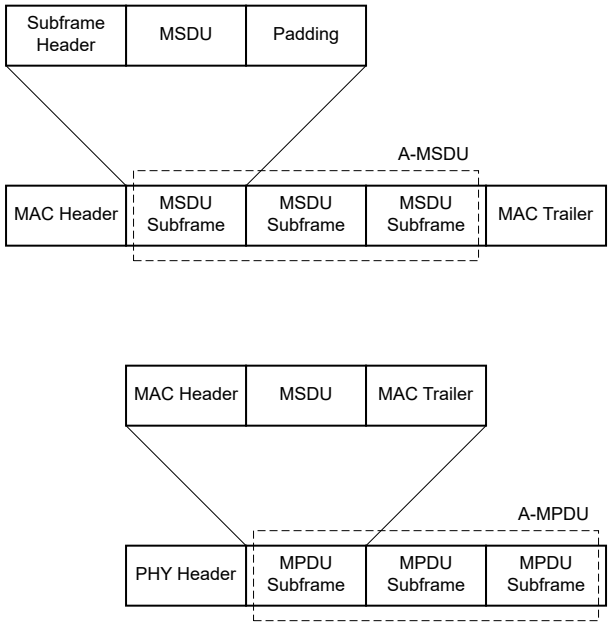

Figure 2-1. A-MSDU and A-MPDU Frame Structure

2.3 BA Sessions

Block acknowledgment (BA) is a feature introduced in the 802.11e IEEE Wi-Fi protocol and became mandatory in the 802.11n Wi-Fi protocol commonly referred to as Wi-Fi 4. It is used in conjunction with A-MPDUs and A-MSDUs to increase channel efficiency. As mentioned in Section 2.2, BA sessions are used to acknowledge multiple MPDUs together in a single BA frame rather than transmitting an individual ACK for every MPDU or frame. The BA protocol can only be used with QoS data frames (discussed in Section 2.7) and the number of possible links are dependent on the device and transmission direction (TX/RX). The CC33xx supports four BA sessions per each device link for data transmission (TX) and eight BA sessions per each device link when receiving data (RX).

This BA session is initialized through the transmission of a request and response exchange of initialization frames, referred to as ADDBA frames, between the AP and STA. This initialization includes an information exchange specifying parameters such as the QoS Transmission ID (TID) and buffer size. After initialization, multiple QoS data frames (the number of frames depends on buffer size) can be transmitted and acknowledged by a single block. This process is repeated until the BA session termination that is initiated by the BA session originator transmitting a session termination request known as a DELBA frame.

2.4 Keep Alive

2.4.1 STA

The keep alive feature works in conjunction with the features described below to ensure that when the CC33xx acts as a station it retains connection to APs during periods of no activity. As part of many of the protocols, the device is inherently not required to transmit any data back that can cause an AP to think that it is an inactive device. To account for this, the keep alive feature is automatically implemented in parallel to the below protocols.

If, after 55 seconds, the CC33xx has not transmitted any traffic to the AP, the device sends a null frame. This null frame informs the AP that the station is still active and should not be forced off the network.

2.4.2 AP

When the CC33xx device is in AP mode it tracks whether or not there is activity from the connected stations. If there is no activity from a station, the CC33xx device starts a timer and if no data is sent within that timeframe it sends a packet to the station in question to see if it is still connected. If the station does not respond then the CC33xx disconnects the station to save power.

2.5 Wake on WLAN (WoW)

The WoW mode allows the host to go to sleep (low power mode) while the CC33xx chip remains active as in STA mode. The host can be triggered to wake up through 3 different triggers:

- **WoW Any**: wakes up from any frame sent by the firmware to the host
- **WoW on Magic Packet:** the host will only wake up in the case of a specific packet being sent
- **WoW on Pattern**: wake up from a packet containing one of 8 different user defined patterns

2.6 Antenna Diversity

CC33xx supports two-antenna diversity on the 2.4 and 5-GHz bands, using an external single pole, double throw (SPDT) switch. The CC33xx algorithm studies and analyzes the best signal path based on RSSI level. It chooses the better of the two paths for transmitting and/or receiving an RF signal to increase the likelihood that a packet will be correctly received, and maximizing throughput.

2.7 Quality of Service (QoS)

The purpose of the IEEE 802.11 Quality of Service (QoS) feature is to assign different traffic types (voice, video, or best effort traffic) different priority levels of packet transmission. Packets belonging to delay-sensitive applications are assigned higher priorities and thus have a statistically higher chance of being transmitted before lower-priority packets.

When QoS is enabled a technique referred to as enhanced distributed channel access (EDCA) is utilized in the MAC layer to properly transmit packets based on their priority.

The levels of priority in EDCA are called access categories (ACs) and ACs with for higher priority traffic wait less time, on average, to be sent than the ACs for lower-priority traffic. The contention window (CW) can be set according to the traffic expected in each AC, with a wider window needed for categories with heavier traffic. The CWmin and CWmax values are calculated from aCWmin and aCWmax values, respectively, that are defined for each physical layer supported by 802.11e.

EDCA provide four different ACs (from lowest to highest priority):

- Background (AC_BK)
- Best Effort (AC_BE)
- Video (AC_VI)
- Voice (AC_VO)

CC33xx devices, in both AP and STA modes, supports EDCA in both software and hardware: while the software maintains the different queues within the AC categories, the hardware determines which packet is sent out from which AC queue in real-time. Table 2-3 shows the default EDCA values for the CW min and max, the AIFSN, and the max TXOP. The arbitration inter-frame spacing (AIFSN) is how long the transmitter defers before starting the backoff period based on the contention window, thus the lower the AIFSN number the higher the probability

of the frame being transmitted. The TXOP (transmission opportunity) is a parameter that specifies the interval of time during which a client can initiate transmissions to an AP.

Table 2-3. QoS Access Categories

AC	CWmin	CWmax	AIFSN	Max TXOP
Background (AC_BK)	15	1023	7	0
Best Effort (AC_BE)	15	1023	3	0
Video (AC_VI)	7	15	2	3.008 ms
Voice (AC_VO)	3	7	2	1.504 ms

The actual EDCA parameters are published by the AP side. When running a CC33xx device as an AP role, you can configure the EDCA parameters in the TI configuration file. There is no option to disable QoS from the STA role (enabled by default), but there is an option in the hostapd.conf file to disable the QoS.

A frame is handled as a QoS frame only if it arrived from the network with QoS information. Each frame without QoS information is handled as a non-QoS frame. The default parameters of non-QoS frames are the same as best-effort frames (that is also the case when the AP does not support QoS).

The EDCA QoS is compatible with the Wi-Fi Alliance WMM Certification, with a small modification. WMM defines eight different TIDs (Traffic ID 0-7), while each traffic ID (TID) gets a specific AC handling.

For the CC33xx devices, four TIDs are supported for transmission while eight are supported for receiving. The eight TIDs outlined by the WMM are described in Table 2-4 and the ones supported for transmission are noted.

Table 2-4. QoS TIDs

TID	AC	Transmission
0	AC_BE	Supported
1	AC_BK	Supported
2	AC_BK	
3	AC_BE	
4	AC_VI	Supported
5	AC_VI	
6	AC_VO	
7	AC_VO	Supported

2.8 Security

Wireless encryption and authentication only allow devices with the corresponding authentication and encryption types to be connected. To connect a wireless device to a certain router, the device also requires the correct key (password).

2.8.1 Authentication Types

The CC33xx supports the following three authentication types: open, personal and enterprise. However, which types are supported depends on what mode the CC33xx is in.

- STA Mode: open, personal and enterprise
- AP Mode: open and personal

The first authentication type is open, which refers to APs that do not require a password to join.

The second is personal authentication, where the password is configured to the AP and the AP itself authenticates the peer device using a password. The supported personal authentication types are:

- Wi-Fi Protected Access v2 (WPA2)
- Wi-Fi Protected Access v3 (WPA3)

The third is enterprise authentication (supported in STA Mode), where a RADIUS (Remote Authentication Dial-In Service) server behind the AP authenticates the peer device. The following list the supported enterprise authentication types:

- WPA3 GCMP support + 192-bit
- EAP Methods
  - TLS
  - TTLS
  - TTLS-MSCHAP
  - PEAPv0-MSCHAP
  - PEAPv1-TLS

2.8.2 Encryption Types

Each encryption type can be used with any of the authentication types.

- Open (no encryption)
- AES (advanced encryption standard)

2.9 Wi-Fi Provisioning

Wi-Fi provisioning refers to the process of connecting a Wi-Fi station to an AP by loading the station with the SSID and proper security credentials. Provisioning can be accomplished through three main methods: Soft AP Provisioning, Bluetooth Low Energy Provisioning and WPS.

2.9.1 AP Provisioning

When this mode is enabled, the unprovisioned CC33xx device is initially set-up as an AP with a pre-defined SSID. While the CC33xx device is operating as an AP, the user can connect and enter the required credentials. Once the security credentials have been entered, the device switches from AP mode to STA mode and connect to the network using those previously provided credentials.

2.9.2 Bluetooth Low Energy Provisioning

In the Bluetooth Low Energy provisioning mode, the Bluetooth Low Energy role is active and the user can connect to the CC33xx device via bluetooth. Once connected, the user can send the necessary credentials over and then the device can utilize STA mode to connect to the desired AP. A benefit CC33xx device is that it can have Bluetooth Low Energy and STA mode active simultaneously.

2.9.3 Wi-Fi Protected Setup (WPS)

The WPS method is an additional way to establish a Wi-Fi connection. The WPS-capable devices declare this capability in the beacons and probes. In this method, the connection is secured and the data exchange encrypted. The WPS connection method is invoked in two ways: hardware and software. Both the hardware and the software processes are invoked using one of two WPS connection methods: PBC or PIN. When one device has started a WPS connection process, the second device has two minutes to respond to the connection initiator device. After two minutes, the connection initiator stops the process. An advantage in either WPS method is that the secured Wi-Fi network can be joined without knowing the privacy key.

A disadvantage is that during the WPS connection process, no specific SSID is defined. This limitation can result in a situation where two independent stations start a WPS process concurrently, for example, within a two-minute time frame, and the peer station will not know which of them to connect to. This situation is called WPS overlapping. The peer station is only able to connect when one station terminates the WPS connection process.

2.9.3.1 WPS PBC

The WPS push-button connection method can be invoked by running a dedicated command on wirelesslanconnect.

2.9.3.2 WPS PIN

A PIN method is another option for establishing the WPS connection. In this case, one Wi-Fi device has a pre-defined PIN key printed on the label, usually 8 digits in length, while the other Wi-Fi device inserts this key after starting the WPS connection process. The side with the pre-defined key is called Label and the device inserting the key is called Keypad. Both relate to the PIN method. After inserting the key, the connection process is the same as with the PBC method.

2.10 Wi-Fi Power Management Modes

2.10.1 Power Levels

2.10.1.1 Active

In this mode, the WLAN on the chip always stays awake, even if there is no activity such as traffic, scans, and so forth. This mode has the highest power consumption, but also, the best throughput and lowest latency.

2.10.2 Power Save Delivery

2.10.2.1 Legacy Power Save

In this mode, the behavior of the CC33xx device depends on whether it is acting as a STA or AP, but in either case it will act in a manner consistent to the protocol described below.

In this power saving protocol, when a STA detects that the AP has data for it in the beacon frame, it sends a trigger packet named PS-POLL to the AP. In response, the AP sends the first queued frame to the STA; if the More Data field in this frame is on, it sends another PS-POLL frame to the AP. The STA continues to send PS-POLL frames to receive all the queued frames, until there are no data packets left. After this, the station returns to sleep until the next listening interval.

This method is suitable for very low data usage, since it requires additional overhead to receive each packet.

3 Single Role: Station

3.1 Scanning

While in STA mode, the scanning feature is utilized to find and connect to available APs on available channels. The CC33xx device can be configured to utilize either a passive or active scan. The fundamental difference is that during an active scan the device is actively sending probes out as it switches channels while in a passive scan it listens on each channel for beacons sent out by APs.

3.1.1 Active

When the station is in active mode it transmits probe requests to various channels to search for available APs. Once probe request is broadcasted on a channel, the CC33xx device remains on the channel to wait for a response for a specified period of time referred to as dwell time. If it does not receive a response within dwell time, it transfers to the next channel and broadcast another probe request. If it does receive a probe response, which contains certain parameters such as SSID, timing synchronization function (TSF), robust security network (RSN), and so forth., then it adds this AP to the list of APs available for connection.

The device then moves onto the next channel and repeats the process until all channels have been scanned. After the active scan is completed, the user can view the APs and select one to connect to using appropriate credentials.

3.1.2 Passive

When the device is utilizing a passive scan, it spends a certain amount of time listening on each channel to receive beacons stating that an AP is available to connect to. After a period of time the device switches to the next channel and repeats the process. The beacon sent from APs to the station contains info elements (IE) such as the SSID, RSN, and country code that allow the device to know whether it is permitted to transmit on that channel.

A passive scan generally takes significantly longer to complete than active scan due to the device needing to spend much more time on each channel so that there is enough time for the APs to send a beacon. A similar process is followed on the active scan, where after waiting the necessary period of time, the device switches to a different channel to continue listening for beacon frames. Once the scan is completed, the available APs are stored in memory as possible connections.

3.2 Wi-Fi 6

CC33xx supports IEEE 802.11ax standard popularly known as Wi-Fi 6. Some of the Wi-Fi 6 features are listed below:

- **Orthogonal frequency division multiple access (OFDMA)** - In Wi-Fi 6, the number of subcarrier frequencies per channel have increased to 4X and subcarrier spacing has been reduced to one fourth the subcarrier spacing of previous 802.11 revisions. This allows for much better equalization, enhancing channel robustness and performance.
- **Trigger Frames** – This is a technique in which the AP sends a trigger to all connected stations so that they all send data simultaneously. It is used in uplink OFDMA to coordinate clients transmitting to the AP at the same time as well as in TWT.
- **Target wake time (TWT)** - This feature enables Wi-Fi 6 devices to sleep more efficiently compared to legacy Wi-Fi 6 devices. A Wi-Fi 6 AP can negotiate with the participating STAs the use of the Target Wake Time (TWT) function to define a specific time or set of times for individual stations to access the medium. This results in much better and more efficient implementation of power save mechanism, directly resulting in extended product battery life.

Note

For more information, see the latest software release notes.

3.3 Multicast Filtering

Multicast filtering is done within the hardware. On initialization, the multicast filter is disabled and all multicast frames are sent to the host. Once the device is initialized, multicast filtering is automatically enabled and the user can register for specific multicast addresses to begin receiving packets. Only frames from the registered addresses are filtered in, while all other multicast frames are dropped. The CC33xx software supports up to twenty different configurable multicast groups that can be configured. The multicast filter only works for the STA role, as the AP role should distribute all multicast frames to all other devices.

3.4 Preferred Networks

Preferred networks or profiles refer to Wi-Fi networks that you have been explicitly predefined or been learned and stored by WLAN capable devices. A preferred network definition consists of the SSID, security type, whether it is a hidden or non-hidden network, and the priority of the network.

These networks are defined in the WLAN supplicant configuration file and can be automatically connected once discovered during scanning. The device or application intending to invoke a connection initiates a scan phase and connect to one of the preferred networks that is discovered, assuming correct credentials have been saved. The decision on when and if to start a scan phase varies between operating systems and applications that manage Wi-Fi connections. Typically, once Wi-Fi is enabled on the device, and one or more profiles are defined in the supplicant, the scanning starts.

After getting a scan result, the device checks one or more of the networks that are suitable and compares them to the profiles that were stored. When a match to one of the stored profiles is found, the device initiates a connection to the network. The network is considered to be suitable for connection if it has the same network name and security type. However, in the case of a network with security, the connection process only succeeds if all the credentials are correct. If the profile's security type matched but the security key is wrong, the connection process will start, but a complete connection will fail.

After the scan cycle, if there is more than one match with the stored profiles' list, the device or application managing the connection process selected the Wi-Fi network based on priority, security type, and RSSI.

3.5 Channel Switch

The dynamic frequency selection (DFS) is a process that is applied to 5-GHz channels, 52 to 140, where radar can operate. Channel switch is a mechanism that dynamically switches the operating frequency of the 5GHz radio to avoid co-channel operation with radar systems.

This feature verifies that the STA does not transmit any packets in channels where DFS operates upon radar detection.

The AP must detect the radar and notify the any connected stations that the AP is moving to a new channel by sending a channel switch announcement (CSA) using beacon and probe response frames. A STA that receives a channel switch announcement element can choose not to perform the specified switch and take alternative action instead.

The Channel Switch feature is enabled when the CC33xx is in STA mode.

3.6 Wi-Fi Power Management Modes

Because it is important to reduce the current consumption of the device, CC33xx features an extreme low power (ELP) level that is used in many of the power saving modes described below. ELP is a device power state during which the device sleeps to drastically decrease power consumption in between activity. This device enters this state as required by the Wi-Fi power management protocols described below.

3.6.1 Power Save Delivery

3.6.1.1 Unscheduled Asynchronous Power Save Delivery (U-APSD)

The unscheduled automatic power-save delivery (U-APSD) mechanism is also known as wireless multimedia (WMM) power-save. Legacy power-save methods can decrease the quality of periodic bi-directional traffic consisting of short frames as in VOIP. Because VOIP data should send data periodically on a fixed time (20 msec. for VOIP call), the legacy mechanism is not efficient enough. The U-APSD mechanism was built to optimize the legacy mechanism.

U-APSD is basically a polling scheme, similar to the legacy power-save delivery. However, in U-APSD mode, any transmitted frame, while in power-save mode, acts as a polling frame and triggers the AP to release a buffered frame from the same access category (AC) as the transmitted packet (the number of frames that are released by the AP is configurable and determined during the connection phase). For example, a voice packet releases only voice-buffered packets. If there are no transmitted packs, STA sends QoS null data packets (after the AP publicizes in its beacon that it has data for the specific associated station), which polls the buffered data. This is very efficient for bi-directional traffic streams, such as VOIP call.

As the STA awakes from power save to transmit the data, the STA then takes advantage of it to get any data buffered from the AP. This feature only works if the STA and AP are configured to WMM-enabled.

3.6.1.2 Target Wake Time (TWT)

A feature of Wi-Fi 6 that allows devices to sleep more efficiently compared to legacy Wi-Fi 6 devices. For more information, see Section 3.2.

3.6.2 TI Specific Features

3.6.2.1 Auto Power-Save Mode

In this mode, the STA automatically switches between active and power-save mode. When the STA is connected in idle mode and has no need to send or transmit any data, the STA is in power-save mode. However, if the STA must perform any activity in the network, such as receiving traffic, it sends a null data frame with the power save bit off. Thus, the STA is in active mode from that point until the activity has been finished. After a pre-configured amount of time, the null data frame with the power save bit on is sent to the access point, and the STA returns to power-save mode. This ensures a balance between power consumption and best performance.

3.6.2.2 Long Sleep Interval

The CC33xx devices feature configurable Long sleep Interval (LSI) that reduces the power consumption of the device. The CC33xx can be configured to sleep for specific intervals so that it awakens every ‘n’ DTIMs (delivery traffic indication messages). This creates a tradeoff where the device is able to significantly reduce power consumption, but there is a possibility of losing multicast/broadcast frames between received DTIMs while the device is still asleep.

While the device is asleep, data will be buffered within the AP the CC33xx is connected to until the next DTIM that the CC33xx awakens for, at which point it receives the data. The potential tradeoff of losing data can occur if the buffer reaches capacity before the station can retrieve the data. The amount of time the device is asleep for is configurable in terms of DTIM intervals - the number of beacons sent between each DTIM. Thus the CC33x is able to awaken for a single broadcast within the specified interval of beacons sent.

For guidance on how to configure the LSI feature, please consult the CC33xx SDK.

4 Single Role: AP

4.1 Hidden SSID

Hiddien SSID is a method to make it harder for a station to determine the network name. When hidden SSID is used, the network ID (SSID) is not broadcasted in the AP beacons.

The AP does not reply with a probe response to any device, other than from a probe request with the specific SSID. This method is not secured, as it is possible to see the SSID of the specific AP from the probe request, using the sniffer. When scanning the air with a wireless device, the AP with the hidden SSID will not be found.

A connection scan must be performed for a wireless device to connect, which means transmitting a unicast probe request with the SSID.

4.2 Maximum Connected Stations

When the CC33xx is operating as an AP it is able to support up to four or sixteen stations depending on if QoS is enabled. The device features a fixed amount of memory to buffer the data being transmitted to the connected stations. The amount of memory needed for each varies depending on whether QoS is enabled as additional memory is needed for each station to support the access category (AC) queues.

If QoS is enabled it must be enabled for all supported stations; therefore, each station requires four queues for the four different ACs resulting in a total of sixteen queues. Conversely, when the CC33xx has not enabled QoS, each station utilizes the memory space needed for one queue allowing the device to support sixteen different stations. For more information on QoS, see Section 2.7.

4.3 Aging

The purpose of the aging mechanism is to save AP resources by disassociating and deauthenticating stations that have been disconnected. If the station does not send anything in a configurable number of seconds (by default 300 sec, that is, 5 minutes), the CC33xx sends an empty data frame. If the data framed is not acknowledged by the station, it is disassociated and then deauthenticated by the AP.

Aging mechanisms usually come into play when there is a sudden network loss of an external connected station, thus, the mechanism frees up allocated space. It has default configurations, but can also be altered according to need.

5 Multirole Multichannel

CC33xx devices support the multi-role multi-channel (MRMC) operation. The supported combinations of roles are described below.

5.1 AP-STA

CC33xx can have an active AP and STA roles, allowing devices to connect to CC33xx while C33xx is also connected to a separate AP. While utilizing the AP-STA feature, the CC33xx can support multiple stations, described in Section 4.2 while also being connected to an AP. This can allow the device to act as a bridge or gateway from a multitude of stations to a singular AP.

5.2 STA-STA

The CC33xx can act as two different stations (STA-STA) wherein, it is able to connect to two different APs simultaneously, however it is unable to use Wi-Fi 6 with both APs. The device can utilize Wi-Fi 6 features with one of the the STA roles and up to Wi-Fi 802.11n (Wi-Fi 4) with the other STA role.

6 Wi-Fi/Bluetooth Low Energy Coexistence

Wi-Fi and Bluetooth Low Energy are both implemented on the CC33xx to eliminate the need for separate devices to implement Bluetooth Low Energy and Wi-Fi. This provides a more compact, inexpensive solution that provides superior coordination of the transmission of Wi-Fi and Bluetooth Low Energy signals. This coordination is accomplished using the coexistence (COEX) hardware module that enables multiplexed air access for internal Wi-Fi and Bluetooth Low Energy signals as well as external SOC signals operating at the same 2.4 GHz frequency.

The COEX interface implemented for CC33xx devices is compatible with other 2.4 GHz technologies that support Packet Traffic Arbitration (PTA). This is one of the approaches recommended and described by IEEE 802.15.2.

The same antenna is used for any signal transmission on the 2.4 GHz frequency band, thus the COEX module minimizes and handles real time air-access collisions based on the assigned priorities to different signals.

Signals from the BLE Core and WiFi module both pass through the COEX hardware and are multiplexed to be transmitted from the antenna. It is also possible to connect an external SOC that will also be multiplexed via the COEX hardware to transmit through that same antenna.

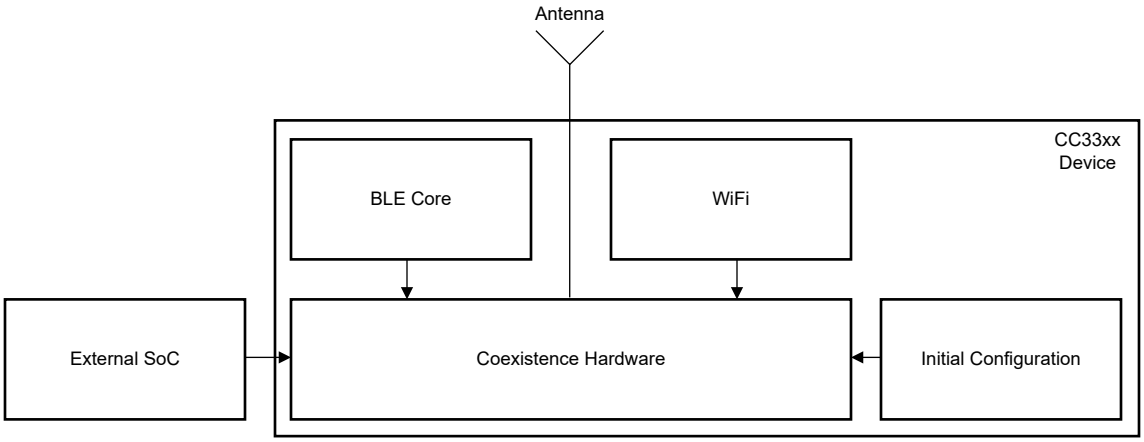

Figure 6-1. Coexistence in CC33xx Device

7 References

- Texas Instruments: *CC330x SimpleLink™ Wi-Fi 6 and Bluetooth® Low Energy companion IC Data Sheet*

8 Revision History

NOTE: Page numbers for previous revisions may differ from page numbers in the current version.

Changes from Revision A (December 2023) to Revision B (April 2024)	Page
• Updated Section 1.2	2
• Updated Table 1-3	3
• Added Section 2.5	7
• Added Section 2.6	7
• Added Section 3.5	12

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265