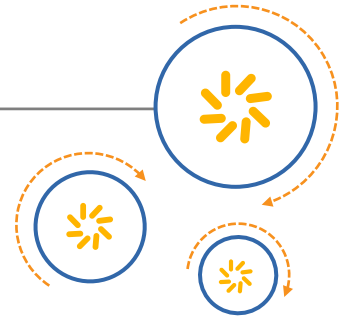




Qualcomm Atheros, Inc.



AP 10.2 Command Line Interface (CLI)

User Guide

80-Y7207-3 Rev. L

September 18, 2015

QUALCOMM®
2015-10-27 01:43:49 PDT
jinwei5@hikvision.com

Confidential and Proprietary – Qualcomm Atheros, Inc.

© 2013-2015 Qualcomm Atheros, Inc. All rights reserved.

NO PUBLIC DISCLOSURE PERMITTED: Please report postings of this document on public servers or websites to:
DocCtrlAgent@qualcomm.com.

Not to be used, copied, reproduced, or modified in whole or in part, nor its contents revealed in any manner to others without the express written permission of Qualcomm Atheros, Inc.

Questions or comments: <https://createpoint.qti.qualcomm.com/>

QUALCOMM®
2015-10-27 01:43:49 PDT
jinwei5@hikvision.com

Restricted Distribution: Not to be distributed to anyone who is not an employee of either Qualcomm Atheros, Inc. or its affiliated companies without the express approval of Qualcomm Configuration Management.

Qualcomm is a trademark of Qualcomm Incorporated, registered in the United States and other countries. All Qualcomm Incorporated trademarks are used with permission. Other product and brand names may be trademarks or registered trademarks of their respective owners.

This technical data may be subject to U.S. and international export, re-export, or transfer ("export") laws. Diversion contrary to U.S. and international law is strictly prohibited.

Qualcomm Atheros, Inc.
5775 Morehouse Drive
San Diego, CA 92121
U.S.A.

Revision history

Revision	Date	Description
A	November 2013	Initial release for AP 10.2 software. For 10.1 software, see 80-Y0984-1. The following is a summary of the changes documented between AP software versions 10.1 and 10.2. Added sections on channel loading, channel hopping, Intelligent Channel Selection (ICS), aggregate size scaling, Hy-Fi, 256QAM. Added get command to ANI. Added to DCS-IM commands. Added burst/get_burst commands to aggregation parameters. Added value 5 for mcastenhance. Added HMWDS/HMMC.
B	December 2013	Modified parameter spelling for set_dcs_coch_th, get_dcs_coch_th, set_dcs_maxcu, get_dcs_maxcu (Table 1-11); and getacscriflags (Table 1-53).
C	March 2014	Added content for Smart Antenna feature.
D	April 2014	In the following tables, removed “et” from the “get” command names: <ul style="list-style-type: none"> ■ Table 1-11: g_dcs_phyerrth ■ Table 1-13: g_dgaf_disable ■ Table 1-15: g_mcastenhance ■ Table 1-33: g_dscp_override ■ Table 1-53: g_acs_bksanen, g_acs_rssivar, g_acs_dbgtrace Updated Table 1-38 . Added Section 1.3.31.1 . Updated Table 1-29 with commands for Enhanced Independent Repeater feature
E	May 2014	In the following tables, removed “et” from the “get” command names: <ul style="list-style-type: none"> ■ Table 1-14: g_disablecoext ■ Table 1-22: g_periodicScan Added Section 1.3.33 .
F	October 2014	Removed or reformatted red text in Table 1-25 , Table 1-29 , Table 1-31 , and Table 1-50 . The commands shown in revisions D and E in the subsection titled “Uncategorized protocol layer parameters” have been removed until further notice. Added Section 1.5.7 , UCI Wireless configuration (qca-wifi) .
G	April 2015	<ul style="list-style-type: none"> ■ Updated the Section 1.4.2.2 ■ Added Section 1.5.7.4, Band steering configuration commands ■ Added Table 1-55, Table 1-56, Table 1-41, and Table 1-49
H	May 2015	<ul style="list-style-type: none"> ■ Added Section 1.3.34 and Section 1.4.6.
J	June 2015	<ul style="list-style-type: none"> ■ Added Section 1.3.35 ■ Updated Section 1.5.4 and Section 1.5.7.4
K	July 2015	<ul style="list-style-type: none"> ■ Updated Table 1-41, Table 1-42, and Table 1-49
L	September 2015	<ul style="list-style-type: none"> ■ Updated Table 1-49 ■ Added Section 1.3.31.4 ■ Updated Section 1.3.12 and Section 1.3.28 ■ Added Section 1.5.7.5



Contents

1	AP Driver Command Line Interface	11
1.1	Wireless tools	11
1.2	iwconfig parameters	13
1.3	iwpriv parameters	16
1.3.1	Aggregation parameters	17
1.3.2	ANI parameters	20
1.3.3	Association/ACL parameters	21
1.3.4	Beacon configuration parameters	22
1.3.5	Channel width parameters	25
1.3.6	Debug parameters	28
1.3.7	Dynamic Channel Selection for Interference Mitigation (DCS-IM) Parameters	31
1.3.8	Green AP parameters	32
1.3.9	Hotspot 2.0	32
1.3.10	HT20/HT40 coexistence parameters	33
1.3.11	iQue parameters	34
1.3.12	Physical layer parameters	37
1.3.13	Protection mechanism parameters	40
1.3.14	Radio-related parameters	41
1.3.15	Radio resource management (802.11k)	51
1.3.16	Regulatory parameters	56
1.3.17	Security parameters	57
1.3.18	STA parameters	62
1.3.19	TDLS Parameters	64
1.3.20	Turbo parameters	64
1.3.21	Tx beamforming parameters	65
1.3.22	Unassociated power consumption improvement parameters	66
1.3.23	Smart antenna	67
1.3.24	WDS parameters	70
1.3.25	WMM parameters	71
1.3.26	256QAM rate support parameters	73
1.3.27	Hy-Fi options – WMM DSCP prioritization	73
1.3.28	Channel loading/Channel hopping parameters	75
1.3.29	802.11k parameters	76

1.3.30	Aggregate size scaling parameters	76
1.3.31	Wifitool Utility	76
1.3.32	Target recovery parameters	79
1.3.33	2.4 GHz VHT 256-QAM Broadcom interoperability support	80
1.3.34	Airtime Fairness (ATF) Parameters	80
1.3.35	Dynmic Frequency Selection (DFS) Parameters	82
1.4	wlanconfig utility	83
1.4.1	Create a VAP	83
1.4.2	List VAP parameters	83
1.4.3	Delete an interface	88
1.4.4	NAWDS configuration parameters	88
1.4.5	HMWDS/HMMC commands	91
1.4.6	Configure ATF Parameters	92
1.5	Other commands	94
1.5.1	Athssd parameters	94
1.5.2	DFS	94
1.5.3	NAT parameters	95
1.5.4	Radartool	95
1.5.5	Spectraltool parameters	96
1.5.6	Intelligent channel manager parameters	97
1.5.7	UCI Wireless configuration (qca-wifi)	102
1.5.8	UCI command to enable ATF	116
A	Country Code Definitions	117

Tables

Table 1-1 iwconfig parameters	13
Table 1-2 11ac interface aggregation parameters	17
Table 1-3 11na and 11ac interfaces specific statistics	18
Table 1-4 ANI parameters	20
Table 1-5 Association/ACL parameters	21
Table 1-6 Beacon configuration parameters	22
Table 1-7 Channel width parameters	25
Table 1-8 Debug parameters	28
Table 1-9 802.11 Protocol layer debug bitmask	28
Table 1-10 HAL debug flags	29
Table 1-11 DCS-IM parameters	31
Table 1-12 Green AP Parameters	32
Table 1-13 Hotspot 2.0 parameters	32
Table 1-14 HT20/HT40 coexistence parameters	33
Table 1-15 iQue parameters	34
Table 1-16 Physical layer parameters	37
Table 1-17 Protection mechanism parameters	40
Table 1-18 Radio-related parameters	41
Table 1-19 Radio resource management (802.11k) parameters	51
Table 1-20 Regulatory parameters	56
Table 1-21 Security-related parameters	57
Table 1-22 STA parameters	62
Table 1-23 TDLS Parameters	64
Table 1-24 Turbo parameters	64
Table 1-25 Tx beamforming parameters	65
Table 1-26 Unassociated power consumption improvement parameters	66
Table 1-27 Smart antenna parameters	67
Table 1-28 dword3 parameters	67
Table 1-29 WDS parameters	70
Table 1-30 Access categories and modes	71
Table 1-31 WMM parameters	71
Table 1-32 256QAM parameters	73
Table 1-33 Hy-Fi parameters	73
Table 1-34 Channel loading/Channel hopping parameters	75
Table 1-35 802.11k Parameters	76
Table 1-36 Aggregate Size Parameters	76
Table 1-37 Wifitool 802.11k parameters	76
Table 1-38 Wifitool channel loading parameters	77
Table 1-39 Block channel list	78
Table 1-40 2.4 GHz VHT 256-QAM Broadcom interoperability support	80
Table 1-41 ATF Parameters	80

Table 1-42 DFS Parameters	82
Table 1-43 AP list elements	84
Table 1-44 STA list elements	85
Table 1-45 Channel list elements	86
Table 1-46 Capabilities list elements	87
Table 1-47 Configure NAWDS parameters	88
Table 1-48 Configure HMWDS/HMMC parameters	91
Table 1-49 Configuration/show ATF parameters	92
Table 1-50 Athssd Parameters	94
Table 1-51 Spectraltool parameters	96
Table 1-52 ICM command line parameters	99
Table 1-53 ACS/DCS/OBSS iwpriv commands	100
Table 1-54 Per-VAP configuration parameters	102
Table 1-55 Parameters in the configuration file	108
Table 1-56 Parameters in the configuration file	108
Table 1-57 Parameters for the CFG	113
Table A-1 Country code definitions	117

Preface

This user guide provides information on the Qualcomm Atheros AP Driver Command Line Interface, which is a part of the Qualcomm Atheros AP system. This system consists of the OS kernel, utility functions, and the Qualcomm Atheros AP driver.

About this document

The document consists of the following chapters and appendixes:

Chapter 1	AP Driver Command Line Interface
Appendix A	Country Code Definitions

Additional resources

Qualcomm Atheros reference design hardware, software, and documentation contain proprietary information of Qualcomm Atheros, Inc., and are provided under a license agreement containing restrictions on use and disclosure, and are also protected by copyright law. Reverse engineering of this hardware, software, or documentation is prohibited.

For additional information, refer to the following documents:

- *AP 10.2 Programmer's Guide* (80-Y7207-1)
- *AP 10.2 Driver User's Guide* (80-Y7207-2)

Document conventions

Text conventions

bold	<p>Bold type within paragraph text indicates commands, file names, directory names, paths, or returned values.</p> <p>Example: The DK_Client package will not function unless you use the wdreg_install batchfile.</p>
<i>italic</i>	<p>Within commands, italics indicate a variable that the user must specify.</p> <p>Example: mem_alloc <i>size_in_bytes</i></p> <p>Titles of manuals or other published documents are also set in italics.</p>
Courier	<p>The Courier font indicates output or display.</p> <p>Example:</p> <pre>Error:Unable to allocate memory for transfer!</pre>
[]	<p>Within commands, items enclosed in square brackets are optional parameters or values that the user can choose to specify or omit.</p>
{ }	<p>Within commands, items enclosed in braces are options from which the user must choose.</p>
	<p>Within commands, the vertical bar separates options.</p>
...	<p>An ellipsis indicates a repetition of the preceding parameter.</p>
>	<p>The right angle bracket separates successive menu selections.</p> <p>Example: Start > Programs > DK > wdreg_install.</p>

1 AP Driver Command Line Interface

The AP driver command line interface consists of wireless tools presented in this document to view and modify AP driver environment variables.

1.1 Wireless tools

The wireless tools interface is the primary interface used in Linux for configuring and operating the WLAN interface. The tools themselves are open source, and require specific support through the IOCTL interface for the driver. The Qualcomm Atheros WLAN driver supports these tools out of the box without modification. Any version of wireless tools after the version 28 can be used with the Qualcomm Atheros WLAN driver system.

The wireless tools use device names to determine the device to configure. In the Qualcomm Atheros driver, two device types are created when AP is brought up. The radio layer, also known as the ATH/HAL layer, is instantiated as a **wifiN** device, where N is the specific instance starting with zero. The first radio instance, for example, would be called **wifi0**. The protocol, or 802.11 layer, is instantiated as an **athN** device. These devices are also known as virtual APs (VAPs). Multiple VAPs can be associated with a single radio, but only one radio may be associated with any particular VAP (one-to-many relationship). Each layer controls specific aspects of system operation, and therefore each layer has specific commands that apply to it.

The two main programs of the wireless tools suite are **iwconfig** and **iwpriv**. These commands are used to get or change specific configuration or system operating parameters. Many commands are only effective before the AP interface is in the up state, so these commands must be performed prior to issuing the **ifconfig up** command to the interface. This document defines the valid parameters and commands for each command.

NOTE The radio layer does not support the **iwconfig** command, which is used exclusively in the protocol layer. Also, any **ifconfig** commands used on the AP must be applied to the protocol layer (ATH) device and has no effect on the radio layer.

There are two WLAN driver models available in the 10.2 AP software — Direct Attach (DA) and Offload (OL).

In the Direct Attach (DA) model, the entire WLAN driver runs on the host platform and interfaces with the WLAN hardware through the host bus interface (that is, PCI, PCIe, AHB, and so on). Examples of Direct Attach chipsets are AR928x, AR938x, AR939x, AR958x, AR959x, AR934x, AR935x, QCA953x and QCA955x.

In the Offload (OL) model, the WLAN driver component runs on the target and thin interface layer software is added on both the host and target for the host-target communications. Examples of Offload chipsets are QCA988x and QCA989x.

CLI commands table in this document will consist of two columns labeled “DA” and OL” to indicate the WLAN driver model which a CLI command supports.

QUALCOMM®
2015-10-27 01:43:49 PDT
jinwei5@hikvision.com

1.2 iwconfig parameters

The **iwconfig** command encompasses a fixed set of parameters used to set up and operate the WLAN interface. They are used in the same way as the **ifconfig** command and its parameters, but are specific to 802.11 device operations. Thus, they interface to the particular VAP interface.

NOTE The radio layer does not support **iwconfig**.

Table 1-1 iwconfig parameters

Parameter	Format	DA	OL	Description
ap	<code>iwconfig athN ap macaddr</code>	N	N	<p>Selects the specific AP with which a client will associate; used only for WDS client modes in the AP environment. The only valid argument is the MAC address of the desired AP. The help text also indicates <i>off</i> and <i>auto</i> choices, but these only disable the selection of a specific MAC address.</p> <p>Disabled by default.</p> <p>The AP command is not currently supported.</p> <pre>#iwconfig ath0 ap 00:03:7f:01:23:45</pre>
channel	<code>iwconfig athN channel opchannel</code>	Y	Y	<p>Selects the operation channel. In AP mode, it is the channel the AP operates in. For STA operations, the STA associates to the appropriate AP based on the MAC address setting and the ESSID, so the channel is not important.</p> <p>The channel argument only takes the channel number. See the freq command for setting the specific frequency. If an invalid channel is selected, this command returns an error status. The VAP for this interface should be destroyed at this point, as it will not be properly configured with a channel. It has no default value. The provided scripts bring up the first interface on channel 6 by default, and the second on channel 40 by default (for dual concurrent operations).</p> <p>Note: Issue the “ifconfig athN down” command before issuing the channel change command and “ifconfig athN up” after making the channel change.</p> <pre>#iwconfig ath0 channel 11</pre>

Table 1-1 iwconfig parameters (cont.)

Parameter	Format	DA	OL	Description
enc key	iwconfig athN key [index] <i>keyvalue</i>	Y	Y	<p>The commands enc and key are synonyms for the same command to set and manage WEP keys. The hardware will support up to four WEP keys per radio module. The optional index value indicates which key is being set/activated. The index value can be from 1 to 4.</p> <ul style="list-style-type: none"> ■ The <i>keyvalue</i> parameter can be specified in either hex mode or as an ASCII string. ■ Key values can be specified for either WEP 64 (40) bit mode, requiring 5 bytes, or WEP 128 (108) bit mode, requiring 13 bytes. ■ In hexadecimal mode, this comes out to 10 or 26 hex digits, respectively. ■ Hex digits are separated in groups of 4 by hyphens. ■ When specifying ASCII keys, the keys will require 5 or 13 characters, respectively. ■ All ASCII key strings are preceded by the s: indicator. <p>To turn WEP off, use the off command without index. WEP is automatically turned on when a key is specified. Specifying a key index without a key value will select that key as the active key.</p> <pre>#iwconfig ath0 key [2] DEAD-BEEF-EA #iwconfig ath0 key [1] s:AnASCIIkeyVal #iwconfig ath0 key off</pre>
essid	iwconfig athN essid "Name of Network"	Y	Y	<p>Sets the name of the BSS as it is provided in the beacon message. While no official definition exists for ESSID in the 802.11 specification; this term is commonly used for a BSS network name in the Linux environment. The network name can be up to 32 characters in length and can contain spaces. When running in AP mode, it is the name of the network as advertised in the beacon message. In STA mode, it is the network name that the STA associates with. The name can be quoted ("") or not, <i>but must be quoted when including spaces</i>. The ESSID is blank by default. The provided scripts set the ESSID to Atheros_Xspan_2G for the first and Atheros_Xspan_5G for the second interface in a dual concurrent configuration.</p> <pre>#iwconfig ath0 essid AP50_Test</pre>
frag	iwconfig athN frag <i>maxfragsize</i>			<p>Sets the fragmentation threshold, which is the maximum fragment size. The fragmentation threshold must be an even number. If the input value is odd, the threshold value is set to the even number that precedes it; that is, "input-1".</p> <p>Note that this is not valid for 802.11n aggregation operations. In addition, this parameter is not supported for QCA988x/989x radios. The argument level indicates the maximum fragment size, or setting to off disables fragmentation. Fragmentation is off by default.</p> <pre>#iwconfig ath0 frag 512</pre>
		Y	Y	Non-HT mode
		Y	N	HT mode

Table 1-1 iwconfig parameters (cont.)

Parameter	Format	DA	OL	Description
freq	<code>iwconfig athN freq <i>opfreq</i></code>	Y	Y	<p>Similar to the channel command, this command selects the frequency of operation. Note that the frequency value <i>opfreq</i> must be a valid frequency supported by the regulatory requirements table for the device. This command takes both channel numbers and frequency values. For frequency values, the suffix K, M, or G can be appended to the value to specify kHz, MHz, or GHz. The values of 2.412G, 2412M, and 2412000K are all the same value.</p> <p>If the value of <i>opfreq</i> is set to 0, Auto Channel Selection is triggered, which will enable automatic selection of the best possible operational channel for the AP in the presence of various types of interference.</p> <p>This command also returns an error if the indicated frequency is invalid for the device.</p> <pre># iwconfig ath0 freq 5.2G #iwconfig ath0 freq 40</pre>
rate	<code>iwconfig athN rate <i>rateval</i> <i>auto</i></code>	Y	Y	<p>Selects a fixed rate for transmit, or enables the internal rate control logic. When <i>rateval</i> is provided, it specifies the bit rate desired. Using the M or k suffix can be used to indicate the rate, such as 36M. Specifying <i>auto</i> instead of a fixed rate will enable the rate control logic internal to the driver. This is the default configuration.</p> <p>Setting 802.11n and 802.11ac fixed rates adds more complexity. Selecting MCS rates cannot be accomplished through this command.</p> <p>For 802.11n rates – use iwpriv commands Set11NRates and Set11NRetries</p> <p>For 802.11ac rates – use iwpriv commands nss and vhtmcs.</p> <p>Not supported on QCA955x.</p> <pre>#iwconfig ath0 rate 36M</pre>
retry	—	N	N	Software retry is not supported
rts	<code>iwconfig athN rts <i>minpktsize</i></code>	Y	Y	<p>Sets the minimum packet size for which RTS/CTS protection is used. This setting is used to reduce the amount of arbitration that occurs with short packet transmission, improving throughput. The value of <i>minpktsize</i> is set to the minimum packet size for which to use the RTS/CTS handshake. Setting <i>minpktsize</i> to a value of 0 disables RTS/CTS handshake entirely. The use of RTS/CTS in 802.11n is governed by rate tables and other settings, so this command may not have the desired effect when using 802.11n rates. The threshold should be more than 256 B (as defined by iwconfig).</p> <pre>#iwconfig ath0 rts 256</pre>
sens	—	N	N	Receiver sensitivity control is not supported.
txpower	<code>iwconfig athN txpower <i>pwrsetting</i></code>	Y	Y	<p>Sets the Tx power for all packets on the device. This power is limited by the regulatory limits encoded into the driver, and selected by setting the country code (see the iwpriv command setCountry). The value of <i>pwrsetting</i> is provided in units of dBm. Setting the power_setting value to off will enable the internal power control logic for setting power level. Default Tx power levels are dependent on information in the selected regulatory table.</p> <pre>#iwconfig ath0 txpower 30</pre>

1.3 iwpriv parameters

This section defines all of the **iwpriv** parameters available for each layer.

NOTE There are some duplicate parameters between the layers. It is recommended to use the radio layer (**wifiN**) parameters over the protocol layer (**athN**) parameters when duplication exists.

The radio layer parameters are provided to configure the radio layer for all VAPs attached to the radio. Common parameters for the radio include the frequency (channel), the channel width mode (HT20/40), and other parameters that apply to radio operations.

NOTE All VAPS attached to the specific radio are affected by the configurations made to the radio layer.

For all parameters having a corresponding “get” parameter, the current value(s) are returned.

QUALCOMM
2015-10-27 01:43:49 PDT
jinwei5@hikvision.com

1.3.1 Aggregation parameters

Table 1-2 11ac interface aggregation parameters

Parameter	Format	DA	OL	Description
addba delba	<code>iwpriv athN addba AID AC BufSize</code> <code>iwpriv athN delba AID AC initiator reason</code>			Test commands used to manually add or delete block acknowledge aggregation streams. Automatic addba/delba processing must be turned off prior to using these commands (see setaddbaoper). Both require the AID and AC specified. The AID value is shown by the wlanconfig list command. When adding an aggregation link with addba, BufSize must be set to the maximum number of subframes sent in an aggregate. When deleting aggregation links, the initiator field indicates whether this link was initiated by the AP (1) or the remote STA (0). The 8-bit code indicates the reason the link shut down. No corresponding get parameters or default values. <code>#iwpriv ath0 addba 1 0 32</code> <code>#iwpriv ath0 delba 1 0 1 36</code>
addbaresp	<code>iwpriv athN addbaresp AID AC status</code>			Sends an addba response frame on the indicated AID and AC. AID is the value shown under the AID column using the command wlanconfig list . The status value is an 8-bit value indicating the status field of the response. Normally used only during testing of the aggregation interface. The command does not have a corresponding get parameter, nor does it have a default value. <code>#iwpriv ath0 addbaresp 1 0 25</code>
AMPDU getAMPDU	<code>iwpriv wifiN AMPDU {1 0}</code>	Y	N	Enables (1) or disables (0) Tx AMPDU aggregation for the entire interface. Receiving aggregate frames will still be performed, but no aggregate frames will be transmitted if this is disabled. The get parameter returns the current value. Default is 1. Specific to 802.11n. <code>#iwpriv wifi0 AMPDU 1</code> <code>#iwpriv wifi0 getAMPDU</code> <code>wifi0 getAMPDU:1</code>
ampdu get_ampdu	<code>iwpriv athN ampdu {1...64}</code>	N	Y	Sets maximum number of mpdus gets aggregated in a single AMPDU. Specific to 802.11ac. <code>#iwpriv ath0 ampdu 1</code> <code>#iwpriv ath0 get_ampdu</code> <code>ath0 get_ampdu:1</code>
amsdu get_amsdu	<code>iwpriv athN amsdu {1...32}</code>	N	Y	Sets maximum number of AMSDU subframes. Specific to 802.11ac. <code>#iwpriv ath0 amsdu 1</code> <code>#iwpriv ath0 get_amsdu</code> <code>ath0 get_amsdu:1</code>
maxampdu get_maxampdu	<code>iwpriv athN maxampdu {0...3}</code>	N	Y	Set/gets HT capability field, Maximum A-MPDU length exponent. Value range is 0 to 3. Maximum A-MPDU length exponent indicates the maximum length of A-MPDU that the station can receive. Specific to 802.11ac. <code>#iwpriv ath0 maxampdu 1</code> <code>#iwpriv ath0 get_maxampdu</code> <code>ath0 get_maxampdu:1</code>

Table 1-2 11ac interface aggregation parameters (cont.)

Parameter	Format	DA	OL	Description
vhtmaxampdu get_vhtmaxampdu	iwpriv athN vhtmaxampdu {0...7}	N	Y	Set/gets VHT capability field, Maximum A-MPDU length exponent. Value range is 0 to 7. Maximum A-MPDU length exponent indicates the maximum length of A-MPDU that the station can receive. Specific to 802.11ac. #iwpriv ath0 vhtmaxampdu 1 #iwpriv ath0 get_vhtmaxampdu ath0 get_vhtmaxampdu:1
getadbbastatus	iwpriv athN getadbbastatus status			Gets the ADDBA (Add Block Acknowledgement) status for AID (Association Identifier) and TID (Traffic Identifier). <i>What is the format of aid, tid when returned?</i> #iwpriv ath0 getadbbastatus aid ath0 getadbbastatus:
			aid	AID number of STA
			tid	TID number between 0-15
setaddbaoper getaddbaoper	iwpriv athN setaddbaoper 1 0			Enables/disables automatic processing for aggregation/block ACK setup frames. To use the manual addba/delba commands, it must be set to 0 (off) to keep the driver from also responding. Has a corresponding get parameter, and its default value is 1 (enabled). #iwpriv ath0 setaddbaoper 0 #iwpriv ath0 getaddbaoper ath0 getaddbaoper:0

Table 1-3 11na and 11ac interfaces specific statistics

Parameter	Format	DA	OL	Description
addba delba	iwpriv athN addba AID AC BufSize iwpriv athN delba AID AC initiator reason			Test commands used to manually add or delete block acknowledge aggregation streams. Automatic addba/delba processing must be turned off prior to using these commands (see setaddbaoper). Both require the AID and AC specified. The AID value is shown by the wlanconfig list command. When adding an aggregation link with addba, BufSize must be set to the maximum number of subframes sent in an aggregate. When deleting aggregation links, the initiator field indicates whether this link was initiated by the AP (1) or the remote STA (0). The 8-bit code indicates the reason the link shut down. No corresponding get parameters or default values. #iwpriv ath0 addba 1 0 32 #iwpriv ath0 delba 1 0 1 36
addbaresp	iwpriv athN addbaresp AID AC status			Sends an addba response frame on the indicated AID and AC. AID is the value shown under the AID column using the command wlanconfig list . The status value is an 8-bit value indicating the status field of the response. Normally used only during testing of the aggregation interface. The command does not have a corresponding get parameter, nor does it have a default value. #iwpriv ath0 addbaresp 1 0 25

Table 1-3 11na and 11ac interfaces specific statistics (cont.)

Parameter	Format	DA	OL	Description
burst get_burst	iwpriv wifiN burst {1 0}	N	Y	Enables (1) or disables (0) SIFS bursting for the entire interface. The AMPDU size is dynamically determined based on Rate chosen and burst duration is also dynamically chosen. The get parameter returns the current value. Default is 1 for certain peregrine cards. It is 0 for the rest. Specific to 802.11n. #iwpriv wifi0 burst 1 #iwpriv wifi0 get_burst get_burst:1
txrx_fw_stats	iwpriv athN txrx_fw_stats {1...6}	N	Y	Tx and Rx related statistics from target #iwpriv ath0 txrx_fw_stats 1
getadbbastatus	iwpriv athN getadbbastatus status			Gets the ADDBA (Add Block Acknowledgment) status for AID (Association Identifier) and TID (Traffic Identifier). <i>What is the format of aid, tid when returned?</i> #iwpriv ath0 getadbbastatus aid ath0 getadbbastatus:
			aid	AID number of STA
			tid	TID number between 0-15
setaddbaoper getaddbaoper	iwpriv athN setaddbaoper 1 0			Enables/disables automatic processing for aggregation/block ACK setup frames. To use the manual addba/delba commands, it must be set to 0 (off) to keep the driver from also responding. Has a corresponding get parameter, and its default value is 1 (enabled). #iwpriv ath0 setaddbaoper 0 #iwpriv ath0 getaddbaoper ath0 getaddbaoper:0

1.3.2 ANI parameters

Table 1-4 ANI parameters

Parameter	Format	DA	OL	Description
addba delba	<code>iwpriv athN addba AID AC BufSize</code> <code>iwpriv athN delba AID AC initiator reason</code>			Test commands used to manually add or delete block acknowledge aggregation streams. Automatic addba/delba processing must be turned off prior to using these commands (see setaddbaoper). Both require the AID and AC specified. The AID value is shown by the wlanconfig list command. When adding an aggregation link with addba, BufSize must be set to the maximum number of subframes sent in an aggregate. When deleting aggregation links, the initiator field indicates whether this link was initiated by the AP (1) or the remote STA (0). The 8-bit code indicates the reason the link shut down. No corresponding get parameters or default values. <code>#iwpriv ath0 addba 1 0 32</code> <code>#iwpriv ath0 delba 1 0 1 36</code>
addbaresp	<code>iwpriv athN addbaresp AID AC status</code>			Sends an addba response frame on the indicated AID and AC. AID is the value shown under the AID column using the command wlanconfig list . The status value is an 8-bit value indicating the status field of the response. Normally used only during testing of the aggregation interface. The command does not have a corresponding get parameter, nor does it have a default value. <code>#iwpriv ath0 addbaresp 1 0 25</code>
ani_enable get_ani_enable	<code>iwpriv wifiN ani_enable {1 0}</code>	Y	Y	Enables (1) or disables (0) ANI functionality. The default is 0. This command is specific to 802.11ac. <code>#iwpriv wifi0 ani_enable 1</code> <code>#iwpriv wifi0 get_ani_enable</code> <code>wifi0 get_ani_enable:0</code>
ANIEna GetANIEna	<code>iwpriv wifiN ANIEna {1 0}</code>	Y	N	Enables (1) or disables (0) ANI functionality. The default is 1. <code>#iwpriv wifi0 ANIEna 0</code> <code>#iwpriv wifi0 GetANIEna</code> <code>wifi0 GetANIEna:0</code>
getaddbastatus	<code>iwpriv athN getaddbastatus status</code>			Gets the ADDBA (Add Block Acknowledgment) status for AID (Association Identifier) and TID (Traffic Identifier). <i>What is the format of aid, tid when returned?</i> <code>#iwpriv ath0 getaddbastatus aid ath0 getaddbastatus:</code>
				aid AID number of STA
				tid TID number between 0-15
setaddbaoper getaddbaoper	<code>iwpriv athN setaddbaoper 1 0</code>			Enables/disables automatic processing for aggregation/block ACK setup frames. To use the manual addba/delba commands, it must be set to 0 (off) to keep the driver from also responding. Has a corresponding get parameter, and its default value is 1 (enabled). <code>#iwpriv ath0 setaddbaoper 0</code> <code>#iwpriv ath0 getaddbaoper</code> <code>ath0 getaddbaoper:0</code>

1.3.3 Association/ACL parameters

Table 1-5 Association/ACL parameters

Parameter	Format	DA	OL	Description										
addmac delmac getmac maccmd get_maccmd	<i>iwpriv athN addmac macaddr</i> <i>iwpriv athN delmac macaddr</i> <i>iwpriv athN maccmd cmd</i>	Y	Y	<p>These parameters set up and modify the MAC filtering list. MAC filtering allows users to either limit specific MAC addresses from associating with the AP, or specifically indicates which MAC addresses can associate with the AP.</p> <p>addmac adds specified MAC addresses to the access control list (ACL). delmac deletes addresses from the ACL. These parameters have no get equivalents. getmac displays the list of MAC addresses monitored by the ACL.</p> <pre>#iwpriv ath0 addmac 00:03:7f:00:00:20 #iwpriv ath0 delmac 00:03:7f:00:12:34 #iwpriv ath0 getmac ath0 getmac:00:03:7f:00:00:20</pre> <p>maccmd instructs how the ACL is used to limit access the AP. The default is 0. The get parameter returns the current value.</p> <p>Valid <i>cmd</i> values:</p> <table><tr><td>0</td><td>Disable ACL checking</td></tr><tr><td>1</td><td>Only allow association with MAC addresses on the list</td></tr><tr><td>2</td><td>Deny association with any MAC address on the list</td></tr><tr><td>3</td><td>Flush the current ACL list</td></tr><tr><td>4</td><td>Suspend current ACL policies. Re-enable with a 1 or 2 command.</td></tr></table> <pre>#iwpriv ath0 maccmd 1 #iwpriv ath0 get_maccmd ath0 get_maccmd:1</pre>	0	Disable ACL checking	1	Only allow association with MAC addresses on the list	2	Deny association with any MAC address on the list	3	Flush the current ACL list	4	Suspend current ACL policies. Re-enable with a 1 or 2 command.
0	Disable ACL checking													
1	Only allow association with MAC addresses on the list													
2	Deny association with any MAC address on the list													
3	Flush the current ACL list													
4	Suspend current ACL policies. Re-enable with a 1 or 2 command.													
ap_bridge get_ap_bridge	<i>iwpriv athN ap_bridge mode</i>	Y	Y	<p>Enables or disables bridging within the AP driver; has the effect of allowing a STA associated to the AP to access any other STA associated to the AP. This command eliminates bridging between clients. Its default value is 1. The get parameter returns the current value.</p> <pre>#iwpriv ath0 ap_bridge 0 #iwpriv ath0 get_ap_bridge ath0 get_ap_bridge:0</pre>										
kickmac	<i>iwpriv athN kickmac macaddr</i>	Y	Y	<p>Forces the AP to disassociate the specified STA.</p> <pre>#iwpriv ath0 kickmac 00:18:41:9b:c8:87</pre>										
sko get_sko	<i>iwpriv athN sko max_retries</i>			<p>Sets STA quick kick-out maximum consecutive retries value. If the node is not a NAWDS repeater and failed count reaches this value, it kicks out the node. The default value is 50. The get parameter returns the current value.</p> <pre>#iwpriv ath0 sko 50 #iwpriv ath0 get_sko ath0 get_sko:50</pre>										

1.3.4 Beacon configuration parameters

Table 1-6 Beacon configuration parameters

Parameter	Format	DA	OL	Description
ampdudensity get_ ampdudensity	iwpriv athN ampdudensity MPDU_density			Sets the value of MPDU density. The default is 6. The get parameter returns the current value. #iwpriv ath0 ampdudensity 6 #iwpriv ath0 get_ampdudensity ath0 get_ampdudensity:6
			0	No time restriction
			1	0.25 μ s
			2	0.5 μ s
			3	1 μ s
			4	2 μ s
			5	4 μ s
			6	8 μ s
			7	16 μ s
amsdu get_amsdu	iwpriv athN amsdu 0/1			Sets the aggregated MSDUs (AMSDUs) transmission setting. #iwpriv ath0 amsdu 0 #iwpriv ath0 get_amsdu ath0 get_amsdu:0
			0	Disable AMSDU transmission
			1	Enable AMSDU transmission
amsdulimit get_amsdulimit	iwpriv athN amsdulimit AMPDU_limits			Sets the value of 11n A-MPDU limits. #iwpriv ath0 amsdulimit #iwpriv ath0 get_amsdulimit ath0 get_amsdulimit:
bintval get_bintval	iwpriv athN bintval beaconinterval	Y	Y	Sets the AP's beacon interval value, in ms. The value determines the number of ms between beacon transmissions. For the multiple VAP case, the beacons are transmitted evenly within this interval. Thus, if four VAPs are created and the beacon interval is 200 ms, a beacon will be transmitted from the radio portion every 50 ms, from each VAP in a round-robin fashion. The default value of the interval is 100 ms. The get parameter returns the current value. #iwpriv ath0 bintval 400 #iwpriv ath0 get_bintval ath0 get_bintval:200

Table 1-6 Beacon configuration parameters (cont.)

Parameter	Format	DA	OL	Description
blockdfschan	iwpriv athN blockdfschan {1 0}	Y	Y	Disables the selection of DFS channels when the 802.11h channel switch processing is selecting a new channel. Typically, when a radar signal is detected on a channel, a new channel is picked randomly from the list. DFS channels are normally included in the list, so if there are several radars in the area, another hit is possible. Setting this selection to 0 enables the use of DFS channels in the selection process, while a value of 1 disables DFS channels. The default value is 1. This limits the number of available channels. No get parameter available. #iwpriv ath0 blockdfschan 1
countryie get_countryie	iwpriv athN countryie {1 0}	Y	Y	An enable/disable control that determines if the country IE is to be sent out as part of the beacon. The country IE is used by 802.11h processing to allow STAs to self-configure regulatory tables to the country. Sending this IE configures all such STAs to the country the AP is configured to. The default value is 1 (enabled). The get parameter returns the current value. Result is correct; ignore error message on the console. #iwpriv ath0 countryie 1 #iwpriv ath0 get_countryie ath0 get_countryie:1
doth get_doth	iwpriv athN doth {1 0}	Y	Y	Enables or disables support for 802.11h regulatory information selection. For the AP, this enables or disables transmission of country IE information in the beacon. STAs supporting 802.11h configures regulatory information according to the information in the country IE. The default value is 1 (enabled). The get parameter returns the current value. Result is correct; ignore error message on the console. #iwpriv ath0 doth 1 #iwpriv ath0 get_doth ath0 get_doth:1
doth_chanswitch	iwpriv athN doth_chanswitch <i>channel</i> <i>tbtt</i>			Forces the AP to perform a channel change, and forces a channel change announcement message. Used to test the 802.11h channel switch mechanism. Has no corresponding get parameter. #iwpriv ath0 doth_chanswitch 3 5
				channel Specifies channel to which AP will switch
				tbtt Number of beacons to wait before doing the switch
dtim_period get_dtim_period	iwpriv athN dtim_period <i>deliveryperiod</i>	Y	Y	Used to set the DTIM period. The DTIM is an interval specified by the AP to the STA indicating when multi-cast traffic may be available for the STA, requiring the STA to be awake to receive the messages. This parameter will set the AP DTIM period, in ms. A longer DTIM will provide for a greater power savings, but will increase multi-cast latency. This parameter has a default value of 1 ms. The get parameter returns the current value. #iwpriv ath0 dtim_period 5 #iwpriv ath0 get_dtim_period wifi0 get_dtim_period:1

Table 1-6 Beacon configuration parameters (cont.)

Parameter	Format	DA	OL	Description
hide_ssid get_hide_ssid	iwpriv athN hide_ssid {1 0}	Y	Y	Hides the SSID, disabling it in the transmitted beacon, when enabled. Used for secure situations where the AP does not want to advertise the SSID name. A value of 0 will enable the SSID in the transmitted beacon. The get parameter returns the current value. The default value is 0. #iwpriv ath0 hide_ssid 1 #iwpriv ath0 get_hide_ssid ath0 get_hide_ssid:1
pureg get_pureg	iwpriv athN pureg {1 0}	Y	Y	Enables or disables pure G mode. This mode does not allow 802.11b rates, and only uses OFDM modulation. The get parameter returns the current value. The default value is 0. Result is correct; ignore error message on the console. #iwpriv ath0 pureg 1 #iwpriv ath0 get_pureg ath0 get_pureg:1
puren get_puren	iwpriv athN puren {1 0}	Y	Y	Enables/disables pure 11N mode, which does not accept STAs that do not have HT caps in AP mode. Result is correct; ignore error message on the console. #iwpriv ath0 puren 1 #iwpriv ath0 get_puren ath0 get_puren:1
set_bcnburst get_bcnburst	iwpriv wifiN set_bcnburst {1 0}	Y	Y	Set the beaconing scheme. to burst or staggered mode. The default is staggered mode. #iwpriv wifi0 set_bcnburst 0 #iwpriv wifi0 get_bcnburst wifi0 get_bcnburst: 0
				1 burst mode
				0 staggered mode
setoptie getoptie	iwpriv athN setoptie iwpriv athN getoptie			Sets/gets application specific optional IE buffer. #iwpriv ath0 setoptie #iwpriv ath0 getoptie ath0 getoptie:
shortgi get_shortgi	iwpriv athN shortgi {1 0}	Y	Y	Enables/disables the short gating interval (shortgi) when transmitting HT40 frames. This effectively increases the PHY rate by 25%. This is a manual control typically used for testing. The get parameter returns the current value. The default value is 1. #iwpriv ath0 shortgi 1 #iwpriv ath0 get_shortgi ath0 get_shortgi:1

Table 1-6 Beacon configuration parameters (cont.)

Parameter	Format	DA	OL	Description
vap_contryie get_vapcontryie	iwpriv athN vap_ contryie 1/0	Y	N	Enables/disables Country IE support of the specified VAP athN in nBSSID mode. Default value is 1. Not supported. #iwpriv ath0 vap_contryie 1 #iwpriv ath0 get_vapcontryie ath0 get_vapcontryie:1
				1 Enable Country IE support
				0 Disable Country IE support
vap_doth get_vapdoth	iwpriv athN vap_doth 1/0	Y	Y	Enables (1) or disables (0) 802.11h support of the specified VAP in mBSSID mode. Default value is 1. Result is correct; ignore error message on the console. #iwpriv ath0 vap_doth 1 #iwpriv ath0 get_vap_doth ath0 get_vap_doth:1
				1 Enable 802.11h support
				0 Disable 802.11h support
vap_ind get_vap_ind	iwpriv athN vap_doth 1/0			Enables/disables VAP WDS independence set
				0 Disable wds independence set
				1 Enable wds independence set

1.3.5 Channel width parameters

Table 1-7 Channel width parameters

Parameter	Format	DA	OL	Description
chextoffset get_chextoffset	iwpriv athN chextoffset channeloffset	Y	Y	Sets the extension (secondary) channel offset field in the AP beacon High Throughput Information Element (HT IE). If this parameter is not executed, then the extension channel offset is taken from the device settings. This parameter has a corresponding get parameter. The default value is 0. #iwpriv ath0 chextoffset 0 #iwpriv ath0 get_chextoffset ath0 get_chextoffset:0
				0 Use the device settings
				1 None
				2 Extension (Secondary) channel is above the control (Primary) channel
				3 Extension (Secondary) channel is below the control (Primary) channel

Table 1-7 Channel width parameters (cont.)

Parameter	Format	DA	OL	Description
chwidth get_chwidth	iwpriv athN chwidth <i>channelwidth</i>	Y	Y	Sets the channel width field in the AP beacon High Throughput Information Element (HTIE). If this command is not executed, then the channel width is taken from the device settings. The get parameter returns the current value. The default value is 0.
				Sets the current channel width setting. Not necessarily the value set by cwmode , because it can be automatically overridden.
				#iwpriv ath0 chwidth 0 #iwpriv ath0 get_chwidth ath0 get_chwidth:0
				0 Use the device settings
				1 20 MHz
				2 20/40 MHz
				3 VHT80
cwmenable get_cwmenable	iwpriv athN cwmenable {1 0}	Y	Y	Enables or disables automatic channel width management. If set to 0, the CWM state machine is disabled (1 enables the state machine). Used when static rates and channel widths are desired. The default is 1. The get parameter returns the current value.
				#iwpriv ath0 cwmenable 1 #iwpriv ath0 get_cwmenable ath0 get_cwmenable:1

Table 1-7 Channel width parameters (cont.)

Parameter	Format	DA	OL	Description																												
mode get_mode	<code>iwpriv athN mode</code> <i>operatingmode</i>	Y	Y	<p>Sets the current operating mode of the interface. The argument is a string that defines the desired mode of operation. The mode also affects the configuration of the radio layer. The argument for mode is provided as a string. The default value is AUTO. The get parameter returns the mode as a string value.</p> <pre>#iwpriv ath0 mode 11NAHT20 # iwpriv ath0 get_mode ath0 get_mode:11ng20</pre> <p>The operating modes include:</p> <table><tr><td>AUTO</td><td>Mode is set automatically</td></tr><tr><td>11A</td><td>Legacy operation in 802.11a (5 GHz)</td></tr><tr><td>11B</td><td>Legacy operation in 802.11b (2.4 GHz)</td></tr><tr><td>11G</td><td>802.11g</td></tr><tr><td>11NAHT20</td><td>802.11n A-band 20 MHz channels</td></tr><tr><td>11NGHT20</td><td>802.11n G-band 20 MHz channels</td></tr><tr><td>11NAHT40PLUS</td><td>802.11n A-band 40 MHz channels. Select frequency channels higher than the primary control channel as the extension channel</td></tr><tr><td>11NAHT40MINUS</td><td>802.11n A-band 40 MHz channels. Select frequency channels lower than the primary control channel as the extension channel</td></tr><tr><td>11NGHT40PLUS</td><td>802.11n G-band 40 MHz channels. Select frequency channels higher than the primary control channel as the extension channel</td></tr><tr><td>11NGHT40MINUS</td><td>802.11n G-band 40 MHz channels. Select frequency channels lower than the primary control channel as the extension channel</td></tr><tr><td>11ACVHT20</td><td>802.11ac A-band 20 MHz channels</td></tr><tr><td>11ACVHT40PLUS</td><td>802.11ac A-band 40 MHz channels. Select frequency channels higher that control channel as the extension channel.</td></tr><tr><td>11ACVHT40MINUS</td><td>802.11ac A-band 40 MHz channels. Select frequency channels lower that control channel as the extent ion channel.</td></tr><tr><td>11ACVHT80</td><td>802.11ac A-band 80 MHz channels</td></tr></table>	AUTO	Mode is set automatically	11A	Legacy operation in 802.11a (5 GHz)	11B	Legacy operation in 802.11b (2.4 GHz)	11G	802.11g	11NAHT20	802.11n A-band 20 MHz channels	11NGHT20	802.11n G-band 20 MHz channels	11NAHT40PLUS	802.11n A-band 40 MHz channels. Select frequency channels higher than the primary control channel as the extension channel	11NAHT40MINUS	802.11n A-band 40 MHz channels. Select frequency channels lower than the primary control channel as the extension channel	11NGHT40PLUS	802.11n G-band 40 MHz channels. Select frequency channels higher than the primary control channel as the extension channel	11NGHT40MINUS	802.11n G-band 40 MHz channels. Select frequency channels lower than the primary control channel as the extension channel	11ACVHT20	802.11ac A-band 20 MHz channels	11ACVHT40PLUS	802.11ac A-band 40 MHz channels. Select frequency channels higher that control channel as the extension channel.	11ACVHT40MINUS	802.11ac A-band 40 MHz channels. Select frequency channels lower that control channel as the extent ion channel.	11ACVHT80	802.11ac A-band 80 MHz channels
AUTO	Mode is set automatically																															
11A	Legacy operation in 802.11a (5 GHz)																															
11B	Legacy operation in 802.11b (2.4 GHz)																															
11G	802.11g																															
11NAHT20	802.11n A-band 20 MHz channels																															
11NGHT20	802.11n G-band 20 MHz channels																															
11NAHT40PLUS	802.11n A-band 40 MHz channels. Select frequency channels higher than the primary control channel as the extension channel																															
11NAHT40MINUS	802.11n A-band 40 MHz channels. Select frequency channels lower than the primary control channel as the extension channel																															
11NGHT40PLUS	802.11n G-band 40 MHz channels. Select frequency channels higher than the primary control channel as the extension channel																															
11NGHT40MINUS	802.11n G-band 40 MHz channels. Select frequency channels lower than the primary control channel as the extension channel																															
11ACVHT20	802.11ac A-band 20 MHz channels																															
11ACVHT40PLUS	802.11ac A-band 40 MHz channels. Select frequency channels higher that control channel as the extension channel.																															
11ACVHT40MINUS	802.11ac A-band 40 MHz channels. Select frequency channels lower that control channel as the extent ion channel.																															
11ACVHT80	802.11ac A-band 80 MHz channels																															

1.3.6 Debug parameters

Table 1-8 Debug parameters

Parameter	Format	DA	OL	Description
dbgLVL getdbgLVL	iwpriv athN dbgLVL {1 0}	Y	Y	Controls the debug level of the VAP-based debug print statements. It is normally set to zero, eliminating all prints. See Table 1-9 . #iwpriv ath0 dbgLVL 256 # iwpriv ath0 getdbgLVL ath0 getdbgLVL:256
				0 Disable debug prints
				1 Enable debug prints (note that each bitmask has its own debug level)
HALDbg GetHALDbg	iwpriv wifiN HALDbg {1 0}			Sets the debug level in the HAL code; can be modified as required. The HAL must be built with the AH_DEBUG parameter defined for this command to be available; otherwise, it is conditionally compiled out. The value provided is a bitmask selecting specific categories of debug information from which to select. NOTE: Some categories will produce copious amounts of output, and should be used sparingly for a few seconds. See Table 1-9 on page 28 . The get parameter returns the current value in decimal format (convert to hexadecimal to match the list in the table). The default is 0 (no debugging), but it does not disable the unmaskable prints. For example, to set and get debug information for an 802.1x radius client: #iwpriv wifi0 HALDbg 0x00008000 #iwpriv wifi0 GetHALDbg wifi0 GetHALDbg:32768
				0 Disable debugging
				1 Enable debugging

Table 1-9 802.11 Protocol layer debug bitmask

Symbolic name	Bit value	Description
IEEE80211_MSG_P2P_PROT	0x0100000000	P2P protocol driver debug
IEEE80211_MSG_RRM	0x0200000000	Radio resource measurement debug
IEEE80211_MSG_WNM	0x0400000000	Wireless network management debug
IEEE80211_MSG_PROXYARP	0x0800000000	Proxy ARP debug
IEEE80211_MSG_L2TIF	0x1000000000	Hotspot 2.0 L2 TIF debug
IEEE80211_MSG_WIFIPOS	0x2000000000	Wi-Fi positioning feature debug
IEEE80211_MSG_DFS	0x0400000000	DFS debug message
IEEE80211_MSG_MLME	0x80000000	MLME mode debug
IEEE80211_MSG_DEBUG	0x40000000	IFF_DEBUG equivalent
IEEE80211_MSG_DUMPPKTS	0x20000000	IFF_LINK2 equivalent

Table 1-9 802.11 Protocol layer debug bitmask (cont.)

Symbolic name	Bit value	Description
IEEE80211_MSG_CRYPTO	0x10000000	Crypto work
IEEE80211_MSG_INPUT	0x08000000	Input handling
IEEE80211_MSG_XRATE	0x04000000	Rate set handling
IEEE80211_MSG_ELEMID	0x02000000	Element ID parsing
IEEE80211_MSG_NODE	0x01000000	Node handling
IEEE80211_MSG_ASSOC	0x00800000	Association handling
IEEE80211_MSG_AUTH	0x00400000	Authentication handling
IEEE80211_MSG_SCAN	0x00200000	Scanning
IEEE80211_MSG_OUTPUT	0x00100000	Output handling
IEEE80211_MSG_STATE	0x00080000	State machine
IEEE80211_MSG_POWER	0x00040000	Power save handling
IEEE80211_MSG_DOT1X	0x00020000	802.1x authenticator
IEEE80211_MSG_DOT1XSM	0x00010000	802.1x state machine
IEEE80211_MSG_RADIUS	0x00008000	802.1x radius client
IEEE80211_MSG_RADDUMP	0x00004000	Dump 802.1x radius packets
IEEE80211_MSG_RADKEYS	0x00002000	Dump 802.1x keys
IEEE80211_MSG_WPA	0x00001000	WPA/RSN protocol
IEEE80211_MSG_ACL	0x00000800	ACL handling
IEEE80211_MSG_WME	0x00000400	WME protocol
IEEE80211_MSG_SUPG	0x00000200	SUPERG
IEEE80211_MSG_DOTH	0x00000100	802.11h
IEEE80211_MSG_INACT	0x00000080	Inactivity handling
IEEE80211_MSG_ROAM	0x00000040	STA-mode roaming
IEEE80211_MSG_ACTION	0x00000020	Action management frames
IEEE80211_MSG_WDS	0x00000010	WDS handling
IEEE80211_MSG_SCANENTRY	0x00000008	Scan entry
IEEE80211_MSG_SCAN_SM	0x00000004	Scan state machine
IEEE80211_MSG_ACS	0x00000002	Auto channel selection
IEEE80211_MSG_TDLS	0x00000001	TDLS
IEEE80211_MSG_ANY	0xFFFFFFFF	Anything

Table 1-10 HAL debug flags

Symbolic name	Enable Bit	Description
HAL_DBG_RESET	0x00000001	Information pertaining to reset processing and initialization
HAL_DBG_PHY_IO	0x00000002	PHY read/write states
HAL_DBG_REG_IO	0x00000004	Register I/O, including all register values. Use with caution.

Table 1-10 HAL debug flags (cont.)

Symbolic name	Enable Bit	Description
HAL_DBG_RF_PARAM	0x00000008	RF parameter information and table settings
HAL_DBG_QUEUE	0x00000010	Queue management for WMM support
HAL_DBG_EEPROM_DUMP	0x00000020	Large EEPROM information dump; system must be compiled with a defined EEPROM_DUMP conditional variable
HAL_DBG_EEPROM	0x00000040	EEPROM read/write and status information
HAL_DBG_NF_CAL	0x00000080	Noise Floor calibration debug information
HAL_DBG_CALIBRATE	0x00000100	All other calibration debug information
HAL_DBG_CHANNEL	0x00000200	Channel selection and channel settings
HAL_DBG_INTERRUPT	0x00000400	Interrupt processing. WARNING: this produces a LOT of output, use in short bursts.
HAL_DBG_DFS	0x00000800	DFS settings
HAL_DBG_DMA	0x00001000	DMA debug information
HAL_DBG_REGULATORY	0x00002000	Regulatory table settings and selection
HAL_DBG_TX	0x00004000	Transmit path information
HAL_DBG_TXDESC	0x00008000	Transmit descriptor processing
HAL_DBG_RX	0x00010000	Receive path information
HAL_DBG_RXDESC	0x00020000	Receive descriptor processing
HAL_DBG_ANI	0x00040000	Debug information for automatic noise immunity (ANI)
HAL_DBG_BEACON	0x00080000	Beacon processing and setup information
HAL_DBG_KEYCACHE	0x00100000	Encryption key management
HAL_DBG_POWER_MGMT	0x00200000	Power and Tx Power level management
HAL_DBG_MALLOC	0x00400000	Memory allocation
HAL_DBG_FORCE_BIAS	0x00800000	Force bias related processing
HAL_DBG_POWER_OVERRIDE	0x01000000	Tx power override processing
HAL_DBG_SPUR_MITIGATE	0x02000000	Mitigate
HAL_DBG_PRINT_REG	0x04000000	Print reg.
HAL_DBG_TIMER	0x08000000	Debug timer
HAL_DBG_UNMASKABLE	0xFFFFFFFF	Will be printed in all cases if AH_DEBUG is defined

1.3.7 Dynamic Channel Selection for Interference Mitigation (DCS-IM) Parameters

Table 1-11 DCS-IM parameters

Parameter	Format	DA	OL	Description
dcx_enable get_dcs_enable	iwpriv wifiN dcs_enable <i>value</i>	Y	Y	Enable or disable DCS. #iwpriv wifi0 dcs_enable 0 #iwpriv wifi0 get_dcs_enable wifi0 get_dcs_enable:0
			0	Disable DCS
			1	Enable DCS for CW interference mitigation (CW_IM).
			2	Enable DCS for WLAN interference mitigation. Since the algorithm defined in this section primarily mitigates WLAN interferences, DCS for WLAN is referred to as WLAN interference mitigation (WLAN_IM).
			3	Enable both DCS for CW_IM and DCS for WLAN_IM
set_dcs_intrth get_dcs_intrth	iwpriv wifiN set_dcs_intrth <i>value</i>	Y	N	Configures co-channel interference threshold (in percent) to trigger channel change. Default <i>value</i> of co-channel interference threshold is 30%. #iwpriv wifi0 set_dcs_intrth 30 #iwpriv wifi0 get_dcs_intrth wifi0 get_dcs_intrth:30
set_dcs_errth get_dcs_errth	iwpriv wifiN set_dcs_errth <i>value</i>	Y	Y	Configures transmission failure rate threshold, used to indicates the presence of interference. Default <i>value</i> of transmission failure rate threshold is 30%. #iwpriv wifi0 set_dcs_errth 30 #iwpriv wifi0 get_dcs_errth wifi0 get_dcs_errth:30
s_dcs_phyerrth g_dcs_phyerrth	iwpriv wifiN s_dcs_phyerrth <i>value</i>	Y	Y	Configures channel time wasted due to each PHY error (PHY error Penalty). Default <i>value</i> of PHY error penalty is set as 500 ?sec. #iwpriv wifi0 s_dcs_phyerrth 500 #iwpriv wifi0 g_dcs_phyerrth wifi0 g_dcs_phyerrth:500
set_dcs_coch_th get_dcs_coch_th	iwpriv wifiN set_dcs_coch_th <i>value</i>	N	Y	Configures co-channel interference threshold (in percent) to trigger channel change. Default <i>value</i> of co-channel interference threshold is 30. #iwpriv wifi1 set_dcs_coch_th 30 #iwpriv wifi1 get_dcs_coch_th dcs_coch_th:30

Table 1-11 DCS-IM parameters (cont.)

Parameter	Format	DA	OL	Description
set_dcs_maxcu get_dcs_maxcu	iwpriv wifiN set_dcs_maxcu <i>value</i>	N	Y	Configures the maximum user channel utilization at which adjacent channel interference should be detected. Default value is 50. #iwpriv wifi1 set_dcs_maxcu 50 #iwpriv wifi1 get_dcs_maxcu get_dcs_maxcu:50
set_dcs_debug get_dcs_debug	iwpriv wifiN set_dcs_debug <value>	N	Y	Configuration to display debug info. Default value is 0. 0 – disable debug info 1 – Enable critical prints only #iwpriv wifi1 set_dcs_debug 50 #iwpriv wifi1 get_dcs_debug get_dcs_debug:50

1.3.8 Green AP parameters

Table 1-12 Green AP Parameters

Parameter	Format	DA	OL	Description
ant_ps_on get_ant_ps_on	iwpriv athN ant_ps_on {1 0}	Y	Y	Enables (1) or disables (0) green AP power save logic. The default value is 1. #iwpriv ath0 ant_ps_on 1 #iwpriv ath0 get_ant_ps_on ath0 get_ant_ps_on:1
ps_timeout get_ps_timeout	iwpriv athN ps_timeout <i>transition_time</i>	Y	Y	Sets the transition time in seconds between power save off to power save on mode. The default value is 20. #iwpriv ath0 ps_timeout 20 #iwpriv ath0 get_ps_timeout ath0 get_ps_timeout:20

1.3.9 Hotspot 2.0

Table 1-13 Hotspot 2.0 parameters

Parameter	Format	DA	OL	Description
qbssload get_qbssload	iwpriv athN qbssload {1 0}	Y	Y	Enables (1) or disables (0) BSS Load IE functionality. The get parameter returns the current value. #iwpriv ath0 qbssload 1 #iwpriv ath0 get_qbssload ath0 get_qbssload:1
proxyarp get_proxyarp	iwpriv athN proxyarp {1 0}	Y	Y	Enables (1) or disables (0) ProxyARP functionality. The get parameter returns the current value. #iwpriv ath0 proxyarp 1 #iwpriv ath0 get_proxyarp ath0 get_proxyarp:1

Table 1-13 Hotspot 2.0 parameters (cont.)

Parameter	Format	DA	OL	Description
l2tif get_l2tif	iwpriv athN l2tif {1 0}	Y	Y	Enables (1) or disables (0) Layer 2 Isolation Function (L2TIF). The get parameter returns the current value. #iwpriv ath0 l2tif 1 #iwpriv ath0 get_l2tif ath0 get_l2tif:1
dgaf_disable g_dgaf_disable	iwpriv athN dgaf_disable {1 0}	Y	Y	Enables (1) or disables (0) Downstream Group Address Forwarding Disable (DGAF Disable) functionality. The get parameter returns the current value. #iwpriv ath0 dgaf_disable 1 #iwpriv ath0 g_dgaf_disable ath0 g_dgaf_disable:1

1.3.10 HT20/HT40 coexistence parameters

Table 1-14 HT20/HT40 coexistence parameters

Parameter	Format	DA	OL	Description
disablecoext g_disablecoext	iwpriv athN disablecoext 1/0	Y	N	Sets HT20/HT40 coexistence support. The default value is 0. The get parameter returns the current value. #iwpriv ath0 disablecoext 0 #iwpriv ath0 g_disablecoext ath0 g_disablecoext:0
				0 Enable HT20/HT40 Coexistence support
				1 Disable HT20/HT40 Coexistence support
chscaninit get_chscaninit	iwpriv athN chscaninit interval_value			Sets the overlapping BSS scan interval value. The get parameter returns the current value. #iwpriv ath0 chscaninit #iwpriv ath0 get_chscaninit ath0 get_chscaninit:
ht40intol get_ht40intol	iwpriv athN ht40intol 1/0			Sets support for HT20/HT40 coexistence management frame support. The default value is 0. The get parameter returns the current value. #iwpriv ath0 ht40intol 0 #iwpriv ath0 get_htol40intol ath0 get_htol40intol:0
				0 Disable HT20/HT40 Coexistence Management frame support
				1 Enable HT20/HT40 Coexistence Management frame support

1.3.11 iQue parameters

Table 1-15 iQue parameters

Parameter	Format	DA	OL	Description
get_hbrstate	<code>iwpriv athN get_hbrstate</code>	N	N	Displays Head of Line Block (HBR) related statistics: VoW, node address, state, trigger, block, dropped VI frames.
get_iqueconfig	<code>iwpriv athN get_iqueconfig</code>	Y	N	Prints all iQUE configuration settings.
hbrparams	<code>iwpriv athN hbrparams ac mode perlowbound</code>	N	N	Sets HBR mitigation. See Table 1-30 for access categories. For example, to enable HBR for video (vi) streams, use <code>iwpriv ath0 hbrparams 2 1 x</code> . The “x” value valid range is from 0-49, and indicates the lower bound PER; a PER better than this value causes HBR to unblock the node.
hbrPER_high get_hbrPER_high	<code>iwpriv wifiN hbrPER_high PER%</code>	N	N	Sets the upper bound PER (Packet Error Rate). If PER is greater than this value and MCS is low, HBR blocks the node (UDP video traffic to this node gets blocked). The PER is expressed as a percentage; for example, 25 means a 25% packet error rate. The get parameter returns the current value.
hbrPER_low get_hbrPER_low	<code>iwpriv wifiN hbrPER_ low PER%</code>	N	N	Sets the lower bound PER. If PER is better than this value while probing, HBR unblocks the node (UDP video traffic to this node gets resumed). The PER is expressed as a percentage; for example, 25 means a 25% packet error rate. The get parameter returns the current value.
hbrtimer get_hbrtimer	<code>iwpriv athN hbrtimer timeout</code>	N	N	Sets the HBR timer timeout value in milliseconds. The default value is 2000 msec (2 seconds). <pre>#iwpriv ath0 hbrtimer 2000 #iwpriv ath0 get_hbrtimer ath0 get_hbrtimer:2000</pre>

Table 1-15 iQue parameters (cont.)

Parameter	Format	DA	OL	Description		
mcastenhance g_ mcastenhance	iwpriv athN mcastenhance <i>mode</i>	Y	Y	Set multi-cast enhancement mode. #iwpriv ath0 mcastenhance 0 #iwpriv ath0 g_mcastenhance ath0 g_mcastenhance:0		
				AP software versions 9.2/9.3/9.4		
				0	Disable multi-cast enhancement	
				1	Enable multi-cast enhancement; use tunneling mode.	
				2	Enable multi-cast enhancement; use translating mode.	
				AP software versions 9.5/9.5.1/9.5.2/9.5.3		
				Value	Snooping	Multi-cast enhancement
				0	Enabled	True multi-cast packet is send if any interested member is present.
				1	Enabled	Tunneled unicast packet is send to interested members.
				2	Enabled	Translated unicast packet is send to interested members.
4	Enabled	Disabled (Set bit 2 = 1)				
5	Disabled	Enables Hy-Fi managed multi-cast functionality.				
me_adddeny	iwpriv athN me_ adddeny <i>groupaddresstbl</i>	Y	N	Adds the table of group addresses that are not to be learned. The <i>groupaddresstbl</i> value is to be entered as 4 integers (for example:- 239 255 255 1) Two addresses exist in the snoop deny table by default: 224.0.0.1, 239.255.255.1		
me_cleardeny	iwpriv athN me_cleardeny <i>value</i>	Y	N	Clears the snoop deny table entries. <i>value</i> can be any integer; however, the parameter clears the snoop deny table regardless of <i>value</i> .		
me_length get_me_length	iwpriv athN me_length <i>tablelength</i>	Y	N	Sets the snoop table length as number of entries. The default value is 32. The <i>param</i> range is 0 – 32. The get parameter returns the current value.		
me_showdeny	iwpriv athN me_showdeny <i>groupaddresstbl</i>	Y	N	Displays the table of group addresses that are not to be learned. Two addresses exist in the snoop deny table by default: 224.0.0.1, 239.255.255		
medebug get_medebug	iwpriv athN medebug <i>debuglevel</i>	Y	N	Sets the debug level for multicast enhancement. Param argument can accept any combination of the values below. The get parameter returns the current value.		
				0	IEEE80211_ME_DBG_NONE	
				1	IEEE80211_ME_DBG_INFO	
				2	IEEE80211_ME_DBG_DEBUG	
				4	IEEE80211_ME_DBG_DUMP	
				8	IEEE80211_ME_DBG_ALL	

Table 1-15 iQue parameters (cont.)

Parameter	Format	DA	OL	Description
medropmcast get_ medropmcast	iwpriv athN medropmcast {1 0}	Y	N	Enables/disables medropmcast feature, which drops multi-cast packets if the snoop table is empty. The default value is 1.
				0 Disables medropmcast
				1 Enables medropmcast
medump	iwpriv athN medump	Y	N	Dumps the snoop table for multi-cast enhancement. Note: For fulloffload implementations, due to the driver limitation, the snoop table can only be displayed on the Target console.
metimeout get_metimeout	iwpriv athN metimeout <i>timeoutper</i>	Y	N	Sets the timeout in ms for a STA to be removed from the snoop table if idle. The <i>param</i> value may be any unsigned integer value. The default is 120000 (2 minutes). The get parameter returns the current value.
metimer get_metimer	iwpriv athN metimer <i>timer</i>	Y	N	Sets the timer in ms to check the status of the snoop table. The <i>timer</i> value may be any unsigned integer. The default is 30000 (30 seconds). The get parameter returns the current value.
retrydur get_retrydur	iwpriv wifiN retrydur <i>threshold_period</i>	Y	N	Sets the retry threshold in μ s. Feature disabled if set at 0. #iwpriv wifi0 retrydur 0 #iwpriv wifi0 get_retrydur wifi0 get_retrydur: 0

1.3.12 Physical layer parameters

Table 1-16 Physical layer parameters

Parameter	Format	DA	OL	Description
noedgech get_noedgech	iwpriv athN noedgech			Forces the AP to avoid band edge channels when selecting a channel. #iwpriv ath0 noedgech #iwpriv ath0 get_noedgech ath0 get_noedgech:
LDPC getLDPC	iwpriv wifiN LDPC {1 0}	Y	N	Enables (1) or disables (0) the Low-density parity check feature, as described in 802.11n specification. The default value is 1. This option will have an effect only on chips supporting the LDPC feature. On other chips, this option will have no effect. Specific to 802.11n. # iwpriv wifi0 LDPC 1 # iwpriv wifi0 getLDPC wifi0 getLDPC:1
setCountryID getCountryID	iwpriv wifiN setCountryID countryidnum	Y	Y	Sets the AP to the regulatory requirements of the country. See Table A-1 on page 117 for a full list of country IDs and strings. Default values are taken from the EEPROM. Country ID must be defined during initialization, as required for final system configuration. The get parameters return the current values. #iwpriv wifi0 setCountryID 250 #iwpriv wifi0 setCountry FR #iwpriv wifi0 getCountryID wifi0 getCountryID:250 #iwpriv wifi0 getCountry wifi0 getCountry:FR
				SetCountryID Takes an integer value that represents the country, such as 250 for France
				setCountry Takes an argument including the 2-character country string plus I (indoor) or O (outdoor)

Table 1-16 Physical layer parameters (cont.)

Parameter	Format	DA	OL	Description	
txchainmask rxchainmask get_ txchainmask get_ rxchainmask	iwpriv wifiN txchainmask mask iwpriv wifiN rxchainmask mask	Y	Y	Sets the Tx and Rx chainmask values. For MIMO devices, indicates the number of Tx/Rx streams, and which chains are used. For some Qualcomm Atheros devices, up to 3 chains can be used, others are restricted to 2 or 1. NOTE: The maximum number of chains available for the device. For dual chain devices, chain 2 is not available. Single chain devices only support chain 0. The chains are represented in the bit mask as:	
				Chain 0	0x01
				Chain 1	0x02
				Chain 2	0x04
				Chainmask selection can affect several performance factors. For a 3-chain device, an Rx chainmask of 0x05 (or 0x03) is used for 2x2 stream reception. For near range operations, a Tx chainmask of 0x05 (or 0x03) minimizes near range effects. For far range, a mask of 0x07 is used for Tx. The default chainmask values are stored in EEPROM. This iwpriv command overrides the chainmask settings. The get parameters returns the current values. #iwpriv wifi0 txchainmask 0x05 #iwpriv wifiN rxchainmask 0x05 #iwpriv wifiN get_txchainmask wifi0 get_txchainmask:5 #iwpriv wifiN get_rxchainmask mask wifi0 get_rxchainmask:5	
TXPowLim2G TXPowLim5G getTxPowLim2G getTxPowLim5G	iwpriv wifiN TXPowLim2G limit iwpriv wifiN TXPowLim5G limit	Y	Y	Sets the maximum transmit power limit for the 2 GHz band or 5 GHz band. The maximum transmit power is also governed by country-specific regulatory requirements set by the iwpriv setCountry or setCountryID parameters. The iwconfig txpower command is similar but sets maximum transmit power for all frequencies. The TxPowLim2G/TxPowLim5G settings can be overridden by TxPwrOvr. The TxPowLim2G/TxPowLim5G values may be also updated by other portions of the code, so the effect of the value may be temporary. The limit is expressed as an integer that equals +0.5 dBm for each value of 1. For example, 0 = 0 dBm; 10 = 5 dBm; 100 = 50 dBm. The default is 100 for both parameters. The get parameters return the current values. #iwpriv wifi0 TXPowLim2G 100 #iwpriv wifi0 getTxPowLim2G wifi0 getTxPowLim2G:100	

Table 1-16 Physical layer parameters (cont.)

Parameter	Format	DA	OL	Description
txstbc rxstbc get_txstbc get_rxstbc	iwpriv wifiN rxstbc 1/0 iwpriv wifiN txstbc 1/0	Y	N	Enables (1) or disables (0) the Space Time Coding Block (STBC) feature, as described in 802.11n specification, in the transmit (txstbc) or receive (rxstbc) direction. The default value is 1. This option will have an effect only on chips supporting STBC. On other chips, this options will have no effect. Specific to 802.11n. # iwpriv wifi0 txstbc 1 # iwpriv wifi0 rxstbc 1 # iwpriv wifi0 get_txstbc 1 wifi0 get_txstbc:1 # iwpriv wifi0 get_rxstbc 1 wifi0 get_rxstbc:1
g_phyofdmerr	iwpriv wifi0 g_phyofdmerr	Y	Y	The number of packets that were received with a Physical Layer Convergence Protocol (PLCP) header error.
g_fcseerr	iwpriv wifi0 g_fcseerr	Y	Y	The number of packets that were received with a FCS error.

1.3.13 Protection mechanism parameters

Table 1-17 Protection mechanism parameters

Parameter	Format	DA	OL	Description
protmode get_protmode	iwpriv athN protmode {1 0}	Y	Y	Enables or disables 802.11g protection mode. Causes RTS/CTS sequence (or CTS to self) to be sent when 802.11b devices are detected on the 802.11g network. Used to protect against Tx by devices that do not recognize OFDM modulated frames. The default is 0. The get parameter returns the current value. #iwpriv ath0 protmode 0 #iwpriv ath0 get_protmode ath0 get_protmode:0
				0 No protection
				1 CTS to self
				2 RTS/CTS
extprotmode get_extprotmode	iwpriv athN extprotmode protectionmode	Y	Y	Sets the protection mode used on the extension (secondary) channel when using 40 MHz channels. The default is 0. The get parameter returns the current value. #iwpriv ath0 extprotmode 0 #iwpriv ath0 get_extprotmode ath0 get_extprotmode:0
				0 None, no protection
				1 CTS to self
				2 RTS/CTS

1.3.14 Radio-related parameters

Table 1-18 Radio-related parameters

Parameter	Format	Description
6MBAck Get6MBAck	<code>iwpriv wifiN 6MBAck 1 0</code>	This command enables (1) or disables (0) the use of the 6 Mbps (OFDM) data rate for ACK frames. If disabled, ACK frames will be sent at the CCK rate. The default value is 0. The get parameter returns the current value. #iwpriv wifi0 6MBAck 1 #iwpriv wifi0 Get6MBAck wifi0 Get6MBAck:1
AddSWBbo SWBcnRespT DMABcnRespT GetAddSWBbo GetSWBcnRespT GetDMABcnRespT	<code>iwpriv wifiN SWBcnRespT</code> <code>iwpriv wifiN DMABcnRespT</code> <code>iwpriv wifiN AddSWBbo</code>	Adjust the calculation of the ready time for the QoS queues to adjust the QoS queue performance for optimal timing. These parameters are used for experimental adjustment of queue performance. In the AP application they are not relevant, so they should not be modified. Their default value is 0. Each get parameter returns the current value for its parameter. #iwpriv wifi0 SWBcnRespT 1 #iwpriv wifi0 DMABcnRespT 2 #iwpriv wifi0 AddSWBbo 10 #iwpriv wifi0 GetSWBcnRespT wifi0 GetSWBcnRespT:1 #iwpriv wifi0 GetDMABcnRespT wifi0 GetDMABcnRespT:2 #iwpriv wifi0 GetAddSWBbo wifi0 GetAddSWBbo:10
		SWBcnRespT Software beacon response time represents the time, in ms, required to process beacons in software
		DMABcnRespT DMA beacon response time, the time required to transfer a beacon message from memory to the MAC queue
		AddSWBbo Additional software beacon back-off is an estimated variable for final adjustment of the ready time offset

Table 1-18 Radio-related parameters (cont.)

Parameter	Format	Description
AggrProt AggrProtDur AggrProtMax getAggrProt getAggrProtDur getAggrProtMax	<i>iwpriv wifiN AggrProt 1 0</i> <i>iwpriv wifiN AggrProtDur duration</i> <i>iwpriv wifiN AggrProtMax size</i>	Enable RTS/CTS protection on aggregate frames and control the size of the frames receiving RTS/CTS protection. Typically used as a test commands to set a specific condition in the driver. Each get parameter returns the current value for its parameter. <pre>#iwpriv wifi0 AggrProt 1 #iwpriv wifi0 AggrProtDuration 8192 #iwpriv wifi0 AggrProtMax 8192 #iwpriv wifi0 getAggrProt wifi0 getAggrProt:1 #iwpriv wifi0 getAggrProtDur wifi0 getAggrProtDur:8192 #iwpriv wifi0 getAggrProtMax wifi0 getAggrProtMax:8192</pre>
		AggrProt Enables (1) or disables (0 = Default) this function.
		AggrProtDur Indicates the amount of time to add to the duration of the CTS period to allow for additional packet bursts before a new RTS/CTS is required. Default is 8192 ms.
		AggrProtMax Indicates the largest aggregate size to receive RTS/CTS protection. Default is 8192 bytes.
ANIEna GetANIEna	<i>iwpriv wifiN ANIEna 0 1</i>	Enables the automatic noise immunity (ANI) processing in both the driver and the baseband unit. ANI mitigates unpredictable noise spurs in Rx channels that are due to the host system the device is installed in. This feature was added for CardBus and PCIE devices sold in the retail market are not pre-installed in host systems. Most AP implementations do not enable ANI, preferring to limit noise spurs by design. The get parameter returns the current value. <pre>#iwpriv wifi0 ANIEna 1 #iwpriv wifi0 GetANIEna wifi0 GetANIEna:1</pre>

Table 1-18 Radio-related parameters (cont.)

Parameter	Format	Description
AntSwap DivtyCtl GetAntSwap GetDivtyCtl	iwpriv wifiN AntSwap 1 0 iwpriv wifiN DivtyCtl AntSel/	Control antenna switching behavior. For 802.11n devices, these control which chains are used for Tx. For Legacy devices, used to determine if diversity switching is enabled or disabled. The get parameters return the current values. <pre>#iwpriv wifi0 AntSwap 1 #iwpriv wifi0 DivtyCtl 2 #iwpriv wifi0 GetAntSwap wifi0 GetAntSwap:0 #iwpriv wifi0 GetDivtyCtl wifi0 GetDivtyCtl:0</pre>
		AntSwap Indicates when antenna A and B are swapped from the usual configuration, causing antenna A to be used by chain 1 or 2, and antenna B by chain 0. Default is 0 (that is, antennas are not swapped; antenna A to chain 0 and antenna B to chain 1, 2).
		DivtyCtl Enables/disables antenna switching altogether. If set to antenna A (1) or antenna B (2), the Tx antenna will not change based on receive signal strength. If set to variable (0), the Tx antenna is selected based on received signal strength.
BcnNoReset getBcnNoReset	iwpriv wifiN BcnNoReset 1 0	Controls a debug flag that will either reset the chip or not when a stuck beacon is detected. If enabled (1), the system will NOT reset the chip upon detecting a stuck beacon, but will dump several registers to the console. Additional debug messages will be output if enabled, also. The default value is 0. The get parameter returns the current value. <pre>#iwpriv wifi0 BcnNoReset 1 #iwpriv wifi0 getBcnNoReset wifi0 getBcnNoReset:1</pre>
CABlevel getCABlevel	iwpriv wifiN CABlevel %Multicast	Sets the amount of space that can be used by Multi-cast traffic in the content after beacon (CAB) queue. CAB frames are also called beacon gated traffic frames and are sent attached to every beacon. In certain situations, so much multi-cast traffic may be transmitted that no time is left to send management or best effort (BE) traffic. TCP traffic gets starved out in these situations. This parameter controls how much of the CAB queue can be used by Multi-cast traffic, freeing the remainder for BE traffic. The default value of this parameter is 80 (80% Multi-cast). The get parameter returns the current value. <pre>#iwpriv wifi0 CABlevel 50 #iwpriv wifi0 getCABlevel wifi0 getCABlevel:50</pre>

Table 1-18 Radio-related parameters (cont.)

Parameter	Format	Description
CCKTrgLow CCKTrgHi GetCCKTrgLow GetCCKTrgHi	<i>iwpriv wifiN CCKTrgLow</i> <i>Low Threshold</i> <i>iwpriv wifiN CCKTrgHi</i> <i>High Threshold</i>	<p>Controls the CCK PHY errors/second threshold settings for the ANI immunity levels. A PHY error rate below the low trigger causes the ANI algorithm to lower immunity thresholds, and a PHY error rate exceeding the high threshold causes immunity thresholds to increase. When a limit is exceed, the ANI algorithm modifies one of several baseband settings to either increase or decrease sensitivity. Thresholds are increased/decreased in this order:</p> <p>Increase:</p> <ul style="list-style-type: none"> ■ Raise the noise immunity level to MAX from 0, if the spur immunity level is at MAX ■ Raise the noise immunity level to next level from a non-zero value ■ Raise spur immunity level ■ (If using CCK rates) raise the CCK weak signal threshold and raise the FIR step level ■ Disable the ANI PHY Err processing to reduce CPU load <p>Decrease:</p> <ul style="list-style-type: none"> ■ Lower the noise immunity level ■ Lower the FIR step level ■ Lower the CCK weak signal threshold ■ Lower the spur immunity level <p>The default values for these settings are 200 errors/second for the high threshold, and 100 errors/second for the low threshold.</p> <p>The get parameters return the current values.</p> <pre>#iwpriv wifi0 CCKTrgLow 80 #iwpriv wifi0 CCKTrgHi 220 #iwpriv wifi0 GetCCKTrgLow wifi0 GetCCKTrgLow:100 #iwpriv wifi0 GetCCKTrgHi wifi0 GetCCKTrgHi:200</pre>
CCKWeakThr GetCCKWeakThr	<i>iwpriv wifiN CCKWeakThr</i> <i>1 0</i>	<p>Selects either normal (0) or weak (1) CCK signal detection thresholds in the baseband; used to toggle between a more sensitive threshold and a less sensitive one, as part of the ANI algorithm. The actual settings are set at the factory and are stored in EEPROM. If ANI is enabled, this parameter may be changed independent of operator setting, so this command may be overridden during operation. The default value for this parameter is 0. The get parameter returns the current value.</p> <pre>#iwpriv wifi0 CCKWeakThr 1 #iwpriv wifi0 GetCCKWeakThr wifi0 GetCCKWeakThr:1</pre>

Table 1-18 Radio-related parameters (cont.)

Parameter	Format	Description								
chanbw get_chanbw	iwpriv athN chanbw <i>channel bandwidth</i>	Sets manual channel bandwidth. The values indicate which channel bandwidth to use. NOTE: This command only applies to legacy rates; HT rates are controlled with the corresponding 802.11n commands. The default value is 0. The get parameter returns the current value. <pre>#iwpriv ath0 chanbw 1 #iwpriv ath0 get_chanbw ath0 get_chanbw:1</pre> <table><tr><th>Value</th><th>Description</th></tr><tr><td>0</td><td>Full channel bandwidth</td></tr><tr><td>1</td><td>Half channel bandwidth</td></tr><tr><td>2</td><td>Quarter channel bandwidth</td></tr></table>	Value	Description	0	Full channel bandwidth	1	Half channel bandwidth	2	Quarter channel bandwidth
Value	Description									
0	Full channel bandwidth									
1	Half channel bandwidth									
2	Quarter channel bandwidth									
CWMIgnExCCA GetCWMIgnExCCA	iwpriv wifiN CWMIgnExCCA 1 0	Allows the system to ignore CCA on the extension channel for 802.11n devices operating in HT40 mode. Normally, to transmit, the device requires no energy detected on both the control and extension channels for a minimum of PIFS duration. This control allows for ignoring energy on the extension channel, is not in conformance with the latest draft of the 802.11n specifications, and should only be used in test mode. The default value is 0 (do not ignore extension channel CCA). The get parameter returns the current value. <pre>#iwpriv wifi0 CWMIgnExCCA 1 #iwpriv wifi0 GetCWMIgnExCCA wifi0 GetCWMIgnExCCA:0</pre>								
extbusythres g_extbusythres	iwpriv athN extbusythres <i>pctBusy</i>	Used as part of the channel width management state machine. This threshold is used to determine when to command the channel back down to HT20 mode when operating at HT40 mode. If the extension channel is busy more often then the specified threshold (in percent of total time), then CWM will shut down the extension channel and set the channel width to HT20. The default value is 30%. The get parameter returns the current value. <pre>#iwpriv ath0 extbusythres 50 #iwpriv ath0 g_extbusythres ath0 g_extbusythres:50</pre>								
fastcc get_fastcc	iwpriv athN fastcc 1 0	Enables fast channel change. A value of 1 indicates that channel changes within band will be done without resetting the chip. A value of 0 indicates that any channel change will require a chip reset. The default value is 0. The get parameter returns the current value. <pre>#iwpriv ath0 fastcc 1 #iwpriv ath0 get_fastcc ath0 get_fastcc:1</pre>								

Table 1-18 Radio-related parameters (cont.)

Parameter	Format	Description
FIRStepLvl GetFIRStepLvl	<code>iwpriv wifiN FIRStepLvl level</code>	Adjusts the FIR filter parameter that determines when a signal is in band for weak signal detection. Raising this level reduces the likelihood of adjacent channel interference causing a large number of (low RSSI) PHY errors; lowering the level allows easier weak signal detection for extended range. It is also modified by the ANI algorithm, so it may change during operation, usually in steps of single units. The default value for this parameter is 0. The get parameter returns the initialization (starting) value and not the value currently in the operating registers. #iwpriv wifi0 FIRStepLvl 1 #iwpriv wifi0 GetFIRStepLvl wifi0 GetFIRStepLvl:0
ForceBias ForBiasAuto GetForceBias GetForBiasAuto	<code>iwpriv wifiN ForBiasAuto 1/0</code> <code>iwpriv wifiN ForceBias Bias</code>	This command activates the force bias feature; used as a workaround to a directional sensitivity issue in the AR5133 PHY chip in 2.4 GHz bands. The get parameters return the current values. #iwpriv wifi0 ForBiasAuto 1 #iwpriv wifi0 ForceBias 2 #iwpriv wifi0 GetForBiasAuto wifi0 GetForBiasAuto:0 #iwpriv wifi0 GetForceBias wifi0 GetForceBias:1
		ForBiasAuto Automatically selects the bias level depending on the selected frequency.
		ForceBias Sets the bias to a value between 0 and 7. These commands are only available when the driver is compiled with the <code>#define ATH_FORCE_BIAS</code> parameter defined. Even when this switch is enabled, the default values for both parameters are 0 (disabled); they should only be enabled if the sensitivity issue is actually present.
getchaninfo	Used by external applications to get channel information from the driver. An example application is the wlanconfig tool that uses this interface to get the channel information. The wireless tools do not know how to parse the information provided, since it is returned in an Atheros driver specific data structure. This command has no command line equivalent interface. The data structures used are defined as: struct ieee80211req_chaninfo { u_int16_t nchans; struct ieee80211_channel ic_chans[IEEE80211_CHAN_MAX]; }; struct ieee80211_channel { u_int16_t ic_freq; /* setting in MHz */ u_int32_t ic_flags; /* see below */ u_int8_t ic_flagext; /* see below */ u_int8_t ic_ieee; /* IEEE channel number */ int8_t ic_maxregpower; /* max. regulatory Tx power in dBm */ int8_t ic_maxpower; /* max. Tx power in dBm */ int8_t ic_minpower; /* min. Tx power in dBm */ };	

Table 1-18 Radio-related parameters (cont.)

Parameter	Format	Description
HTEna GetHTEna	<code>iwpriv wifiN HTEna 1 0</code>	Enables (1) or disables (0) 802.11n (HT) data rates. Normally, only used as a test command. The parameter is set to 1 (enabled) by default. The get parameter returns the current value. #iwpriv wifi0 HTEna 1 #iwpriv wifi0 GetHTEna wifi0 GetHTEna:1
mcast_rate get_mcast_rate	<code>iwpriv athN mcast_rate rate</code>	Sets multi-cast to a fixed rate. The rate value is specified in units of kilobits per second (kbps). This allows the user to limit the impact of multi-cast on the overall performance of the system. Default is 11 Mbps in 2.4 GHz mode and 6 Mbps in 5 GHz mode. The get parameter returns the current value. #iwpriv ath0 mcast_rate 10000 #iwpriv ath0 get_mcast_rate ath0 get_mcast_rate: 10000
NoiseImmLvl GetNoiseImmLvl	<code>iwpriv wifiN NoiseImmLvl level</code>	Selects a specific noise immunity level parameter during initialization. This command only has effect prior to creating a specific HAL instance and should be used only during system initialization. Each noise immunity level corresponds to a set of baseband parameters that adjust baseband receiver sensitivity. Values are set at the factory and selected as a set by this parameter. The level is also controlled by the ANI algorithm, so initial immunity level is modified during operation to select the optimal level for current conditions. The default is 4 and should not be changed without a specific reason. The get parameter returns the current value. #iwpriv wifi0 NoiseImmLvl 3 #iwpriv wifi0 GetNoiseImmLvl wifi0 GetNoiseImmLvl:4

Table 1-18 Radio-related parameters (cont.)

Parameter	Format	Description
OFDMTrgLow OFDMTrgHi GetOFDMTrgLow GetOFDMTrgHi	<i>iwpriv wifiN OFDMTrgLow</i> <i>Low Threshold</i> <i>iwpriv wifiN OFDMTrgHi</i> <i>High Threshold</i>	<p>Controls the OFDM PHY errors/second threshold settings for the ANI immunity levels. A PHY error rate below the low trigger causes the ANI algorithm to lower immunity thresholds, and a PHY error rate exceeding the high threshold increases immunity thresholds. When a limit is exceed, the ANI algorithm modifies one of several baseband settings to either increase or decrease sensitivity in this order:</p> <p>Increase:</p> <ul style="list-style-type: none"> ■ Raise the noise immunity level to MAX from 0, if the spur immunity level is at MAX ■ Raise the noise immunity level to next level from a non-zero value ■ Raise spur immunity level ■ (If using CCK rates) raise the CCK weak signal threshold and raise the FIR step level ■ Disable the ANI PHY Err processing to reduce CPU load <p>Decrease:</p> <ul style="list-style-type: none"> ■ Lower the noise immunity level ■ Lower the FIR step level ■ Lower the CCK weak signal threshold ■ Lower the spur immunity level OFDM weak signal detection on, with the existing spur immunity level 0 <p>The default values for these settings are 500 errors/second for the high threshold, and 200 errors/second for the low threshold. The get parameters return the current values.</p> <pre>#iwpriv wifi0 OFDMTrgLow 100 #iwpriv wifi0 OFDMTrgHi 550 #iwpriv wifi0 GetOFDMTrgLow wifi0 GetOFDMTrgLow:200 #iwpriv wifi0 GetOFDMTrgHi wifi0 GetOFDMTrgHi:500</pre>
OFDMWeakDet GetOFDMWeakDet	<i>iwpriv wifiN OFDMWeakDet</i> <i>1 0</i>	<p>Selects normal (0) or weak (1) OFDM signal detection thresholds in the baseband register. The actual thresholds are factory set and are loaded in the EEPROM. This parameter corresponds to the initialization value for the ANI algorithm, and is only valid prior to system startup. The default value for this parameter is 1 (detect weak signals). The get parameter returns the initialization value only.</p> <pre>#iwpriv wifi0 OFDMWeakDet 0 #iwpriv wifi0 GetOFDMWeakDet wifi0 GetOFDMWeakDet:1</pre>

Table 1-18 Radio-related parameters (cont.)

Parameter	Format	Description
rate11a rate11b rate11g get_rate11a get_rate11b get_rate11g	<i>iwpriv athN rate11a roaming_rate</i> <i>iwpriv athN rate11b roaming_rate</i> <i>iwpriv athN rate11g roaming_rate</i>	<p>Sets the roaming rate for each band usage. These rates are used to determine if a new AP is required. If the data rate on the link drops below these values, the scan module will determine if a better AP on the same ESS can be used. Values are specified in 500 Kbps increments, so a value of 48 indicates a rate of 24 MBps. This command has a corresponding get parameter, and its default value is 48 for 802.11a and 18 for 802.11bg.</p> <pre>#iwpriv ath0 ratella 32 #iwpriv ath0 ratellb 2 #iwpriv ath0 ratellg 10 #iwpriv ath0 get_ratella ath0 get_ratella:32 #iwpriv ath0 get_ratellb ath0 get_ratellb:2 #iwpriv ath0 get_ratellg ath0 get_ratellg:10</pre>
rssi11a rssi11b rssi11g get_rssi11a get_rssi11b get_rssi11g	<i>iwpriv athN rssi11a roaming_threshold</i> <i>iwpriv athN rssi11b roaming_threshold</i> <i>iwpriv athN rssi11g roaming_threshold</i>	<p>Sets the RSSI threshold for roaming in 802.11a, 802.11b, and 802.11g modes. These thresholds are used to make roaming decisions based on signal strength from the current set of APs available. The values are provided in dB. Have corresponding get parameters. The default value for 802.11b and 802.11g is 24 dBm.</p> <pre>#iwpriv ath0 rssi11a 30 #iwpriv ath0 rssi11b 30 #iwpriv ath0 rssi11g 30 #iwpriv ath0 get_rssi11a ath0 get_rssi11a:30 #iwpriv ath0 get_rssi11b ath0 get_rssi11b:30 #iwpriv ath0 get_rssi11g ath0 get_rssi11g:30</pre>
RSSIThrLow RSSIThrHi GetRSSIThrLow GetRSSIThrHi	<i>iwpriv wifiN RSSIThrLow far threshold</i> <i>iwpriv wifiN RSSIThrHi near threshold</i>	<p>Determines the relative distance of the AP from the STA; used to determine how the ANI immunity levels are selected.</p> <ul style="list-style-type: none"> ■ If the average beacon RSSI of beacons from the AP > RSSIThrHi, the STA is determined to be at close-range ■ If < RSSIThrHi but >RSSIThrLow, the STA is mid-range ■ If <RSSIThrLow, the STA is long-range ■ Defaults are 40 for the high (near) threshold and 7 for low (far). <p>The get parameters return the current values.</p> <pre>#iwpriv wifi0 RSSIThrLow 6 #iwpriv wifi0 RSSIThrHi 45 #iwpriv wifi0 GetRSSIThrLow wifi0 GetRSSIThrLow:7 #iwpriv wifi0 GetRSSIThrHi wifi0 GetRSSIThrHi:40</pre>

Table 1-18 Radio-related parameters (cont.)

Parameter	Format	Description
rtparams	<code>iwpriv wifiN rtparams ratetable_indexPER value probe_interval</code>	Configures the rate table. No get parameter available. Rate Table Index: 0: BE/BK traffic 1: VI/VO traffic PER Value: If the PER value for a rate is above this threshold, then this rate will not be included in the rate series. Probe Interval: Determines probe frequency. <code>#iwpriv wifi0 rtparams</code>
scanvalid get_scanvalid	<code>iwpriv athN scanvalid period</code>	Sets the period that scan data is considered value for roaming purposes. If scan data is older than this period, a scan is forced to determine if roaming is required. The period is specified in seconds. This command has a corresponding get parameter, and its default is 60 seconds. <code>#iwpriv ath0 scanvalid 30</code> <code>#iwpriv ath0 get_scanvalid</code> <code>ath0 get_scanvalid:30</code>
set11NRates get11NRates	<code>iwpriv athN Set11NRates rate_series</code>	When performing tests at fixed data rates, specifies the data rate. rate_series is specified as a group of 4 bytes in a 32-bit word. Each byte represents the MCS rate to use for each of 4 rate fallbacks. If hardware does not receive an ACK when transmitting at the first rate, it falls back to the second rate and retry, etc. through the fourth rate. As a convention, the high bit in the rate byte is always set, so for a rate of MCS-15 the rate value would be 0x8F. This command has a corresponding get parameter. It has no default value <code>#iwpriv ath0 set11NRates 0x8F8F8C8C</code> <code>#iwpriv ath0 get11NRates</code> <code>ath0 get11NRates: 2408549516</code>
set11NRetries get11NRetries	<code>iwpriv athN set11NRetries RetryCountPerStep</code>	For each rate in the rate series, the hardware can retry the same rate step multiple times. This value sets the number of retries for each step in the rate series. This is expressed as a group of 4 bytes in a 32-bit word, with each byte indicating the number of times to retry the rate step. Has a corresponding get parameter, and no default value. <code>#iwpriv ath0 set11NRetries 0x01010404</code> <code>#iwpriv ath0 get11NRetries</code> <code>ath0 get11NRetries: 16843780</code>

Table 1-18 Radio-related parameters (cont.)

Parameter	Format	Description
setchanlist getchanlist		Used by an application to set the channel list manually. Channels that are not valid from a regulatory perspective will be ignored. This command is passed a byte array 255 bytes long that contains the list of channels required. A value of 0 indicates no channel, but all 255 bytes must be provided. getchanlist receives this array from the driver in a 255 byte array that contains the valid channel list. The response is a binary array that WLAN tools cannot parse; therefore this cannot be used on the command line.
SpurImmLvl GetSpurImmLvl	<code>iwpriv wifiN SpurImmLvl level</code>	Sets the spur immunity level corresponding to the baseband parameter (cyc_pwr_thr1) that determines the minimum cyclic RSSI causing OFDM weak signal detection. Raising this level reduces the number of OFDM PHY errors/second (caused due to board spurs, or interferences with OFDM symbol periodicity). Lowering it allows detection of weaker OFDM signals (extending range). Note this value is the initialization, not the operating value. Default is 2. The get parameter returns the current value. <pre>#iwpriv wifi0 SpurImmLvl 3 #iwpriv wifi0 GetSpurImmLvl wifi0 GetSpurImmLvl:2</pre>

1.3.15 Radio resource management (802.11k)

The Radio Resource Management (RRM) functionality constitutes a partial implementation of the 802.11k specification. In this implementation, the AP attempts to gain information of the surrounding environment from the connected client by sending various messages to it and then receiving responses.

NOTE The 802.11k functions requires **wifitool** for configuration, after 802.11k functionality has been enabled with the **iwpriv rrm** command.

Table 1-19 Radio resource management (802.11k) parameters

quiet get_quiet	<code>iwpriv athN rrm</code>	Enable (1) or disable (0) Radio Management Resource (RRM) and Quiet Period functions, which are part of the 802.11k specification. The default quiet period parameters are used when this feature is turned on. get_quiet returns the current status. <pre>#iwpriv ath0 quiet 1 #iwpriv ath0 get_quiet ath0 get_quiet:1</pre>
rrm get_rrm	<code>iwpriv athN rrm</code>	Enable (1) or disable (0) Radio Management Resource (RRM) functions, which are part of the 802.11k specification. get_rrm returns the current status. <pre>#iwpriv ath0 rrm 1 #iwpriv ath0 get_rrm ath0 get_rrm:1</pre>

Table 1-19 Radio resource management (802.11k) parameters (cont.)

sendtsmrpt	wifitool athN sendtsmrpt dstmac num_rpt rand_ivl meas_dur tid peeracaddr bin0-range trig_cond avg_err_thresh cons_err_thresh delay_thresh trig_timeout	Transmits a stream report	
		dstmac	Destination MAC address
		num_rpt	Number of repetition
		rand_ivl	Random interval
		meas_dur	Measurement duration
		tid	Traffic Identifier field contains the TID subfield.
		peeracaddr	Peer STA Address contains a MAC address indicating the RA in the MSDUs to be measured
		bin0-range	Bin 0 Range indicates the delay range of the first bin (Bin 0) of the Transmit Delay Histogram, expressed in units of TUs.
		trig_cond	Triggered Reporting. Refer to the IEEE 802.11k specification for details.
		avg_err_thresh	Average error threshold. Refer to the IEEE 802.11k specification for details.
		cons_err_thresh	Consecutive Error Threshold. Refer to the IEEE 802.11k specification for details.
		delay_thresh	Delay Threshold. Refer to the IEEE 802.11k specification for details.
		trig_timeout	Trigger Time-out. Refer to the IEEE 802.11k specification for details.
sendneigrpt	wifitool athN sendneigrpt mac_addr ssid	Transmits a neighbor report	
		mac_addr	Destination MAC address
		ssid	SSID for which report is required
sendlmreq	wifitool athN sendlmreq mac_addr	Transmits a link measurement report	
		mac_addr	Destination MAC address

Table 1-19 Radio resource management (802.11k) parameters (cont.)

sendbcnrpt	wifitool athN sendbcnrpt	dstmac	Destination MAC address.	
	dstmac	regclass	Regulatory class.	
	regclass	channum	Channel number set to zero if report required for all possible channel on that band.	
	channum	rand_ivl	Random interval, see 802.11k specification for details	
	rand_ivl	duration	Measurement duration, refer to 802.11k specification for definition.	
	duration	mode	Measurement mode.	
	mode	0	passive	
		1	active	
		2	beacon table	
	req_ssid	Sets SSID matching requirement. If enabled (1), only reports matching to QCA BSS will be generated by the station. Default value is disabled (0).		
	rep_cond	The beacon reporting Information sub-element indicates the condition for issuing a beacon report. Default value is zero. Refer to the 802.11k specification for details.		
	rpt_detail	The reporting detail contains a 1-octet reporting detail data field that defines the level of detail per AP to be reported to the requesting STA. Default value is zero. Refer to 802.11k specification for details.		
req_ie	For current implementation, this should be set to zero			
chanrpt_mode	Reporting condition for beacon report. See 802.11k specification for details.			

Table 1-19 Radio resource management (802.11k) parameters (cont.)

sendstastats	wifitool athN sendstastats <i>mac_addr</i> <i>duration</i> <i>gid</i>	mac_addr	Destination MAC address	
		duration	Measurement duration.	
		gid	Group Identity.	
			0	STA counters from dot11CountersTable
			1	STA counters from dot11CountersTable
			2	QoS STA counters for UP0 from dot11QosCountersTable
			3	QoS STA counters for UP1 from dot11QosCountersTable
			4	QoS STA counters for UP2 from dot11QosCountersTable
			5	QoS STA counters for UP3 from dot11QosCountersTable
			6	QoS STA counters for UP4 from dot11QosCountersTable
			7	QoS STA counters for UP5 from dot11QosCountersTable
			8	QoS STA counters for UP6 from dot11QosCountersTable
			9	QoS STA counters for UP7 from dot11QosCountersTable
			10	BSS Average Access
			11-25	Reserved.
sendchload	wifitool athN sendchload <i>dstmac</i> <i>n_rpts</i> <i>regclass</i> <i>chnum</i> <i>rand_ivl</i> <i>mandatory_duration</i> <i>optional_condtion</i> <i>condition_val</i>	Transmits a channel load report		
		mac_addr	Destination MAC address	
		n_rpts	Number of repetitions client should perform. Refer to 802.11k specification for details.	
		regclass	Regulatory class.	
		chnum	Channel number.	
		rand_ivl	Random interval. Refer to 802.11k specification for details.	
		mandatory_duration	Measurement duration. Refer to 802.11k specification for definition.	
		optional_condtion	Se optional condition to (1) if desired as part of request. Default is (0).	
		condition_val	Condition value if optional condition is true. Refer to 802.11k specification for details.	

Table 1-19 Radio resource management (802.11k) parameters (cont.)

sendnhist	wifitool athN sendnhist <i>dstmac</i> <i>n_rpts</i> <i>regclass</i> <i>chnum</i> <i>rand_ivl</i> <i>mandatory_duration</i> <i>optional_condtion</i> <i>condition_val</i>	Transmits a noise histogram report	
		mac_addr	Destination MAC address
		n_rpts	Number of repetitions client should perform. Refer to 802.11k specification for details.
		regclass	Regulatory class.
		chnum	Channel number.
		rand_ivl	Random interval. Refer to 802.11k specification for details.
		mandatory_duration	Measurement duration. Refer to 802.11k specification for definition.
		optional_condtion	Set optional condition to (1) if desired as part of request. Default is (0).
		condition_val	Condition value if optional condition is true. Refer to 802.11k specification for details.
sendlcireq	wifitool athN sendlcireq <i>dstmac</i> <i>location</i> <i>latitude_res</i> <i>longitude_res</i> <i>altitude_res</i> <i>azimuth_res</i> <i>optional_condtion</i> <i>condition_val</i>	Transmits a noise histogram report	
		dstmac	Destination MAC address
		location	Location of requesting/reporting station refer 802.11k specifications for details
		latitude_res	Number of most significant bits (max 34) for fixed-point value of latitude. Refer to 802.11k specifications for details.
		longitude_res	Number of most significant bits (max 34) for fixed-point value of longitude. Refer to 802.11k specification for details.
		altitude_res	Number of most significant bits (max 30) for fixed-point value of altitude. Refer to 802.11k specification for details.
		azimuth_res	Number of most significant bits (max 9) for fixed-point value of Azimuth. Refer to 802.11k specification for details.
		optional_condtion	Set optional condition to (1) if desired as part of request. Default is (0).
rrmstats	wifitool athN rrmstats (<i>mac_addr</i>)	Gets an RRM report in user space.	
		mac_addr	Optionally specifies MAC address of client. If not given, command will print all RRM statistics collected up to the command for all connected clients.
bcnrpt	wifitool athN bcnrpt	Gets a beacon report in user space. Will provide most information received in a beacon report.	

1.3.16 Regulatory parameters

These commands interface with the regulatory information in the driver, and are used to control the settings affecting local requirements.

Table 1-20 Regulatory parameters

doth_pwr tgt get_doth_pwr tgt	<code>iwpriv athN doth_pwr tgt <i>target</i></code>	<p>Sets the desired maximum power on the current channel, as reported in the beacon and probe response messages. Used by STAs to set required output values. The value is capped by the regulatory maximum power value. The power value target is expressed in 0.5 dBm steps. The parameter has no default value. The get parameter returns the current value.</p> <pre>#iwpriv ath0 doth_pwr tgt 25 #iwpriv ath0 get_doth_pwr tgt ath0 get_doth_pwr tgt:25</pre>
doth_reassoc	<code>iwpriv athN doth_reassoc <i>value</i></code>	<p>Instructs the driver to generate a re association request. The single value provided is not used; it is more of a single-shot action than a setting. This command has no default, and no corresponding get parameter.</p> <pre>#iwpriv ath0 doth_reassoc 1</pre>

1.3.17 Security parameters

The security-related parameters relate to the security subsystem, and are specific interfaces required by the hostapd and wpa_supplicant programs. Table 1-21 lists a subset of the configurable security parameters. Other parameters are passed to the driver by iwconfig (for WEP) and by hostapd/wpa_supplicant (for WPA).

Table 1-21 Security-related parameters

Parameter	Format	DA	OL	Description	
authmode get_authmode	iwpriv athN authmode <i>mode</i> {open shared auto}	Y	Y	Sets the authentication mode for WEP operation. Authentication mode can be set to open, shared or auto. In 'auto' mode, both shared and open mode clients are allowed to authenticate. Default mode is open. The get parameter returns the current <i>mode</i> value. The terms open, shared, and auto may be given as 1, 2, or 4 instead, respectively. Result is correct; ignore error message in console.	
authmode get_authmode	iwpriv athN authmode mode			Selects the authentication mode to configure the driver for. This command is also used by host_apd to configure the driver when host_apd is used as an authenticator. The user will normally not use these commands. The default value is 0. The get parameter returns the current value. <i>Note that the get parameter will be implemented in a future release.</i> #iwpriv ath0 authmode 2 #iwpriv ath0 get_authmode ath0 get_authmode:2 The mode values are:	
				Value	Mode
				0	None specified
				1	Open authentication
				2	Shared key (WEP) authentication
				3	802.1x authentication
				4	Auto select/accept authentication (used by host_apd)
				5	WPA PSK with 802.1x PSK
				countermeasures get_countermeasures	iwpriv athN countermeasures 1 0

Table 1-21 Security-related parameters (cont.)

Parameter	Format	DA	OL	Description
driver_caps get_driver_caps	iwpriv athN driver_caps caps			Manually sets the driver capabilities flags; normally used for testing, because the driver fills in the proper capability flags. has a corresponding get parameter. has no default value. #iwpriv ath0 driver_caps 0x034000003 #iwpriv ath0 get_driver_caps ath0 get_driver_caps:872415235 The flags are defined as:
				0x00000001 WEP 0x00004000 Short Slot Time
				0x00000002 TKIP 0x00008000 Short Preamble
				0x00000004 AES 0x00010000 Monitor Mode
				0x00000008 AES_CCM 0x00020000 TKIP MIC
				0x00000010 HT Rates 0x01000000 WPA 2
				0x00000020 CKIP 0x00800000 WPA 1
				0x00000040 Fast Frame 0x02000000 Burst
				0x00000080 Turbo 0x04000000 WME
				0x00000001 IBSS 0x08000000 WDS
				0x00000002 Power Management 0x10000000 WME TKIP MIC
				0x00000004 Host AP 0x20000000 Background Scan
				0x00000008 Ad Hoc Demo 0x40000000 UAPSD
				0x00000010 Software Retry 0x80000000 Fast Channel Change
				0x00000020 Tx Power Mgmt
dropunencrypted get_dropunencry	iwpriv athN dropunencrypted 0 1			Enables/disables dropping the unencrypted non-PAE frames received. Passing a value of 1 enables dropping of unencrypted non-PAE frames, a value of 0 disables. This command has a corresponding get parameter, and its default value is zero. #iwpriv ath0 dropunencrypted 1 #iwpriv ath0 get_dropunencry ath0 get_dropunencry:1

Table 1-21 Security-related parameters (cont.)

Parameter	Format	DA	OL	Description	
keymgtalgs get_keymgtalgs	iwpriv ath <i>N</i> keymgtalgs algs			Used by host_apd to manage WPA keys (essentially the same as the WPA command). Has a corresponding get parameter. #iwpriv ath0 keymgtalgs 3 #iwpriv ath0 get_keymgtalgs ath0 get_keymgtalgs:3 The algorithms supported are:	
				Value	Algorithm
				0	WPA_ASE_NONE
				1	WPA_ASE_8021X_UNSPEC
				2	WPA_ASE_8021X_PSK
				3	The command combines the supported algorithms, so a value of 3 indicates both unspecified and PSK support
mcastcipher get_mcastcipher	iwpriv ath <i>N</i> mcastcipher <i>cipher</i>			Used mainly by the hostapd daemon; sets the cipher used for multi-cast. The iwpriv command sets the VAP cipher type, as required to support operation of the host_apd authenticator. Has no default value; has a corresponding get parameter. #iwpriv ath0 mcastcipher 1 #iwpriv ath0 get_mcastcipher ath0 get_mcastcipher:1 The cipher values include:	
				Value	Cipher type
				0	IEEE80211_CIPHER_WEP
				1	IEEE80211_CIPHER_TKIP
				2	IEEE80211_CIPHER_AES_OCB
				3	IEEE80211_CIPHER_AES_CCM
				5	IEEE80211_CIPHER_CKIP
				6	IEEE80211_CIPHER_NONE
mcastkeylen get_mcastkeylen	iwpriv ath <i>N</i> mcastkeylen <i>length</i>	Y	Y	Only valid for WEP operations; sets the multi-cast/group key length of the WEP key. Key lengths of 5 (40 bits) or 13 (104 bits) are the only valid values, corresponding to 64 or 128 bit WEP encoding. Has no default value; has a corresponding get parameter. #iwpriv ath0 mcastkeylen 5 #iwpriv ath0 get_mcastkeylen ath0 get_mcastkeylen:5	

Table 1-21 Security-related parameters (cont.)

Parameter	Format	DA	OL	Description
privacy get_privacy	iwpriv athN privacy 1 0			Flag used to indicate WEP operations; not normally used by an application other than host_apd. WEP operations are normally configured through the appropriate iwconfig command. Has a corresponding get parameter, and its default value is 0. #iwpriv ath0 privacy 1 #iwpriv ath0 get_privacy ath0 get_privacy:1
rsncaps get_rsncaps	iwpriv athN rsncaps flags			Sets the RSN capabilities flags. The only valid capability flag is 0x01, RSN_CAP_PREAUTH, which configures the AP for pre-authorization functionality. Normally used only by host_apd when configuring the VAP. Has a corresponding get parameter. #iwpriv ath0 rsncaps 0x01 #iwpriv ath0 get_rsncaps ath0 get_rsncaps:1
setfilter	iwpriv athN setfilter filter			Allows applications to specify the management frames it wants to receive from the VAP, causing the VAP to forward indicated frames to the networking stack. Normally used by host_apd to configure the VAP; has no corresponding get parameter. #iwpriv ath0 setfilter 0x24
				Value Algorithm
				0x01 Beacon
				0x02 Probe request
				0x04 Probe response
				0x08 Association request
				0x10 Association response
				0x20 Authentication
				0x40 De-authentication
				0x80 Disassociation
				0xFF ALL
setiebuf getiebuf	Used by an application to set/get application information elements into/from various frame types. The structure ieee80211req_getset_appiebuf is passed as an argument to the IOCTL. These commands have no command line equivalent, but the command does show up as a valid iwpriv command. The definition of the required data structure is: struct ieee80211req_getset_appiebuf { u_int32_t app_frmtype; /*mgmt frame type for which buffer is added */ u_int32_t app_buflen; /*application supplied buffer length */ u_int8_t app_buf[]; };			

Table 1-21 Security-related parameters (cont.)

Parameter	Format	DA	OL	Description
setkey delkey	host_apd setkey			<p>The host_apd application must do periodic rekeying of the various connections. These commands allow for management of the key cache. The setkey command receives the argument ieee80211req_key structure. Neither command has any corresponding command line equivalents. This structure is:</p> <pre>struct ieee80211req_key { u_int8_t ik_type; /* key/cipher type */ u_int8_t ik_pad; u_int16_t ik_keyix; /* key index */ u_int8_t ik_keylen; /* key length in bytes */ u_int8_t ik_flags; u_int8_t ik_macaddr[IEEE80211_ADDR_LEN]; u_int64_t ik_keyrsc; /* key Rx sequence counter */ u_int64_t ik_keytsc; /* key Tx sequence counter */ u_int8_t ik_keydata[IEEE80211_KEYBUF_SIZE+IEEE80211_MICBUF_SIZE]; };</pre>
	delkey			<p>Passes the structure ieee80211req_del_key:</p> <pre>struct ieee80211req_del_key { u_int8_t idk_keyix; /* key index */ u_int8_t idk_macaddr[IEEE80211_ADDR_LEN]; };</pre>
setmlme	<p>Another of the host_apd support commands, this command performs direct access to the MLME layer in the driver, thus allowing an application to start or terminate a specific association. Note that the MLME_ASSOC sub command only makes sense for a STA (the AP will not start an association).</p> <p>This command has no command line equivalent. It passes the ieee80211req_mlme structure:</p> <pre>struct ieee80211req_mlme { u_int8_t tim_op; /* operation to perform */ defineIEEE80211_MLME_ASSOC1/* associate STA */ defineIEEE80211_MLME_DISASSOC2/* disassociate STA */ defineIEEE80211_MLME_DEAUTH3/* deauthenticate STA */ defineIEEE80211_MLME_AUTHORIZE4/* authorize STA */ defineIEEE80211_MLME_UNAUTHORIZE5/* unauthorize STA */ u_int16_t tim_reason; /* 802.11 reason code */ u_int8_t tim_macaddr[IEEE80211_ADDR_LEN]; };</pre>			
ucastcipher get_uciphers	iwpriv athN ucastcipher			<p>Used mainly by the host_apd authenticator, and sets the unicast cipher type to the indicated value. See the mcastcipher command for the definition of the values. There is no default value. The get parameter returns the current value.</p> <pre>#iwpriv ath0 ucastcipher 2 #iwpriv ath0 get_uciphers ath0 get_uciphers:2</pre>
ucastciphers get_ucastciphers	iwpriv athN ucastciphers cipher_types			<p>Set support for cipher types. The values are preserved here to maintain binary compatibility with applications such as wpa_supplicant and hostapd. The default value is 7.</p>

Table 1-21 Security-related parameters (cont.)

Parameter	Format	DA	OL	Description
ucastkeylen get_ucastkeylen	iwpriv athN ucastkeylen length			Only valid for WEP operations. This command is used to set the key length of the WEP key for unicast frames. Key lengths of 5 (40 bits) or 13 (104 bits) are the only valid values, corresponding to 64 or 128 bit WEP encoding, respectively. Has no default value. The get parameter returns the current value. #iwpriv ath0 ucastkeylen 5 #iwpriv ath0 get_ucastkeylen ath0 get_ucastkeylen:5
wpa get_wpa	iwpriv athN wpa WPA Mode			Sets the desired WPA modes. Typically overridden by the setting in the hostapd configuration file, which uses the same interface to set the WPA mode. Thus, this command is not normally used during configuration. The default value is 0. The get parameter returns the current value. #iwpriv ath0 wpa 3 #iwpriv ath0 get_wpa ath0 get_wpa:0 The value of WPA Mode indicates the level of support:
				0 No WPA support
				1 WPA support
				2 WPA2 support
				3 Both WPA and WPA2 support
wps get_wps	iwpriv athN wps WPS Mode			Sets the desired WPS mode. The default is 0. The get parameter returns the current value. #iwpriv ath0 wps 0 #iwpriv ath0 get_wps ath0 get_wps:0
				0 Disable WPS mode.
				1 Enable WPS mode.

1.3.18 STA parameters

Table 1-22 STA parameters

Parameter	Format	Description
autoassoc get_autoassoc	iwpriv athN autoassoc 1 0	Sets the auto-association mode. Default is 0.
bgscan get_bgscan	iwpriv athN bgscan 1 0	Enables or disables background scanning. Background scanning occurs on a specified interval to update the list of known APs. This command is only valid when a VAP is operating in STA mode. The default value is 1. The get parameter returns the current value. #iwpriv ath0 bgscan 1 #iwpriv ath0 get_bgscan ath0 get_bgscan:1

Table 1-22 STA parameters (cont.)

Parameter	Format	Description
bgscanidle get_bgscanidle	<code>iwpriv athN bgscanidle</code> <i>idlePeriod</i>	Sets the amount of time the background scan must be idle before it is restarted; it is different from the background scan interval, in that if the background scan is delayed for a long period, when it is complete it will be idle for this period even if the scan interval times out. This time is indicated in seconds. The default value is 250 seconds. The get parameter returns the current value. #iwpriv ath0 bgscanidle 200 #iwpriv ath0 get_bgscanidle ath0 get_bgscanidle:200
bgscanintvl get_bgscanintvl	<code>iwpriv athN bgscanintvl</code> <i>interval</i>	Sets the interval to perform background scans. A scan is started each time the interval times out, or if the idle interval is not timed out when the idle interval is complete. The interval timer is started when the scan is started, so a idle period timeout shifts all subsequent scan intervals. The interval value is specified in seconds. The default value is 300. The get parameter returns the current value. #iwpriv ath0 bgscanintvl 250 #iwpriv ath0 get_bgscanintvl ath0 get_bgscanintvl:250
eospdrop get_eospdrop	<code>iwpriv athN eospdrop 1 0</code>	Sets support for forcing uapsd EOSP drop (AP only). The get parameter returns the current value. #iwpriv ath0 eospdrop 0 #iwpriv ath0 get_eospdrop ath0 get_eospdrop:0
		0 Disable forcing uapsd EOSP drop
		1 Enable forcing uapsd EOSP drop
periodicScan g_periodicScan	<code>iwpriv athN periodicScan</code> <i>enable and set</i>	Sets STA periodic scan support. 0 is disable and other values are enable. If the value is less than 30000, it will be set to 30000. The get parameter returns the current value. #iwpriv ath0 periodicScan 0 #iwpriv ath0 g_periodicScan ath0 g_periodicScan:0
		0 Disable periodic scan
		>0 Enable periodic scan and set periodic scan period
powersave get_powersave	<code>iwpriv athN powersave</code> <i>powersave mode</i>	Sets support for the STA power save mode. The default is 0. The get parameter returns the current value.
		0 STA power save none
		1 STA power save low
		2 STA power save normal
		3 STA power save maximum

1.3.19 TDLS Parameters

Table 1-23 TDLS Parameters

Parameter	Format	Description
clr_ttls_rmac set_ttls_rmac	iwpriv athN clr_ttls_rmac	
tdls get_ttls	iwpriv athN tdls	
tdlsaction gettdlsaction	iwpriv athN tdlsaction	
tdlsmacaddr1 gettdlsmacaddr1	iwpriv athN tdlsmacaddr1	
tdlsmacaddr2 gettdlsmacaddr2	iwpriv athN tdlsmacaddr2	

1.3.20 Turbo parameters

Table 1-24 Turbo parameters

Parameter	Format	Description
burst get_burst	iwpriv athN burst 1 0	Enables (1) or disables (0) Qualcomm Atheros super AG bursting support in the driver. Passing a value of 1 to the driver enables Super G bursting. Passing a value of 0 to the driver disables Super A/G bursting; not normally used when using 802.11n devices. The default value is 0. The get parameter returns the current value. #iwpriv ath0 burst 0 #iwpriv ath0 get_burst ath0 get_burst:0
compression get_compression	iwpriv athN compression 1 0	Enables/disables Data compression support Qualcomm Atheros supper G The get parameter returns the current value. #iwpriv ath0 compression 0 #iwpriv ath0 get_compression ath0 get_compression:0
	0	Disable
	1	Enable
ff get_ff	iwpriv athN ff 1 0	Enables/disables fast frames support of Qualcomm Atheros supper G. The get parameter returns the current value. #iwpriv ath0 ff 0 #iwpriv ath0 get_ff ath0 get_ff:0
	0	Disable
	1	Enable

Table 1-24 Turbo parameters (cont.)

Parameter	Format	Description
periodicScan get_periodicScan	iwpriv athN periodicScan enable_and_set	Sets STA periodic scan support. 0 is disable and other values are enable. If the value is less than 30000, it will be set to 30000. The get parameter returns the current value. #iwpriv ath0 periodicScan 0 #iwpriv ath0 get_periodicScan ath0 get_periodicScan:0
		0 Disable periodic scan
		>0 Enable periodic scan and set periodic scan period
turbo get_turbo	iwpriv athN turbo 1 0	Enables/disables turbo prime support, which is related to Qualcomm Atheros super G dynamic turbo.
		0 Disable
		1 Enable

1.3.21 Tx beamforming parameters

Table 1-25 Tx beamforming parameters

Parameter	Format	Description
set_cvtimeout get_cvtimeout	iwpriv wifiN set_cvtimeout	Set CV update period in 1 ms resolution. The get parameter returns the current value. The macro "ATH_SUPPORT_TxBF" controls whether the commands are supported.
TxBFCTL GetTxBFCTL	iwpriv wifiN TxBFCTL	Set TxBF control. The get parameter returns the current value. The macro "ATH_SUPPORT_TxBF" controls whether the commands are supported.
		bit0 Reserved
		bit2 Enable Explicit Beamforming with no compressed report request (Bfer side)
		bit3 Enable Explicit Beamforming with compressed report request (Bfer side)
		bit4 Reserved
		bit5 Enable Explicit Beamforming with no compressed immediate report (Bfee side)
		bit6 Enable Explicit Beamforming with compressed immediate report (Bfee side)
		bit7 Enable Explicit Beamforming with no compressed delay report (Bfee side)
		bit8 Enable Explicit Beamforming with compressed delay report (Bfee side)
		bit9 Disable applying steering CV matrix

1.3.22 Unassociated power consumption improvement parameters

Table 1-26 Unassociated power consumption improvement parameters

Parameter	Format	Description
ignore11d get_ignore11d	iwpriv athN ignore11d 1 0	Processes or ignores 11d beacon #iwpriv ath0 ignore11d 0 #iwpriv ath0 get_ignore11d ath0 get_ignore11d:0
		0 Process 11d beacon
		1 Ignore 11d beacon
scanprsleep get_scanprsleep	iwpriv athN scanprsleep	Sets the value of scan pre-sleep. The get parameter returns the current value.
sleepprscan get_sleepprscan	iwpriv athN sleepprscan	Sets the value of sleep pre-scan. The get parameter returns the current value.

1.3.23 Smart antenna

To change default settings for smart antenna and to read Smart Antenna settings, iwprivs are implemented. These iwprivs are tied with wifiN interface instead of athN because Smart Antenna treats all the VAPs created over a physical (wifiN) device in same manner.

Table 1-27 Smart antenna parameters

Parameter	Format	DA	OL	Description								
set_sa_param get_sa_param	iwpriv wifidev [wifi0 wifi1] set_sa_param dword1 dword2 dword3 dword4 iwpriv wifidev [wifi0 wifi1] get_sa_param dword1 dword2 dword3	Y	Y	Sets and gets Smart Antenna parameters. Each dword attribute is defined as given in this table. At any time, iwpriv wifi0 set_sa_param 0 0 0 0 can be used to list all the paramID that are used as a third argument in set_sa_param. NOTE dword4 is not required on the get command.								
				dword1: 0xAABBCCDD <table><tr><td>0xAA</td><td>param type: 0 = radio param, 1 = node param For radio param, MAC is 00:00:00:00:00:00. For node param, proper MAC address must be specified.</td></tr><tr><td>0xBB</td><td>Reserved (should be 00)</td></tr><tr><td>0xCCDD</td><td>bytes 5 and 6 of MAC</td></tr></table> dword2: 0xEEFFGGHH <table><tr><td>0xEEFFGGHH</td><td>bytes 4, 3, 2, 1 of MAC. For example, if the MAC address is 00:03:7f:48:d8:73 then: CC = 00, DD = 03, EE = 7f, FF = 48, GG = d8, HH = 73.</td></tr></table> dword3: paramID. See definitions and descriptions in Table 1-28 . dword4: paramValue (required only for set_sa_param)	0xAA	param type: 0 = radio param, 1 = node param For radio param, MAC is 00:00:00:00:00:00. For node param, proper MAC address must be specified.	0xBB	Reserved (should be 00)	0xCCDD	bytes 5 and 6 of MAC	0xEEFFGGHH	bytes 4, 3, 2, 1 of MAC. For example, if the MAC address is 00:03:7f:48:d8:73 then: CC = 00, DD = 03, EE = 7f, FF = 48, GG = d8, HH = 73.
0xAA	param type: 0 = radio param, 1 = node param For radio param, MAC is 00:00:00:00:00:00. For node param, proper MAC address must be specified.											
0xBB	Reserved (should be 00)											
0xCCDD	bytes 5 and 6 of MAC											
0xEEFFGGHH	bytes 4, 3, 2, 1 of MAC. For example, if the MAC address is 00:03:7f:48:d8:73 then: CC = 00, DD = 03, EE = 7f, FF = 48, GG = d8, HH = 73.											

Table 1-28 dword3 parameters

ParamName	Param ID	Node or Radio param	Description
smart_ant_param_help	0	Radio	Displays current available commands list
smart_ant_param_train_mode	1	Radio	Self-packet generation or existing traffic mode. Currently only existing traffic mode is supported. 0 = existing; 1 = mixed.

Table 1-28 dword3 parameters (cont.)

ParamName	Param ID	Node or Radio param	Description
smart_ant_param_train_per_threshold	2	Radio	Smart antenna lower, upper and per diff thresholds. Here byte 0 is lower_bound, byte 1 is upper_bound, byte 3 is per_diff_threshold and byte 4 is config. By default lower bound is 20, upper bound is 80, per_diff_threshold is 3 and config is 1. Config is a bit map of 4 possible values: #define SA_CONFIG_INTENSETRAIN 0x1 /* setting this bit in config indicates training with double number of packets */ #define SA_CONFIG_EXTRATRAIN 0x2 /* setting this bit in config indicates to do extra training in case of conflicts in first metric */ #define SA_CONFIG_SELECTSPROTEXTRA 0x4 /* setting this bit in config indicates to protect extra training frames with self CTS */ #define SA_CONFIG_SELECTSPROTALL 0x8 /* setting this bit in config indicates to protect all training frames with self CTS */
smart_ant_param_pkt_len	3	Radio	Packet length of proprietary generated training packet. By default is 1536.
smart_ant_param_num_pkts	4	Radio	Number of packets used for training. If not set, default value of 640 will be used.
smart_ant_param_train_start	5	Node	Start smart antenna training.
smart_ant_param_train_enable	7	Radio + Node	Bitmap for init, periodic & performance triggers. #define SA_INIT_TRAIN_EN 0x1 #define SA_PERIOD_TRAIN_EN 0x2 #define SA_PERF_TRAIN_EN 0x4 #define SA_RX_TRAIN_EN 0x10
smart_ant_param_retrain_interval	9	Radio	Periodic retrain interval in milliseconds. By default it is 2 minutes.
smart_ant_param_goodput_avg_interval	12	Radio	Goodput averaging interval. By default it is 2 seconds.
smart_ant_param_default_antenna	13	Radio	Default antenna for Rx, Tx multi-cast and Tx broadcast. By default it is antenna 0.
smart_ant_param_default_tx_antenna	14	Radio	Default Tx antenna for Tx. By default it is antenna 0. Once a new node connects, by default this antenna is used as unicast Tx antenna.
smart_ant_param_tx_antenna	15	Node	Once this command is set, no training will be done for this node and this antenna will be used for all unicast Tx.

Table 1-28 dword3 parameters (cont.)

ParamName	Param ID	Node or Radio param	Description
smart_ant_param_dbg_level	16	Radio	It is a 4 bit value used for controlling the prints. By default it is log level 1. Bit 1 controls log level 1, bit 2 controls log level 2, bit 3 controls log level 3 and bit 4 controls log level 4.
smart_ant_param_pretrain_pkts	17	Radio	Number of pre-train packets. Once a node is connected these many packets are sent before starting the training. By default it is 600.
smart_ant_param_other_bw_pkts_th	18	Radio	Threshold for other bw packets to detect bandwidth change. By default it is 5.
smart_ant_param_goodput_ignore_interval	19	Radio	By default goodput ignoring interval is 1 second.
smart_ant_param_min_pkt_th_bw20	20	Radio	Minimum number of packets in 20 MHz BW to indicate active BW. By default it is 20.
smart_ant_param_min_pkt_th_bw40	21	Radio	Minimum number of packets in 40 MHz BW to indicate active BW. By default it is 10.
smart_ant_param_min_pkt_th_bw80	22	Radio	Minimum number of packets in 80 MHz BW to indicate active BW. By default it is 5.
smart_ant_param_debug_info	23	Node	Displays Last training time, Periodic triggers and performance triggers for specific node.

1.3.24 WDS parameters

Table 1-29 WDS parameters

Parameter	Format	DA	OL	Description
nobeacon get_nobeacon	<code>iwpriv athN nobeacon</code>			Enables/disables VAP to transmit beacon and probe response. The get parameter returns the current value. The macro "ATH_SUPPORT_AP_WDS_COMBO" controls whether the commands are supported.
				0 Disable
				1 Enable
extap get_extap	<code>iwpriv athN extap {0-3}</code>	Y	Y	Sets Extender AP support. The get parameter returns the current value. <code>#iwpriv ath0 extap 0</code> <code>#iwpriv ath0 get_extap</code> <code>ath0 get_extap:0</code>
				0 Disable Extender AP support
				1 Enable Extender AP support
				2 Enable Extender AP support with DEBUG. Result is correct; ignore error message in console.
				3 Enable Extender AP support with DEBUG
vap-ind	<code>iwpriv athN vap-ind {1 0}</code>	N	N	Enables (1) or disables (0) repeater independent mode. If this option is disabled, the AP VAP will wait for the STA VAP to connect before starting to transmit the beacons. If this option is enabled, the AP VAP will start transmitting beacons independently of the STA VAP status.
athnewind get_athnewind	<code>iwpriv athN athnewind {1 0}</code>	Y	N	Enables (1) or disables (0) enhanced independent repeater mode. If this option is enabled, the STA VAP will scan for the Root AP in all the available channels and connect to it. The AP VAP will start and continue to transmit beacons independently of the STA VAP connection status. The default value is 0. The get parameter returns the current value. <code>#iwpriv ath0 athnewind 1</code> <code>#iwpriv ath0 get_athnewind</code> <code>ath0 get_athnewind:1</code>
wds get_wds	<code>iwpriv athN wds {1 0}</code>	Y	Y	Enables (1) or disables (0) 4-address frame format for this VAP. Used for WDS configurations (see "WiFi Distribution System (WDS)" in the <i>AP Driver User's Guide</i> for details). The default value is 0. The get parameter returns the current value. <code>#iwpriv ath0 wds 1</code> <code>#iwpriv ath0 get_wds</code> <code>ath0 get_wds:1</code>

1.3.25 WMM parameters

WMM parameters manage the WMM link settings. To set parameters, each command must specify the access category (AC) and mode (STA or AP).

Table 1-30 Access categories and modes

Value	Symbol	Description
Access Categories		
0	AC_BE	Best effort
1	AC_BK	Background
2	AC_VI	Video
3	AC_VO	Voice
Mode Parameter		
0	AP	AP mode: Update the AP WMM table
1	STA	STA mode: Update the STA WMM tables

The parameters accessible for WMM operations are specified in the WMM (including WMM Power Save) Specifications. These parameters control the way in which the time slots or TXOPs are metered out for each traffic stream. [Table 1-31](#) lists the parameters accessible in the Qualcomm Atheros driver.

Table 1-31 WMM parameters

Parameter	Format	DA	OL	Description
acparams	<code>iwpriv athN acparams ac {0-3} rts {1 0} aggrscaling {0-3} min_rate[Mbps]</code>	Y	Y	Configures the access category. See table Table 1-30 . <i>Access category:</i> 0: BE 1: BK 2: VI 3: VO <i>Enable RTS/CTS:</i> Applies to all rate series. <i>Aggregate scaling:</i> Controls the maximum air time that the aggregates can use. 0: Disable, ≥ 4 ms 1: ≥ 2 ms 2: ≥ 1 ms 3: ≥ 0.5 ms <i>Minimum Rate:</i> Sets the per-access category lower threshold rate, which used by the voice (VO) and video (VI) rate algorithm. If the operating rate drops below this threshold, then HBR applies.
qosnull	<code>iwpriv athN qosnull 0/1</code>			Force sends QoS null data and sets power management bit on (1) or off (0). This is an action command, thus does not have any get parameter or default value. <code>#iwpriv ath0 qosnull 0</code>

Table 1-31 WMM parameters (cont.)

Parameter	Format	DA	OL	Description	
setwmmparams getwmmparams	iwpriv athN setwmmparam wmeparam {1-6} ac {0-3} bss {1 0} wmevalue	Y	Y	Sets WMM sub-parameters. The range and units of measure for <i>wmevalue</i> are listed with the WME parameter below. The get parameter returns the current settings. #iwpriv ath0 setwmmparams 1 0 0 4 #iwpriv ath0 getwmmparams 1 0 0 ath0 getwmmparams:4 Each WME parameter can be executed independently, without using “setwmmparams” or “getwmmparams”, as shown in the following examples. The access category, BSS/local, and value arguments remain the same. Each set parameter has a corresponding get parameter that returns the current value. For example, the <i>cwmin</i> parameter may be given as follows: #iwpriv ath0 cwmin 3 1 2 #iwpriv ath0 get_cwmin 3 1 ath0 get_cwmin: 2 The WME parameters may thus be given as follows: #iwpriv athN acm #iwpriv athN aifs #iwpriv athN cwmax h#iwpriv athN cwmin #iwpriv athN noackpolicy #iwpriv athN txoplimit	
				WME Parameters (<i>wmeparam</i> , <i>wmevalue</i>)	
				1	CWMIN (<i>wmevalue</i> = 0-15, in units of slot time)
				2	CWMAX (<i>wmevalue</i> = 0-15, in units of slot time)
				3	AIFS (<i>wmevalue</i> = 0-15, in units of slot time)
				4	TXOPLIMIT (<i>wmevalue</i> = 0-8192, in units of 32 μ s)
				5	ACM (<i>wmevalue</i> = 0 for disable, 1 for enable)
				6	NOACKPOLICY (<i>wmevalue</i> = 0 for disable, 1 for enable)
				Access Category Parameters (<i>ac</i>)	
				0	Best effort (BE)
1	Background (BK)				
2	Video (VI)				
3	Voice (VO)				
BSS/Local Parameters (<i>bss</i>)					
1	BSS (channel parameters broadcast to STAs)				
0	Local (channel parameters applied to self)				

Table 1-31 WMM parameters (cont.)

Parameter	Format	DA	OL	Description
uapsd get_uapsd	iwpriv athN uapsd {1 0}	Y	Y	Enables (1) or disables (0) the corresponding bit in the capabilities field of the beacon and probe response messages; has no other effect. The default value is 0. This get parameter returns the current value. #iwpriv ath0 uapsd 1 #iwpriv ath0 get_uapsd ath0 get_uapsd:1
wmm get_wmm	iwpriv athN wmm {1 0}	Y	Y	Enables (1) or disables (0) WMM capabilities in the driver. The WMM capabilities perform special processing for multimedia stream data including voice and video data. This command has a corresponding get parameter, and its default is 1 (WMM enabled). #iwpriv ath0 wmm 1 #iwpriv ath0 get_wmm ath0 get_wmm:1

1.3.26 256QAM rate support parameters

Table 1-32 256QAM parameters

Parameter	Format	DA	OL	Description
vht_11ng get_vht_11ng	iwpriv athN vht_11ng {1 0}	N	Y	Enables (1) or disables (0) 256QAM rate support. The default value is 0. This command enables 256QAM rate support in 2.4GHz band HT modes only (such as 11NGHT20, 11NGHT40PLUS, 11NGHT40MINUS). The get parameter returns the current value. #iwpriv ath0 vht_11ng 1 #iwpriv ath0 get_vht_11ng ath0 get_vht_11ng:1

1.3.27 Hy-Fi options – WMM DSCP prioritization

Table 1-33 Hy-Fi parameters

Parameter	Format	DA	OL	Description
aldstats	iwpriv wifx aldstats {1 0}	Y	N	To enable/disable few Hy-Fi link metrics stats. This option should be enabled to collect packet drops to no buffs, excessive retries and transmitted packet count stats per access category per destination node. This command is applicable only for direct attach VAPs #iwpriv wifi0 aldstats 1
s_dscp_override g_dscp_override	iwpriv wifx s_dscp_override {1 0}	Y	Y	To enable/disable DSCP override feature. Packets with specific DSCP value set can be mapped to a specific TID through this feature. #iwpriv wifi0 s_dscpo_override 1 #iwpriv wifi0 g_dscpo_override g_dscpo_override:1

Table 1-33 Hy-Fi parameters

Parameter	Format	DA	OL	Description
reset_dscp_map	iwpriv wifx reset_dscp_map <tid>	Y	N	To reinitialize all the DSCPs with a default TID value. This command is not available for offload vap. #iwpriv wifx0 reset_dscp_map 1
set_dscp_tidmap get_dscp_tidmap	iwpriv athX set_dscp_tidmap <tid><map> iwpriv athX get_dscp_tidmap <tid>	Y	Y	To configure a specific TID for specific map value. Iwpriv option set_dscp_tidmap should be set to <tid> <map> value #iwpriv ath0 set_dscp_tidmap 1 2 #iwpriv ath0 get_dscp_tidmap 1
slgmpDscpOvrid glgmpDscpOvrid	iwpriv wifx slgmpDscpOvrid 1	Y	Y	To enable IGMP TID override. #iwpriv wifx sIgmpDscpOvrid 1 #iwpriv wifx gIgmpDscpOvrid gIgmpDscpOvrid:1
slgmpDscpTidMap glgmpDscpTidMap	iwpriv wifx slgmpDscpTidMap <tid>	Y	Y	To configure a specific TID for IGMP packets. All IGMP transmitted will go through the TID configured. iwpriv option slgmpDscpOvrid should be set to 1 for this command to work. #iwpriv wifx sIgmpDscpTidMap <tid> #iwpriv wifx gIgmpDscpTidMap sIgmpDscpTidMap: <tid>
sHmmcDscpOvrid gHmmcDscpOvrid	iwpriv wifx sHmmcDscpOvrid {1/0}	Y	Y	To enable/disable HMMC DSCP override. To push all multi-cast to unicast converted packets through a specific TID #iwpriv wifx sHmmcDscpOvrid #iwpriv wifx gHmmcDscpOvrid gHmmcDscpOvrid
sHmmcDscpTidMap gHmmcDscpTidMap	iwpriv wifx sHmmcDscpTidMap <tid>	Y	Y	To configure a specific TID for unicast packets derived from multi-cast packets. iwpriv option sHmmcDscpOvrid should be set to 1 for this command to work #iwpriv wifx sHmmcDscpTidMap <tid> #iwpriv wifx gHmmcDscpTidMap gHmmcDscpTidMap:<tid>
setBlkReportFld getBlkReportFld	iwpriv wifx setBlkReportFld {1/0}	Y	Y	To enable/disable report flooding. Enabling this feature would block flooding reports to other STAs associated with the AP. #iwpriv wifx setBlkReportFld 1 #iwpriv wifx getBlkReportFld getBlkReportFld: 1
setDropSTAQuery getDropSTAQuery	iwpriv wifx setDropSTAQuery {1/0}	Y	Y	To enable/disable DropSTAQuery feature. Enabling feature would drop IGMP Querys from STA #iwpriv wifx setDropSTAQuery 1 #iwpriv wifx getDropSTAQuery getDropSTAQuery:1
nopbn get_nopbn	iwpriv athX nopbn {1/0}	Y	Y	To disable VAPs being notified when jump start button gets pushed. #iwpriv ath0 nopbn 1 #iwpriv ath0 get_nopbn 1 get_nopbn:1

1.3.28 Channel loading/Channel hopping parameters

Table 1-34 Channel loading/Channel hopping parameters

Parameter	Format	DA	OL	Description
acsmindwell get_acsmindwell	<code>iwpriv athN acsmindwell value_in_ms</code>	Y	Y	Minimum time in milliseconds to spend on each channel even if channel is idle. #iwpriv ath0 acsmindwell 100 #iwpriv ath0 get_acsmindwell ath0 get_acsmindwell:100
acsmaxdwell get_acsmaxdwell	<code>iwpriv athN acsmaxdwell value_in_ms</code>	N	N	Maximum time in milliseconds than can be spent on a channel. Default value is 300 msec. #iwpriv ath0 acsmaxdwell 100 #iwpriv ath0 get_acsmaxdwell ath0 get_acsmindwell:100
acsreprt	<code>lwpriv athN acsreport value_in_ms</code>	Y	Y	Enable (1) or disable (0) channel loading. #iwpriv ath0 acsreport 100
ch_hop_en get_ch_hop_en	<code>iwpriv athN ch_hop_en {1 0}</code>	Y	N	Enables (1) or disables (0) channel hopping feature #iwpriv ath0 ch_hop_en 1 #iwpriv ath0 get_ch_hop_en ath0 get_ch_hop_en:1
ch_long_dur get_ch_long_dur	<code>iwpriv athN ch_long_dur value_in_seconds</code>	Y	N	Set/get long duration timer value in seconds #iwpriv ath0 ch_long_dur 60 #iwpriv ath0 get_ch_long_dur ath0 get_ch_long_dur:60
ch_nhop_dur get_ch_nhop_dur	<code>lwpriv athN ch_nhop_dur {value in seconds}</code>	Y	N	Set/get no hop duration for channel hopping #iwpriv ath0 ch_nhop_dur 60 #iwpriv ath0 get_ch_nhop_dur ath0 get_ch_nhop_dur:60
ch_cntwn_dur get_ch_cntwn_dur	<code>lwpriv athN ch_cntwn_dur {value in seconds}</code>	Y	N	Set/get counter window duration for channel hopping #iwpriv ath0 ch_cntwn_dur 60 #iwpriv ath0 get_ch_cntwn_dur get_ch_cntwn_dur:60
ch_noise_th get_ch_noise_th	<code>lwpriv athN ch_noise_th {value}</code>	Y	N	Set/get noise threshold in dB iwpriv ath0 ch_noise_th -90 #iwpriv ath0 get_ch_noise_th get_ch_noise_th:-90
ch_cnt_th get_ch_cnt_th	<code>lwpriv athN ch_cnt_th {value}</code>	Y	N	Set/get counter threshold iwpriv ath0 ch_cnt_th 60 iwpriv ath0 get_ch_cnt_th get_ch_cnt_th:60
g_chanutil	<code>iwpriv wifi0 g_chanutil</code>	Y	Y	Indicates the fraction of the time AP senses that the channel is in use by the neighboring AP for transmissions

1.3.29 802.11k parameters

Table 1-35 802.11k Parameters

Parameter	Format	DA	OL	Description
rrm get_rrm	<code>iwpriv athN rrm</code> <code>{1 0}</code>	Y	Y	Enables or disables 802.11k. Default is disabled. # <code>iwpriv ath0 rrm 1</code> # <code>iwpriv ath0 get_rrm</code> <code>get_rrm:1</code>

1.3.30 Aggregate size scaling parameters

Table 1-36 Aggregate Size Parameters

Parameter	Format	DA	OL	Description
acparams	<code>iwpriv athN acparams</code> <code>{AC-0,1,2,3,4} {0}</code> <i>{Scaling factor: 0-3} {0}</i>	N	Y	Configures aggregate size scaling factor for the AC. # <code>iwpriv ath0 acparams 0 0 1 0</code> # <code>iwpriv ath0 acparams 2 0 1 0</code>

1.3.31 Wifitool Utility

Qualcomm Atheros provides proprietary Wifitool utility for Linux-based distribution. The primary purpose of this utility is to get stats and configure various features like 802.11k and channel loading or any other feature that requires a large number of parameters as input and output.

1.3.31.1 802.11k

Table 1-37 Wifitool 802.11k parameters

Parameter	Format	Description
sendbcnrpt	<code>wifitool interface_name</code> <code>sendbcnrpt dest_mac</code> <code>bssid chan_num reg_</code> <code>class</code>	Beacon report <ul style="list-style-type: none"> ■ <code>dest_mac</code>: MAC address of associated station to which beacon request is sent. ■ <code>bssid</code> is the BSSID of desired AP (RSSI to be determined). ■ <code>chan_num</code>: chan number for which stats are to be determined ■ <code>reg_class</code>: reg class of the operating channel.
sendchload	<code>wifitool interface_name</code> <code>sendchload cmd</code> <code>reg_class destmac</code> <code>channel</code>	<ul style="list-style-type: none"> ■ <code>cmd</code>: reserved for future use, in current implementation it should be passed as any positive value greater than zero. ■ <code>reg_class</code>: reg class of operating channel. ■ <code>destmac</code>: MAC address of associated station. ■ <code>channel</code>: channel on which we want station to calculate channel load.

Table 1-37 Wifitool 802.11k parameters (cont.)

Parameter	Format	Description
sendstastats	wifitool <i>interface_name</i> sendstastats <i>dst_mac</i> <i>duration</i> <i>gid</i>	<ul style="list-style-type: none"> dst mac: MAC address of associated client duration: interval for which we want to take this statistics. Value is in ms. gid: group id, this value is taken from 802.11k specification.
sendnhist	wifitool <i>interface_name</i> sendnhist <i>dstmac</i> <i>duration</i> <i>regclass</i> <i>channel</i>	<ul style="list-style-type: none"> dst mac: MAC address of associated client. duration: interval for which we want to take this statistics. Value is in msec. regclass: reg class of operating channel. channel: channel on which station will calculate channel load will be calculated.

1.3.31.2 Channel loading

Table 1-38 Wifitool channel loading parameters

Parameter	Format	Description
acsreport	wifitool athN acs_report	Get channel loading in user layers with the wifitool utility
setchanlist	wifitool athN setchanlist <i>ch1 ch2....chN</i>	To set list of channels for participating in the channel loading algorithm
getchanlist	wifitool athN getchanlist	To get the list of valid channels for channel loading

```

> sleep 300
> done

~ # FWLOG: [6601207] WHAL_ERROR_RESET_CHANNF1 ( )
FWLOG: [6601207] WHAL_ERROR_RESET_ERRID ( 0x1 )
FWLOG: [6909431] WHAL_ERROR_RESET_CHANNF1 ( )
FWLOG: [6909431] WHAL_ERROR_RESET_ERRID ( 0x1 )

~ #
~ #
~ # wifitool ath0 acsreport
Channel | BSS | minrssi | maxrssi | NF | Ch load | spect load | sec_chan
-----|-----|-----|-----|-----|-----|-----|-----
2412( 1) | 0 | 0 | 0 | -118 | 2 | 0 | 0
2417( 2) | 0 | 0 | 0 | -118 | 1 | 0 | 0
2422( 3) | 0 | 0 | 0 | -118 | 2 | 0 | 0
2427( 4) | 0 | 0 | 0 | -118 | 1 | 0 | 0
2432( 5) | 0 | 0 | 0 | -117 | 2 | 0 | 0
2437( 6) | 4 | 7 | 24 | -116 | 33 | 0 | 0
2442( 7) | 0 | 0 | 0 | -117 | 5 | 0 | 0
2447( 8) | 0 | 0 | 0 | -116 | 1 | 0 | 0
2452( 9) | 0 | 0 | 0 | -118 | 1 | 0 | 0
2457( 10) | 0 | 0 | 0 | -117 | 1 | 0 | 0
2462( 11) | 0 | 0 | 0 | -118 | 2 | 0 | 0
~ #
CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.6.2 | VT102 | Offline

```

Figure 1-1 Channel loading

1.3.31.3 Block channel list

To block any set of channel from participating in ACS algorithm this command can be used.

Table 1-39 Block channel list

Parameter	Format	Description
block_acs_channel	wifitool athN block_acs_channel <i>channel1,channel2,channel3</i> <i>.....channel N</i>	Set list of channels to be blocked from ACS channel selection

Max value for N is 255.

After successful execution of this API, user should view the following log on console:

“Following channels are blocked from ACS”

[channel 1] [channel2].....[channel]

Every successful execution of command will amend previously stored list in driver. If the user want to flush previously stored list, then they should execute this command with single channel with value as zero.

e.g

```
Wifitool ath0 block_acs_channel 1,2,3
Wifitool ath0 block_acs_channel 4,5,6
```

Will block acs to block channel 1 2 3 4 5 6 to participate in acs channel selection, where as

```
Wifitool ath0 block_acs_channel 1,2,3
Wifitool ath0 block_acs_channel 0
Wifitool ath0 block_acs_channel 4,5,6
```

Will block only channel 4,5,6

1.3.31.4 TR069 Parameters

Parameter	Format	Description
tr069_get_fail_retrans	wifitool athN tr069_get_fail_retrans	The number of packets that were not transmitted successfully due to the number of retransmission attempts exceeding an 802.11 retry limit.
tr069_get_success_retrans	wifitool athN tr069_get_success_retrans	The number of packets that were successfully transmitted after one or more retransmissions.
tr069_get_success_mul_retrans	wifitool athN tr069_get_success_mul_retrans	The number of packets that were successfully transmitted after more than one retransmission.
tr069_get_ack_failures	wifitool ath0 tr069_get_ack_failures	The number of expected ACKs that were never received.
tr069_get_retrans	wifitool ath0 tr069_get_retrans	The total number of transmitted packets which were retransmissions.
tr069_get_aggr_pkts	wifitool ath0 tr069_get_aggr_pkts	The number of aggregated packets that were transmitted.
tr069_get_sta_bytes_sent	wifitool ath0 tr069_get_sta_bytes_sent <STA MAC>	The total number of bytes transmitted to the client device.
tr069_get_sta_bytes_rcvd	wifitool ath0 tr069_get_sta_bytes_rcvd <STA MAC>	The total number of bytes received from the client device.

1.3.32 Target recovery parameters

Parameter	Format	DA	OL	Description
seth.get_fwrecovery	iwpriv wifi1 set_fw_recovery {1 0}	Y	Y	Enables (1) or disables (0) the target recovery mechanism for the Peregrine radio <pre>#iwpriv wifi1 set_fw_recovery 1 (enable)</pre> <pre>#iwpriv wifi1 set_fw_recovery 0 (disable)</pre>
get_fw_recovery	iwpriv wifi1 get_fw_recovery	Y	Y	This parameter is used to check if the target recovery mechanism is enabled or disabled.

1.3.33 2.4 GHz VHT 256-QAM Broadcom interoperability support

Table 1-40 lists the parameters for 2.4 GHz VHT 256-QAM Broadcomm interoperability support.

Table 1-40 2.4 GHz VHT 256-QAM Broadcom interoperability support

Parameter	Format	DA	OL	Description
11ngvhtintop g_11ngvhtintop	iwpriv athN 11ngvhtintop {1/0}	N	Y	Enables (1) or disables (0) 2.4 GHz 256-QAM interoperability support with Broadcom based devices. The default value is 0. This command enables VHT 256-QAM rate support with Broadcom based devices. The get parameter returns the current value. #iwpriv ath0 11ngvhtintop 1 #iwpriv ath0 g_11ngvhtintop

1.3.34 Airtime Fairness (ATF) Parameters

Table 1-41 lists the various ATF parameters.

Table 1-41 ATF Parameters

Parameter	Format	DA	OL	Description
commitatf	iwpriv athN commitatf {1/0}	Y	Y	This command must be issued after any ATF configuration which includes ssid/sta airtime allocation using wlanconfig tool. Usage: #iwpriv ath0 commitatf 1 /*setting effective*/ #iwpriv ath0 commitatf 0
getcommitatf	iwpriv athN get_commitatf			This command displays the value set for commitatf Usage: lwpriv ath0 get_commitatf: Displays if commitatf is set or cleared.
atfstrictsched	iwpriv wifiN atfstrictsched {1/0}	Y	Y	This command is for enabling or disabling ATF strict scheduling. Example command: /* enable strict scheduling */ #iwpriv wifi0 atfstrictsched 1 /* disable strict scheduling - enabled Fair queue scheduling */ #iwpriv wifi0 atfstrictsched 0 NOTE Fair-queue ATF Scheduling is enabled by default in both direct attach and partial offload architecture

Parameter	Format	DA	OL	Description
gatifstrictsched	iwpriv wifiN gatifstrictsched	Y	Y	The command is used to check whether ATF strict scheduling is enabled or disabled. Example command: # iwpriv wifi0 gatifstrictsched wifi0 gatifstrictsched:1
atf_sched_dur	iwpriv wifiN atf_sched_dur ac {0-3} dur {ac is the access category and dur is the token}	N	Y	This command is used to set the number of tokens to be allocated for a particular access category Example Command: iwpriv wifi1 atf_sched_dur 2 5 The first parameter is the Access Category which should be between 0 and 3 0 – Best Effort 1 – Background 2 – Video 3 – Voice The second parameter should be the number of tokens which should be a positive value.
atfobssched	iwpriv wifiN atfobssched 1/0	Y	N	This command is used to enable ATF OBSS module, which considers interference from other APs, before distributing the tokens to the associated STAs Example Command: #iwpriv wifi0 atfobssched 1 /* enable OBSS scheduling */ #iwpriv wifi0 atfobssched 0 /* disable OBSS scheduling */
g_atfobssched	iwpriv wifiN g_ atfobssched	Y	N	This command is used to get the current state of ATF OBSS module, if it is enabled or not. # iwpriv wifi0 gatifobssched wifi0 gatifobssched:0
atf_shr_buf	iwpriv athN atf_shr_buf {1/0}	Y	N	This command is used to enable/disable sharing of Tx Buffers between the clients in the ratio of airtime. Example command: #iwpriv ath0 atf_shr_buf 1 /* enable Tx Buffer sharing */
g_atf_shr_buf	iwpriv athN g_atf_shr_buf	Y	N	This command is used to query whether Tx Buffer sharing between clients is enabled or not. Example Command: #iwpriv ath0 g_atf_shr_buf ath0 g_atf_shr_buf:1
atfmaxclient	iwpriv athN atfmaxclient	Y	N	This command is used to enable maxclient support on direct attach architecture. This feature is disabled by default #iwpriv ath0 atfmaxclient
g_atfmaxclient	iwpriv athN g_ atfmaxclient	Y	N	This command is used to query whether maxclient support is enabled #iwpriv ath0 g_atfmaxclient

1.3.35 Dynamic Frequency Selection (DFS) Parameters

Table 1-42 DFS Parameters

Parameter	Format	DA	OL	Description
staDFSEn	iwpriv wifiN staDFSEn {1/0}	Y	Y	<p>For a radio (in STA mode) whose TX Power > 23dBm should support DFS. STA mode DFS can be enabled/Disabled by using the command.</p> <p>Note: At present, STA mode CAC is performed only for ETSI domain.</p> <p>Usage:</p> <pre>#iwpriv wifi0 staDFSEn 1 #iwpriv wifi0 staDFSEn 0</pre>
get_staDFSEn	iwpriv wifiN get_ staDFSEn	Y	Y	<p>This command is used to query whether sta mode DFS is Enabled</p> <p>Usage:</p> <pre>#iwpriv wifi1 get_staDFSEn wifi1 get_staDFSEn:0</pre>

1.4 wlanconfig utility

The Qualcomm Atheros **wlanconfig** utility manages VAP instances. It is an integral part of the configuration scripts and provides the primary method to:

- [Create a VAP](#)
- [List VAP parameters](#)
- [Delete an interface](#)

NOTE Although commands may have adverse effects, not all effects may have been documented. Consider the nature of multiple VAP configurations that use multiple radios, and use caution when changing parameters.

1.4.1 Create a VAP

Creating a VAP requires parameters indicating the specific nature of the VAP. A VAP can be either a client node (managed node) or an infrastructure node (master node).

```
#wlanconfig ATH[N] create wlandev wifiN wlanmode [ap|sta|mon|adhoc]
[bssid|-bssid] [nosbeacon]
```

Where:

Argument	Description				
ATH[N]	VAP name. If the number at the end of the name is omitted, the system will automatically use the next available interface number. The VAP name ATH is not required, any text string will do. Note that when the index is occupied by another VAP, create VAP will fail.				
create	Create action				
wlandev wifiN	Indicates to which interface the VAP will attach. The interface number is required for this argument. For dual concurrent operations, <i>N</i> indicates which radio to attach the VAP to.				
wlanmode mode	Indicates the mode to open the VAP into. The valid modes are: <table border="1"> <tr> <td>ap</td><td>AP (infrastructure) mode</td></tr> <tr> <td>sta</td><td>STA (client) mode</td></tr> </table>	ap	AP (infrastructure) mode	sta	STA (client) mode
ap	AP (infrastructure) mode				
sta	STA (client) mode				
bssid -bssid	Optional parameter indicating that the MAC address should be cloned from the first VAP for this interface. Not normally specified. Note that -bssid is not supported by wlanconfig, but is supported by the Qualcomm Atheros driver.				
nosbeacon	Indicates that no beacons will be transmitted from this VAP. Used as part of STA mode.				

1.4.2 List VAP parameters

The argument to the **list** command defines the type of listing to produce. Each type is described in this section:

- AP list elements
- STA list Elements
- Channel list elements
- Capabilities list elements
- WME list elements

The list command provides an extended listing of parameters from the VAP, depending on the type of list for each associated STA. The list command generates a print of the VAP association list with the associated parameters:

```
# wlanconfig athN list [ap|sta|chan|keys|caps|wme]
```

1.4.2.1 AP list elements

Table 1-43 describes the AP list elements. It only applies to VAPs that are STA VAPs. This scan result provides a list of nearby APs. The following is an example:

```
# wlanconfig athN list ap
SSID          BSSID          CHAN  RATE  S:N  INT  CAPS
Atheros Guests 00:0b:85:5b:a6:e1 52    54M   13:0 100  E
ney-11a        00:03:7f:00:de:ea 60    54M   22:0 100  Es WME
perseus-cis    00:1d:45:29:39:50 36    54M   30:0 100  E WME
BILL-AP        00:03:7f:00:ce:ee 36    54M   27:0 100  Es WME
apps-atheros1  00:03:7f:00:ce:d3 36    54M   26:0 100  EPs WME ATH
```

Table 1-43 AP list elements

Element	Description					
BSSID	BSSID value of the AP. Takes the form of a MAC address					
CAPS	Current capabilities of the AP These are alphanumeric characters corresponding to specific 802.11 capability bits in the beacon and probe response Responses are defined as:					
	E	ESS	P	Privacy	s	Short Slot Time
	I	IBSS	S	Short Preamble	D	DSSS/OFDM
	c	Pollable	B	PBCC		
	C	Poll Request	A	Channel Agility		
CHAN	Channel the AP is servicing					
INT	Beacon interval, in ms					
RATE	Maximum rate of the AP					
S:N	Signal to Noise ratio. The first number is the last received RSSI from the device, and the last number is the noise value.					
SSID	Name string of the AP as broadcast in the beacon					
(No Header)	All information elements (IE) for the attached STA are printed. They have the values:					
	WPA	WPA IE	ATH	Qualcomm Atheros Vendor IE	RSN	aRSN IE
	WME	WMM IE	VEN	Vendor-Specific IE	???	Unknown IE

1.4.2.2 STA list Elements

Table 1-44 describes the list elements for each STA associated with the indicated VAP. This listing is produced:

Normal format

```

/# wlanconfig athX list sta
ADDR          AID CHAN TXRATE RXRATE RSSI IDLE  TXSEQ RXSEQ  CAPS ACAPS ERP
STATE  HTCAPS STATE MAXRATE(DOT11) HTCAPS ASSOCTIME IEs MODE PSMODE
00:34:56:78:b0:b0 1    36    468M 935M 68 0 0   65535 Es 0 b 0 AWPSM 00:00:22 WME
IEEE80211_MODE_11AC_VHT80 0

```

Human readable command

```

root@OpenWrt:/# wlanconfig ath0 list -H
ADDR :00:34:56:78:b0:b0 AID:    1 CHAN:   36 TXRATE:468M RXRATE:   935M RSSI:   68
IDLE:   0 TXSEQ:       0 RXSEQ: 65535 CAPS:   Es ACAPS:       ERP:   0 STATE:
b MAXRATE(DOT11):       0 HTCAPS:       AWPSM ASSOCTIME:00:00:15 WME
MODE: IEEE80211_MODE_11AC_VHT80
PSMODE: 0

```

NOTE The data for the ACAPS element data is no longer reported. In the example output above, the data 0, 33, Q, and WME correspond to ERP, STATE, HTCAPS, and (no header) elements listed in Table 1-44.

Table 1-44 STA list elements

Element	Description					
ADDR	MAC address of the STA					
AID	Association ID; determines the specific AP/STA association pair used in 802.11n test commands					
CAPS	E	ESS	P	Privacy	s	Short Slot Time
	I	IBSS	S	Short Preamble	D	DSSS/OFDM
	c	Pollable	B	PBCC		
	C	Poll Request	A	Channel Agility		
CHAN	Channel the device is associated on					
ERP	Extended Rate PHY capabilities in dBm. A value of 0 indicates a legacy STA. Printed in hex.					
HTCAPS	HT capabilities flags; these are character indicators that represent a capability of the 802.11n STA					
	A	Advanced coding	Q	Static MIMO power save	S	Short GI enabled (HT40)
	W	HT40 channel width	R	Dynamic MIMO power save	D	Delayed block ACK
	P	MIMO power save enabled	G	Greenfield preamble	M	Max AMSDU size
IDLE	Current setting of the STA inactivity timer. This is the time in ms when the STA will go into power save of no activity occurs on the link.					
RATE	Current data rate of the association					

Table 1-44 STA list elements (cont.)

Element	Description					
RSSI	Signal strength of the last received packet. For MIMO devices, this is an average value over all active receive chains.					
RXSEQ	Receive sequence number of the last received packet					
STATE	Current state of the STA. This is an hexadecimal value that consists of these bits:					
	0x0001	Authorized for Data Transfer	0x0010	Power Save Mode Enabled	0x0100	uAPSD SP in Progress
	0x0002	QoS enabled	0x0020	Auth Reference held	0x0200	An ATH Node
	0x0004	ERP Enabled	0x0040	uAPSD Enabled	0x0400	WDS Workaround Req.
	0x0008	HT Rates Enabled	0x0080	uAPSD Triggerable	0x0800	WDS Link
TXSEQ	Transmit sequence number of the last received packet					
(No Header)	All information elements (IE) for the attached STA are printed. They have the values:					
	WPA	WPA IE	ATH	Qualcomm Atheros Vendor IE	RSN	RSN IE
	WME	WMM IE	VEN	Vendor-Specific IE	???	Unknown IE

1.4.2.3 Channel list elements

Table 1-45 describes the channel list elements, listing available channels and frequencies followed by strings indicating specific VAP channel capabilities. This example lists channels with channel number and frequency in MHz:

```
# wlanconfig ath0 list chan
```

```
Channel 36: 5180 Mhz 11na C CU V VU V80-42 Channel 120: 5600 *~ Mhz 11na C CL V VL V80-122
Channel 40: 5200 Mhz 11na C CL V VL V80-42 Channel 124: 5620 *~ Mhz 11na C CU V VU V80-122
Channel 44: 5220 Mhz 11na C CU V VU V80-42 Channel 128: 5640 *~ Mhz 11na C CL V VL V80-122
Channel 48: 5240 Mhz 11na C CL V VL V80-42 Channel 132: 5660 *~ Mhz 11na C CU V VU V80-138
Channel 52: 5260 *~ Mhz 11na C CU V VU V80-58 Channel 136: 5680 *~ Mhz 11na C CL V VL V80-138
Channel 56: 5280 *~ Mhz 11na C CL V VL V80-58 Channel 140: 5700 *~ Mhz 11na C CU V VU V80-138
Channel 60: 5300 *~ Mhz 11na C CU V VU V80-58 Channel 144: 5720 *~ Mhz 11na C CL V VL V80-138
Channel 64: 5320 *~ Mhz 11na C CL V VL V80-58 Channel 149: 5745 Mhz 11na C CU V VU V80-155
Channel 100: 5500 *~ Mhz 11na C CU V VU V80-106 Channel 153: 5765 Mhz 11na C CL V VL V80-155
Channel 104: 5520 *~ Mhz 11na C CL V VL V80-106 Channel 157: 5785 Mhz 11na C CU V VU V80-155
Channel 108: 5540 *~ Mhz 11na C CU V VU V80-106 Channel 161: 5805 Mhz 11na C CL V VL V80-155
Channel 112: 5560 *~ Mhz 11na C CL V VL V80-106 Channel 165: 5825 Mhz 11na C V
Channel 116: 5580 *~ Mhz 11na C CU V VU V80-122
```

Table 1-45 Channel list elements

Column 1	FHSS	FHSS channel
Column 2	11na	5 GHz band 802.11n capable
	11a	5 GHz band legacy
	11ng	2.4 GHz band 802.11n capable
	11g	2.4 GHz band legacy
	11b	2.4 GHz band DSSS only

Table 1-45 Channel list elements

Column 3	C	802.11n control channel capable
	CU	802.11n upper extension channel enabled
	CL	802.11n lower extension channel enabled
Column 4	V	80211ac (VHT - 20 MHz band) control channel capable
Column 5	VU	80211ac (VHT - 40 MHz band) upper extension channel enabled
	VL	80211ac (VHT - 40 MHz band) lower extension channel enabled
Column 6	V80-<CH>	80211ac (VHT - 80 MHz band) channel. With center frequency CH

1.4.2.4 Capabilities list elements

Table 1-46 describes the capabilities list strings; the list provides a list of the VAP capabilities output as a comma-delimited string.

```
# wlanconfig ath0 list caps
ath0=3782e41f<WEP,TKIP,AES,AES_
CCM,HOSTAP,TXPMGT,SHSLOT,SHPREAMBLE,TKIPMIC,WPA1,WPA2,
BURST,WME>
```

Table 1-46 Capabilities list elements

AES	AES OCB available	MONITOR	Monitor mode	TXPMGT	Tx power mgmt.
AES_CCM	AES CCM	PMGT	Power mgmt. available	WEP	WEP available
AHDEMO	Ad hoc demo mode	SHPREAMBLE	Short GI preamble available	WME	WME capable
BURST	Frame bursting capable	SHSLOT	Short Slot available	WPA1	WPA1 available
CKIP	CKIP available	SWRETRY	Tx software retry	WPA2	WPA2 available
HOSTAP	Host AP mode	TKIP	TKIP available		
IBSS	IBSS mode available	TKIPMIC	TKIP MIC available		

1.4.2.5 WME list elements

This list provides the current settings of the VAP WME settings:

```
# wlanconfig ath0 list wme
AC_BE cwmmin 4 cwmax 6 aifs 3 txopLimit 0
    cwmmin 4 cwmax 10 aifs 3 txopLimit 0
AC_BK cwmmin 4 cwmax 10 aifs 7 txopLimit 0
    cwmmin 4 cwmax 10 aifs 7 txopLimit 0
AC_VI cwmmin 3 cwmax 4 aifs 1 txopLimit 3008
    cwmmin 3 cwmax 4 aifs 2 txopLimit 3008
AC_VO cwmmin 2 cwmax 3 aifs 1 txopLimit 1504
    cwmmin 2 cwmax 3 aifs 2 txopLimit 1504
```

1.4.3 Delete an interface

The VAP must be down before deleting an interface to avoid bad interactions with other VAPs. This command applies only to the VAP interface specified and uses the form:

```
# wlanconfig athN destroy
```

1.4.4 NAWDS configuration parameters

The NAWDS parameter has several subparameters, each of which may have its own set of options and settings. For example, the *add-repeater* subparameter has *mac_addr* and *caps* as options. Each NAWDS subparameter is listed in [Table 1-47](#) as a separate entry.

Table 1-47 Configure NAWDS parameters

Parameter	Format	DA	OL	Description
add-repeater	<i>wlanconfig athN nawds add-repeater mac_addr caps</i>	Y	Y	Add a NAWDS AP with the specified MAC address and capability. The definition of CAPS is the same as the CAPS mentioned in defcaps.
				mac_addr MAC address
				caps Capabilities

Table 1-47 Configure NAWDS parameters (cont.)

Parameter	Format	DA	OL	Description	
defcaps	wlanconfig athN nawds defcaps caps	Y	Y	When a NAWDS AP is operating in learning mode, it must discover which capability the NAWDS AP peer has. In this situation, defcaps would be used. The CAPS is defined as follows: #define NAWDS_REPEATER_CAP_HT20 0x01 #define NAWDS_REPEATER_CAP_HT2040 0x02 #define NAWDS_REPEATER_CAP_DS 0x04 If CAPS equals 0, the HT rate would be disabled. To enable NAWDS_REPEATER_CAP_DS, at least one of NAWDS_REPEATER_CAP_HT20 and NAWDS_REPEATER_CAP_HT2040 must be specified. The range of CAPS values are defined as follows:	
				0x0	HT Rate Disabled
				0x1	Single stream HT20 Rates
				0x2	Single Stream HT40 Rates
				0x5	Double Stream HT20 Rates
				0x6	Double Stream HT40 Rates
				0x9	Triple Stream HT20 Rates
				0xa	Triple Stream HT40 Rates
del-repeater	wlanconfig athN nawds del-repeater mac_addr	Y	Y	Delete a NAWDS AP with the specified MAC address.	
				mac_addr	MAC address
list	wlanconfig athN nawds list	Y	Y	Display current NAWDS configurations.	
mode	wlanconfig athN nawds mode value	Y	Y	Configures the mode in which NAWDS AP is operating. Whenever the mode is changed, the NAWDS MAC table would be cleared. value may specify one of the following:	
				0	NAWDS Disabled
				1	STATIC Repeater mode
				2	STATIC Bridge mode
				3	LEARNING Repeater mode
4	LEARNING Bridge mode				
override	wlanconfig athN nawds override value	Y	Y	Enables (1) or disables (0) override command. value may specify one of the following:	
				0	No more MAC address my be added to the NAWDS table when the table is full.
				1	When running out of entry space in NAWDS MAC table (either by configuring too many NAWDS APs or by learning too many AP using the learning feature), enabling the override would delete MAC addresses occupied by dead NAWDS APs.

1.4.4.1 Configuration examples

Static bridge and peer node supports HT20 rates

```
Cfg -a AP_PRIMARY_CH=149
Cfg -a AP_CHMODE=11NAHT40PLUS
Cfg -a AP_SSID=Anish_test
Apup
Iwpriv ath0 wds 1
Wlanconfig ath0 nawds mode 2
Wlanconfig ath0 nawds add-repeater 00:03:7f:xx:xx:xx:xx 0x1
```

Learning bridge and by default peer NAWDS AP supports HT40/DS rates

```
Cfg -a AP_PRIMARY_CH=149
Cfg -a AP_CHMODE=11ACVHT80
Cfg -a AP_SSID=Anish_test
Apup
Iwpriv ath0 wds 1
Wlanconfig ath0 nawds mode 4
Wlanconfig ath0 nawds defcaps 0x6
```

Static bridge and peer node supports VHT rates

```
Cfg -a AP_PRIMARY_CH=149
Cfg -a AP_CHMODE=11ACVHT80
Cfg -a AP_SSID=Anish_test
Apup
Iwpriv ath0 wds 1
Wlanconfig ath0 nawds mode 2
Wlanconfig ath0 nawds add-repeater 00:03:7f:xx:xx:xx:xx 0x88
```

VHT Example Rates: 3x3

```
wlanconfig ath0 nawds add-repeater <mac> 0x88 - 3x3 HT80
wlanconfig ath0 nawds add-repeater <mac> 0x48 - 3x3 HT40
wlanconfig ath0 nawds add-repeater <mac> 0x28 - 3x3 HT20
```

VHT Example Rates: 2x2

```
wlanconfig ath0 nawds add-repeater <mac> 0x84 - 2x2 HT80
wlanconfig ath0 nawds add-repeater <mac> 0x44 - 2x2 HT40
wlanconfig ath0 nawds add-repeater <mac> 0x24 - 2x2 Ht20
```

VHT Example Rates: 1x1

```
wlanconfig ath0 nawds add-repeater <mac> 0x80 - 1x1 HT80
wlanconfig ath0 nawds add-repeater <mac> 0x40 - 1x1 HT40
wlanconfig ath0 nawds add-repeater <mac> 0x20 - 1x1 HT20
```

1.4.5 HMWDS/HMMC commands

Table 1-48 Configure HMWDS/HMMC parameters

Parameter	Format	DA	OL	Description
hmmc add	wlanconfig athX hmmc add <ipv4 mcast address> <netmask>	Y	Y	To add a range of multicast address defined by <ipv4mcastaddr>/<netmask> for which all mcast packets should converted to unicast for all the stations associated to the ap.
hmmc del	wlanconfig athX hmmc del <ipv4 mcast address> <netmask>	Y	Y	To delete the mcast ip range of address.
hmmc dump	wlanconfig athX hmmc dump	Y	Y	To display the ranges configured so far.
hmwds add_addr	wlanconfig ath0 hmwds add_addr <wds_mac_addr> <peer_mac_addr>	Y	Y	To add a managed WDS address through an associated peer.
hmwds reset_addr	wlanconfig ath0 hmwds reset_addr <mac_addr>	Y	Y	Resets all the managed WDS entries in the global WDS table if both <wds_mac_addr> and <peer_mac_addr> are not specified.
hmwds read_addr	wlanconfig ath0 hmwds read_addr <peer_mac_addr>	Y	Y	Lists all the managed WDS addresses behind the given peer.
hmwds read_table	wlanconfig ath0 hmwds read_table	Y	Y	Lists all the managed WDS addresses configured.

1.4.6 Configure ATF Parameters

Table 1-49 lists the ATF configuration parameters which can be used to configure airtime for a VAP or station

Table 1-49 Configuration/show ATF parameters

Parameter	Format	DA	OL	Description
addssid	wlanconfig athX addssid <ssid name> <airtime percentage>	Y	Y	Assign percentage of airtime to the SSID. The airtime percentage value range is 0~100. Example: #wlanconfig ath0 addssid BEE0 12
delssid	wlanconfig athX delssid <ssid name>	Y	Y	Delete the SSID assigned. Example: # wlanconfig ath0 delssid BEE0
addsta	wlanconfig athX addsta <sta mac addr> <airtime percentage>	Y	Y	Assign percentage of airtime to the STA. The airtime percentage value range is 0~100. Example: #wlanconfig ath0 addsta 220011abef6660
delsta	wlanconfig athX delsta <sta mac addr>	Y	Y	Delete the STA assigned. Example: # wlanconfig ath0 delsta 220011abef66
showatftable	wlanconfig athX showatftable	Y	Y	Displays the ATF table. The SSIDs and STAs part of the ATF table will be listed Example: #wlanconfig ath0 showatftable
showairtime	wlanconfig athX showairtime	Y	Y	Lists all STAs and percentage of ATF. Example: #wlanconfig ath0 showairtime Note: Displays STA's added in the ATF table. The airtime value shown is in terms of 1000.
flushatftable	wlanconfig athX flushatftable	Y	Y	This flushes all the configurations and data present in the atf table. Example #wlanconfig ath0 flushatftable NOTE When this command is issued there is a reset of bss and the stations which are connected will get disconnected and connected again.

Table 1-49 Configuration/show ATF parameters

Parameter	Format	DA	OL	Description
addatfgroup	wlanconfig athX addatfgroup <group name> <ssid name>	Y	N	Creates a new atfgroup, if the group doesn't exist already and adds the SSID to the group created. If the group already exists, the SSID will be added to the group. Example: #wlanconfig ath0 addatfgroup group1 myvap
configatfgroup	wlanconfig athX configatfgroup <group name> <airtime percentage>	Y	N	Assigns/Configures airtime percentage to the group. Example: #wlanconfig ath0 configatfgroup group1 80
delatfgroup	wlanconfig athX delatfgroup <group name>	Y	N	Deletes a group. Example: #wlanconfig ath0 delatfgroup group1
showatfgroup	wlanconfig athX showatfgroup	Y	N	Displays all groups configured , SSIDs for each group & the airtime percentage assigned to each group Example: #wlanconfig ath0 showatfgroup

1.5 Other commands

The following tables describe additional commands and parameters beyond iwconfig, iwpriv, and wlanconfig.

1.5.1 Athssd parameters

Table 1-50 Athssd Parameters

Configuration	Format	DA	OL	Description
Standalone Scan	athssd -i wifiN -j athN -s <i>val</i>			Start athssd, configuring it to carry out a standalone scan on channel <i>val</i> . <i>val</i> can be 0, in which case the current channel will be used.
		Y	Y	s=0
		Y	N	s>0
External GUI	athssd -i wifi0 -j athN -s	N	N	Start athssd, configuring it to work with external GUI. Typically the GUI is an internal tool.

1.5.2 DFS

Configuring the AP for DFS involves setting up certain parameters. They can be set using cfg -a command or appropriate iwpriv commands. Please refer to iwpriv command reference for further details.

1. Check the current set up using the command, cfg -e.
2. Use the command, cfg -x to set it up in default mode
3. Set up the following parameters:
 - a. Set up country code
 - b. Select the proper RADIO
 - c. Select the proper mode. Possible modes are
 - i. 11A
 - ii. 11NAHT20
 - iii. 11NAHT40PLUS
 - iv. 11NAHT40MINUS
 - v. 11ACVHT20
 - vi. 11ACVHT40PLUS
 - vii. 11ACVHT40MINUS
 - viii. 11ACVHT80
 - d. Select the appropriate channel
 - e. For FCC testing following extra set up is necessary:
 - i. Set rate control to manual mode (cfg -a RATECTL=manual)

- ii. Set manual rate to 9 Mbps (cfg -a MANRATE=0x0f0f0f0f)
- iii. Iwpriv command can also be used for (i) and (ii)

1.5.3 NAT parameters

For Host Network Address Translation (HNAT), the rules are programmed through Linux command “iptables”.

The simple NAT rule for egress and ingress TCP traffic is as follows:

```
iptables -t nat -A POSTROUTING -o eth1.2 -p tcp -j MASQUERADE
iptables -t nat -A PREROUTING -i eth1.2 -p tcp -j DNAT --to 192.168.1.100
```

For further information about syntax and usage, refer to

http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO:_Ch14:_Linux_Firewalls_Using_ipables

1.5.4 Radartool

Radartool parameters

Parameter	Format	DA	OL	Description	
usenol	radartool -i wifi [0 1] usenol [0/1]	Y	Y	usenol 0: Sets the test system in test mode so that it stays in the same channel during the test. By default the AP will switch channel when it detects radar. usenol 1: Causes the AP to switch channels when radar is detected.	
dfsdebug	radartool -i wifi [0 1] dfsdebug debug_level	Y	Y	Sets the debug level.	
				0x00000100	minimal DFS debug
				0x00000200	normal DFS debug
				0x00000400	maximal DFS debug
				0x00000800	display matched filter ID
				0x00001000	display TLV related information
				0x00002000	display radar NOL
				0x00004000	display PHY error summary
				0x00008000	display PHY error FFT reports

Radartool parameters (cont.)

Parameter	Format	DA	OL	Description
shownol	radartool -i wifi [0 1] shownol <i>debug_level</i>	Y	Y	Displays the NOL list. Set dfsdebuglevel to 0x2000 before using command
shownolhistory	radartool -i wifi [0 1] shownolhistory	Y	Y	Displays the NOL History. The NOL History is meaningful when the Wi-Fi device supports STA (station) mode DFS. STA mode DFS can be enabled or disabled by using the command: iwpriv wifi[0/1] staDFSEn 1/0. NOL history bit is set for a channel if radar is seen in the channel at least once. The NOL history persists until the wireless driver is removed from the Operating System.

1.5.5 Spectraltool parameters**Table 1-51 Spectraltool parameters**

Parameter	Format	DA	OL	Description
fft_period	spectraltool -i wifiN fft_period <i>val</i>	Y	N	Set skip interval for FFT reports. (<i>Not applicable for 11ac chipsets.</i>)
scan_period	spectraltool -i wifiN scan_period <i>val</i>	Y	Y	Set Spectral Scan period. Period increment resolution is 256*Tclk, where Tclk = 1/44 MHz (Gmode), 1/40 MHz (Amode)
scan_count	spectraltool -i wifiN scan_count <i>val</i>	Y	Y	Set number of reports to return
short_report	spectraltool -i wifiN short_report {1 0}	Y	N	Set to 1 to report only one set of FFT results per spectral_scan_period. (<i>Not applicable for 11ac chipsets.</i>)
priority	spectraltool -i wifiN priority {1 0}	Y	Y	Set priority.
fft_size	spectraltool -i wifiN fft_size <i>val</i>	N	Y	Set the number of FFT data points to compute, defined as a log index: num_fft_pts = 2 ^{fft_size} Value can range from 2 (num_fft_pts=4) to 9 (num_fft_pts=512). (<i>Only for 11ac chipsets</i>)
gc_ena	spectraltool -i wifiN gc_ ena {1 0}	N	Y	Set to enable targeted gain change before starting the spectral scan FFT. (<i>Only for 11ac chipsets</i>)
noise_floor_ref	spectraltool -i wifiN noise_floor_ref <i>val</i>	N	Y	Set noise floor reference number (signed) for the calculation of bin power (dBm). (<i>Only for 11ac chipsets</i>)
init_delay	spectraltool -i wifiN init_delay <i>val</i>	N	Y	Disallow spectral scan triggers after Tx/Rx packets by setting this delay value to roughly SIFS time period or greater. Delay timer counts in units of 0.25 μ s. (<i>Only for 11ac chipsets</i>)
nb_tone_thr	spectraltool -i wifiN nb_tone_thr <i>val</i>	N	Y	Set number of strong bins (inclusive) per sub-channel, below which a signal is declared a narrow band tone. (<i>Only for 11ac chipsets</i>)

Table 1-51 Spectraltool parameters (cont.)

Parameter	Format	DA	OL	Description
str_bin_thr	spectraltool -i wifiN str_bin_thr val	N	Y	Set bin/max_bin ratio threshold over which a bin is declared strong, for spectral scan bandwidth analysis. <i>(Only for 11ac chipsets)</i>
wb_rpt_mode	spectraltool -i wifiN wb_rpt_mode {1/0}	N	Y	Set this to 1 to report spectral scans as EXT_BLOCKER (phy_error=36), if none of the sub-channels are deemed narrow band. <i>(Only for 11ac chipsets)</i>
rss_i_thr	spectraltool -i wifiN rss_i_thr val	N	Y	ADC RSSI must be greater than or equal to this threshold (signed Db) to ensure spectral scan reporting with normal PHY error codes (see rss_i_rpt_mode in this table). <i>(Only for 11ac chipsets)</i>
pwr_format	spectraltool -i wifiN pwr_format {0/1}	N	Y	Format of frequency bin magnitude for spectral scan triggered FFTs. <i>(Only for 11ac chipsets)</i>
				0 linear magnitude
				1 log magnitude (20*log10(lin_mag), 1/2 dB step size)
rpt_mode	spectraltool -i wifiN rpt_mode val	N	Y	Format of per-FFT reports to software for spectral scan triggered FFTs. <i>(Only for 11ac chipsets)</i>
				0 No FFT report (only pulse end summary)
				1 2-dword summary of metrics for each completed FFT
				2 2-dword summary + 1x-oversampled bins (in-band) per FFT
				3 2-dword summary + 2x-oversampled bins (all) per FFT
bin_scale	spectraltool -i wifiN bin_scale val	N	Y	Number of LSBs to shift out to scale the FFT bins for spectral scan triggered FFTs. <i>(Only for 11ac chipsets)</i>
dBm_adj	spectraltool -i wifiN dBm_adj {1/0}	N	Y	Set to 1 (with pwr_format=1), to report bin magnitudes converted to dBm power using the noisefloor calibration results. <i>(Only for 11ac chipsets)</i>
chn_mask	spectraltool -i wifiN chn_mask val	N	Y	Set per chain enable mask to select input ADC for search FFT. <i>(Only for 11ac chipsets)</i>

1.5.6 Intelligent channel manager parameters

ICM is a channel selection application external to the driver. It is intended to provide a number of advantages over the current in-driver ACS, the main ones being flexibility and use of spectral data to identify non-802.11 interferences during channel selection. Future potential benefits include use of historical data, utilization of other radios to speed up scan, and so on. It can be used either standalone, or as a server carrying out scans and ranking for an external entity. We describe only the former below, since the latter functionality is currently for QCA internal use. As at present, ICM is supported only for the AP135 platform from 10.2 onwards.

Since ICM has functionality similar to ACS, the configuration settings are similar to those for ACS. The only difference is that if a channel is set to a static value while ICM is enabled, ICM will still come up and rank the channels for future use with DCS, but it will not set the best channel at bring-up (compared to

ACS, which will not be activated in the first place). Since ICM also interacts with DCS, the DCS settings apply as-is.

We only provide the following additional configurations specific to ICM:

Standalone configuration

```
cfg -a ICM_ENABLE=1
cfg -a ICM_MODE="standalone"
```

ICM_MODE can also be set to "server" (cfg -a ICM_MODE="server"). However, this is currently for QCA internal use only, as noted previously.

1.5.6.1 Enabling selection debug information

In case it is desired to view additional debug information pertaining to the selection process (e.g. number of APs on every channel, Noise floor, Noise floor threshold, presence of various interferer's, etc.), there are two options available: Console prints and CSV dump. The CSV dump is much more detailed than the Console prints.

1.5.6.1.1 Console prints

In case it is desired to view selection debug information on the console, then the ICM debug level should be lowered from 3 to 2 by setting ICM_DEBUG_LEVEL to 2 (The valid values are described in section 1.5.6.2 below – see option '-q' for setting debug level). A table will be printed on the console at the end of each selection algorithm run. Refer to legend printed before table to understand contents. It is highly recommended to disable kernel console prints at this ICM Debug Level, else such prints can pop up in-between and make it hard to understand the tables.

```
echo 0 > /proc/sys/kernel/printk
```

Console print configuration

```
cfg -a ICM_DEBUG_LEVEL=2
```

CSV dump

In case it is desired to view a very detailed selection debug information dump in CSV format, then this can be enabled by setting ICM_ENABLE_SELDEBUG_DUMP to 1.

CSV dump configuration

```
cfg -a ICM_ENABLE_SELDEBUG_DUMP=1
```

The CSV file created is /tmp/icmseldebug.csv. It can be by FTP to the host and viewed in a suitable application such as MS Excel. If the file is already present on the AP when ICM is launched, its contents are first emptied. Information is appended to the file for every run of the selection algorithm. A column titled 'Record Set No.' is updated for every run. Row entries having the same record set number correspond to the same algorithm run.

Note that unlike the ICM Console Print method, this does not require disabling Kernel Prints.

1.5.6.2 ICM command line parameters (debugging only)

ICM is intended to be invoked from a bring-up script such as apup. The command line parameters need not be used directly except for debugging purposes.

NOTE The following ICM command line parameters are only for reference.

Table 1-52 ICM command line parameters

Parameter	Format	Description
-e	icm -e	Run as daemon. By default, non-daemon execution is used.
-f	icm -f	Enable use of Dynamic noise floor
-h	icm -h	Display help
-s	icm -s val	Server mode: Socket type to listen on for messages from external entity. Not applicable for standalone mode. Listed here only for completeness. The default value is 1.
		0 TCP
		1 UDP
-t	icm -t	Enable some internal unit tests. NOTE: This is only for developers. It is not intended for general use. It is mentioned here for completeness. It is disabled
-v	icm -v val	Enable (1) or Disable (0) server mode. It is disabled by default.
-i	icm -i	Dump selection debug information to /tmp/icmseldebug.csv
-q	icm -q val	Set debug level. The default is 3.
		1 Minor
		2 Default
		3 Major
		4 Critical

Table 1-52 ICM command line parameters

Parameter	Format	Description
-u	icm -u val	Set debug module bitmap, formed by O-ring bit positions corresponding to each module. The default is 0xFF.
		0x01 Main
		0x02 Scan
		0x04 Selector
		0x08 Utilities
		0x10 Test
		0x20 Socket
		0x40 Spectral
		0x80 Command

1.5.6.3 ACS/DCS/OBSS enhancements: iwpriv CLI commands

Table 1-53 ACS/DCS/OBSS iwpriv commands

Command	Format	Description
acs_bkscanen	iwpriv wifi1 acs_bkscanen <value>	Bit 1 – Enabled ACS/OBSS background scan depending on the value "acs_ctriflags". Bit 0 – Disables acs/obss background scan timer.
g_acs_bkscanen	iwpriv wifi1 g_acs_bkscanen	ACS/OBSS background scan value
acs_bkscanintvl	iwpriv wifi1 acs_bkscanintvl <value>	Set the background scan value default is one minute
get_acsscanintvl	iwpriv wifi1 get_acsscanintvl	Display the background scan timer value
acs_rssivar	iwpriv wifi1 acs_rssivar <value>	Set the RSSI variance. Used for ignoring the difference between two channel. If the two channel differ with value less then rssivar then both channel are considered as having same RSSI Default Value: 30
g_acs_rssivar	g_acs_rssivar	Display RSSI variance value
acs_chloadvar	iwpriv wifi1 acs_chloadvar <value>	Set the channel load variance If two channel differ with channel load value less then ch load variance .They are treated as having same channel load for next level evaluation Default Value: 20
acs_lmtobss	iwpriv wifi1 acs_lmtobss 1	Enable limited BSS check.
get_acslmtobss	iwpriv wifi1 get_acslmtobss <value>	Status of limited BSS check enable/disable

Table 1-53 ACS/DCS/OBSS iwpriv commands

Command	Format	Description
acs_ctrlflags	iwpriv wifi1 acs_ctrlflags 0xx	Back ground scan ACS control flags 0x1 – Full ACS check 0x2 -Only OBSS check this is used for manual configuration of channel.
getacsctrlflags	iwpriv wifi1 getacsctrlflags <value>	Get value of ACS control flag set
acs_dbgtrace	iwpriv wifi1 acs_dbgtrace 0xxx	Set ACS run time debug option The values signify EACS_DBG_DEFAULT 0x1 EACS_DBG_FUNC 0x8000 EACS_DBG_CHLOAD 0x4 EACS_DBG_RSSI 0x80 EACS_DBG_OBSS 0x100 EACS_DBG_REGPOWER 0x200 EACS_DBG_NF 0x400 EACS_DBG_SCAN 0x800 EACS_DBG_ADJCH 0x1000
g_acs_dbgtrace	lwpriv wifi1 g_acs_dbgtrace	Display the debug option specified

1.5.7 UCI Wireless configuration (qca-wifi)

The UCI commands listed in this section are applicable only to AP 10.2.3 and later software versions. For details of UCI, visit <http://wiki.openwrt.org/doc/uci>.

QSDK supports qca-wifi driver natively. The UCI database section to configure is called *wireless*. It can be accessed using the following command:

```
uci show wireless
```

This command will show the whole wireless section; it will be organized in the following subsection:

- **radioN:** a radio subsection represents an actual radio hardware. One subsection will be initialized per-radio during the first boot. This sub-section contains configuration parameters such as mode (11n, 11ac...), channel (1, 6 11, 36...).
- **wifi-iface[N]:** a wifi-iface section represents a Wi-Fi VAP. It supports configuration parameters such as SSID, shortgi, and so on. The underlying radio interface is specified using the configuration item *device*. It should refer to a radioN section as specified above.

The driver will create the wifiN interface at init time, and the initial boot sequence will use /sys to detect these network devices and populate the UCI database accordingly.

When enabling a wifi interface, the driver will read the UCI database, and create VAPs interface using wlanconfig - one per wifi-iface subsection.

The interface names will use the following convention:

- for radio 0, the vap network devices will be called: ath0, ath01, ath02, ath03...
- for radio 1, the vap network devices will be called: ath1, ath11, ath12, ath13...

If more than 10 VAPs are create, numbering will continue as expected: ath010/ath011/ath012... for radio 0, and ath110/ath111/ath112... for radio 1.

Table 1-54 Per-VAP configuration parameters

Parameter	Format	Description
scanband	uci set wireless.@wifi-iface[0].scanband=1	ALL (0), 2G_ONLY (1), 5G_ONLY (2).
periodicScan	uci set wireless.@wifi-iface[0].periodicScan=18000	This command sets support of sta periodic scan. 0 is disable and other value is enable. If the value is less than 30000, it will be set to 30000.
nawds_mode	uci set wireless.@wifi-iface[0].nawds_mode=3	DISABLED = 0, STATIC_REPEATER = 1, STATIC_BRIDGE = 2, LEARNING_REPEATER = 3, LEARNING_BRIDGE = 4.
nawds_override	uci set wireless.@wifi-iface[0].nawds_override=00:03:7F:10:00:86	When disabled, no more MAC entry can be added to the NAWDS list when the list is full. If enabled, new MAC entry will override the dead NAWDS AP entry.
nawds_add_repeater	uci add_list wireless.@wifi-iface[0].nawds_add_repeater='00:03:7F:10:00:85 0x1'	Adds nawds repeater mac address with its capabilities into the list. More than one can be added.

Table 1-54 Per-VAP configuration parameters (cont.)

Parameter	Format	Description
nawds_defcaps	uci set wireless.@wifi- iface[0].nawds_ defcaps=0x2	Set the default capability for nawds mode. HT20(0x1), HT2040(0x2), DS(0x4) .
nawds_del_repeater	uci set wireless.@wifi- iface[0].nawds_del_ repeater=00:03:7F:10:0 0:85	Remove the nawds repeater MAC from the nawds list.

1.5.7.1 Example UCI Configurations

11ac Open mode

```
uci set wireless.wifi0=wifi-device
uci set wireless.wifi0.type=qcawifi
uci set wireless.wifi0.macaddr=00:60:02:00:c9:c9
uci set wireless.wifi0.hwmode=11ac
uci set wireless.wifi0.disabled=0
uci set wireless.wifi0.htmode=HT80
uci set wireless.wifi0.channel=100
uci set wireless.wifi0.txchainmask=15
uci set wireless.wifi0.rxchainmask=15
uci set wireless.wifi0.mode=ap
uci set wireless.@wifi-iface[0]=wifi-iface
uci set wireless.@wifi-iface[0].device=wifi0
uci set wireless.@wifi-iface[0].network=lan
uci set wireless.@wifi-iface[0].mode=ap
uci set wireless.@wifi-iface[0].ssid=5g_open
uci set wireless.@wifi-iface[0].encryption=none
uci commit wireless
```

11ac WPA2-PSK

```
uci set wireless.wifi0=wifi-device
uci set wireless.wifi0.type=qcawifi
uci set wireless.wifi0.macaddr=00:60:02:00:c9:c9
uci set wireless.wifi0.hwmode=11ac
uci set wireless.wifi0.disabled=0
uci set wireless.wifi0.htmode=HT80
uci set wireless.wifi0.channel=100
uci set wireless.wifi0.txchainmask=15
uci set wireless.wifi0.rxchainmask=15
uci set wireless.wifi0.mode=ap
uci set wireless.@wifi-iface[0]=wifi-iface
uci set wireless.@wifi-iface[0].device=wifi0
uci set wireless.@wifi-iface[0].network=lan
uci set wireless.@wifi-iface[0].mode=ap
uci set wireless.@wifi-iface[0].ssid=5g_wpa2
uci set wireless.@wifi-iface[0].encryption=psk2+ccmp
uci set wireless.@wifi-iface[0].key=12345678
uci commit wireless
```

For other WPA2 security modes replace encryption type

```
uci set wireless.@wifi-iface[0].encryption=psk2+ccmp
uci set wireless.@wifi-iface[0].encryption=psk2+ccmp-256
uci set wireless.@wifi-iface[0].encryption=psk2+gcmp
uci set wireless.@wifi-iface[0].encryption=psk2+gcmp-256
```

For WPA-PSK security mode replace encryption type

```
uci set wireless.@wifi-iface[0].encryption=tkip
```

For PMF(protected management frames) enabled AP

```
uci set wireless.wifi0=wifi-device
uci set wireless.wifi0.type=qcawifi
uci set wireless.wifi0.macaddr=00:60:02:00:c9:c9
uci set wireless.wifi0.hwmode=11ac
uci set wireless.wifi0.disabled=0
uci set wireless.wifi0.htmode=HT80
uci set wireless.wifi0.channel=100
uci set wireless.wifi0.txchainmask=15
uci set wireless.wifi0.rxchainmask=15
uci set wireless.wifi0.mode=ap
uci set wireless.@wifi-iface[0]=wifi-iface
uci set wireless.@wifi-iface[0].device=wifi0
uci set wireless.@wifi-iface[0].network=lan
uci set wireless.@wifi-iface[0].mode=ap
uci set wireless.@wifi-iface[0].ssid=5g_pmf
uci set wireless.@wifi-iface[0].encryption=psk2+ccmp
uci set wireless.@wifi-iface[0].key=12345678
uci set wireless.@wifi-iface[0].ieee80211w=2
uci set wireless.@wifi-iface[0].group_mgmt_cipher=AES-128-CMAC
uci commit wireless
```

For enabling BIP CMAC/GMAC

```
uci set wireless.@wifi-iface[0].group_mgmt_cipher=AES-128-CMAC
uci set wireless.@wifi-iface[0].group_mgmt_cipher=BIP-GMAC-128
uci set wireless.@wifi-iface[0].group_mgmt_cipher=BIP-GMAC-256
uci set wireless.@wifi-iface[0].group_mgmt_cipher=BIP-CMAC-256
```

WEP security configuration

```
uci set wireless.wifi0=wifi-device
uci set wireless.wifi0.type=qcawifi
uci set wireless.wifi0.macaddr=00:60:02:00:c9:c9
uci set wireless.wifi0.hwmode=11ac
uci set wireless.wifi0.disabled=0
uci set wireless.wifi0.htmode=HT80
uci set wireless.wifi0.channel=100
uci set wireless.wifi0.txchainmask=15
uci set wireless.wifi0.rxchainmask=15
uci set wireless.wifi0.mode=ap
uci set wireless.@wifi-iface[0]=wifi-iface
uci set wireless.@wifi-iface[0].device=wifi0
uci set wireless.@wifi-iface[0].network=lan
uci set wireless.@wifi-iface[0].mode=ap
uci set wireless.@wifi-iface[0].ssid=5g_wep
uci set wireless.@wifi-iface[0].encryption=wep
```



```
uci set wireless.@wifi-iface[0].key1=1111111111
uci set wireless.@wifi-iface[0].key2=2222222222
uci set wireless.@wifi-iface[0].key3=3333333333
uci set wireless.@wifi-iface[0].key4=4444444444
uci set wireless.@wifi-iface[0].key=3
uci commit wireless
```

For WEP+Shared configuration, change encryption type

```
uci set wireless.@wifi-iface[0].encryption=wep+shared
```

WAPI security configuration

```
uci set wireless.wifi0=wifi-device
uci set wireless.wifi0.type=qcawifi
uci set wireless.wifi0.macaddr=00:60:02:00:c9:c9
uci set wireless.wifi0.hwmode=11ac
uci set wireless.wifi0.disabled=0
uci set wireless.wifi0.htmode=HT80
uci set wireless.wifi0.channel=100
uci set wireless.wifi0.txchainmask=15
uci set wireless.wifi0.rxchainmask=15
uci set wireless.wifi0.mode=ap
uci set wireless.@wifi-iface[0]=wifi-iface
uci set wireless.@wifi-iface[0].device=wifi0
uci set wireless.@wifi-iface[0].network=lan
uci set wireless.@wifi-iface[0].mode=ap
uci set wireless.@wifi-iface[0].ssid=5g_wapi
uci set wireless.@wifi-iface[0].encryption=wapi-psk
uci set wireless.@wifi-iface[0].key=12345678
uci commit wireless
```

1.5.7.2 QWRAP configuration (basic)

QWRAP per radio configuration

```
uci set wireless.wifi0.channel=36
uci set wireless.wifi0.qwrap_enable=1
uci set wireless.wifi0.wlanaddr='00:00:00:00:00:00'
uci set wireless.wifi0.disabled=0
```

QWRAP 'wrap' interface

```
uci set wireless.@wifi-iface[0].mode=wrap
uci set wireless.@wifi-iface[0].ssid=QWRAP_ROOT2
uci set wireless.@wifi-iface[0].encryption=psk2+ccmp
uci set wireless.@wifi-iface[0].key=1234567890abcdexyz
uci set wireless.@wifi-iface[0].wpa_group_rekey=2000
uci set wireless.@wifi-iface[0].device=wifi0
uci set wireless.@wifi-iface[0].network=lan
uci set wireless.@wifi-iface[0].vap_ind=1
```

QWRAP 'sta' interface

```
uci add wireless wifi-iface
uci set wireless.@wifi-iface[1].mode=sta
uci set wireless.@wifi-iface[1].device=wifi0
uci set wireless.@wifi-iface[1].network=lan
```

```
uci set wireless.@wifi-iface[1].encryption=psk2+ccmp
uci set wireless.@wifi-iface[1].key=1234567890abcdexyz
uci set wireless.@wifi-iface[1].wpa_group_rekey=2000
uci set wireless.@wifi-iface[1].ssid=QWRAP_ROOT1

uci commit wireless
uci export wireless
wifi
```

1.5.7.3 QWRAP configuration (DBDC)

QWRAP DBDC configuration 1

```
rm -rf /etc/config/wireless
wifi detect > /etc/config/wireless

uci set wireless.wifi1=wifi-device
uci set wireless.wifi0.type=qcawifi
uci set wireless.wifi0.channel=36
uci set wireless.wifi0.macaddr=8c:fd:f0:24:fa:d7
uci set wireless.wifi0.hwmode=11ac
uci set wireless.wifi0.qwrap_dbdc_enable=1
uci set wireless.@wifi-iface[0]=wifi-iface
uci set wireless.@wifi-iface[0].device=wifi0
uci set wireless.@wifi-iface[0].network=lan
uci set wireless.@wifi-iface[0].mode=ap
uci set wireless.@wifi-iface[0].ssid=kris
uci set wireless.@wifi-iface[0].encryption=psk2+ccmp
uci set wireless.@wifi-iface[0].key=12345678
uci set wireless.@wifi-iface[0].qwrap_ap=1
uci set wireless.wifi1=wifi-device
uci set wireless.wifi1.type=qcawifi
uci set wireless.wifi1.channel=6
uci set wireless.wifi1.macaddr=8c:fd:f0:24:fa:d8
uci set wireless.wifi1.wlanaddr=00:00:00:00:00:00
uci set wireless.wifi1.hwmode=11ng
uci set wireless.wifi1.qwrap_enable=1
uci set wireless.@wifi-iface[1]=wifi-iface
uci set wireless.@wifi-iface[1].device=wifi1
uci set wireless.@wifi-iface[1].network=lan
uci set wireless.@wifi-iface[1].mode=sta
uci set wireless.@wifi-iface[1].ssid=kris_bee
uci set wireless.@wifi-iface[1].encryption=psk2+ccmp
uci set wireless.@wifi-iface[1].key=12345678
```

QWRAP DBDC configuration 2

```
rm -rf /etc/config/wireless
wifi detect > /etc/config/wireless

uci set wireless.wifi0=wifi-device
uci set wireless.wifi0.type=qcawifi
uci set wireless.wifi0.channel=36
uci set wireless.wifi0.macaddr=8c:fd:f0:24:fa:d8
uci set wireless.wifi0.hwmode=11ac
uci set wireless.wifi0.qwrap_enable=1
```

```
uci set wireless.@wifi-iface[0]=wifi-iface
uci set wireless.@wifi-iface[0].device=wifi0
uci set wireless.@wifi-iface[0].network=lan
uci set wireless.@wifi-iface[0].mode=ap
uci set wireless.@wifi-iface[0].ssid=dbdc-ap1
uci set wireless.@wifi-iface[0].encryption=psk2+ccmp
uci set wireless.@wifi-iface[0].key=12345678
uci set wireless.@wifi-iface[0].qwrap_ap=1

uci add wireless wifi-iface
uci set wireless.@wifi-iface[1]=wifi-iface
uci set wireless.@wifi-iface[1].device=wifi0
uci set wireless.@wifi-iface[1].network=lan
uci set wireless.@wifi-iface[1].mode=sta
uci set wireless.@wifi-iface[1].ssid=kris_bee
uci set wireless.@wifi-iface[1].encryption=psk2+ccmp
uci set wireless.@wifi-iface[1].key=12345678

uci set wireless.wifi1=wifi-device
uci set wireless.wifi1.type=qcawifi
uci set wireless.wifi1.channel=11
uci set wireless.wifi1.macaddr=8c:fd:f0:24:fa:d7
uci set wireless.wifi1.hwmode=11ng
uci set wireless.wifi1.qwrap_dbdc_enable=1

uci set wireless.@wifi-iface[2]=wifi-iface
uci set wireless.@wifi-iface[2].device=wifi1
uci set wireless.@wifi-iface[2].network=lan
uci set wireless.@wifi-iface[2].mode=wrap
uci set wireless.@wifi-iface[2].ssid=dbdc-ap2
uci set wireless.@wifi-iface[2].encryption=psk2+ccmp
uci set wireless.@wifi-iface[2].key=12345678
uci set wireless.@wifi-iface[2].qwrap_ap=1
```

1.5.7.4 Band steering configuration commands

NOTE This section is applicable only to the version 10.2.4 and above.

To start the load balancing daemon, you first need to enable the load balancing feature either via UCI or from the web interface.

To enable and start it via UCI, use the following commands:

```
uci set lbd.@config[0].Enable=1 uci commit lbd
/etc/init.d/lbd start
```

If there is no UCI or web interface, lbd daemon can be manually started with a configuration file.

Following are the paramters can be updated in lbd configuration file.

- Enable ACS on VAP for all Radios.
- ```
iwconfig <vap> channel 0
```

■ Start lbd daemon

```
lbd -d -C lbd.conf
```

**NOTE** All VAP interfaces need to be added in the lbd.conf file

Following are the parameters can be updated in lbd configuration file.

**Table 1-55 Parameters in the configuration file**

| Configuration file | Section | Options       | Description                                                         | Default |
|--------------------|---------|---------------|---------------------------------------------------------------------|---------|
| config             | config  | Enable        | Whether the load balancing logics is enabled or not                 | 0       |
| config             | config  | Matching SSID | The SSID to match when limiting band steering to only a single SSID |         |

**Table 1-56 Parameters in the configuration file**

| Configuration file | Section  | Option                 | Description                                                                                                                    | Default |
|--------------------|----------|------------------------|--------------------------------------------------------------------------------------------------------------------------------|---------|
| WlanIF             | WlanIF2G | InactIdleThreshold     | Number of seconds for the inactivity value under no overload conditions on 2.4 GHz Wi-Fi                                       | 60      |
| WlanIF             | WlanIF2G | InactOverloadThreshold | Number of seconds for the inactivity value when 2.4 GHz band is overloaded                                                     | 30      |
| WlanIF             | WlanIF2G | InactCheckInterval     | How frequently (in seconds) to check for inactive associated STAs on 2.4 GHz                                                   | 10      |
| WlanIF             | WlanIF2G | RSSISteeringPoint      | The point at which the measured or estimated RSSI on 2.4 GHz dictates a node associated on 5 GHz should be steered to 2.4 GHz. | 20      |
| WlanIF             | WlanIF2G | LowRSSIXingThreshold   | RSSI threshold to generate an indication when a client crosses it (in dB)                                                      | 10      |
| WlanIF             | WlanIF2G | MUCheckInterval        | How frequently (in seconds) to check the medium utilization on 2.4 GHz                                                         | 10      |

**Table 1-56 Parameters in the configuration file**

| Configuration file | Section  | Option                 | Description                                                                                                                 | Default |
|--------------------|----------|------------------------|-----------------------------------------------------------------------------------------------------------------------------|---------|
| WlanIF             | WlanIF2G | MUAvgPeriod            | Number of seconds to average before generating a new utilization report on 2.4 GHz                                          | 300     |
| WlanIF             | WlanIF2G | InactCheckInterval     | How frequently (in seconds) to check for inactive associated STAs on 2.4 GHz                                                | 10      |
| WlanIF             | WlanIF5G | InactIdleThreshold     | Number of seconds for the inactivity value under no overload conditions on 5 GHz Wi-Fi                                      | 60      |
| WlanIF             | WlanIF5G | InactOverloadThreshold | Number of seconds for the inactivity value when 5 GHz band is overloaded                                                    | 30      |
| WlanIF             | WlanIF5G | RSSISteeringPoint      | The point at which the measured or estimated RSSI on 5 GHz dictates a node associated on 2.4 GHz should be steered to 5 GHz | 30      |
| WlanIF             | WlanIF5G | LowRSSIXingThreshold   | RSSI threshold to generate an indication when a client crosses it (in dB)                                                   | 10      |
| WlanIF             | WlanIF5G | MUCheckInterval        | How frequently (in seconds) to check the medium utilization on 5 GHz                                                        | 10      |
| WlanIF             | WlanIF5G | MUAvgPeriod            | Number of seconds to average before generating a new utilization report on 5 GHz                                            | 300     |
| WlanIF             | WlanIF5G | InactCheckInterval     | How frequently (in seconds) to check for inactive associated STAs on 5 GHz                                                  | 10      |
| StaDB              | StaDB    | IncludeOutOfNetwork    | Whether out of network devices should be included in the database or not.                                                   | 1       |

**Table 1-56 Parameters in the configuration file**

| Configuration file | Section    | Option                | Description                                                                                                                                                                                                      | Default               |
|--------------------|------------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| StaDB              | StaDB      | AgingSizeThershold    | The number of entries allowed in the station database before periodic aging is triggered.                                                                                                                        | 100                   |
| StaDB              | StaDB      | AgingFrequency        | Once aging is triggered, how frequently (in seconds) to perform aging of the station database.                                                                                                                   | 60                    |
| StaDB              | StaDB      | OutOfNetworkMaxAge    | The number of seconds that must elapse since the last update for an out-of-network entry before it is considered too old and is removed from the database.                                                       | 300                   |
| StaDB              | StaDB      | InNetworkMaxAge       | The number of seconds that must elapse since the last update for an in-network entry before it is considered too old and is removed from the database. Only unassociated entries will be considered for removal. | 259200<br>0 (30 days) |
| StaMonitor         | StaMonitor | RSSIMeasureSamples_W2 | Number of RSSI measurements to average using NDP before generating a RSSI report on 2.4 GHz                                                                                                                      | 5                     |
| StaMonitor         | StaMonitor | RSSIMeasureSamples_W5 | Number of RSSI measurements to average using NDP before generating a RSSI report on 5 GHz                                                                                                                        | 5                     |
| StaMonitor         | StaMonitor | RSSIDiff_EstW5FromW2  | Difference when estimate 5 GHz RSSI value from the one measured on 2.4 GHz                                                                                                                                       | -20                   |

**Table 1-56 Parameters in the configuration file**

| Configuration file | Section      | Option                       | Description                                                                                                                      | Default |
|--------------------|--------------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------|---------|
| StaMonitor         | StaMonitor   | RSSIDiff_EstW2FromW5         | Difference when estimate 2.4 GHz RSSI value from the one measured on 5 GHz                                                       | 10      |
| StaMonitor         | StaMonitor   | RSSIAgeLimit                 | Maximum number of seconds elapsed allowed for a "recent" RSSI measurement                                                        | 5       |
| BandMonitor        | BandMonit or | MUSlightOverloadThreshold_W2 | Medium utilization threshold (in percentage) for a slight overload condition on 2.4 GHz                                          | 70      |
| BandMonitor        | BandMonit or | MUHeavyOverloadThreshold_W2  | Medium utilization threshold (in percentage) for a heavy overload condition on 2.4 GHz                                           | 80      |
| BandMonitor        | BandMonit or | MUSlightOverloadThreshold_W5 | Medium utilization threshold (in percentage) for a slight overload condition on 5 GHz                                            | 70      |
| BandMonitor        | BandMonit or | MUHeavyOverloadThreshold_W5  | Medium utilization threshold (in percentage) for a heavy overload condition on 5 GHz                                             | 80      |
| BandMonitor        | BandMonit or | MUReserve_W5                 | Percentage of the medium that is reserved on 5 GHz for high bandwidth / strict QoS devices (like STBs)                           | 0       |
| BandMonitor        | BandMonit or | RSSIMaxAge                   | The maximum age (in seconds) for an RSSI measurement before it is considered too old to make a pre-association steering decision | 5       |
| SteerExec          | SteerExec    | SteeringProhibitTime         | Number of seconds to wait prior to steering the client again after a steering                                                    | 300     |
| SteerExec          | SteerExec    | TSteering                    | Number of seconds allowed for the client to reconnect before AP aborts steering                                                  | 15      |

**Table 1-56 Parameters in the configuration file**

| Configuration file | Section   | Option                     | Description                                                                                                   | Default       |
|--------------------|-----------|----------------------------|---------------------------------------------------------------------------------------------------------------|---------------|
| SteerExec          | SteerExec | InitialAuthRejCoalesceTime | Number of seconds to coalesce multiple authentication rejects down to a single 1                              | 2             |
| SteerExec          | SteerExec | AuthRejMax                 | The number of consecutive authentication rejects that cause the device to be marked as steering unfriendly    | 3             |
| SteerExec          | SteerExec | SteeringUnfriendlyTime     | The amount of time a device is considered steering unfriendly before another attempt.                         | 600           |
| SteerExec          | SteerExec | TargetLowRSSIThreshold_W2  | RSSI threshold (in dB) indicating 2.4 GHz band is not strong enough for association                           | 15            |
| SteerExec          | SteerExec | TargetLowRSSIThreshold_W5  | RSSI threshold (in dB) indicating 5 GHz band is not strong enough for association                             | 15            |
| SteerExec          | SteerExec | BlacklistTime              | The amount of time (in seconds) before automatically removing the blacklist (independent of RSSI conditions). | 86400 (1 day) |



### 1.5.7.5 Band steering configuration commands for CFG

1. When the command 'apup' is issued, the lbd.conf generates and the lbd daemon will start running.
2. lbd daemon stops running after issuing 'apdown'
3. The following [Table 1-57](#), shows the configuration options for CFG commands corresponding to UCI commands
4. The configuration value is assigned using "cfg -a"
5. The configuration value is saved using "cfg -c"
6. All the configurations is listed using "cfg -s"
7. Configurations will be reset using "cfg -x"

Ex: cfg -a BS\_ENABLE=1 → Enable the Band Steering Option

cfg -c → save the option

cfg -s | grep BS\_ENABLE → show all the configs

Then issue the commands, 'apdown' and 'apup'

**Table 1-57 Parameters for the CFG**

| Configuration Type | UCI Option             | CFG Option                  | Description                                                                                                                    |
|--------------------|------------------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Config             | Enable                 | BS_ENABLE                   | Whether the Band Steering logic is enabled or not                                                                              |
| Config             | MatchingSSID           | BS_MATCHING_SSID            | The SSID to match when limiting band steering to only a single SSID.                                                           |
| WlanIF             | InactIdleThreshold     | BS_2G_INACTIDLETHRESHOLD    | Number of seconds for the inactivity value under no overload conditions on 2.4 GHz Wi-Fi                                       |
| WlanIF             | InactOverloadThreshold | BS_2G_INACTOVERLOADTHRESHLD | Number of seconds for the inactivity value when 2.4 GHz band is overloaded                                                     |
| WlanIF             | RSSISTeeringPoint      | BS_2G_RSSISTEERINGPOINT     | The point at which the measured or estimated RSSI on 2.4 GHz dictates a node associated on 5 GHz should be steered to 2.4 GHz. |
| WlanIF             | LowRSSIXingThreshold   | BS_2G_LOWRSSIXINGTHRESHLD   | RSSI threshold to generate an indication when a client crosses it (in dB)                                                      |
| WlanIF             | MUCheckInterval        | BS_2G_MUCHECKINTERVAL       | How frequently (in seconds) to check the medium utilization on 2.4 GHz                                                         |
| WlanIF             | MUAvgPeriod            | BS_2G_MUAVGPERIOD           | Number of seconds to average before generating a new utilization report on 2.4 GHz                                             |

**Table 1-57 Parameters for the CFG**

|           |                        |                                |                                                                                                                                                                                                                  |
|-----------|------------------------|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WlanIF    | InactCheckInterval     | BS_2G_INACTCHECKINTERVAL       | How frequently (in seconds) to check for Inactive associated STAs on 2.4 GHz                                                                                                                                     |
| WlanIF    | InactIdleThreshold     | BS_5G_INACTIDLETHRESHOLD       | Number of seconds for the inactivity value under no overload conditions on 5GHz Wi-Fi                                                                                                                            |
| WlanIF    | InactOverloadThreshold | BS_5G_INACTOVERLOADTHRESHOLD   | Number of seconds for the inactivity value when 5 GHz band is overloaded                                                                                                                                         |
| WlanIF    | RSSISteeringPoint      | BS_5G_RSSISTEERINGPOINT        | The point at which the measured or estimated RSSI on 5 GHz dictates a node associated on 2.4 GHz should be steered to 5 GHz.                                                                                     |
| WlanIF    | LowRSSIXingThreshold   | BS_5G_LOWRSSIXINGTHRESHOLD     | RSSI threshold to generate an indication when a client crosses it (in dB)                                                                                                                                        |
| WlanIF    | MUCheckInterval        | BS_5G_MUCHECKINTERVAL          | How frequently (in seconds) to check the medium utilization on 5 GHz                                                                                                                                             |
| WlanIF    | MUAvgPeriod            | BS_5G_MUAVGPERIOD              | Number of seconds to average before generating a new utilization report on 5 GHz                                                                                                                                 |
| WlanIF    | InactCheckInterval     | BS_5G_INACTCHECKINTERVAL       | How frequently (in seconds) to check for Inactive associated STAs on 5 GHz                                                                                                                                       |
| StaDB     | IncludeOutOfNetwork    | BS_STADB_INCLUDEOUTOFNETWORK   | Whether out of network devices should be included in the database or not                                                                                                                                         |
| StaDB_Adv | AgingSizeThershold     | BS_STADBADV_AGINGSIZETHRESHOLD | The number of entries allowed in the station database before periodic aging is triggered.                                                                                                                        |
| StaDB_Adv | AgingFrequency         | BS_STADBADV_AGINGFREQUENCY     | Once aging is triggered, how frequently (seconds) to perform aging of the station database.                                                                                                                      |
| StaDB_Adv | OutOfNetworkMaxAge     | BS_STADBADV_OUTOFNETWORKMAXAGE | The number of seconds that must elapse since the last update for an out-of-network entry before it is considered too old and is removed from the database.                                                       |
| StaDB_Adv | InNetworkMaxAge        | BS_STADBADV_INNETWORKMAXAGE    | The number of seconds that must elapse since the last update for an in-network entry before it is considered too old and is removed from the database. Only unassociated entries will be considered for removal. |

**Table 1-57 Parameters for the CFG**

|             |                              |                                 |                                                                                                                                                                        |
|-------------|------------------------------|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| StaDB_Adv   | ProbeMaxInterval             | BS_STADBADV_PROBEMAXINTERVAL    | The maximum amount of time (in seconds) between two consecutive probe requests for them to be grouped together in determining the average probe RSSI.                  |
| StaMonitor  | RSSIMeasureSamples_W2        | BS_STAMON_RSSIMEASURESAMPLES_W2 | Number of RSSI measurements to average using NDP before generating a RSSI report on 2.4 GHz                                                                            |
| StaMonitor  | RSSIMeasureSamples_W5        | BS_STAMON_RSSIMEASURESAMPLES_W5 | Number of RSSI measurements to average using NDP before generating a RSSI report on 5 GHz                                                                              |
| StaMonitor  | RSSIDiff_EstW5FromW2         | BS_STAMON_RSSIDIFF_ESTW5FROMW2  | Difference when estimate 5 GHz RSSI value from the one measured on 2.4 GHz                                                                                             |
| StaMonitor  | RSSIDiff_EstW2FromW5         | BS_STAMON_RSSIDIFF_ESTW2FROMW5  | Difference when estimate 2.4 GHz RSSI value from the one measured on 5 GHz                                                                                             |
| StaMonitor  | RSSIAgeLimit                 | BS_STAMON_RSSIAGELIMIT          | Maximum number of seconds elapsed allowed for a 'recent' RSSI measurement                                                                                              |
| StaMonitor  | ProbeCountThreshold          | BS_STAMON_PROBECOUNTTHRESHOLD   | The number of consecutive probe request RSSI values that must be available to consider using the average RSSI on the unassociated band when making steering decisions. |
| BandMonitor | MUSlightOverloadThreshold_W2 | BS_BM_MUSLI8OVERLOADTHRESHLDW2  | Medium utilization threshold (in percentage) for a slight overload condition on 2.4 GHz                                                                                |
| BandMonitor | MUHeavyOverloadThreshold_W2  | BS_BM_MUHEAVYOVERLOADTHRESHLDW2 | Medium utilization threshold (in percentage) for a heavy overload condition on 2.4 GHz                                                                                 |
| BandMonitor | MUSlightOverloadThreshold_W5 | BS_BM_MUSLI8OVERLOADTHRESHLDW5  | Medium utilization threshold (in percentage) for a slight overload condition on 5 GHz                                                                                  |
| BandMonitor | MUHeavyOverloadThreshold_W5  | BS_BM_MUHEAVYOVERLOADTHRESHLDW5 | Medium utilization threshold (in percentage) for a heavy overload condition on 5 GHz                                                                                   |
| BandMonitor | MUReserve_W5                 | BS_BANDMON_MURESERVE_W5         | Percentage of the medium that is reserved on 5 GHz for high bandwidth / strict QoS devices (like STBs)                                                                 |

**Table 1-57 Parameters for the CFG**

|             |                             |                                 |                                                                                                                                                               |
|-------------|-----------------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BandMonitor | RSSIMaxAge                  | BS_BANDMON_RSSIMAXAGE           | The maximum age (in seconds) for an RSSI measurement before it is considered too old to make a pre-association steering decision.                             |
| BandMonitor | ProbeCountThreshold         | BS_BANDMON_PROBECOUNTTHRESHOLD  | The number of consecutive probe request RSSI values that must be available to consider using the average RSSI when making pre-association steering decisions. |
| SteerExec   | SteeringProhibitTime        | BS_SE_STEERINGPROHIBITTIME      | Number of seconds to wait prior to steering the client again after a steering                                                                                 |
| SteerExec   | TSteering                   | BS_SE_TSTEERING                 | Number of seconds allowed for the client to reconnect before AP aborts Steering                                                                               |
| SteerExec   | InitialAuthRejCoalesce Time | BS_SE_INITAUTHREJCOALESCETIME   | Number of seconds to coalesce multiple authentication rejects down to a single 1                                                                              |
| SteerExec   | AuthRejMax                  | BS_SE_AUTHREJMAX                | The number of consecutive authentication rejects that cause the device to be marked as steering unfriendly                                                    |
| SteerExec   | SteeringUnfriendlyTime      | BS_SE_STEERINGUNFRIENDLYTIME    | The amount of time a device is considered steering unfriendly before another attempt.                                                                         |
| SteerExec   | TargetLowRSSIThreshold_W2   | BS_SE_TARGETLOWRSSITHRESHOLD_W2 | RSSI threshold (in dB) indicating 2.4 GHz band is not strong enough for association                                                                           |
| SteerExec   | TargetLowRSSIThreshold_W5   | BS_SE_TARGETLOWRSSITHRESHOLD_W5 | RSSI threshold (in dB) indicating 5 GHz band is not strong enough for association                                                                             |
| SteerExec   | BlacklistTime               | BS_SE_BLACKLISTTIME             | The amount of time (in seconds) before automatically removing the blacklist (independent of RSSI conditions).                                                 |

## 1.5.8 UCI command to enable ATF

Execute the following UCI commands to enable ATF. These commands would add a module param 'atf\_mode' to umac module to enable/disable the ATF feature.

**NOTE** These commands are available only in openwrt build environment.

Implement similar commands to enable ATF on solutions using other build environments (for example, buildroot).

```
uci set wireless.qcawifi=qcawifi
uci set wireless.qcawifi.atf_mode=1
```

# A Country Code Definitions

---

Table A-1 identifies the country definition, country string, and country code used to set the country ID for 802.11d and regulatory requirements.

**Table A-1 Country code definitions**

| Country definition     | Country string | Country ID |
|------------------------|----------------|------------|
| CTRY_DEBUG             | DB             | 0          |
| CTRY_DEFAULT           | NA             | 0          |
| CTRY_ALBANIA           | AL             | 8          |
| CTRY_ALGERIA           | DZ             | 12         |
| CTRY_ARGENTINA         | AR             | 32         |
| CTRY_ARMENIA           | AM             | 51         |
| CTRY_AUSTRALIA         | AU             | 36         |
| CTRY_AUSTRALIA2        | AU             | 5000       |
| CTRY_AUSTRIA           | AT             | 40         |
| CTRY_AZERBAIJAN        | AZ             | 31         |
| CTRY_BAHRAIN           | BH             | 48         |
| CTRY_BELARUS           | BY             | 112        |
| CTRY_BELGIUM           | BE             | 56         |
| CTRY_BELGIUM2          | BE             | 5002       |
| CTRY_BELIZE            | BZ             | 84         |
| CTRY_BOLIVIA           | BO             | 68         |
| CTRY_BOSNIA_HERZ       | BA             | 70         |
| CTRY_BRAZIL            | BR             | 76         |
| CTRY_BRUNEI_DARUSSALAM | BN             | 96         |
| CTRY_BULGARIA          | BG             | 100        |
| CTRY_CANADA            | CA             | 124        |
| CTRY_CANADA2           | CA             | 5001       |
| CTRY_CHILE             | CL             | 152        |
| CTRY_CHINA             | CN             | 156        |
| CTRY_COLOMBIA          | CO             | 170        |
| CTRY_COSTA_RICA        | CR             | 188        |
| CTRY_CROATIA           | HR             | 191        |

**Table A-1 Country code definitions (cont.)**

| Country definition      | Country string | Country ID |
|-------------------------|----------------|------------|
| CTRY_CYPRUS             | CY             | 196        |
| CTRY_CZECH              | CZ             | 203        |
| CTRY_DENMARK            | DK             | 208        |
| CTRY_DOMINICAN_REPUBLIC | DO             | 214        |
| CTRY_ECUADOR            | EC             | 218        |
| CTRY_EGYPT              | EG             | 818        |
| CTRY_EL_SALVADOR        | SV             | 222        |
| CTRY_ESTONIA            | EE             | 233        |
| CTRY_FAEROE_ISLANDS     | FO             | 234        |
| CTRY_FINLAND            | FI             | 246        |
| CTRY_FRANCE             | FR             | 250        |
| CTRY_GEORGIA            | GE             | 268        |
| CTRY_GERMANY            | DE             | 276        |
| CTRY_GREECE             | GR             | 300        |
| CTRY_GUATEMALA          | GT             | 320        |
| CTRY_HONDURAS           | HN             | 340        |
| CTRY_HONG_KONG          | HK             | 344        |
| CTRY_HUNGARY            | HU             | 348        |
| CTRY_ICELAND            | IS             | 352        |
| CTRY_INDIA              | IN             | 356        |
| CTRY_INDONESIA          | ID             | 360        |
| CTRY_IRAN               | IR             | 364        |
| CTRY_IRAQ               | IQ             | 368        |
| CTRY_IRELAND            | IE             | 372        |
| CTRY_ISRAEL             | IL             | 376        |
| CTRY_ITALY              | IT             | 380        |
| CTRY_JAMAICA            | JM             | 388        |
| CTRY_JAPAN              | JP             | 392        |
| CTRY_JAPAN1             | JP             | 393        |
| CTRY_JAPAN2             | JP             | 394        |
| CTRY_JAPAN3             | JP             | 395        |
| CTRY_JAPAN4             | JP             | 396        |
| CTRY_JAPAN5             | JP             | 397        |
| CTRY_JAPAN6             | JP             | 4006       |
| CTRY_JAPAN7             | JP             | 4007       |
| CTRY_JAPAN8             | JP             | 4008       |

**Table A-1 Country code definitions (cont.)**

| Country definition | Country string | Country ID |
|--------------------|----------------|------------|
| CTRY_JAPAN9        | JP             | 4009       |
| CTRY_JAPAN10       | JP             | 4010       |
| CTRY_JAPAN11       | JP             | 4011       |
| CTRY_JAPAN12       | JP             | 4012       |
| CTRY_JAPAN13       | JP             | 4013       |
| CTRY_JAPAN14       | JP             | 4014       |
| CTRY_JAPAN15       | JP             | 4015       |
| CTRY_JAPAN16       | JP             | 4016       |
| CTRY_JAPAN17       | JP             | 4017       |
| CTRY_JAPAN18       | JP             | 4018       |
| CTRY_JAPAN19       | JP             | 4019       |
| CTRY_JAPAN20       | JP             | 4020       |
| CTRY_JAPAN21       | JP             | 4021       |
| CTRY_JAPAN22       | JP             | 4022       |
| CTRY_JAPAN23       | JP             | 4023       |
| CTRY_JAPAN24       | JP             | 4024       |
| CTRY_JAPAN25       | JP             | 4025       |
| CTRY_JAPAN26       | JP             | 4026       |
| CTRY_JAPAN27       | JP             | 4027       |
| CTRY_JAPAN28       | JP             | 4028       |
| CTRY_JAPAN29       | JP             | 4029       |
| CTRY_JAPAN30       | JP             | 4030       |
| CTRY_JAPAN31       | JP             | 4031       |
| CTRY_JAPAN32       | JP             | 4032       |
| CTRY_JAPAN33       | JP             | 4033       |
| CTRY_JAPAN34       | JP             | 4034       |
| CTRY_JAPAN35       | JP             | 4035       |
| CTRY_JAPAN36       | JP             | 4036       |
| CTRY_JAPAN37       | JP             | 4037       |
| CTRY_JAPAN38       | JP             | 4038       |
| CTRY_JAPAN39       | JP             | 4039       |
| CTRY_JAPAN40       | JP             | 4040       |
| CTRY_JAPAN41       | JP             | 4041       |
| CTRY_JAPAN42       | JP             | 4042       |
| CTRY_JAPAN43       | JP             | 4043       |
| CTRY_JAPAN44       | JP             | 4044       |

**Table A-1 Country code definitions (cont.)**

| Country definition | Country string | Country ID |
|--------------------|----------------|------------|
| CTRY_JAPAN45       | JP             | 4045       |
| CTRY_JAPAN46       | JP             | 4046       |
| CTRY_JAPAN47       | JP             | 4047       |
| CTRY_JAPAN48       | JP             | 4048       |
| CTRY_JAPAN49       | JP             | 4049       |
| CTRY_JAPAN50       | JP             | 4050       |
| CTRY_JAPAN51       | JP             | 4051       |
| CTRY_JAPAN52       | JP             | 4052       |
| CTRY_JAPAN53       | JP             | 4053       |
| CTRY_JAPAN54       | JP             | 4054       |
| CTRY_JAPAN55       | JP             | 4055       |
| CTRY_JAPAN56       | JP             | 4056       |
| CTRY_JAPAN57       | JP             | 4057       |
| CTRY_JAPAN58       | JP             | 4058       |
| CTRY_JAPAN59       | JP             | 4059       |
| CTRY_JORDAN        | JO             | 400        |
| CTRY_KAZAKHSTAN    | KZ             | 398        |
| CTRY_KENYA         | KE             | 404        |
| CTRY_KOREA_NORTH   | KP             | 408        |
| CTRY_KOREA_ROC     | KR             | 410        |
| CTRY_KOREA_ROC3    | KR             | 412        |
| CTRY_KUWAIT        | KW             | 414        |
| CTRY_LATVIA        | LV             | 428        |
| CTRY_LEBANON       | LB             | 422        |
| CTRY_LIBYA         | LY             | 434        |
| CTRY_LIECHTENSTEIN | LI             | 438        |
| CTRY_LITHUANIA     | LT             | 440        |
| CTRY_LUXEMBOURG    | LU             | 442        |
| CTRY_MACAU         | MO             | 446        |
| CTRY_MACEDONIA     | MK             | 807        |
| CTRY_MALAYSIA      | MY             | 458        |
| CTRY_MALTA         | MT             | 470        |
| CTRY_MEXICO        | MX             | 484        |
| CTRY_MONACO        | MC             | 492        |
| CTRY_MOROCCO       | MA             | 504        |
| CTRY_NETHERLANDS   | NL             | 528        |



**Table A-1 Country code definitions (cont.)**

| Country definition        | Country string | Country ID |
|---------------------------|----------------|------------|
| CTRY_NETHERLANDS_ANTILLES | AN             | 530        |
| CTRY_NEW_ZEALAND          | NZ             | 554        |
| CTRY_NICARAGUA            | NI             | 558        |
| CTRY_NORWAY               | NO             | 578        |
| CTRY_OMAN                 | OM             | 512        |
| CTRY_PAKISTAN             | PK             | 586        |
| CTRY_PANAMA               | PA             | 591        |
| CTRY_PARAGUAY             | PY             | 600        |
| CTRY_PERU                 | PE             | 604        |
| CTRY_PHILIPPINES          | PH             | 608        |
| CTRY_POLAND               | PL             | 616        |
| CTRY_PORTUGAL             | PT             | 620        |
| CTRY_PUERTO_RICO          | PR             | 630        |
| CTRY_QATAR                | QA             | 634        |
| CTRY_ROMANIA              | RO             | 642        |
| CTRY_RUSSIA               | RU             | 643        |
| CTRY_SAUDI_ARABIA         | SA             | 682        |
| CTRY_SERBIA_MONTENEGRO    | CS             | 891        |
| CTRY_SINGAPORE            | SG             | 702        |
| CTRY_SLOVAKIA             | SK             | 703        |
| CTRY_SLOVENIA             | SI             | 705        |
| CTRY_SOUTH_AFRICA         | ZA             | 710        |
| CTRY_SPAIN                | ES             | 724        |
| CTRY_SRI_LANKA            | LK             | 144        |
| CTRY_SWEDEN               | SE             | 752        |
| CTRY_SWITZERLAND          | CH             | 756        |
| CTRY_SYRIA                | SY             | 760        |
| CTRY_TAIWAN               | TW             | 158        |
| CTRY_THAILAND             | TH             | 764        |
| CTRY_TRINIDAD_Y_TOBAGO    | TT             | 780        |
| CTRY_TUNISIA              | TN             | 788        |
| CTRY_TURKEY               | TR             | 792        |
| CTRY_UAE                  | AE             | 784        |
| CTRY_UKRAINE              | UA             | 804        |
| CTRY_UNITED_KINGDOM       | GB             | 826        |
| CTRY_UNITED_STATES        | US             | 840        |

**Table A-1 Country code definitions (cont.)**

| Country definition       | Country string | Country ID |
|--------------------------|----------------|------------|
| CTRY_UNITED_STATES2      | US             | 841        |
| CTRY_UNITED_STATES_FCC49 | PS             | 842        |
| CTRY_URUGUAY             | UY             | 858        |
| CTRY_UZBEKISTAN          | UZ             | 860        |
| CTRY_VENEZUELA           | VE             | 862        |
| CTRY_VIET_NAM            | VN             | 704        |
| CTRY_YEMEN               | YE             | 887        |
| CTRY_ZIMBABWE            | ZW             | 716        |