AP Command Line Interface User's Guide

Aquila 9.2

PRELIMINARY

Revision November 2011

ATHEROS®

Notice

The information in this document has been carefully reviewed and is believed to be accurate. Nonetheless, this document is subject to change without notice, and Atheros Communications, Inc. (Atheros) assumes no responsibility for any inaccuracies that may be contained in this document, and makes no commitment to update or to keep current the contained information, or to notify a person or organization of any updates. Atheros reserves the right to make changes, at any time, in order to improve reliability, function or design and to attempt to supply the best product possible. Atheros does not represent that products described herein are free from patent infringement or from any other third party right.

No part of this document may be reproduced, adapted or transmitted in any form or by any means, electronic or mechanical, for any purpose, except as expressly set forth in a written agreement signed by Atheros. Atheros or its affiliates may have patents or pending patent applications, trademarks, copyrights, maskwork rights or other intellectual property rights that apply to the ideas, material and information expressed herein. No license to such rights is provided except as expressly set forth in a written agreement signed by Atheros.

ATHEROS MAKES NO WARRANTIES OF ANY KIND WITH REGARD TO THE CONTENT OF THIS DOCUMENT. IN NO EVENT SHALL ATHEROS BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL SPECULATORY OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBLITY OF SUCH DAMAGES. IN PARTICULAR, ATHEROS SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA TRANSMITTED OR OTHERWISE USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING OR RECOVERING SUCH HARDWARE, SOFTWARE OR DATA. ATHEROS SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE AS THEY MIGHT OTHERWISE APPLY TO THIS DOCUMENT AND TO THE IDEAS, MATERIAL AND INFORMATION EXPRESSED HEREIN.

Document Number: MKG-15363 Ver. 2.0

Document Conventions

Text Conventions

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

Revision History

Revision	Description of Changes
November 2010	Initial release.
November 2011	Added command descriptions to Chapter 1 and recategorized some existing commands. New command categories: HT20/ HT40 Coexistence, iQue, Security, WDS. This revision applies to the Aquila 9.2 release.

Contents

List of Tables

Preface

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

Atheros Reference Design hardware, software, and documentation contain proprietary information of Atheros Communications, 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, see the document:

- *AP Middleware User's Guide*

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.

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 Atheros WLAN driver supports these tools out of the box without modification. Any version of wireless tools after version 28 can be used with the Atheros WLAN driver system.

The wireless tools use device names to determine which device to configure. In the Atheros driver, two device types are created when the AP is brought up. The radio layer, also known as the ATH/HAL layer, is instantiated as a **wifi***N* 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 **ath***N* 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 that the radio layer does not support the **iwconfig** command, which is used exclusively in the protocol layer. Also note that any **ifconfig** commands used on the AP must be applied to the protocol layer (ATH) device and has no effect on the radio layer.

iwconfig Commands

The **iwconfig** commands are a fixed set of commands used to set up and operate the WLAN interface. They are used in much the same way as **ifconfig** commands, but are specific to 802.11 device operations. Thus they interface to the particular VAP interface. Note that the Radio Layer does not support **iwconfig**.

Table 1-1. **iwconfig Commands**

Parameter	Format	Description
ap	`iwconfig athN ap MAC`	Selects the specific AP for a client to associate with; 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 *off* and *auto* choices, but these only disable the selection of a specific MAC address. Disabled by default. `#iwconfig ath0 ap 00:03:7f:01:23:45`
channel	`iwconfig athN channel args`	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. 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). `#iwconfig ath0 channel 11`

enc
key
	`iwconfig athN key [index] key_value`	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.
		The *key_value* 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.
		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.
		`#iwconfig ath0 key [2] DEAD-BEEF-EA`
		`#iwconfig ath0 key [1] s:AnASCIIkeyVal`
		`#iwconfig ath0 key off`

Table 1-1. **iwconfig Commands (continued)**

Parameter	Format	Description
essid	`iwconfig athN essid "Name of Network"`	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 the commonly used for 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, but must be quoted when including spaces. 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. `#iwconfig ath0 essid AP50_Test`
frag	`iwconfig athN frag level`	Sets the fragmentation threshold, which is the maximum fragment size. Note that this is not valid for 802.11n aggregation operations. The argument level indicates the maximum fragment size, or setting to off disables fragmentation. Fragmentation is off by default. `#iwconfig ath0 frag 512`

freq	`iwconfig athN freq frequency`	Similar to the channel command, this command selects the frequency of operation. Note that the frequency value 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.
		This command also returns an error if the indicated frequency is invalid for the device.
		`#iwconfig ath0 freq 5.2G`
		`#iwconfig ath0 freq 40`

rate	`iwconfig athN rate rateval|auto`	Selects a fixed rate for transmit, or enables the internal rate control logic. When *rateval* 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 *auto* instead of a fixed rate will enable the rate control logic internal to the driver. This is the default configuration. Setting 802.11n fixed rates is a bit more complicated, and is accomplished using the iwpriv commands **Set11NRates** and **Set11NRetries**. Selecting MCS rates cannot be accomplished through this command. `#iwconfig ath0 rate 36M`
retry	—	Software retry is not supported
rts	`iwconfig athN rts pkt_size`	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 *pkt_size* is set to the minimum packet size for which to use the RTS/CTS handshake. Setting pkt_size 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). `#iwconfig ath0 rts 256`

Table 1-1. **iwconfig Commands (continued)**

Parameter	Format	Description
sens	—	Receiver sensitivity control is not supported.
txpower	`iwconfig athN txpower power_setting`	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 power_setting 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 dependant on information in the selected regulatory table. `#iwconfig ath0 txpower 30`

iwpriv Commands

This section defines all of the **iwpriv** commands available for each layer. Note that there are some duplicate commands between the layers. It is recommended to use the radio layer commands over the protocol layer command (**wifi***N* commands over **ath***N* commands) when duplication exists.

The radio layer commands 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 that ALL VAPS attached to the specific radio are affected by the configurations made to the radio layer.

Aggregation Commands

Table 1-2. **Aggregation Commands**

Parameter	Format	Description

AMPDU
getAMPDU
	`iwpriv wifiN AMPDU 1|0`	Enables/disables 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 command returns the current value. Default is 1 (enabled).
		`#iwpriv wifi0 AMPDU 1`
		`#iwpriv wifi0 getAMPDU`
		`wifi0 getAMPDU:1`

AMPDUFrames
getAMPDUFrames
	`iwpriv wifiN AMPDUFrames numFrames`	Sets the maximum number of subframes to place into an AMPDU aggregate frame. Frames are added to an aggregate until either:
		■ The transmit duration is exceeded
		■ The number of subframes is exceeded
		■ The maximum number of bytes is exceeded, or
		■ The corresponding queue is empty.
		The subframe that causes the excess conditions is not included in the aggregate frame, but queues up to be transmitted with the next aggregate frame. The default value is 32. The get command returns the current value.
		`#iwpriv wifi0 AMPDUFrames 24`
		`#iwpriv wifi0 getAMPDUFrames`
		`wifi0 getAMPDUFrames:24`

AMPDULim
getAMPDULim
	`iwpriv wifiN AMPDULim Byte_Limit`	Limit the number of bytes included in an AMPDU aggregate frame. Frames are added to an aggregate until either:
		■ The transmit duration is exceeded
		■ The number of subframes is exceeded
		■ The maximum number of bytes is exceeded, or
		■ The corresponding queue is empty.
		The subframe that causes the excess conditions will not be included in the aggregate frame, but queues up to be transmitted with the next aggregate frame. The default value of this parameter is 50000. The get command returns the current value.
		`#iwpriv wifi0 AMPDULim 48000`
		`#iwpriv wifi0 getAMPDULim`
		`wifi0 getAMPDULim:48000`

Association/ACL Commands

Table 1-3. **Association/ACL Commands**

<table>
<tr><th>Command</th><th>Format</th><th>Description</th></tr>
<tr><td>addmac
delmac
getmac
maccmd
get_maccmd</td><td>iwpriv athN addmac mac_addr
iwpriv athN delmac mac_addr
iwpriv athN maccmd cmd</td><td>These commands 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.
addmac adds specified MAC addresses to the access control list (ACL). delmac deletes addresses from the ACL. These commands have no get equivalents. getmac displays the list of MAC addresses monitored by the ACL.
<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>maccmd instructs how the ACL is used to limit access the AP. The default is 0. The get command returns the current value.
Valid commands:
<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></td></tr>
<tr><td>ap_bridge
get_ap_bridge</td><td>iwpriv athN ap_bridge mode</td><td>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 command returns the current value.
<pre>#iwpriv ath0 ap_bridge 0
#iwpriv ath0 get_ap_bridge
   ath0 get_ap_bridge:0</pre></td></tr>
<tr><td>kickmac</td><td>iwpriv athN kickmac</td><td>Forces the AP to disassociate the specified STA.
<pre>#iwpriv ath0 kickmac 00:18:41:9b:c8:87</pre></td></tr>
</table>

Beacon Configuration Commands

Table 1-4. **Beacon Configuration Commands**

Command	Format	Description

bintval
get_bintval
	`iwpriv athN bintval` *`beacon_interval`*	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 command returns the current value.
		`#iwpriv ath0 bintval 400`
		`#iwpriv ath0 get_bintval`
		`ath0 get_bintval:200`

blockdfschan	`iwpriv athN blockdfschan 1|0`	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 command available. `#iwpriv ath0 blockdfschan 1`

countryie
get_countryie
	`iwpriv athN countryie 1|0`	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 command returns the current value.
		`#iwpriv ath0 countryie 1`
		`#iwpriv ath0 get_countryie`
		`ath0 get_countryie:1`

doth
get_doth
	`iwpriv athN doth 1|0`	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 command returns the current value.
		`#iwpriv ath0 doth 1`
		`#iwpriv ath0 get_doth`
		`ath0 get_doth:1`

Table 1-4. **Beacon Configuration Commands (continued)**

Command	Format	Description

dtim_period
get_dtim_period
	`iwpriv athN dtim_period delivery_period`	Used to set the DTIM period. The DTIM is an interval specified by the AP to the STA indicating when multicast traffic may be available for the STA, requiring the STA to be awake to receive the messages. This command will set the AP DTIM period, in ms. A longer DTIM will provide for a greater power savings, but will increase multicast latency. This parameter has a default value of 1 ms. The get command returns the current value.
		`#iwpriv ath0 dtim_period 5`
		`#iwpriv ath0 get_dtim_period`
		`wifi0 get_dtim_period:1`

hide_ssid
get_hide_ssid
	`iwpriv athN hide_ssid 1|0`	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 command 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`	Enables or disables pure G mode. This mode does not allow 802.11b rates, and only uses OFDM modulation. The get command returns the current value. The default value is 0.
		`#iwpriv ath0 pureg 1`
		`#iwpriv ath0 get_pureg`
		`ath0 get_pureg:1`

puren
get_puren
	`iwpriv athN puren 1|0`	Enables/disables Pure 11N mode, which does not accept STAs that do not have HT caps in AP mode.
		`#iwpriv ath0 puren 1`
		`#iwpriv ath0 get_puren`
		`ath0 get_puren:1`
		1 — Enable Pure 11N mode
		0 — Disable Pure 11N mode

shortgi
get_shortgi
	`iwpriv athN shortgi 1|0`	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 command returns the current value. The default value is 1.
		`#iwpriv ath0 shortgi 1`
		`#iwpriv ath0 get_shortgi`
		`ath0 get_shortgi:1`

Channel Width Commands

Table 1-5. **Channel Width Commands**

Command	Format	Description

chextoffset
get_chextoffset
	`iwpriv athN chextoffset channel_offset`	Sets the Extension (Secondary) Channel Offset field in the AP beacon High Throughput Information Element (HT IE). If this command is not executed, then the extension channel offset is taken from the device settings. This command has a corresponding get command. 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

chwidth
get_chwidth
	`iwpriv athN chwidth channel_width`	Sets the Channel Width field in the AP beacon High Throughput Information Element (HT IE). If this command is not executed, then the channel width is taken from the device settings. The get command 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

cwmenable
get_cwmenable
	`iwpriv athN cwmenable 1|0`	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 command returns the current value.
		`#iwpriv ath0 cwmenable 1`
		`#iwpriv ath0 get_cwmenable`
		`ath0 get_cwmenable:1`

Table 1-5. **Channel Width Commands (continued)**

<table>
<tr><th>Command</th><th>Format</th><th>Description</th></tr>
<tr><td>mode
get_mode</td><td><code>iwpriv athN mode</code>
<code>desired_mode</code></td><td>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 command returns the mode as a string value.
<code>#iwpriv ath0 mode 11NAHT20</code>
<code># iwpriv ath0 get_mode</code>
<code>ath0 get_mode:11ng20</code>

The operating modes include:
<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>
</table></td></tr>
</table>

Debug Commands

Table 1-6. **Debug Commands**

Command	Format	Description

dbgLVL
getdbgLVL
	`iwpriv athN dbgLVL` *Bitmask*	Controls the debug level of the VAP-based debug print statements. It is normally set to zero, eliminating all prints. See Table 1-7.
		`#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` *debug level*	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 that some categories will produce copious amounts of output, and should be used sparingly for a few seconds. See Table 1-8 on page 1-13. The get command 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 1-7. **802.11 Protocol Layer Debug Bitmask**

Symbolic Name	Bit Value	Description
IEEE80211_MSG_MLME	0x80000000	MLME mode debug
IEEE80211_MSG_DEBUG	0x40000000	IFF_DEBUG equivalent
IEEE80211_MSG_DUMPPKTS	0x20000000	IFF_LINK2 equivalent
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 1-8. **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
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

HT20/HT40 Coexistence Commands

Table 1-9. **HT20/HT40 Coexistence Commands**

Command	Format	Description

disablecoext
get_disablecoext
	`iwpriv athN disablecoext 1/0`	Sets HT20/HT40 Coexistence support. The default value is 0. The get command returns the current value.
		`#iwpriv ath0 disablecoext 0`
		`#iwpriv ath0 get_ disablecoext`
		`ath0 get_disablecoext:0`
		0 — Enable HT20/HT40 Coexistence support
		1 — Disable HT20/HT40 Coexistence support

iQue Commands

Table 1-10. **iQue Commands**

Command	Format	Description
get_hbrstate	`iwpriv athN get_hbrstate`	Displays HBR related statistics: node address, state, trigger, block, dropped VI frames.
get_iqueconfig	`iwpriv athN get_iqueconfig`	Prints all iQUE configuration settings.
hbrparams	`iwpriv athN hbrparams ac 1/0`	Sets Head of Line Block (HBR) mitigation. See Table 1-16 for access categories. For example, to enable HBR for video (vi) streams, use `iwpriv ath0 hbrparams 2 1 x`. The "x" value valid range is from 0-50, and indicates the lower bound PER; a PER better than this value causes HBR to unblock the node.
hbrPER_high **get_hbrPER_high**	`iwpriv wifiN hbrPER_high PER%`	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 command returns the current value.
hbrPER_low **get_hbrPER_low**	`iwpriv wifiN hbrPER_low PER%`	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 command returns the current value.
hbrtimer	`iwpriv athN hbrtimer timeout`	Sets the HBR timer timeout value in milliseconds. The default value is 2000 msec (2 seconds).

mcastenhance
get_mcastenhance
	`iwpriv athN mcastenhance mode_enum`	Set multicast enhancement mode.
		`#iwpriv ath0 mcastenhance 0`
		`#iwpriv ath0 get_mcastenhance`
		`ath0 get_mcastenhance:0`
		0 — Disable multicast enhancement
		1 — Enable multicast enhancement; use tunneling mode.
		2 — Enable multicast enhancement; use translating mode.

me_adddeny	`iwpriv athN me_adddeny group_address`	Adds the table of group addresses that are ***not*** to be learned. Group address 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

Table 1-10. **iQue Commands (continued)**

Command	Format	Description	
me_cleardeny	`iwpriv athN me_cleardeny value`	Clears the snoop deny table entries. *value* can be any integer; however, the command clears the snoop deny table regardless of of *value*.	
me_length **get_me_length**	`iwpriv athN me_length param`	Sets the snoop table length as number of entries. The default value is 32. Parameter range is 0 – 32. The get command returns the current value.	
me_showdeny	`iwpriv athN me_showdeny`	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 param`	Sets the debug level for multicast enhancement. Param argument can accept any combination of the values below. The get command 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
medropmcast **get_medropmcast**	`iwpriv athN medropmcast`	Enables/disables medropmcast feature, which drops multicast packets if the snoop table is empty. The default value is 1.	
		0	Disables medropmcast
		1	Enables medropmcast
medump	`iwpriv athN medump`	Dumps the snoop table for multicast enhancement.	
metimeout **get_metimeout**	`iwpriv athN metimeout param`	Sets the timeout in ms for a STA to be removed from the snoop table if idle. The parameter may be any unsigned integer value. The default is 120000 (2 minutes). The get command returns the current value.	
metimer **get_metimer**	`iwpriv athN metimer param`	Sets the timer in ms to check the status of the snoop table. The parameter may be any unsigned integer value. The default is 30000 (30 seconds). The get command returns the current value.	

retrydur
get_retrydur
	`iwpriv wifiN retrydur threshold_period`	Sets the retry threshold in µs. Feature disabled if set at 0.
		`#iwpriv wifi0 retrydur 0`
		`#iwpriv wifi0 get_retrydur`
		`wifi0 get_retrydur: 0`	

Physical Layer Commands

Table 1-11. **Physical Layer Commands**

Command	Format	Description

chainmasksel
get_chainmasksel
	`iwpriv wifiN chainmasksel 1|0`	Enables (1) automatic chainmask selection. This feature allows the system to select between 2 and 3 Tx chains, depending on the signal quality on the channel. For STAs that are distant, using 3-chain Tx allows for better range performance. The default value of this parameter is 0 (disabled). The get command returns the current value.
		`#iwpriv wifi0 chainmasksel 1`
		`#iwpriv wifi0 get_chainmasksel`
		`wifi0 get_chainmasksel:0`

LDPC
getLDPC
	`iwpriv wifiN LDPC 1/0`	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.
		`# iwpriv wifi0 LDPC 1`
		`# iwpriv wifi0 getLDPC`
		`wifi0 getLDPC:1`

setCountryID
getCountryID
setCountry
getCountry
	`iwpriv wifiN setCountryID Country ID Num`
	`iwpriv wifiN setCountry Country String`
		Sets the AP to the regulatory requirements of the country. See Table A-1, "Country Code Definitions," on page A-1 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 commands 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 1-11. **Physical Layer Commands (continued)**

<table>
<tr><th>Command</th><th>Format</th><th>Description</th></tr>
<tr><td>txchainmask
rxchainmask
get_txchainmask
get_rxchainmask</td><td>iwpriv wifiN
txchainmask mask
iwpriv wifiN
rxchainmask mask</td><td>Sets the Tx and Rx chainmask values. For MIMO devices, indicates the number of Tx/Rx streams, and which chains are used. For some 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:
<table>
<tr><td>Chain 0</td><td>0x01</td></tr>
<tr><td>Chain 1</td><td>0x02</td></tr>
<tr><td>Chain 2</td><td>0x04</td></tr>
</table>
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 commands returns the current values.
<pre>#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</pre></td></tr>
<tr><td>TXPowLim2G
TXPowLim5G
getTxPowLim2G
getTxPowLim5G</td><td>iwpriv wifiN
TXPowLim2G limit
iwpriv wifiN
TXPowLim5G limit</td><td>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 commands. 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 commands. The get commands return the current values.
<pre>#iwpriv wifi0 TXPowLim2G 100
#iwpriv wifi0 getTxPowLim2G
   wifi0 getTxPowLim2G:100</pre></td></tr>
</table>

Table 1-11. **Physical Layer Commands (continued)**

Command	Format	Description

TXPwrOvr
getTXPwrOvr
	`iwpriv wifi`*N*
	`TXPwrOvr`
	overrideLimit
		Overrides transmit (Tx) power limits set by the iwconfig txpower command, or the iwpriv TXPowLim2G/TXPowLim5G commands. For testing only, and limited by regulatory power. A value of 0 disables the override function. The default is 0. The get command returns the current value.
		`#iwpriv wifi0 TXPwrOvr 30`
		`#iwpriv wifi0 getTXPwrOvr`
		`wifi0 getTXPwrOvr:30`

txstbc
rxstbc
get_txstbc
get_rxstbc
	`iwpriv wifi0 rxstbc`
	1/0
	`iwpriv wifi0 txstbc`
	1/0
		Enables (1) or disables (0) the Space Time Coding Block (STBC) feature, as described in 802.11n specification, in the transmit (txstbc) or receive (rxtsbc) 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.
		`# 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`

Protection Mechanism Commands

Table 1-12. **Protection Mechanism Commands**

Command	Format	Description	

protmode
get_protmode
	`iwpriv athN protmode 1|0`	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 command 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 protection_mode`	Sets the protection mode used on the extension (secondary) channel when using 40 MHz channels. The default is 0. The get command 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

extprotspac
get_extprotspac
	`iwpriv athN extprotspac channel_spacing`	Sets the channel spacing for protection frames sent on the extension (secondary) channel when using 40 MHz channels. The default is 1. The get command returns the current value.
		`#iwpriv ath0 extprotspac 1`
		`#iwpriv ath0 get_extprotspac`
		`ath0 get_extprotspac:1`	

		0	20 MHz
		1	25 MHz

Security Commands

The security-related commands relate to the security subsystem, and are specific interfaces required by the hostapd and wpa_supplicant programs. Table 1-13 shows 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 1-13. **Security-Related Commands**

Parameter	Format	Description

mcastkeylen
get_mcastkeylen
	`iwpriv athN mcastkeylen length`	Only valid for WEP operations; sets the multicast/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 command.
		`#iwpriv ath0 mcastkeylen 5`
		`#iwpriv ath0 get_mcastkeylen`
		`ath0 get_mcastkeylen:5`

VoW (Video over Wireless) Commands

Table 1-14. **VoW Commands**

Command	Format	Description	

setVowExt
getVowExt
	`iwpriv wifiN setVowExt bit_mask`	Enables VoW (Video over Wireless) extensions. The default is 29. The get command returns the current value.
		`#iwpriv wifi0 setVowExt 29`
		`#iwpriv wifi0 getVowExt`
		`wifi0 getVowExt:29`	

		Default	The default is 29. All extensions are enabled.
		Fair Queuing	Prioritizes buffer allocation to video streams over BE/BK. Set bit 0.
		Adaptive Aggregation Sizing	Reduces latency, jitter & PER. Set bit 2.
		Software Retry Re-order	Sub-frames to be software-retried are put into sequence number order. Improves video quality by reducing latency and avoiding loss from receiver reassembly timeout and BAW limits. Set bit 3.
		Enhanced Rate Control & Aggregation	Optimal selection of data rate & aggregate size for video traffic to minimize the latency/jitter and improve the video quality. Set bit 4

Table 1-14. **VoW Commands (continued)**

Command	Format	Description

set_vsp_enable
get_vsp_enable
	`iwpriv wifiN set_vsp_enable value`	Enable/Disable Video Stream Protection. Protects good video streams over bad video streams (that are using up the resources such as medium, etc.). Default is 1. The get command returns the current value.
		`#iwpriv wifi0 set_vsp_enable 1`
		`#iwpriv wifi0 get_vsp_enable`
		`wifi0 get_vsp_enable:1`
		0 Disable
		1 Enable

WDS Commands

Table 1-15. **WDS Commands**

Command	Format	Description

extap
get_extap
	`iwpriv athN extap 1|0`	Sets Extender AP support. The get command returns the current value.
		`#iwpriv ath0 extap 0`
		`#iwpriv ath0 get_extap`
		`ath0 get_extap:0`
		0 Disable Extender AP support
		1 Enable Extender AP support
		2 Enable Extender AP support with DEBUG
		3 Enable Extender AP support with DEBUG

vap-ind	`iwpriv athN vap-ind 1|0`	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.

wds
get_wds
	`iwpriv athN wds 1|0`	Enables (1) or disables (0) 4-address frame format for this VAP. Used for WDS configurations (see "WiFi Distribution System (WDS)" in the *AP Driver User's Guide* for details). The default value is 0. The get command returns the current value.
		`#iwpriv ath0 wds 1`
		`#iwpriv ath0 get_wds`
		`ath0 get_wds:1`

wdsdetect
get_wdsdetect
	`iwpriv athN wdsdetect 1|0`	Due to the hardware design of early 802.11n chips, a workaround for WDS frames was implemented between Atheros STAs. For ar9000 series or later 802.11n products, this workaround is not required. This value enables (1) or disables (0) the AR5416 workaround for WDS. When the workaround is enabled aggregation is not enabled for the WDS link. The default value is 1. The get command returns the current value.
		`#iwpriv ath0 wdsdetect 1`
		`#iwpriv ath0 get_wdsdetect`
		`ath0 get_wdsdetect:1`

WMM Commands

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

Table 1-16. **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 how the time slots or TXOPs are metered out for each traffic stream. Table 1-17 shows the parameters accessible in the Atheros driver.

Table 1-17. **WMM Parameters**

Parameter	Format	Description
acparams	`iwpriv athN acparams` *`access_category use_rts aggregate_scaling min_rate[Mbps]`*	Configures the access category. See table Table 1-16. *Access Category:* 0: BE 1: BK 2: VI 3: VO *Enable RTS/CTS:* Applies to all rate series. *Aggregate Scaling:* Controls the maximum air time that the aggregates can use. 0: Disable, ≥ 4 ms 1: ≥ 2 ms 2: ≥ 1 ms 3: ≥ 0.5 ms

Table 1-17. **WMM Parameters (continued)**

Parameter	Format	Description	

setwmmparams
getwmmparams
	`iwpriv athN setwmmparam` *`WME parameter access category BSS/local`*	Sets WMM parameters. The range and units of measure for the value argument are listed with the WME parameter below. The get command returns the current settings.
		`#iwpriv ath0 setwmmparams 1 0 0 4`
		`#iwpriv ath0 getwmmparams 1 0 0`
		`ath0 getwmmparams:4`
		
		Each WMM parameter can be executed as a separate subcommand. The access category, BSS/local, and value arguments remain the same. Each subcommands has a corresponding get command that returns the current value. For example, for the `cwmin` subcommand:
		`#iwpriv ath0 cwmin 3 1 2`
		`#iwpriv ath0 get_cwmin 3 1`
		`ath0 get_cwmin: 2`
		
		The remaining subcommands are
		`#iwpriv athN acm`
		`#iwpriv athN aifs`
		`#iwpriv athN cwmax`
		`#iwpriv athN cwmin`
		`#iwpriv athN noackpolicy`
		`#iwpriv athN txoplimit`	

		WME Parameter	
		1	CWMIN (value = 0-15, in units of slot time)
		2	CWMAX (value = 0-15, in units of slot time)
		3	AIFS (value = 0-15, in units of slot time)
		4	TXOPLIMIT (value = 0-8192, in units of 32 µs)
		5	ACM (value = 0 for disable, 1 for enable)
		6	NOACKPOLICY (value = 0 for disable, 1 for enable)
		Access Category	
		0	Best effort (BE)
		1	Background (BK)
		2	Video (VI)
		3	Voice (VO)
		BSS/Local	
		1	BSS (channel parameters broadcast to STAs)
		0	Local (channel parameters applied to self)

Table 1-17. **WMM Parameters (continued)**

Parameter	Format	Description

uapsd
get_uapsd
	`iwpriv athN uapsd 1|0`	Sets 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 command returns the current value.
		`#iwpriv ath0 uapsd 1`
		`#iwpriv ath0 get_uapsd`
		`ath0 get_uapsd:1`
		0 — Disables messages on UAPSD capability
		1 — Enables messages on UAPSD capability

wmm
get_wmm
	`iwpriv athN wmm 1|0`	Enables or disables 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 command, and its default is 1 (WMM enabled).
		`#iwpriv ath0 wmm 1`
		`#iwpriv ath0 get_wmm`
		`ath0 get_wmm:1`

wlanconfig Utility

The 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 Interface"

NOTE: Although this document notes the commands that may have adverse effects, not all effects may have been documented. Keep in mind the nature of multiple VAP configurations that use multiple radios, and use caution when changing parameters.

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).

This command creates a VAP instance:

```
#wlanconfig ATH[N] create wlandev wifiN wlanmode [ap|sta|mon] [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 wifi*N*	Indicates which interface to attach the VAP to. The interface number is required for this argument. For dual concurrent operations, *N* indicates which radio to attach the VAP to.	
wlanmode ***mode***	Indicates the mode to open the VAP into. The valid modes are:	
	ap	AP (infrastructure) mode
	sta	STA (client) mode
	mon	Monitor VAP; not implemented in configuration scripts
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 Atheros driver.	
nosbeacon	Indicates that no beacons will be transmitted from this VAP. Used as part of STA mode.	

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"

AP 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 [sta|ap|chan|keys|caps|wme]
```

Table 1-18 describes the AP list elements. It only applies to VAPs that are STA VAPs. This scan result provides a list of nearby APs. This listing is produced:

```
SSID          BSSID              CHAN  RATE   S:N   INT   CAPS
Atheros Guests00:0b: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 1-18. **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**	Atheros Vendor IE	**RSN**	RSN IE
	WME	WMM IE	**VEN**	Vendor-Specific IE	**???**	Unknown IE

STA List Elements

Table 1-19 describes the list elements for each STA associated with the indicated VAP. This listing is produced:

```
ADDR              AID CHAN RATE RSSI IDLE  TXSEQ RXSEQ  CAPS ACAPS ERP   STATE  HTCAPS
00:03:7f:08:62:23 1   36   6M   59   135   13    12128  E    0     33    Q      WME
```

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 1-19.

Table 1-19. **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					
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**	Atheros Vendor IE	**RSN**	RSN IE
	WME	WMM IE	**VEN**	Vendor-Specific IE	**???**	Unknown IE

Channel List Elements

Table 1-20 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:

```
Channel 1: 2412 MHz 11ng C CU  Channel 64:  5320* MHz 11na C CL
Channel 2: 2417 MHz 11ng C CU  Channel 100: 5500* MHz 11na C CU
Channel 3: 2422 MHz 11ng C CU  Channel 104: 5520* MHz 11na C CL
Channel 4: 2427 MHz 11ng C CU  Channel 108: 5540* MHz 11na C CU
```

Table 1-20. **Channel List Elements**

FHSS	FHSS channel	**11na**	5 GHz band 802.11n capable	**C**	802.11n control channel capable	**CU**	802.11n upper extension channel enabled
		11a	5 GHz band legacy			**CL**	802.11n lower extension channel enabled
		11ng	2.4 GHz band 802.11n capable				
		11g	2.4 GHz band legacy				
		11b	2.4 GHz band DSSS only				

Capabilities List Elements

Table 1-21 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 1-21. **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		

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

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

Delete 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
```

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

Table A-1. **Country Code Definitions (continued)**

Country Definition	Country String	Country ID
CTRY_CHILE	CL	152
CTRY_CHINA	CN	156
CTRY_COLOMBIA	CO	170
CTRY_COSTA_RICA	CR	188
CTRY_CROATIA	HR	191
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

Table A-1. **Country Code Definitions (continued)**

Country Definition	Country String	Country ID
CTRY_JAPAN8	JP	4008
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
CTRY_JAPAN45	JP	4045
CTRY_JAPAN46	JP	4046
CTRY_JAPAN47	JP	4047

Table A-1. **Country Code Definitions (continued)**

Country Definition	Country String	Country ID
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
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

Table A-1. **Country Code Definitions (continued)**

Country Definition	Country String	Country ID
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
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

Atheros Communications, Incorporated
1700 Technology Drive
San Jose, CA 95110
tel: 408.773.5200
fax: 408.773.9940
www.atheros.com