MircoAP

User Guide

Revision 1.0
January 22, 2010

Table of Contents

1 Introduction 4
1.1 Event Monitoring 6
2 USER MANUAL FOR MEHUTL 6
2.1 Supported Commands 6
2.2 The following commands can be issued individually for debug purpose 7
2.3 Details of Commands 7
2.3.1 version 7
2.3.2 debug_level 7
2.3.3 sys_config 8
2.3.4 sys_info 8
2.3.5 sys_reset 8
2.3.6 bss_start 9
2.3.7 bss_stop 9
2.3.8 sta_list 9
2.3.9 sta_deauth 9
2.3.10 sys_cfg_ap_mac_address 9
2.3.11 sys_cfg_ssid 10
2.3.12 sys_cfg_beacon_period 10
2.3.13 sys_cfg_dtim_period 10
2.3.14 sys_cfg_scan_channels 11
2.3.15 sys_cfg_channel 11
2.3.16 sys_cfg_rates 12
2.3.17 sys_cfg_rates_ext 12
2.3.18 sys_cfg_tx_power 13
2.3.19 sys_cfg_bcast_ssid_ctl 13
2.3.20 sys_cfg_preamble_ctl 14
2.3.21 sys_cfg_antenna_ctl 14
2.3.22 sys_cfg_rts_threshold 14
2.3.23 sys_cfg_frag_threshold 14
2.3.24 sys_cfg_rsn_replay_prot 15
2.3.25 sys_cfg_radio_ctl 15
2.3.26 sys_cfg_tx_data_rate 15
2.3.27 sys_cfg_mcbc_data_rate 16
2.3.28 sys_cfg_pkt_fwd_ctl 17
2.3.29 sys_cfg_sta_ageout_timer 17
2.3.30 sys_cfg_auth 18
2.3.31 sys_cfg_protocol 18
2.3.32 sys_cfg_wep_key 18
2.3.33 sys_cfg_cipher 19
2.3.34 sys_cfg_group_rekey_timer 20
2.3.35 sys_cfg_wpa_passphrase 20
2.3.36 sys_cfg_max_sta_num 20
2.3.37 sys_cfg_retry_limit 21
2.3.38 sys_cfg_custom_ie 21
2.3.39 sta_filter_table 22
2.3.40 regrdwr 22
2.3.41 memaccess 23
2.3.42 rdeeprom 24
2.3.43 cfg_data 24
2.3.44 sys_debug 24
2.3.45 powermode 25

3 USER MANUAL FOR MEHEVENT 26
3.1 Supported events 26
3.2 Details of events 26
3.2.1 STA_DEAUTH 26
3.2.2 STA_ASSOC 27
3.2.3 BSS_START 27
3.2.4 BSS_IDLE 27
3.2.5 BSS_ACTIVE 27

Table of Contents

Figure 1: MEH Acting as a 3G Gateway 4
Figure 2: Block Diagram of MEH 4
Figure 3: Table of MEH Default Configuration Settings 5

Revision History:

Revision	Revision Date	Originator	Changes
1.0	1/22/10	EK/AK	Preliminary release.

1 Introduction

Mobile Embedded Hotspot (MEH) is an architecture announced recently by Wi2Wi. In this configuration, WiFi devices from Wi2Wi, which are normally deployed as 802.11 b/g/n clients, can operate as 802.11 access points, able to connect to and carry traffic for other 802.11 clients such as notebooks and smartphones. They can also relay data between clients without having to route it to the host processor or network. Figures below show an MEH acting as a 3G wireless gateway and a high level software block diagram of MEH.

Figure 1: MEH Acting as a 3G Gateway

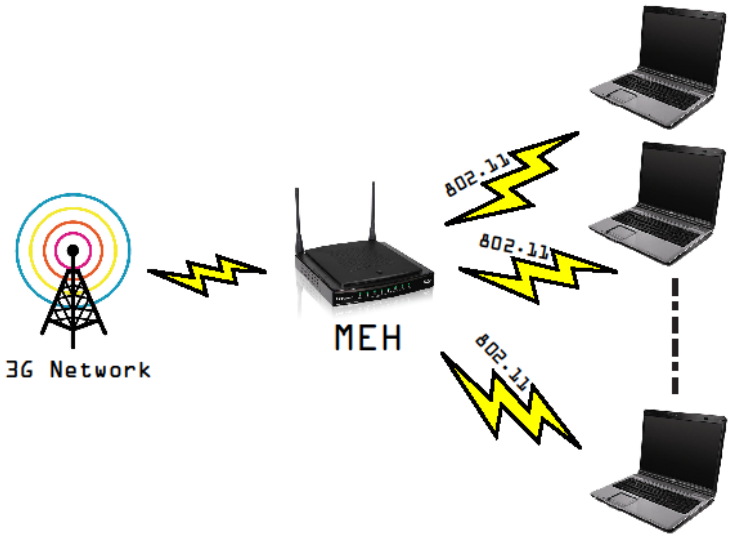
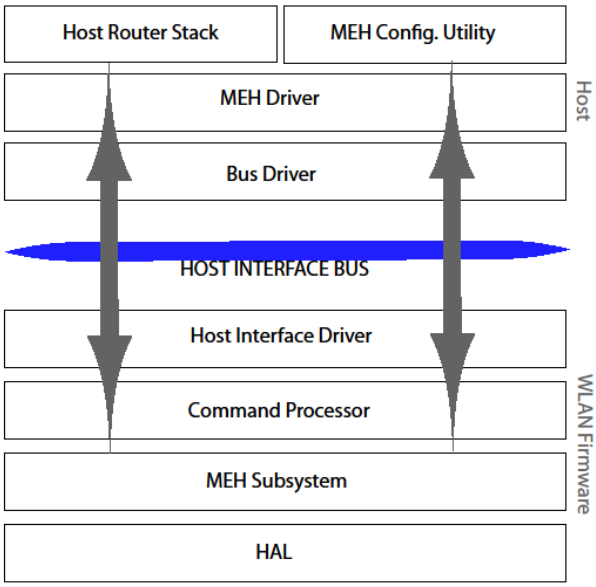


Figure 2: Block Diagram of MEH



This document provides information on commands the host software can send to firmware running on Wi2Wi devices configured as Mobile Embedded Hotspots. MEH functionality is provided in the form of firmware, drivers, and a configuration utility, presently for Linux and soon for Windows CE. Source code is provided for the configuration utility, allowing designers to modify it to suit their needs. Commands

described in this document refer to various functions provided by this utility. Command syntax corresponds to usage in Linux of the utility mehutl.exe.
Sample Configurations

On startup, MEH default configuration in firmware is as shown below.

Figure 3: Table of MEH Default Configuration Settings

Parameter	Default Value
SSID	"MEH"
Beacon Period	100 TU (1 TU = 1024 microseconds)
Channel	6
Basic Rate Ste	1, 2, 5.5, 11 Mbps
Operational Rate Set	6,9,12, 18, 24, 36, 48, 54 Mbps
Transmit Power Level	13 dBm
Broadcast SSID	Enabled
Preamble Type	Short
RTS Threshold	2347
Fragmentation Threshold	2346
DTIM	1
Antenna Mode	Antenna A
Radio State	Off
Transmit Data Rate	Auto
Security Settings	No security and open authentication
WEP Kets	Set to 0
Packet Forwarding Mode	Firmware bridges packets from a client station to another station in the same BSS
Client Station MAC address Filter Table	Disabled, filled with zeroes
Aging Timer	3 minutes
MAC Address	Use MAC address programmed in EEPROM. If that fails default to 00:50:43:FE:01:00. (See item #12 below)
Maximum Station Count	8
Tx Retry Limit (Long and Short)	7
Group Cipher Re-key Time	86400 sections (1 day). This will be used only when using WPA/WPA2

The host can change many configuration parameters at once by making changes in a configuration file (sample config file mehutl.conf is shown in appendix) and using the sys_config command. Then, a basic setup simply involves issuing a bss_start command. The firmware then turns the radio on, starts sending out beacons, and is ready to associate with clients.
To add WEP security, the host can stop the MEH by using the bss_stop command, and set the authentication mode to open or shared key via the sys_cfg_auth command. The encryption protocol can

be set to WEP using sys_cfg_protocol, followed by WEP keys with sys_cfg_wep_key command. With bss_start, the MEH is running again.

1.1 Event Monitoring

Certain events from MEH can be monitored at the host and suitable actions taken. Examples are when a station connects or disconnects from the MEH. The utility mehevent.exe in Linux allows these to be displayed on the console. As source code for this utility is provided, customers can modify it to suit their application.

2 USER MANUAL FOR MEHUTL

```
He who covers over an offense promotes love, but he who repeats the matter
separates close friends.
```
NAME

mehutl.exe [options] <command> [comand parameters]]

```
Options:
      help  Display help
      v     Display version
      i <interface>
      d <debug_level=0|1|2>
```

Example:
./mehutl.exe help
"display help for mehutl"

./mehutl.exe sys_config help
"display help for sys_config command"

```
This tool can be used to set/get MEH's settings. To change AP settings,
you might need to issue "bss_stop" command to stop AP before making change
and issue "bss_start" command to restart the AP after making change.
```

2.1 Supported Commands

```
version
debug_level
sys_config [CONFIG_FILE_NAME]
sys_info
sys_reset
bss_start
bss_stop
sta_list
sta_deauth <STA_MAC_ADDRESS> [REASON_CODE]
powermode [MODE] [SLEEP_PARAM=1 CTRL MIN_SLEEP MAX_SLEEP] [INACT_PARAM=2
INACTTO MIN_AWAKE MAX_AWAKE]
```

2.2 The following commands can be issued individually for debug purpose

```
sys_cfg_ap_mac_address [AP_MAC_ADDRESS]
sys_cfg_ssid [SSID]
sys_cfg_beacon_period [BEACON_PERIOD]
sys_cfg_dtim_period [DTIM_PERIOD]
sys_cfg_channel [CHANNEL] [MODE]
sys_cfg_scan_channels [CHANNELS]
sys_cfg_rates [RATES]
sys_cfg_rates_ext [rates RATES] [mbrate RATE] [urate RATE]
sys_cfg_tx_power [TX_POWER]
sys_cfg_bcast_ssid_ctl [1|0]
sys_cfg_preamble_ctl
sys_cfg_antenna_ctl <ANTENNA> [MODE]
sys_cfg_rts_threshold [RTS_THRESHOLD]
sys_cfg_frag_threshold [FRAG_THRESHOLD]
sys_cfg_rsn_replay_prot [1|0]
sys_cfg_radio_ctl [0|1]
sys_cfg_tx_data_rate [TX_DATA_RATE]
sys_cfg_mcbc_data_rate [MCBC_DATA_RATE]
sys_cfg_pkt_fwd_ctl [0}1]
sys_cfg_sta_ageout_timer [STA_AGEOUT_TIMER]
sys_cfg_auth [AUTH_MODE]
sys_cfg_protocol [PROTOCOL]
sys_cfg_wep_key [INDEX ISDEFAULT KEY]
sys_cfg_cipher [PAIRWISE_CIPHER GROUP_CIPHER]
sys_cfg_group_rekey_timer [GROUP_REKEY_TIMER]
sys_cfg_wpa_passphrase [PASSPHRASE]
sys_cfg_max_sta_num [STA_NUM]
sys_cfg_retry_limit [RETRY_LIMIT]
sys_cfg_custom_ie [INDEX] [MASK] [IEBuffer]
sta_filter_table <FILTERMODE> <MACADDRESS_LIST>
regrdwr <TYPE> <OFFSET> [value]
memaccess <ADDR> [value]
rdeeprom <offset> <byteCount>
cfg_data <type> [*.conf]
sys_debug [subcmd] [parameter]
```

2.3 Details of Commands

2.3.1 version

"./mehutl.exe v"

This command prints the MEH utility version information.

2.3.2 debug_level

"./mehutl.exe d <debug_level>"

```
    The supported debug_level are:
        0      no debug
        1      enable MSG_DEBUG
      2      enable all the debug
    This command use to control the debug level of mehutl.exe.
```

Example:
./mehutl.exe d 2 sys_config
Enable all the debug in mehutl.exe

2.3.3 sys_config

```
    "./mehutl.exe sys_config [CONFIG_FILE]"
      This command is used to set or get the current settings of the Micro
      AP.

    The supported options are:
        CONFIG_FILE is file contain all the Micro AP settings.
        empty  Get current Micro AP settings
```

Example:
./mehutl.exe sys_config
Get current settings of the Micro AP.

./mehutl.exe sys_config mehutl.conf
Load Micro AP's settings from mehutl.conf file and set.

2.3.4 sys_info

```
    "./mehutl.exe sys_info"

    This command returns system information such as firmware version
number
    and HW information.
```

2.3.5 sys_reset

```
    "./mehutl.exe sys_reset"

    This command is used to reset the Micro AP back to its initial state.
    For example, this can be used to recover from a serious error, or
before
    creating a new BSS.

    This command has the following effects:
        1. The WLAN hardware MAC is reset.
        2. All MIB variables are initialized to their respective default
           values.
        3. The firmware internal variables are reset to their respective
           default values.
        4. The firmware state machines are reset to their respective
initial
```

states.

2.3.6 bss_start

"./mehutl.exe bss_start"

This command starts the BSS.

2.3.7 bss_stop

"./mehutl.exe bss_stop"

This command stops the BSS. The command causes the firmware to:
1. Deauthenticate all associated client stations.
2. Turn off the radio (hence stopping beaconing).

2.3.8 sta_list

"./mehutl.exe sta_list"

This command returns the list of client stations that are currently associated with the AP.

The output is formatted as shown below, for each STA:
"STA <STA_NUM> information:
==========
MAC Address: <STA MAC address>
Power mfg status: active|power save
Rssi: <RSSI_VALUE>"

2.3.9 sta_deauth

"./mehutl.exe sta_deauth <STA_MAC_ADDRESS> [REASON_CODE]"

This command is used to deauthentciate a client station for any reason or sepcific reason.

Example:
./mehutl.exe sta_deauth 00:50:43:20:34:58 4
deauth station 00:50:43:20:34:58 with IEEE reason code 4 (Disassociated due to inactivity)

2.3.10 sys_cfg_ap_mac_address

"./mehutl.exe sys_cfg_ap_mac_address [AP_MAC_ADDRESS]"

This command is used to set or get the AP MAC address.

If no arguments are given, this command returns the current AP MAC address.
Otherwise, this MAC address becomes the BSSID of the infrastructure

network created by the AP.

Example:
./mehutl.exe sys_cfg_ap_mac_address 00:50:43:20:aa:bb
Set AP MAC address to 00:50:43:20:aa:bb

./mehutl.exe sys_cfg_ap_mac_address
Get AP MAC address"

2.3.11 sys_cfg_ssid

"./mehutl.exe sys_cfg_ssid [SSID]"

This command is used to set or get the AP SSID.

If no arguments are given, this command returns the current AP SSID. While setting, the maximum length of the SSID can be 32 characters.

Example:
./mehutl.exe sys_cfg_ssid microap
Set AP ssid to "microap"

./mehutl.exe sys_cfg_ssid
Get AP ssid

2.3.12 sys_cfg_beacon_period

"./mehutl.exe sys_cfg_beacon_period [BEACON_PERIOD]"

This command is used to set or get the AP beacon period.

If no arguments are given, this command returns the current AP beacon period.

Beacon period is represented in milliseconds.

Example:
./mehutl.exe sys_cfg_beacon_period 100
Set AP beacon period to 100 TU

./mehutl.exe sys_cfg_beacon_period
Get AP beacon period

2.3.13 sys_cfg_dtim_period

"./mehutl.exe sys_cfg_dtim_period [DTIM_PERIOD]

This command is used to set or get the AP DTIM period.

If no arguments are given, this command returns the current AP DTIM period.

Example:
./mehutl.exe sys_cfg_dtim_period 3
Set AP DTIM period to 3

./mehutl.exe sys_cfg_dtim_period
Get AP DTIM period

2.3.14 sys_cfg_scan_channels

"./mehutl.exe sys_cfg_scan_channels [CHANNELS]"

This command is used to set or get the AP's scan channel list.

If no arguments are given, this command returns the scan channel list.

Each channel must be separated by a space.

Example:
./mehutl.exe sys_cfg_scan_channels 1 11 6
Set AP scan channel list to 1 11 6

./mehutl.exe sys_cfg_scan_channels 11 6
Set AP scan channel list to 11 6
./mehutl.exe sys_cfg_scan_channels
Get AP scan channel list

2.3.15 sys_cfg_channel

"./mehutl.exe sys_cfg_channel [CHANNEL] [MODE]"

This command is used to set or get the AP radio channel.

If no arguments are given, this command returns the current AP radio channel.

MODE can be set to either 0 or 1. 0 for manual and 1 for automatic channel selction(ACS). For ACS channel is required to be 0.

Example:
./mehutl.exe sys_cfg_channel 6
Set AP radio channel to 6

./mehutl.exe sys_cfg_channel 11 0
Set AP radio channel to 11 with Manual Channel Select.

./mehutl.exe sys_cfg_channel 0 1
Set AP to ACS.

./mehutl.exe sys_cfg_channel
Get AP radio channel

2.3.16 sys_cfg_rates

```
    "./mehutl.exe sys_cfg_rates [RATES]"

    If 'Rate' provided, a 'set' is performed else a 'get' is performed
    RATES is provided as a set of data rates, in unit of 500 kilobits
    A rate with MSB bit is basic rate, i.e 0x82 is basic rate.

    'set' will not allowed after bss start.

    Valid rates: 2, 4, 11, 22, 12, 18, 24, 36, 48, 72, 96, 108
      NonBasic rates: 0x02, 0x04, 0x0b, 0x16, 0x0C, 0x12, 0x18, 0x24,
      0x30, 0x48, 0x60, 0x6c
    Basic rates: 0x82, 0x84, 0x8b, 0x96, 0x8C, 0x92, 0x98, 0xA4, 0xB0,
    0xC8, 0xE0, 0xEc

    Each rate must be separated by a space.

    Example:
    ./mehutl.exe sys_cfg_rates 0x82 0x84 0x96 0x0c 0x12 0x18
    ./mehutl.exe sys_cfg_rates
```

2.3.17 sys_cfg_rates_ext

```
    "./mehutl.exe sys_cfg_rates_ext [rates RATES] [mbrate RATE] [urate
RATE]"

    If 'Rate' provided, a 'set' is performed else a 'get' is performed.
    RATES is provided as a set of data rates, in unit of 500 kilobits
    A rate with MSB bit is basic rate, i.e 0x82 is basic rate.
      If only operational rates is provided, MCBC rate and unicast rate
      will be set to auto.

    Valid rates: 2, 4, 11, 22, 12, 18, 24, 36, 48, 72, 96, 108
      NonBasic rates: 0x02, 0x04, 0x0b, 0x16, 0x0C, 0x12, 0x18, 0x24,
      0x30, 0x48, 0x60, 0x6c
    Basic rates: 0x82, 0x84, 0x8b, 0x96, 0x8C, 0x92, 0x98, 0xA4, 0xB0,
    0xC8, 0xE0, 0xEc
    Rates 2, 4, 11 and 22 (in units of 500 Kbps) must be present in either
of
    basic or nonbasic rates. If OFDM rates are enabled then 12, 24 and 48
(in
    units of 500 Kbps) must be present in either basic or nonbasic rates.

    Each rate must be separated by a space.

    rates followed by RATES for setting operational rates.
    mbrate followed by RATE for setting multicast and broadcast rate.
    urate followed by RATE for setting unicast rate.

    operational rates only allow to set before bss start.
```

Example:
./mehutl.exe sys_cfg_rates_ext rates 0x82 0x04 11 0x96 12 24 48 urate 0x2 mbrate 0x16
Set AP operation rates to 0x82,0x04,11,0x96,12,24,48, unicast rate to 2, multicast rate to 0x16

./mehutl.exe sys_cfg_rates_ext rates 0x82 0x04 11 0x96 12 24 48
Set AP operation rates to 0x82,0x04,11,0x96,12,24,48, unicast rate to auto, multicast rate to auto

2.3.18 sys_cfg_tx_power

"./mehutl.exe sys_cfg_tx_power [TX_POWER]"

This command is used to set or get the AP Tx power.

If no arguments are given, this command returns the current AP Tx power.

Tx power level is represented in dBm.

Example:
./mehutl.exe sys_cfg_tx_power 13
Set AP Tx powr to 13 dBm

./mehutl.exe sys_cfg_tx_power
Get AP Tx power

2.3.19 sys_cfg_bcast_ssid_ctl

"./mehutl.exe sys_cfg_bcast_ssid_ctl [1|0]"

This command is used to set or get the SSID broadcast feature setting.

The supported options are:
0 Disable SSID broadcast
1 Enable SSID broadcast
empty Get current SSID broadcast setting

When broadcast SSID is enabled, the AP responds to probe requests from client stations that contain null SSID.

When broadcast SSID is disabled, the AP:
1. Does not respond to probe requests that contain null SSID.
2. Generates beacons that contain null SSID.

Example:
./mehutl.exe sys_cfg_bcast_ssid_ctl 1
Enable SSID broadcast

./mehutl.exe sys_cfg_bcast_ssid_ctl
Get SSID broadcast setting

2.3.20 sys_cfg_preamble_ctl

```
"./mehutl.exe sys_cfg_preamble_ctl"

This command is used to get type of preamble.

Example:
  ./mehutl.exe sys_cfg_preamble_ctl
        Get AP preamble setting
```

2.3.21 sys_cfg_antenna_ctl

```
"./mehutl.exe sys_cfg_antenna_ctl <ANTENNA> [MODE]"

This command is used to set or get the antenna settings.

The supported options are:
    ANTENNA : 0  Rx antenna
              1  Tx antenna
    MODE    : 0        Antenna A
              1        Antenna B
              empty    Get current antenna settings

Example:
  ./mehutl.exe sys_cfg_antenna_ctl 0 1
        Set AP Rx antenna to Antenna B

  ./mehutl.exe sys_cfg_antenna_ctl 1
        Get AP Tx antenna
```

2.3.22 sys_cfg_rts_threshold

```
"./mehutl.exe sys_cfg_rts_threshold [RTS_THRESHOLD]"

This command is used to set or get the RTS threshold value.

If no arguments are given, this command returns the current RTS
threshold
value.

Example:
  ./mehutl.exe sys_cfg_rts_threshold 2347
        Set AP RTS threshold to 2347

  ./mehutl.exe sys_cfg_rts_threshold
        Get AP RTS threshold
```

2.3.23 sys_cfg_frag_threshold

```
"./mehutl.exe sys_cfg_frag_threshold [FRAG_THRESHOLD]"

This command is used to set or get the Fragmentation threshold value.
```

```
If no arguments are given, this command returns the current
Fragmentation threshold
value.

Example:
  ./mehutl.exe sys_cfg_frag_threshold 2346
       Set AP Fragmentation threshold to 2346

  ./mehutl.exe sys_cfg_frag_threshold
       Get AP Fragmentation threshold
```

2.3.24 sys_cfg_rsn_replay_prot

```
"./mehutl.exe sys_cfg_rsn_replay_prot [1|0]"

This command is used to enable or disable RSN replay protection.

The supported options are:
    0      Disable RSN replay protection
    1      Enable RSN replay protection
    empty  Get current RSN replay protection setting

Example:
  ./mehutl.exe sys_cfg_rsn_replay_prot 1
       Enable RSN replay protection

  ./mehutl.exe sys_cfg_rsn_replay_prot
       Get RSN replay protection setting
```

2.3.25 sys_cfg_radio_ctl

```
"./mehutl.exe sys_cfg_radio_ctl [0|1]"

This command is used to set or get the radio settings.

The supported options are:
    0      Turn radio on
    1      Turn radio off
    empty  Get current radio setting

Example:
  ./mehutl.exe sys_cfg_radio_ctl 1
       Turn AP radio off

  ./mehutl.exe sys_cfg_radio_ctl
       Get AP radio setting
```

2.3.26 sys_cfg_tx_data_rate

```
"./mehutl.exe sys_cfg_tx_data_rate [TX_DATA_RATE]"
```

```
    This command is used to set or get the Tx data rate settings.

    The supported options are:
        0      Auto rate
        >0     Set specified data rate
        empty  Get current data rate

    Tx data rate is represented in units of 500 kbps. While setting Tx
data
    rates, only zeron or rates currently configured are allowed.

      Following is the list of supported rates in units of 500 Kbps:
          2,    4,    11,   22,   12,   18,   24,   36,   48,   72,   96,
108
          0x02, 0x04, 0x0b, 0x16, 0x0C, 0x12, 0x18, 0x24, 0x30, 0x48,
0x60, 0x6c
```

Example:

```
  ./mehutl.exe sys_cfg_tx_data_rate 22
        Set AP Tx data rate to 11 M

  ./mehutl.exe sys_cfg_tx_data_rate 0x16
        Set AP Tx data rate to 11 M

  ./mehutl.exe sys_cfg_tx_data_rate
        Get AP Tx data rate
```

2.3.27 sys_cfg_mcbc_data_rate

```
    "./mehutl.exe sys_cfg_mcbc_data_rate [MCBC_DATA_RATE]"

    This command is used to set or get the MCBC data rate to use for
multicast
    or broadcast packet transmission.

    The supported options are:
        0      Auto rate
        >0     Set specified MCBC data rate
        empty  Get current MCBC data rate

    MCBC data rate is represented in units of 500 kbps. While setting MCBC
data
      rates, only zeron or one of rates currently configured as basic
      rates are allowed.

    For example:  If current basic rates is "0x82 0x84 0x8b 0x96", then
    the allowed
                  values for MCBC data rate will be "0x2 0x4 0xb 0x16".
```

Example:

```
  ./mehutl.exe sys_cfg_mcbc_data_rate 22
        Set AP MCBC data rate to 11 M
```

./mehutl.exe sys_cfg_mcbc_data_rate 0
Set AP MCBC data rate to auto

*./mehutl.exe sys_cfg_mcbc_data_*rate
Get AP MCBC data rate

2.3.28 sys_cfg_pkt_fwd_ctl

"./mehutl.exe sys_cfg_pkt_fwd_ctl [0|1]"

This command is used to set or get the packet forwarding control settings.

The supported options are:
0 Forward all packets to the host
1 Firmware handles intraBSS packets
empty Get current packet forwarding setting

Example:
./mehutl.exe sys_cfg_pkt_fwd_ctl 1
Set AP packet forwarding control to firmware handles intraBSS packets mode

./mehutl.exe sys_cfg_pkt_fwd_ctl
Get AP packet forwarding control

2.3.29 sys_cfg_sta_ageout_timer

"./mehutl.exe sys_cfg_sta_ageout_timer [STA_AGEOUT_TIMER]"

This command is used to set or get the STA ageout value.

Value of 0 will mean that stations will never be aged out.

Minimum value for this is 300. Maximum allowed setting should be 864000.

If no arguments are given, this command returns the current STA ageout value.

Ageout timer value is represented in units of 100 ms.

Example:
./mehutl.exe sys_cfg_sta_ageout_timer 1800
Set AP STA ageout time to 180000 ms

./mehutl.exe sys_cfg_sta_ageout_timer
Get AP STA agout time

2.3.30 sys_cfg_auth

```
"./mehutl.exe sys_cfg_auth [AUTHMODE]"

This command is used to set or get the AP authentication mode.

The supported options are:
    AUTHMODE :     0  Open authentication
                   1  Shared key authentication
empty  Get current authentication mode
```

Example:
./mehutl.exe sys_auth 0
Set AP authentication mode to Open.

./mehutl.exe sys_cfg_auth
Get AP authentication mode.

2.3.31 sys_cfg_protocol

```
"./mehutl.exe sys_cfg_protocol [PROTOCOL]"

This command is used to set or get the encryption protocol.

The supported options are:
  PROTOCOL:
             1           No RSN
             2          WEP Static
             8           WPA
             32          WPA2
             40         WPA2 Mixed Mode
empty  Get current encryption protocol
```

Example:
./mehutl.exe sys_cfg_protocol 2
Set AP encryption protocol to static WEP.

./mehutl.exe sys_cfg_protocol
Get AP encryption protocol.

2.3.32 sys_cfg_wep_key

```
"./mehutl.exe sys_cfg_wep_key [INDEX ISDEFAULT Key_0]
                              [INDEX ISDEFAULT Key_1]
                              [INDEX ISDEFAULT Key_2]
                              [INDEX ISDEFAULT Key_3]
                              [INDEX]"

This command is used to set or get the WEP key settings.

The supported options are:
    INDEX:       0  KeyIndex is 0
```

```
                1  KeyIndex is 1
                2  KeyIndex is 2
                3  KeyIndex is 3
  ISDEFAULT:   0: KeyIndex is not the default
              1: KeyIndex is the default transmit key

    KEY_* :      Key value.
    empty  Get current WEP key settings for all the keys
    INDEX  Only INDEX will get the key setting for the particular
            KeyIndex.
```

Example:

./mehutl.exe sys_cfg_wep_key 0 1 55555
Set AP's default transmit key to "55555", key index is 0.

./mehutl.exe sys_cfg_wep_key
Get AP all the WEP keys settings.

./mehutl.exe sys_cfg_wep_key 1
Get WEP key setting for the KeyIndex = 1.

2.3.33 sys_cfg_cipher

```
"./mehutl.exe sys_cfg_cipher [PAIRWISE_CIPHER GROUP_CIPHER]"

This command is used to set or get the key types for the pairwise and
group key.

The supported options are:
  PAIRWISE_CIPHER:
             0           None
             4           TKIP
             8          AES CCMP
             12         AES CCMP + TKIP
    GROUP_CIPHER:
             0           None
             4           TKIP
             8          AES CCMP
  empty  Get current key types

  Valid combinations of [PAIRWISE_CIPHER GROUP_CIPHER] are:
       [0 0], [4 4], [8 8], [12 4].
```

Example:

./mehutl.exe sys_cfg_cipher 4 4
Set AP's pairwise and group key's type to TKIP.

./mehutl.exe sys_cfg_cipher
Get AP's key types for the pairwise and group key.

2.3.34 sys_cfg_group_rekey_timer

```
    "./mehutl.exe sys_cfg_group_rekey_timer [GROUP_REKEY_TIMER]"

    This command is used to set or get the AP group rekey time interval,
    in seconds.

    The supported options are:
        GROUP_REKEY_TIMER is represented in seconds. This is only
applicable
                    if the protocol is WPA or WPA2.

        empty  Get current group rekey timer
```

Example:

```
  ./mehutl.exe sys_cfg_group_rekey_timer 1800
        Set AP's group rekey time interval to 1800 s

  ./mehutl.exe sys_cfg_group_rekey_timer
        Get AP's group rekey time interval.
```

2.3.35 sys_cfg_wpa_passphrase

```
    "./mehutl.exe sys_cfg_wpa_passphrase [PASSPHRASE]"

    This command is used to set or get the WPA or WPA2 passphrase.

    If no arguments are given, this command returns the current WPA or
WPA2
    passphrase.
      While setting, the maximum length of the passphrase can be 64
      characters.
```

Example:

```
  ./mehutl.exe sys_cfg_wpa_passphrase 1234567890
        Set AP's WPA or WPA2 passphrase to "1234567890"

  ./mehutl.exe sys_cfg_wpa_passphrase
        Get AP's WPA or WPA2 passphrase.
```

2.3.36 sys_cfg_max_sta_num

```
    "./mehutl.exe sys_cfg_max_sta_num [STA_NUM]"

    This command is used to set or get the maximum number of stations
    allowed to connect to MEH.

    The maximum STA_NUM allowed is 8.

      If no arguments are given, this command returns the maximum number
      of stations allowed to connect to MEH.
```

Example:
./mehutl.exe sys_cfg_max_sta_num 2
Set AP's maximum station number to 2

./mehutl.exe sys_cfg_max_sta_num
Get AP's maximum station number

2.3.37 sys_cfg_retry_limit

"./mehutl.exe sys_cfg_retry_limit [RETRY_LIMIT]"

This command is used to set or get the retry limit to use for packet transmissions.

The maximum retry_limit allowed is 14.

If no arguments are given, this command returns the current retry limit value.

Example:
./mehutl.exe sys_cfg_retry_limit 2
Set AP's retry limit value to 2

./mehutl.exe sys_cfg_retry_limit
Get AP's retry limit value

2.3.38 sys_cfg_custom_ie

"./mehutl.exe sys_cfg_custom_ie [INDEX] [MASK] [ISBuffer]"

This command is used to set or get custom IEs for management frames.

The supported options are:
INDEX: 0 IE Index is 0
1 IE Index is 1
2 IE Index is 2
3 IE Index is 3
MASK : Management subtype mask value as per bit defintions
: Bit 0 Association request.
: Bit 1 Association response.
: Bit 2 Reassociation request.
: Bit 3 Reassociation response.
: Bit 4 Probe request.
: Bit 5 Probe response.
: Bit 8 Beacon.
MASK : MASK = 0 to clear the mask and the IE buffer

IEBuffer: IE buffer to set in hexadecimal bytes.
The Buffer should not be space separated.
(Maximum length = 256 bytes)
empty Get IE buffer, subtype mask settings for all the indices [03].

INDEX Only INDEX will get the IE buffer configured for the particular Index.

Example:
./mehutl.exe sys_cfg_custom_ie
Get IE buffer, subtype mask settings for all indices [03].

./mehutl.exe sys_cfg_custom_ie 1
Get IE buffer and subtype mask WEP key setting for the Index = 1.

./mehutl.exe sys_cfg_custom_ie 2 0
Clear IE buffer and mask value for Index = 2.

./mehutl.exe sys_cfg_custom_ie 3 0x101 0x1234567890
Set IE buffer and mask value for Index = 3.

2.3.39 sta_filter_table

"./mehutl.exe sta_filter_table <FILTERMODE> [<MACADDRESS_LIST>]"

This command is used to get or set the client station MAC address filter table.

The supported options are:
FILTERMODE : 0 Disable filter table
1 Allow mac address specified in the allwed list
2 Block MAC addresses specified in the banned list
MACADDRESS_LIST is the list of MAC addresses to be acted upon. Each MAC address must be separated with a space. Maximum of 16 MAC addresses are supported.

empty Get current client station MAC address filter table.

Example:
./mehutl.exe sta_filter_table 0
Disable filter table

./mehutl.exe sta_filter_table 1 00:50:43:20:aa:bb
Set AP's filter mode to allow, only MAC address "00:50:43:ab:bb" will be allowed.

./mehutl.exe sta_filter_table
Get AP's filter table settings.

2.3.40 regrdwr

"./mehutl.exe regrdwr <TYPE> <OFFSET> [value]"

These commands are used to read the MAC, BBP, RF and PMIC registers from the card.
TYPE can take 3 values, 0 read/write MAC register

```
                        1  read/write BBP register
                        2  read/write RF  register

OFFSET specifies the offset location that is to be read.
This parameter can be specified either in decimal or in hexadecimal
(by preceding the number with a "0x").

value if specified, then that value will be written to that offset in
the specified register. Value should be
specified in hexadecimal.
```

Example:

./mehutl.exe regrdwr 0 0xa123
read MAC register 0xa123

./mehutl.exe regrdwr 0 0xa123 0xaa
write 0xaa to MAC regiser 0xa123

./mehutl.exe regrdwr 1 0x0123
read BBP register 0x0123

./mehutl.exe regrdwr 1 0x0123 0xaa
write 0xaa to BBP register 0x0123

./mehutl.exe regrdwr 2 0x0123
read RF regisert 0x0123

./mehutl.exe regrdwr 2 0x0123 0xaa
write 0xaa to RF regiser 0x0123

2.3.41 memaccess

```
"./mehutl.exe memaccess <ADDR> [value]"
This commands is used to read/write to a memory address

ADDR specifies the address of the location that is to be read/write
This parameter can be specified either in decimal or in hexadecimal
(by preceding the number with a "0x").

value if specified, then that value will be written to that address
in the specified register.
```

Example:

./mehutl.exe memaccess 0xc00153e4
read contents of memory location 0xc00153e4

./mehutl.exe memaccess 0xc00153e4 0xaabbccdd
write value 0xaabbccdd to memory location 0xc00153e4

2.3.42 rdeeprom

```
"./mehutl.exe rdeeprom <offset> <bytecount>"

This command is used to read bytes from offset location on
EEPROM

offset: 0,4,8,..., multiple of 4
bytecount: 420, multiple of 4
```

Example:
./mehutl.exe rdeeprom 200 12
read 12 bytes from offset 200 ON EEPROM

2.3.43 cfg_data

```
"./mehutl.exe cfg_data <type> [*.conf]"

This command is used to set/get the configuration data to/from the
firmware.

type: 2  cal data
```

Example:
./mehutl.exe cfg_data 2 cal_data.conf
read cal_data from cal_data.conf and download to firmware.
./mehutl.exe cfg_data 2
read cal_data from firmware

2.3.44 sys_debug

```
"./mehutl.exe sys_debug [subcmd] [parameter]
This command is used to set/get debug parameters.
If no [parameter] are given, this command returns the debug
parameters for selected subcmd.

subcmd : 1  used to set/get global debug mode
         2  used to set/get MajorId mask
         3  used to set user scan
          N  Any other value is used for FW specific debugging and
         should not be used.

parameter: parameters for specific subcmd.
        This parameter can be specified either in decimal or
           in hexadecimal (by preceding the number with a "0x").
```

Example:
./mehutl.exe sys_debug 1 1
Enable global debug mode.

./mehutl.exe sys_debug 1 0
Disable global debug mode

./mehutl.exe sys_debug 1
Get current global debug mode

./mehutl.exe sys_debug 2
Get current MajorId mask

./mehutl.exe sys_debug 2 0x123
Set current MajorId mask to 0x123

./mehutl.exe sys_debug 3
Set channel scan. The command displays Channels scanned, number of APs,
CCA count, duration and weight of the channel.

2.3.45 powermode

```
    "./mehutl.exe powermode [MODE] [SLEEP_PARAM=1 CTRL MIN_SLEEP
MAX_SLEEP]
                                    [INACT_PARAM=2 INACTTO MIN_AWAKE
MAX_AWAKE]"

    This command is used to set or get the AP's power mode, sleep param
    and inactivity sleep param.

    inactivity sleep param should only be set when powermode is inactivity
    based power save mode.

    The supported options are:
        MODE :     0  disable power mode
                   1  enable periodic DTIM power save mode
                   2  enable inactivity based power save mode

        SLEEP_PARAM:
            CTRL:  0  disable NULL data protection frame Tx before PS
                   1  enable NULL data protection frame Tx before PS
           MIN_SLEEP: Minimum sleep duration in microseconds, default
           value 10000 us
            MAX_SLEEP: Maximum sleep duration in miroseconds, default
           value 10000 us
            (Current only support same value for MIN_SLEEP and MAX_SLEEP)

        INACT_PARAM:
           INACTTO: Inactivity timeout in miroseconds, default value is
           500000 us
            MIN_AWAKE: Minimum awake duration in microseconds, default
           value is 20000 us
            MAX_AWAKE: Maximum awake duration in microseconds, default
           value is 20000 us
            (Current only support same value for MIN_AWAKE and MAX_AWAKE)

      empty  Get current power mode
```

Example:
./mehutl.exe powrmode 0
Disable AP's power mode.

./mehutl.exe powrmode 1
Enable periodic DTIM power save mode.

./mehutl.exe powrmode 2
Enable inactivity based power save mode.

./mehutl.exe powrmode 1 1 1 20000 20000
Enable periodic DTIM power save mode, and set sleep param, enable NULL data protection, and set minimum sleep during to 20000 us, maximum sleep duration to 20000 us

./mehutl.exe powrmode 2 2 400000 10000 10000
Enable inactivity based power save mode and set inactivity sleep param with inactivity timeout 400000 us, minimum awake duration to 10000us , maximum awake duration to 10000 us

./mehutl.exe powermode
Get current AP's power mode.

---

3 USER MANUAL FOR MEHEVENT

NAME

mehevent.exe

This tool can be used to listen for and obtain events from the MEH driver through the netlink layer.

3.1 Supported events

STA_DEAUTH
STA_ASSOC
BSS_START
BSS_IDLE
BSS_ACTIVE

3.2 Details of events

3.2.1 STA_DEAUTH

For this event, the following information is shown:
+ Deauthenticated STA MAC address.

```
    + Reason for deauthentication.
```

3.2.2 STA_ASSOC

```
For this event, the following information is shown:
    + STA MAC address.
```

3.2.3 BSS_START

```
For this event, the following information is shown:
    + AP MAC address.
```

3.2.4 BSS_IDLE

```
For this event, there is no associated information.
```

3.2.5 BSS_ACTIVE

```
For this event, there is no associated information.
```