Mediant MSBR

Wireless Access Configuration

Version 6.8

HD VoIP
Sounds Better

AudioCodes

Table of Contents

List of Tables

Notice

This Configuration Note shows how to configure the Mediant MSBR Wireless Access feature.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published, nor can it accept responsibility for errors or omissions. Updates to this document and other documents as well as software files can be viewed by registered customers at http://www.audiocodes.com/downloads.

Date Published: February-25-2016

Trademarks

AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNOM and CloudBond 365 are trademarks or registered trademarks of AudioCodes Limited All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our Web site at www.audiocodes.com/support.

Document Revision Record

LTRT	Description
40365	Initial document release.
40366	Updates to the radio transmission CLI commands, diagnostic commands and support for the WEP mode.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at http://www.audiocodes.com/downloads

1 Introduction

AudioCodes' Mediant Multi-Service Business Routers (MSBRs) feature an optional wireless (IEEE 802.11a/b/g/n) integrated access point.

This document shows how to deploy, configure and diagnose wireless access support on the MSBRs.

> **Note:** The Mediant MSBRs include Mediant 500 MSBR and Mediant 800 MSBR.

The wireless interface can like all MSBR features be managed by CLI commands. By default, the MSBR is supplied with the wireless interface disabled.

The Mediant 500 MSBR, in addition to CLI management, features an external radio shutdown push-button which can be used to enable or disable the wireless radio feature (available in Firmware Version 6.8).

This page is intentionally left blank.

2   Topologies

The default wireless configuration includes:

- One wireless access point (`interface dot11radio 1`), no IP address
- One LAN interface (`interface VLAN 1`), no IP address
- A bridge connecting Wi-Fi and LAN
- Virtual IP on the bridge (`interface BVI 1`) including a DHCP server

In this topology, Wi-Fi and LAN are bridged and use the same IP addressing range. A common DHCP server is used to distribute IP addresses to both Wi-Fi stations and LAN computers. This topology is similar to that provided by commodity residential wireless routers, as it allows simple connectivity between existing LAN and Wi-Fi elements.

> **Note:** A Wi-Fi-enabled MSBR differs from other MSBR assemblies in this respect: without Wi-Fi, the factory default is to run IP services directly on VLAN 1, without a BVI interface.

Alternatively, the MSBR administrator can create more sophisticated topologies:

- Up to 4 virtual Wi-Fi access points (four different Service Set IDs (SSIDs))
- IP services can run directly on the Wi-Fi interfaces, implying that traffic between LAN and Wi-Fi will be routed, not bridged
- Some virtual access points can be bridged to a guest network, allowing others to access the corporate LAN or WAN connection
- Different security options for each virtual access point, e.g. for guest access.

This page is intentionally left blank.

3 Basic CLI Configuration Commands

This section shows the basic CLI configuration commands.

They're issued in **interface dot11radio X** context.

Table 3-1: Basic CLI Configuration Commands

Command	Description and Values
ssid [x]	Defines the wireless network name (SSID).
[no] broadcast	Enables or disables a "silent" virtual access point. Stations can connect to the network only if configured with the correct SSID.
bridge-group [x]	Associates the interface with a bridge. Note that the corresponding BVI interface must be enabled (**no shutdown**).
ip (...)	Defines IP characteristics such as IP address and DHCP behavior.
[no] shutdown	Enables or disables the wireless interface.

3.1 Bridged Topology: Example Configuration

The following CLI code shows configuration of a bridged topology:

```
configure data
  interface dot11radio 1
    no ip address
    ssid MSBR-BRIDGE
    security mode NONE
    bridge-group 1
    no shutdown
    exit
  interface VLAN 1
    no ip address
    bridge-group 1
    no shutdown
    exit
  interface BVI 1
    ip address 192.168.0.1 255.255.255.0
    ip dhcp-server network 192.168.0.3 192.168.0.10 255.255.255.0
    service dhcp
    no shutdown
    exit
  exit
```

3.2   Routed Topology: Example Configuration

The following CLI code shows configuration of a routed topology:

```
configure data
  interface dot11radio 1
    ip address 192.168.10.1 255.255.255.0
    ip dhcp-server network 192.168.20.3 192.168.20.10
255.255.255.0
    service dhcp
    ssid MSBR-ROUTE
    security mode NONE
    no shutdown
    exit
  exit
```

4   Security Options

Wi-Fi access points operate in one of the four security modes shown in the table below.

> **Note:**
>
> - **WPA2-Enterprise** mode is the most secure but is hardest to set up due to the requirement for an external authentication server (RADIUS).
> - **MSBR Firmware Version 6.8** includes a built-in RADIUS server, allowing easy deployment of **WPA2-Enterprise** mode *without additional costs*.

Table 4-1: Security Mode Descriptions

Security Mode	Description
Open	No authentication, no encryption. In this mode, anyone can connect to the network; more importantly, any wireless station can read and intercept all traffic between the access-point and other stations. The mode is comparable to an unsecured Ethernet hub. Recommended for guest access only.
WEP	Admission to the network requires knowledge of a shared key (a password). The key is provisioned on each station manually. All stations share the same key so once a wireless station is configured with the password, it can read and intercept all traffic. WEP mode is provided for compatibility purposes and is not recommended for use as the protocol is weak and can easily and quickly be cracked. WEP mode is not applicable for 802.11N mode.
WPA2-PSK	Similar to WEP only the encryption protocol is harder to crack. This is the most commonly deployed security mode. It's important to note that even in this mode an attacker can decode all traffic once they obtain the shared password (even retroactively, by recording the traffic and later obtaining the password).
WPA2-Enterprise	Admission to the network requires verification by an external authentication server using digital keys or user/password combinations (IEEE 802.1x protocol). Each station is provisioned with a separate authentication token and can never intercept traffic destined to other stations.

All four security modes support further access restrictions based on the station's hardware (MAC) address. This is not recommended as hardware addresses are hard to manage and easy to spoof.

4.1 Security Modes: Example Configurations

The table below shows examples of security mode configurations.

Table 4-2: Security Modes – Example Configurations

Security Mode	Code
Open	`security mode NONE`

WEP	`security wep 1 hex 40 0a110b220c`
	`security wep activeKey 1`
	`security mode WEP`

WPA2-PSK	`security wpa psk ascii PLETMEIN`
	`security wpa mode psk`
	`security mode WPA2`

WPA2-Enterprise (external RADIUS)	`security wpa mode 802.1x`
	`security 802.1x radius server ip 192.168.0.50`
	`security 802.1x radius server secret RADSECRET`
	`security mode WPA2`

MAC-based filter	`security mac addr 00:90:8f:11:22:33` `security mac allow`

WPA2-Enterprise (internal RADIUS, firmware version 6.8)	`security wpa mode 802.1x`
	`security 802.1x radius server local`
	`security mode WPA2`
	`dot1x user joe password LetMeIn`

5   Radio Channel Options

All wireless traffic is broadcast over a single radio channel; by default, the MSBR detects the best channel to use at startup. Alternatively, the administrator can select a different channel via CLI.

Channel selection depends on regulatory requirements for the country in which the MSBR is deployed, which must be specified as part of the Purchase Order.

The following CLI commands control radio transmission.

> **Note:** These must be defined in the context of `interface dot11radio 1`, the physical interface.

Table 5-1: Radio Transmission CLI Commands

Command	Description and Values
`channel [x]`	1-13, 36-64, 100-140, 149-165
`channel auto [5-ghz]`	Selects the best channel automatically. 5-ghz, this is a sub-command useful for 802.11n mode only, where auto scan can switch between 2.4GHz and 5GHz depending on the band usage. By default, the MSBR works on 2.4GHz.
`channel width [40/20 | 20]`	Attempts to use double-width channels (40MHz) if possible
`mode [x]`	a, b, g, n, na, ngb, ngba Selects allowed IEEE 802.11 transmission standards
`power [x]`	1-100 percent of maximum transmission power
`beacon period [x]`	Controls the rate of periodic beacon messages transmitted by the access-point (in milliseconds)
`burst num [x]`	Selects how many 802.11 frames are transmitted in sequence. Lower values reduce collisions but impact network speed.
`cts mode [auto | none]`	Enables CTS (Clear-To-Send) protection: the access point circulates a token between all associated stations, allowing only one to transmit at a time. Reduces collisions but significantly impacts network latency.
`rts threshold [x]`	Defines minimum packet size for an RTS (Request-To-Send). Lower values reduce collisions but impact overall speed.
`fragment threshold [256-2346]`	Sets the fragmentation threshold.
`cts type [cts | rts-cts]`	Sets the cts type
`Beacon dtim-period [x]`	Defines the Delivery Time Indication Map for power-save stations.
`wmm`	Turns on/off Wireless Multi-Media support
`channel auto-rescan`	Searches for the best available channel every five minutes if there are no clients connected to the WiFi access point.
`burst [x]`	Sets the burst interval.

This page is intentionally left blank.

6   Master Shutdown (Firmware Version 6.8 Only)

In addition to supporting a shutdown/no-shutdown selector for each `dot11radio` interface, the MSBR supports a global master radio shutdown option which disables all Wi-Fi interfaces regardless of their shutdown state.

The Mediant 500 MSBR also features an external push-button on the device which controls this setting, allowing the administrator to quickly cut off wireless transmissions.

This setting must be entered in global `configure data` context:

Table 6-1: Master Shutdown

Command	Description and Values
`[no] radio shutdown`	Blocks all 802.11 radio interfaces.

This page is intentionally left blank.

7   Diagnostics

The CLI commands shown in the table below displays the current Wi-Fi operational information.

Table 7-1: CLI Commands to Display Wi-Fi Operational Information

Command	Description
`show data dot11radio associations [all │ interface X]`	Displays currently connected stations. Subcommands control filtering of stations by virtual access point.
`show data dot11radio associations stats interface [x] [all │ mac xx:xx:xx:xx:xx:xx]`	Displays traffic counters per connected station.
`show data dot11radio channel`	Displays current channel value.
`show data dot11radio country-code`	Displays regulatory country code (defined in the Feature Key).
`show data dot11radio other-ap`	Scans for other access points in the neighborhood of the MSBR. This command can only be issued in automatic mode.
`show data ip dhcp binding`	Displays current DHCP server database, including Wi-Fi stations and LAN hosts.
`show data interfaces dot11radio [x]`	Displays counters, operational status, and IP information if available.
`show data dot11radio hardware-stats`	Shows the internal hardware counters.
`show data dot11radio channel`	Displays channel width.

7.1 Diagnostics: Example Configurations

The following CLI code shows diagnostics configurations:

```
MSBR# show data dot11radio associations all
dot11radio 1:
ADDR              CHAN  RATE  Power
3c:43:8e:2d:ba:c4   10   65M  20dBm


MSBR# show data dot11radio associations stats interface 1 mac
3c:43:8e:2d:ba:c4
MAC ADDR          Rx packets   Rx bytes     Tx packets   Tx bytes
3c:43:8e:2d:ba:c4     41         3773          41          4460


MSBR# show data dot11radio other-ap
SSID            BSSID             CHAN RATE
Nubo-AP         64:d9:89:43:a8:b0   1   54M  7:0
MP264_3FFDFC    00:90:8f:3f:fe:00   2   54M 14:0
MP252_YK        00:90:8f:2c:e2:e4   2   54M 18:0
audc-ph         00:0b:86:2d:38:72   2   54M 37:0
AudioCodes      00:0b:86:40:41:c0   2   54M 21:0
Guest-AudC      00:0b:86:40:41:c1   2   54M 22:0


MSBR# show data ip dhcp binding
Host name            Ip address     Mac address          IF name
Lease
android_fb172162f8e6 192.168.71.100  3c:43:8e:2d:ba:c4   BVI 1      52
```

This page is intentionally left blank.

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: www.audiocodes.com/info
Website: www.audiocodes.com

Document #: LTRT-40366