Configuration Guide

Multi-Service Business Routers Product Series

Mediant MSBR

Version 7.2

Table of Contents

1 Introduction 7

2 Topologies 9

3 Basic CLI Configuration Commands 11

3.1 Bridged Topology - Example Configuration 11

3.2 Routed Topology - Example Configuration 12

4 Security Options 13

4.1 Security Modes - Example Configurations 14

5 Radio and VAP configuration 15

6 Master Radio Shutdown 17

7 Diagnostics 19

7.1 Diagnostics - Example Configurations 20

List of Tables

Table 3-1: Basic CLI Configuration Commands 11
Table 4-1: Security Mode Descriptions 13
Table 4-2: Security Modes – Example Configurations 14
Table 5-1: Radio Transmission CLI Commands 15
Table 6-1: Master Shutdown 17
Table 7-1: CLI Commands to Display Wi-Fi Operational Information 19

Notice

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 can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: October-06-2020

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 website at https://www.audiocodes.com/services-support/maintenance-and-support

Stay in the Loop with AudioCodes

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.
40367	Update for version 7.2.
40368	Document template update e
40369	MFP security, etc.

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 website at https://online.audiocodes.com/documentation-feedback.

1 Introduction

AudioCodes' Mediant Multi-Service Business Routers (MSBRs) provide an optional wireless (IEEE 802.11a/b/g/n) integrated access point.This document shows how to deploy, configure and diagnose the wireless access support on the MSBRs.

Note: This document is applicable to Mediant 500 MSBR, Mediant 500L MSBR, Mediant 800 MSBR, and Mediant 500Li MSBR.

The wireless interface is managed through the MSBR's CLI. By default, the MSBR is supplied with the wireless interface disabled. For the Mediant 500L/500Li MSBR, in addition to CLI management, provide an external radio shutdown push-button which can be used to enable or disable the wireless radio feature.

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 like 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 or SSIDs)
- IP services can run directly on the Wi-Fi interfaces, implying that traffic between LAN and Wi-Fi are **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 describes the basic CLI configuration commands. They're issued from the **interface dot11radio X** context.

Table 3-1: Basic CLI Configuration Commands

Command	Description and Values
ssid [x]	Defines the wireless network name (SSID).
bridge-group [x]	Associates the interface with a bridge. **Note:** 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 shows configuration of a bridged topology:

```
configure data
interface dot11radio 1
   no ip address
   bridge-group 1
   mtu auto
   desc "LAN Wireless 802.11ngb 2.4GHz Access Point"
   no ipv6 enable
   no service dhcp
   ssid MSBR500
   broadcast
   security mode NONE
   no security mac mode
   mode ngb
   channel width 40/20
   channel auto
   power 100
   beacon dtim-period 100
   beacon period 100
   fragment threshold 2346
   cts mode  auto
   cts type  rts_cts
   burst num 3
   burst time  2
   rts threshold 2347
   wmm
   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 shows the configuration part of a routed topology:

```
configure data
  interface dot11radio 1
    ip address 192.168.10.1 255.255.255.0
    ip dhcp-server network 192.168.10.3 192.168.10.10
255.255.255.0
    service dhcp
    ssid MSBR-ROUTE
    security mode NONE
    no shutdown
    exit
  exit
```

4 Security Options

This section provides the security options and recommendations to configure the Mediant MSBR.

Note:

- **WPA2-Enterprise** mode is the most secure, but is the most difficult to set up due to the requirement for an external authentication server (RADIUS).
- **WPA2-Enterprise** includes a built-in RADIUS server, allowing easy deployment of the 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.

Mediant 500Li MSBR supports the IEEE 802.11w-2009 wireless encryption standard, which is based on the 802.11i framework and protects against subtle attacks on wireless LAN management frames

MFP Mode	Description
Disabled	Disabled MFP for the client (default).
Optional	Sets MFP only with MFP-supporting clients.
Required	Clients are allowed to associate only if MFP is negotiated. If the devices do not support MFP, they are not allowed to join the network.

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 and VAP configuration

The configuration of the dot11radio interface consist of commands used to set logical parameters like security and packet fragmentation as well as physical parameters like transmit power and selected channel.

The dot11radio 1 interface is considered the “leader” of the rest of the VAPs in terms of the physical parameters, as those can’t be set on the VAPs and must be unified. The dot11radio 1 interface can’t be removed from configuration like the other VAPs.

Table 5-1: Radio Transmission CLI Commands

Command	Description and Values
`channel [x]`	1-13 (on MSBR 500L/500Li models). 36-64, 100-140, 149-165 (on MSBR 500/800).
`[no] broadcast`	Enables or disables a “silent” virtual access point. Stations can connect to the network only if configured with the correct SSID.
`channel auto [5-ghz]`	Selects the best channel automatically. 5-ghz 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]`	Selects allowed IEEE 802.11 transmission standards a, b, g, n, ngb (on MSBR 500L/500Li models). a, b, g, n, na, ngb, ngba (on MSBR 500/800 models).
`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 Wi-Fi access point.
`burst [x]`	Sets the burst interval.

Command	Description and Values
`mfp[disabled|optional|required]`	The device supports the IEEE 802.11w-2009 wireless encryption standard, which is based on the 802.11i framework and protects against subtle attacks on wireless LAN management frames (MSBR 500Li only). ▪ Disabled: disabled MFP for the client (default). ▪ Optional: Sets MFP only with MFP-supporting clients. ▪ Required: clients are allowed to associate only if MFP is negotiated. If the devices do not support MFP, they are not allowed to join the network.

6 Master Radio Shutdown

In addition to supporting a shutdown/no-shutdown selector for each **dot11radio** interface, the MSBR 500L/500Li supports a global master radio shutdown option which disables all Wi-Fi interfaces regardless of their state.

The MSBR 500L/500Li 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 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 near 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 (applicable only for MSBR 500).
`show data dot11radio channel`	Displays channel width.

7.1 Diagnostics - Example Configurations

The following CLI commands shows diagnostics configurations for the MSBR 500/800 models:

```
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
```

The following CLI commands show diagnostics configurations for the MSBR 500Li model:

```
M500Li# show data dot11radio associations all
dot11radio 1:
Station 2c:fd:a1:ce:b2:5d (on wlan0)
        inactive time:  403 ms
        rx bytes:       142961
        rx packets:     2615
        tx bytes:       6712
        tx packets:     82
        signal:         -83 dBm
        tx bitrate:     0.2 MBit/s
        rx bitrate:     2.7 MBit/s


M500Li# debug dot11radio events
Waiting for events...
Press Ctrl-C to interrupt.

 [0002487169] MTDUMP LISTEN EVENT:
Peer connection event:
     2C:FD:A1:CE:B2:5C : Peer MAC address
            Shared key : 802.11 authentication type
            Successful : Connection status
```

```
 [0002528016] MTDUMP LISTEN EVENT:
Peer disconnection event:
     2C:FD:A1:CE:B2:5C : Peer MAC address
            Local side : Initiated by
          User request : Disconnect reason
  Additional info:
    Peer capabilities:
                             : Supported network modes
                   802.11b :
                   802.11g :
                   802.11n :
                  802.11ac :
                           :
                      True : WMM is supported
                      True : Channel bonding supported
                      True : SGI20 supported
                      True : SGI40 supported
                      True : STBC supported
                      True : LDPC supported
                     False : Explicit beam forming supported
                     False : 40MHz intolerant
                   Unknown : Vendor
                         1 : Max TX spatial streams
                         1 : Max RX spatial streams
                         3 : Maximum A-MPDU Length Exponent
                         5 : Minimum MPDU Start Spacing
             40847 msec ago : Timestamp of station association
  Additional info:
    Peer packets flow statistics:
       0 : StationID
      Traffic statistics:
Peer Traffic Statistics:
4580 : BytesSent                - Number of bytes sent successfully
128506 : BytesReceived            - Number of bytes received
65 : PacketsSent              - Number of packets transmitted
3157 : PacketsReceived          - Number of packets received
2.0 : LastDataDownlinkRate - Last data transmit rate (to peer) [Mbps]
15.0 : LastDataUplinkRate   - Last data receive rate (from peer)
[Mbps]
0 : AirtimeUsage         - Air Time Used by RX/TX to/from STA [%]
0 : AirtimeEfficiency    - Efficiency of used air time [bytes/sec]
 SignalStrength       - Short-term RSSI average per antenna [dBm]
                        -128 : [0]
                         -89 : [1]
                         -89 : [2]
                         -86 : [3]
```

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

AudioCodes Inc.
200 Cottontail Lane
Suite A101E
Somerset NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: www.audiocodes.com/contact
website: www.audiocodes.com

Document #: LTRT-40369