**Azalea Networks**

Wireless Broadband
Anywhere Anytime

# MSR SERIES WIRELESS MESH ROUTER

# CLI CONFIGURATION GUIDE

**AOS-v1.5.0**

www.azaleanet.com

## Copyright 2007 Azalea Networks

## Trademarks

## Statement of Conditions

In the interest of improving internal design, operation function, and/or reliability, Azalea Networks reserves the right to make changes to products described in this document without notice.
Azalea Networks does not assume any liability that may occur due to the use or application of the product(s) described herein.

## Contact

Azalea Networks Inc.
673 S. Milpitas Blvd, Suite 105,
Milpitas CA
95035 USA

sales@azaleanet.com
http://www.azaleanet.com

# Contents

# List of Figures

# List of Tables

# Chapter 1 About this Guide

This chapter covers the following topics:

- Scope
- Audience
- Related Documents

## Scope

This document provides the configuration instructions and examples for MSR series wireless mesh routers. It contains information on current features and protocols supported by MSR series.

***Note: The command examples and outputs are created with an MSR2000 router and is for demonstration purposes only. The exact output of the commands may vary depending on the router model and its firmware version.***

The scope of this document only includes the command-line interface of MSR series; for Web-based configuration, please see related documents.

## Audience

This document is intended for system/IT or network administrator who is responsible for configuring or maintaining MSR series; this guide is also assumed the user is knowledgeable in wireless/wire Layer2 and Layer 3 networking technologies.

## Related Documents

For more information about MSR series, please refer to the following documents:

- MSR series Quick Start Guide
- MSR series Web-based Configuration Guide

# Chapter 2 Configuration Fundamentals

This section covers the following main topics:

- CLI Modes
- Basic Configuration Information
- Software Image Upgrade

## CLI Modes

- CLI Modes
- The List Command
- CLI Navigation
- Deleting Command Lines in the Configuration
- Obtaining Help
- Entering and Editing Commands

### CLI Modes

The CLI is organized into multiple modes that allow navigation between different protocols and interface. Figure 1 displays the CLI modes and CLI structures that are available if you have full access to the CLI.

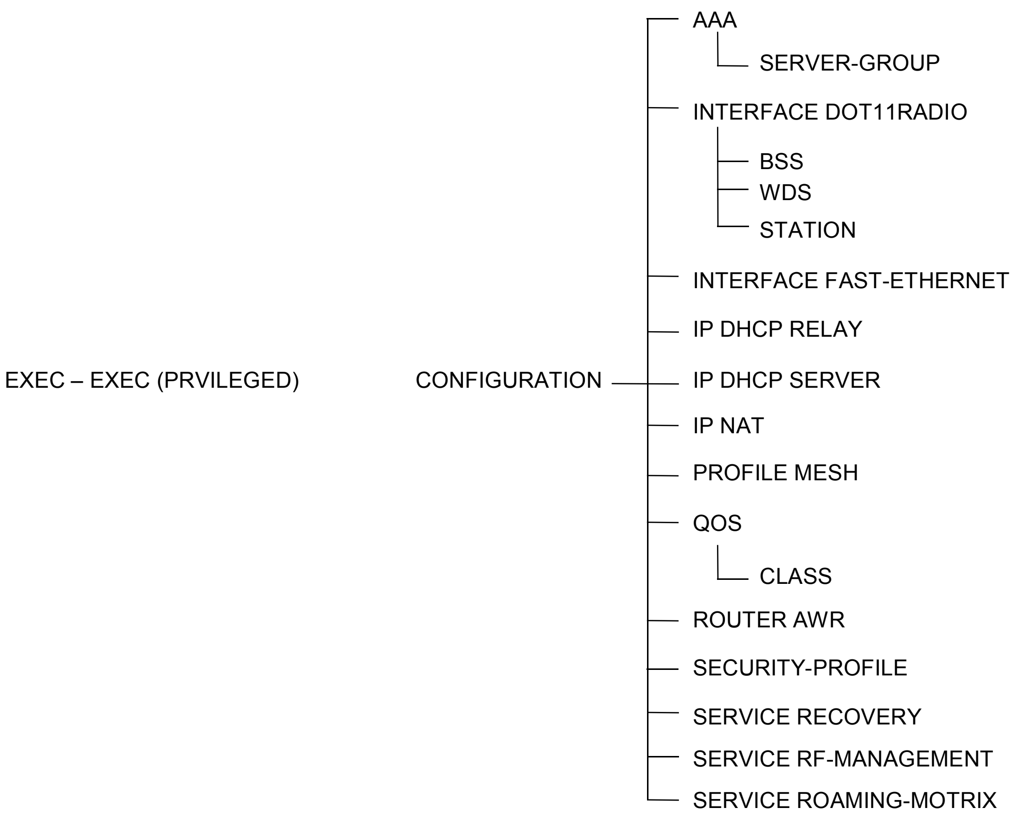


**Figure 1** CLI Modes

When you login, you are in the User EXEC mode where you can enter a limited number of commands, mostly **show** commands. In this mode, you can not make or change any configuration. You can only view system information or execute limited commands. In EXEC mode, the **enable** command prompts you for your password to allow you into Privileged EXEC mode.

**Privileged EXEC mode** has commands to view configuration, manage configuration files, run diagnostics, enable or disable debug operations, reboot the router. By default, the privilege level is 15. To configure the router, use the **configure terminal** command to enter the CONFIGURATION mode.

**CONFIGURATION mode** enables you to configure security features, setup various service and SNMP functions, configure static route, and you can enter protocol, interfaces, and line CLI modes to configure setting, and save the configuration.

**AAA mode** enables you to configure Radius servers used by the router's security features.

**INTERFACE DOT11RADIO mode** enables you to configure wireless and IP-layer settings for each radio card.

**INTERFACE FAST-ETHERNET mode** enables you to configure layer-2 and layer-3 settings for each Ethernet port.

**IP DHCP RELAY mode** enables you to configure the DHCP relay feature of the router. You may configure multiple DHCP Servers by IP address.

**IP DHCP SERVER mode** enables you to configure the built-in DHCP services provided by the router. You may configure the DNS, Domain name, lease time, etc.

**IP NAT mode** enables you to configure the NAT service for the router. You may configure choose an out-going network port to activate the NAT service on.

**PROFILE MESH mode** enables you to configure profiles containing mesh-sepcific settings. You may configure the mesh network ID in each profile.

**ROUTER AWR mode** enables you to configure the wireless routing protocol (AWR). You may enable or disable the protocol.

**QOS mode** enables you to configure the Quality of Service (QoS) features provided by the router.  You may define traffic classes and specify bandwidth control.

**SECURITY PROFILE mode** enables you to configure security profiles to be used on the router. You may configure MAC, IP, and WPA2 profiles.

**SERVICE RECOVERY mode** enables you to configure the automatic fault recovery service provided by the router.

**SERVICE RF-MANAGEMENT mode** enables you to configure the intelligent radio-frequency management service provided by the router.

**SERVICE ROAMING-MOTRIX mode** enables you to configure the Motrix roaming service provided by the router.

## The LIST Command

The LIST command allows a user to list all available commands for the current mode.

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **List** *command* | All **modes** | The **LIST** command lists all commands that may be entered in the current mode. |

The following are examples of using the list command:

```
MSR2000(config)# interface fast-ethernet 0
MSR2000(config-if-ethernet)# list
  dhcp relay
  dhcp server POOL-NAME
  dhcp server automatic
  end
  exit
```

```
help
interface fast-ethernet <0-1>
ip address A.B.C.D/M
ip address dhcp
list
mode access
mode gateway A.B.C.D
mode none
mtu <256-1500>
no dhcp
no ip address
no mode
no mtu
no shutdown
quit
show config
show running-config
shutdown
write file
write memory
write terminal
```

**Figure 2** list Command Examples

## CLI Navigation

To assist with navigation as you move among the CLI modes, the prompt changes to indicate the mode. Table 1 lists the CLI mode, its corresponding prompt, and information on how to access and exit this CLI mode.

**Table 1** CLI Mode Information

| CLI Command Mode | Prompt | To Enter Mode | To Exit mode |
|---|---|---|---|
| **User EXEC** | MSR2000> | Access the router through Telnet and successfully log in | User the **exit** commands. |
| **Privileged EXEC** | MSR2000# | From the EXEC mode, use the **enable** command.<br>From any other mode, use the **end** command. | Use the either the **exit** command. |
| **CONFIGURATION** | MSR2000(config)# | From the Privileged EXEC mode, use the **configure terminal** commands.<br>From every other modes except the EXEC and Privileged EXEC modes, use the **exit** command. | Use the either the **exit** or **end** command. |

| | | | |
|---|---|---|---|
| **AAA** | MSR2000(config-aaa)# | From the CONFIGURATION mode, use the **aaa** command. | |
| **SERVER-GROUP** | MSR2000(config-aaa-server-group)# | From the AAA mode, use the **server-group** command. | |
| **INTERFACE DOT11RADIO** | MSR2000(config-if-dot11radio)# | From the CONFIGURATION mode, use the **interface dot11radoi** command. | |
| **BSS** | MSR2000(config-if-dot11radio-bss)# | From the INTERFACE DOT11RADIO mode, use the **bss** command. | Use the **exit** commands to return to **CONFIGURATION** mode, except of **bss, wds, station** and **class**<br>Use the **end** to return to Privileged EXEC mode. |
| **WDS** | MSR2000(config-if-dot11radio-wds)#<br>MSR2000(config-if-dot11radio-wds-auto)# | From the INTERFACE DOT11RADIO mode, use the **wds or wds auto** command. | |
| **STATION** | MSR2000(config-if-dot11radio-sta)# | From the INTERFACE DOT11RADIO mode, use the **station** command. | |
| **INTERFACE FAST-ETHERNET** | MSR2000(config-if-ethernet)# | From the CONFIGURATION mode, use the **interface fast-ethernet** command. | |
| **IP DHCP RELAY** | MSR2000( config-dhcp-relay)# | From the CONFIGURATION mode, use the **ip dhcp relay** command. | |
| **IP DHCP SERVER** | MSR2000( config-dhcp-server)# | From the CONFIGURATION mode, use the **ip dhcp server** command. | |
| **IP NAT** | MSR2000( config-nat)# | From the CONFIGURATION mode, use the **ip nat** command. | |
| **PROFILE MESH** | MSR2000(config-profile-mesh)# | From the CONFIGURATION mode, use the **profile mesh** command. | |
| **QOS** | MSR2000(config-qos)# | From the CONFIGURATION mode, use the **qos** command. | |
| **CLASS** | MSR2000(config-qos-class)# | From the QOS mode, use the **class <name>** command. | |
| **ROUTER AWR** | MSR2000(config-awr)# | From the CONFIGURATION mode, use the **router awr** command. | |
| **SECURITY-PROFILE** | MSR2000(config-security-profile)# | From the CONFIGURATION mode, use the **security-profile** command. | |
| **SERVICE RECOVERY** | MSR2000 (config-recovery)# | From the CONFIGURATION mode, use the **service recovery** command. | |
| **SERVICE RF-MANAGEMENT** | MSR2000 (config-rfm)# | From the CONFIGURATION mode, use the **service rf-management** command. | |
| **SERVICE ROAMING-MOTIX** | MSR2000 (config-roaming)# | From the CONFIGURATION mode, use the **service roaming-motrix** command. | |

## Deleting Command Lines in the Configuration File

Each command enters a command line in the MSR series running configuration file and the “no” form of the command removes the command line form the running configuration file. To disable a command, use the “no” form of that command. The majority of the commands in the CLI have a “no” command that disables the command or re-enable a disabled function. For example, to delete a static route, use the **no** ip route <*IP destination prefix*> <*Gateway IP address*> command syntax. For both the command syntax and the “no” syntax, refer to *CLI Command Line Interface Reference.*

**Table 2 CLI** Mode Information (**no** command)

```
MSR2000(config)# no ip route 10.2.2.0/24 10.1.1.1
```

## Obtaining Help

CLI mode enables several ways for you to obtain help and list the available commands in that mode for a specific keyword.

To obtain a list of keywords and a brief functional description of those keywords at any CLI mode, do either of the following.

- Type **help** at the prompt
- Type **?** at the prompt or after a keyword.

Figure 3 illustrated the output that appears when you type **help** at any modes prompt. The output tells your how to use **?** to get help.

```
MSR2000(config)# help
When you need help,anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup until
entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument
   (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you
   want to know what arguments match the input
   (e.g. 'show me?'.)
```

**Figure 3** Output of help command

Figure 4 illustrates the output that appears when you type **?** at the INTERFACE mode prompt. All keywords are listed on the left with a brief description of the commands on the right.

```
MSR2000(config-if-ethernet)# ?
```

```
   dhcp         DHCP  (Dynamic  Host  Configuration  Protocol)  method  (server  or
relay) to assign IP addresses
  end        End current mode and return to privilege EXEC mode
  exit       Exit current mode and down to previous mode
  help       Description of the interactive help system
  interface  Select interface to operate
  ip         Interface Internet Protocol config commands
  list       Print command list
  mode       set usage of this interface
  mtu        Set the interface's Maximum Transmission Unit (MTU)
  no         Negate a command or set its defaults
  quit       Exit current mode and down to previous mode
  show       Show running system information
  shutdown   Shutdown this interface
  write      Write running configuration to memory, network, or terminal
```

**Figure 4** Example of **?** command

To obtain a list of available options for a keyword or partial keyword, use the **?**. In figure 4, the keywords are listed on the left with a brief description of the commands on the right. The output is the same if you enter the **help.**

```
MSR2000(config)# snmp-server ?
  community  server read only or read write community string
  host       Set SNMP trap target ip
  v3user     set SNMPv3 user
MSR2000(config)# snmp-server
```

**Figure 5** Keyword **?** Combination for the snmp-server Keyword

```
MSR2000(config)# s?            ← Enter  a  partial  keyword,  in  the  case  "s"
followed
  security-profile  Config security profile
  service           Configure a service
  show              Show running system information
  snmp-server       Set SNMP server read only or read write community string
MSR2000(config)# s
MSR2000(config)# sn?           ← Enter  a  partial  keyword,  in  the  case  "sn"
followed
  snmp-server                immediately by a ?. All keywords that begin with
MSR2000(config)# snmp-sever        "sn" in the CONFIGURATION mode are listed.
```

**Figure 6** Various Keyword **?** Combinations

## Entering and Edition Commands

- The CLI is case sensitive. All CLI commands MUST be in lower case.
- It is convenient to use the TAB key to complete keywords in commands. As long as the letters you type are unique to all available commands, it will auto-complete the commands.
- You can use the up arrow key to display the last enabled command syntax.
- You can use either the BACKSPACE key or DELETE key to erase the previous letter.

Table 3 lists the different key combinations available.

**Table 3** Short-Cut Keys and their actions

| Key Combinations | Action |
|---|---|
| **CTRL-A** | Moves the cursor to the beginning of the command line. |
| **CTRL-B** | Moves the cursor back on character. |
| **CTRL-D** | Deletes character at cursor. |
| **CTRL-E** | Moves the cursor to the end of the line. |
| **CTRL-F** | Moves the cursor forward one character. |
| **CTRL-I** | Completes a keyword. |
| **CTRL-K** | Deletes all characters form the cursor to the end of the command line. |
| **CTRL-L** | Re-enters the previous command. |
| **CTRL-N** | Return to more recent commands in the history buffer after recalling commands with CRTL-P or the up arrow key. |
| **CTRL-P** | Recalls commands, beginning with the last command. |
| **CTRL-U** | Deletes the line. |
| **CTRL-W** | Deletes the previous word. |
| **CTRL-Z** | Ends continuous scrolling of command output. |
| **Esc B** | Moves the cursor back one word. |
| **Esc F** | Moves the cursor forward one word. |
| **Esc D** | Deletes all characters form the cursor to the end of the word. |

## Basic Configuration Information

This section provides information to configure your system to access the network or enable other hosts in your network after the initial system boot. Detailed feature or protocol configuration information is provided in subsequent chapters.

- System Information
- Host name configuration
- Password configuration
- Viewing configuration file information
- Setting CONFIGURATION mode parameters

## System Information

When booting up the router, the system configuration program is not implemented automatically, user has to configure the router by using CLI commands to enable and manage the system.

**Table 4** System Information for Initial Setup

| System Information | Purpose |
|---|---|
| **Hostname** | Allows you to set the host name of the MSR series. Enter a new host name in the form of an alphanumeric string. |

| | |
|---|---|
| **Router-password** | Default password is **public**, it can be changed by using this CLI command |
| **Ethernet port IP address** | By default, IP address 192.168.0.1/24 is configured on FastEthernet 0, user can change it if needed. |
| **Node-id and router-id** | Default node-id is 1 and router-id is 192.168.10.1; these must be set such that they are unique in a single mesh network formed by MSR series routers. |

## Host Name Configuration

The host name appears in the prompt. The default host name is MSR series. Names must start with a letter and end with a letter or digit. Characters within the string can be letters, digits, and hyphens.

To configure a host name, use the following command in the CONFIGUREATION mode:

**Table 5** Configuring a host name

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **hostname** <*name*> | CONFIGURATION | Allows you to set the host name of the MSR series. Enter a new host name in the form of an alphanumeric string. |
| **no hostname** | | Remove the hostname, it goes back to default. Default hostname = MSR series |

## Password Configuration

MSR series has a default password configured, the default password is **public.**

To configure the login password, configure the following command in the Privileged EXEC mode.

**Table 6** Configuring login password

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **router-password root** | Privileged EXEC | Change the login password for the user **root** command. |

```
MSR2000# router-password
   root  Set login password for root

MSR2000# router-password root
Changing password for root
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:
Re-enter new password:
Password changed.
```

## Viewing Configuration File Information

It is highly recommended that you save your configuration often.

To save a configuration file, use either of the following commands in the Privileged EXEC mode:

**Table 7** Save the running configuration to startup configuration

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **copy running-config startup-config** | Privileged EXEC | Save the current running configuration to the startup-config file. |
| **write memory** | Privileged EXEC | Save the current running configuration to the startup-config file. (old way to save configuration) |

Use any of the following commands to display information about the configuration file:

**Table 8** Display running configuration and startup configuration

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **show startup-config** | Privileged EXEC | Displays the configuration information stored in the internal memory. |
| **show running-config** | Privileged EXEC | Displays current configuration information on the system. |

## Setting CONFIGURATION Mode Parameters

The configure command places you in the CONFIGURATION mode where you can configure interfaces and routing protocols.

From the CONFIGURATION mode, enter any of the following commands to configure protocols or interfaces:

**Table 9** Enter CONFIGURATION mode

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **node-id** <1-255> | CONFIGURATION | Set node ID, should be value between 1 and 255. |
| **router-id** <A.B.C.D> | CONFIGURATION | Set router ID<br>A.B.C.D The ip address to be the loopback id of the router |
| **Interface** <*interface*> | CONFIGURATION | Configure a physical or logical interface on MSR series.<br>1.) dot11radio<br>2.) fast-ethernet |
| **show running-config** | CONFIGURATION | Display current configuration information on the system. |

## Software Image Upgrade

You may upgrade the firmware installed on the routers.

**Table 10** Upgrade firmware

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **upgrade** [FTP <ftp server ip> <image file> <ftp user> <ftp password> \| URL <URL to image file>] | Privileged EXEC mode | Upgrade the software image on the router using an FTP or HTTP server. |

```
MSR2000# upgrade ftp 192.168.1.107 /tftpboot/AOS-v1.2.1.img upimg
upimg
% Start downloading image
Connecting to 192.168.1.107[192.168.1.107]:21
new.img              100% |**************************************************|  5405 KB     00:00
ETA
% Start upgrading image, this will take several minutes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
% Upgrade successful MSR2000#

MSR2000# upgrade url http://192.168.1.107/tftpboot/AOS-v1.2.1.img
% Start downloading image
Connecting to 192.168.1.107[192.168.1.107]:21
new.img              100% |**************************************************|  5405 KB     00:00
ETA
% Start upgrading image, this will take several minutes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
% Upgrade successful
```

**Figure 7** Output of firmware upgrade

# Chapter 3 Physical Interfaces

This chapter contains information on defining and configuring and physical interfaces on the MSR series, it has the following sections:

- Interface Modes
- Configuring Fast-Ethernet Interfaces
- Configuring Dot11Radio Interfaces

## Interface Modes

The wireless mesh router contains physical and logical interfaces in both Layer 2 and Layer 3 modes.

**Table 11 List of** Interface types and modes

| **Type of Interface** | **Mode** | **Dynamic Creation** |
|---|---|---|
| fast-ethernet | Physical Layer 3 | No |
| dot11radio | Physical Layer 2 | No |

## Configuring Fast-ethernet Interfaces

MSR series has two physical fast-ethernet interfaces[1] that could connect the wireless mesh network with a wired network or device. Both interfaces support auto-negotiation between 10Mbps and 100Mbps as well as between half-duplex and full-duplex modes.

**Table 12** Configuring Fastethernet Interface

| **Command Syntax** | **Command Mode** | **Purpose** |
|---|---|---|
| **interface fast-ethernet** *<0-1>* | CONFIGURATION or INTERFACE FAST-ETHERNET | Configure a Fast-ethernet interface, it can be either fast-ethernet 0 or fast-ethernet 1 |
| **ip address** *[ip address/mask]* | INTERFACE FAST-ETHERNET | Set IP address of fast-ethernet interface. |
| **ip address dhcp** | | Set IP address to be automatically obtained by using the DHCP protocol; a DHCP server must be running on the network this fast-ethernet interface is connected to |
| **no ip address** | | Remove IP address from Fast-ethernet interface |
| **release-dhcp fast-ethernet <0-1>** | Privileged EXEC | Release the fast-ethernet interface's IP address acquired from DHCP Server |

[1] On some router models, only one Ethernet port (FastEthernet 0) is usable. It is recommended that the FastEthernet1 configuration to be left at default (disabled) for these models.

| | | |
|---|---|---|
| **renew-dhcp fast-ethernet <0-1>** | | Renew the fast-ethernet interface's IP address via DHCP Server |
| **restart-dhcp fast-ethernet <0-1>** | | Restart DHCP client for the fast-ethernet interface |
| **mode access** | INTERFACE FAST-ETHERNET | Set this fast-ethernet interface as a LAN interface, for connecting with client devices |
| **mode gateway** <gateway IP> | | Set this fast-ethernet interface as a WAN interface, for connecting with a wired network. The gateway IP parameter is optional; if specified, the router will use it as the default gateway. |
| **mtu** <*256-1500*> | INTERFACE FAST-ETHERNET | Set Maximum Transmission Unit (MTU)[2] size, 1500 is default<br>***Setting of MTU is optional and should be done with care.*** |
| **no mtu** | | Reset the MTU to the default value |
| **shutdown** | INTERFACE FAST-ETHERNET | Administratively shutdown the interface |
| **no shutdown** | | Administratively activate the interface (Default) |
| **exit, end, or quit** | INTERFACE FAST-ETHERNET | Leave Interface mode and commit the change |
| **dhcp server**<br>**dhcp relay** | INTERFACE FAST-ETHERNET | Configure DHCP server or relay for this Ethernet interface; for details, please refer to the chapter on DHCP and NAT. |

### Viewing fast-ethernet Interface information.

The fast-ethernet interface information may be viewed using the 'show' command. The "show run" command displays the intended configuration of the interface, while the "show interface fast-ethernet" command displays the current state of the interface.

```
MSR2000# show run
...
!
interface fast-ethernet 0
 ip address 192.168.1.162/24
 mode gateway 192.168.1.1
!
...
MSR2000# show int fast-ethernet 0
Interface FastEthernet0
```

[2] MTU (Maximum Transmission Unit) is the threshold at which single layer-3 IP packets become fragmented into multiple, smaller-size packets.

```
mode: gateway   gateway ip: 192.168.1.1
admin status: up  physical status: up
DHCP: disabled  DHCP client: disabled
index 1 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
HWaddr: 00:17:7b:18:18:30
inet 192.168.1.162/24 broadcast 192.168.1.255
  input packets 52320, bytes 4810521, dropped 0, multicast packets 0
  input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
  output packets 23738, bytes 3268042, dropped 0
  output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
  collisions 0
```

**Figure 8** Output of Fast-Ethernet

## Configuring Dot11Radio Interfaces (Layer 2 Interfaces)

The sections describe the default interface configuration and the optional features that you can configure on the physical interfaces:

- Operation Mode
- Common settings (Wireless Mode, Channel, etc)
- Operation-mode specific settings

### Radio Operation Mode

Radio Interface supports three operation modes, Access, Backhaul and Client. When configured for Access mode, 802.11 client devices such as personal computers, PDAs, and WiFi-phones are able to associate with the BSSs configured on the radio interface. When configured for Backhaul mode, other routers are able to connect to the radio interface through manually or automatically created WDS links. When configured for Client mode, the router can connect as a WiFi client to other APs within the range. There are commands that only take effect in one mode but not the others.

An operation mode must be configured on a radio before it could operate in a mesh network.

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **Interface dot11radio** <*0-N*> | CONFIGURATION | Configure one of the dot11radio interfaces; index starts from 0 and ends with one less than the number of radios installed. |
| **mode access** | INTERFACE DOT11RADIO | Configure radio interface for client access, allowing BSS association |
| **mode backhaul**<br>**mode backhaul** <Mesh Profile> | | Configure radio interface for backhaul operation, allowing connection with other MSR series routers. If <Mesh Profile> is specified, then the mesh settings in that profile are used for this backhaul radio; otherwise, the backhaul radio uses default mesh settings. See the later |

| | |
|---|---|
| | section on mesh profiles for details. |
| **mode client** | Configure radio interface to work as a 802.11 client, allowing connection with a generic 802.11 Access Point including BSSs provided by other MSR series routers. A router may only have one radio in client mode. |

## Common settings

Radio Interface supports three types of hard-ware mode: 802.11a, 802.11b (legacy mode), and 802.11g (can be configured to be backward-compatible with 802.11b). Each mode is associated with country codes and specific radio channels. The channel settings on the wireless device correspond to the frequencies available in the regulatory domain.

The following table outlines the physical, layer-2 settings that may configured on each radio interface. These settings apply in both access and backhaul modes.

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **wireless-mode** *<mode> <channel> [country code]* | INTERFACE DOT11RADIO | Configure the physical wireless settings of this radio interface.<br>mode: a, g, or b<br>a: Use 802.11a<br>b: Use 802.11b<br>g: Use 802.11g; compatible with 802.11b in some configurations<br>channel: Mode and country-specific channel number<br>Modes b,g and US: 1-11<br>Modes b,g and JP: 1-14;<br>Modes b,g and CN: 1-13;<br>Mode a and US: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165;<br>Mode a and JP: 36, 40, 44, 48<br>Mode a and CN: 149, 153, 157, 161, 165<br>country-code: US, CN, or JP<br>US: United States<br>CN: P.R. China<br>JP: Japan |
| **shutdown** | INTERFACE DOT11RADIO | Administratively shutdown this radio; all existing operations on this radio will stop |
| **no shutdown** | | Activate the interface |

| | | |
|---|---|---|
| **antenna** *<0-2>* | INTERFACE DOT11RADIO | Configure this radio interface to use one of the two antennas connected to the physical radio card |
| **antenna 0** | | Automatically choose the best antenna (default for indoor models) |
| **antenna 1** | | Always use antenna 1 (default for oudoor models) |
| **antenna 2** | | Always use antenna 2 |
| **no antenna** | | Restore default antenna setting.<br>***Setting of antenna is optional and should be done with care.*** |
| **cts-protection** *<0-3>* | INTERFACE DOT11RADIO | Enable or disable CTS protection on this radio interface. |
| **cts-protection 0**<br>**no cts-protection** | | 0: Automatically enable/disable CTS using OLBC detection[3] (Default) |
| **cts-protection 1** | | Always enable CTS protection |
| **cts-protection 2** | | Always disable CTS protection |
| **cts-protection 3** | | Automatically enable/disable CTS without using OLBC detection[4]<br>***Setting of cts-protection is optional and should be done with care.*** |
| **mtu** *<256-2274>* | INTERFACE DOT11RADIO | Set the layer-3 MTU of this radio interface. |
| **no mtu** | | Reset the MTU to the default value<br>***Setting of radio MTU is not recommended and should be done with extreme caution.*** |
| **retry** <1-32> <1-32> | INTERFACE DOT11RADIO | Sets the 802.11 MAC layer's packet retransmission limit. The first argument is the short retry limit and the second is the long retry limit. |
| **retry** 4 7<br>**no retry** | | Reset retry to default (short retry of 4, long retry of 7) |
| **tx-power-reduction** *<0-65535>* | INTERFACE | Set the reduction in transmission power of |

[3] This setting will enable CTS protection when there are both 802.11g and 802.11b clients associated on one of the BSSs of the current radio or when Overlapping Legacy BSS Condition (OLBC) is detected

[4] This setting will enable CTS protection when there are both 802.11g and 802.11b clients using the current radio, but not when OLBC is detected

| | | |
|---|---|---|
| | DOT11RADIO | this radio interface. The reduction is in 0.1dBm increments. For example, a setting of 10 causes a reduction of 1 dBm. The maximum possible reduction is a setting of 65535 or 6553.5 dBm |
| **no tx-power-reduction** | | Reset the power reduction to the default value.<br>***Transmission power settings should only be changed with extreme caution.*** |

**A note regarding CTS protection**:

IEEE 802.11g uses CTS frames to allow IEEE 802.11b clients notice frames sent at higher rates. This is useful in mixed mode networks consisting of both 802.11b and 802.11g stations. It is disabled automatically if there are no 802.11b stations associated to the AP. This behavior can be changed to enable CTS protection on IEEE 802.11g AP only, if there are IEEE 802.11b stations on the same channel using another AP. In addition, disabling this even when IEEE 802.11b stations are present can improve performance, if most traffic is between IEEE 802.11g devices.

## Backhaul mode Configuration

This section describes settings that only take affect in ***backhaul*** operation mode: The backhaul mode is used to create backhaul wireless links to other mesh routers.

### Mesh Profiles and Settings

Each backhaul radio interface on the MSR series router must participate in a single wireless mesh network. Because each mesh network has its unique characteristics, mesh profiles can be created to specify unique settings for each mesh network.

The following table outlines the mesh profile-related commands:

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **profile mesh** <NAME> | CONFIGURATION | Configure a new or existing mesh profile with the specified name on this router. |
| **no profile mesh** <NAME> | | Remove an existing mesh profile configuration on this router. |
| **mesh-id** <WORD> | PROFILE MESH | Specify the mesh ID for this mesh profile; all mesh routers that forms the single mesh network should use the same mesh ID. |
| **no mesh-id** | | Remove the mesh ID from this mesh profile. |

| | | |
|---|---|---|
| **mode backhaul** <Mesh Profile> | INTERFACE DOT11RADIO | Set a radio interface for backhaul operation and use the settings in the specified mesh profile. |

### Backhaul radio settings

The following table outlines settings that only take affect in ***backhaul*** operation mode:

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **wds** <*0-5*><br>**no wds** <*0-5*> | INTERFACE DOT11RADIO | Configure a new or existing manual WDS interface on this radio; this command is mutually exclusive with the wds auto command below[5];<br>Remove an existing manual WDS interface from this radio |
| **wds auto**<br>**no wds auto** | INTERFACE DOT11RADIO | Enable automatic WDS provisioning on this radio interface and enter the auto WDS configuration mode; this command is mutually exclusive with the wds <0-5> command.[6]<br>Disable auto WDS on this radio interface. |
| **wds-unicast-rate** [*rate*]<br>**no wds-unicast-rate** | INTERFACE DOT11RADIO | Set the forced unicast rate of this radio interface's WDS links; once set, WDS links will attempt to consistently use the specified transmission rate.<br>The rate is specified in units of 100kbps; the available rates are: 10, 20, 55, 110, 60, 90, 120, 180, 240, 360, 480, 540<br>**(Example: if choose 20, then RATE=20*100kbps=2Mbps)**<br>Disables unicast rate setting; WDS links will automatically select the transmission rate and may dynamically vary depending on link quality (default setting) |

## Access mode settings

The following table outlines settings that only take affect in ***access*** operation mode:

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **bss** <*SSID*> | INTERFACE DOT11RADIO | Configure a new or existing BSS on this radio interface[7] |

[5] Please see the next chapter on WDS interfaces for more information.

[6] Please see chapter 7, Radio Frequency Management, for more information about auto WDS discovery and provisioning.

[7] Please see the later chapter on BSS for more information.

| | | |
|---|---|---|
| **no bss** <*SSID*> | | Remove an existing BSS from this radio interface<br>SSID: The 802.11 Service Set ID (SSID) that identifies a BSS on this radio interface |
| **station-isolation** | INTERFACE DOT11RADIO | Disable the internal bridge for the client's data packets; this prevents the layer-2 broadcast traffic from one client to reach another. Broadcasts from the AP can still reach all clients. |
| **no station-isolation** | | Enable the internal bridge for client's data packets; allows clients to communicate with each other through layer-2 broadcasting (default)<br>***It is highly recommended that station-isolation be enabled for security reasons. For example, it can prevent clients on the same AP from discovering each other through Microsoft Windows' Network Neighborhood feature.*** |

## Client mode settings

The following table outlines settings that only take affect in ***client*** operation mode:

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **station <station name>** | INTERFACE DOT11RADIO | Configure a 802.11 client station on this radio interface[8] |
| **no station <station name>** | | Remove 802.11 client station setting from this radio interface<br>Note: currently only one station is allowed on each router |

### Viewing the dot11radio interface information

The "show run" command displays the intended configuration of the dot11radio interface, while the "show interface dot11radio" command displays the current state of the interface.

```
MSR2000# show run
...
interface dot11radio 0
wireless-mode a 149 US
 antenna 0
 cts-protection 2
 mode backhaul
...
```

[8] Please see the later chapter on client mode for more information.

```
MSR2000# show interface dot11radio 0
Interface Dot11Radio0
     operation_mode:backhaul,mesh  id:AzaleaMesh,  country  code:US,  channel
policy:0,
  antenna:0, cts protection:2,
  admin status: up  physical status: up
  index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWmode: a, channel: 149, Fragment thr: 2346, RTS thr: 2347
  HWaddr: 00:17:7b:18:18:38
    input packets 3517383, bytes 627088483, dropped 0, multicast packets 0
    input errors 637111, length 0, overrun 0, CRC 0, frame 12, fifo 0, missed
0
    output packets 254080, bytes 35293576, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

**Figure 9** Output of dot11radio interface

# Chapter 4 Logical Interfaces (WDS)

Wireless Distribution System (WDS) is the underlying technology that allows MSR series routers to communicate each other wirelessly and form the backhaul links of the mesh network. A WDS link is formed between two routers by creating logical WDS interfaces on each router, either through manual configuration or automatic discovery[9].

Each logical WDS interface is bound to a physical Dot11Radio interface. Therefore, WDS interface configuration commands are placed within the 'interface dot11radio' mode. Because WDS is used to form backhaul links, its configuration only takes effect on radio interfaces configured for backhaul mode.

Note: The MSR series can only form backhaul links with the radios on other MSR series routers that has the same mesh-ID configured. Please ensure all the routers in your wireless mesh network use the same mesh-ID and different networks use different IDs. The section on "Mesh Profiles" in the previous chapter describes how mesh profiles and IDs are configured.

**Table 13** Configuring WDS Interface

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **wds** *<0-5>* | INTERFACE DOT11RADIO | Configure a new or existing manual WDS interface on this radio; enters the INTERFACE DOT11RADIO WDS command mode. This command is mutually exclusive with the wds auto command below. |
| **no wds** *<0-5>* | | Remove an existing manual WDS interface from this radio |
| **wds auto** | INTERFACE DOT11RADIO | Enable automatic WDS provisioning on this radio interface and enter the INTERFACE DOT11RADIO WDS AUTO mode for auto WDS configuration; this command is mutually exclusive with the wds <0-5> command.[10] |
| **no wds auto** | | Disable auto WDS on this radio interface. |
| **max-auto-wds** *<1-6>* | INTERFACE DOT11RADIO WDS AUTO | Set the maximum number of auto WDS interfaces that could be created on this radio by RFM[11] |

[9] Please see chapter 5 for more information about automatic discovery of WDS links

[10] Please see chapter 7, Radio Frequency Management, for more information about auto WDS discovery and provisioning.

[11] This setting is related to the automatic WDS link discovery feature of RFM. Please refer to chapter 5 for details.

| | | |
|---|---|---|
| **authentication open**<br>**no authentication** | INTERFACE DOT11RADIO WDS | Allow all compatible mesh routers to form WDS links with this radio interface. |
| **authentication open key-management wpa <wpa-profile-name>** | | Enable WPA security for this WDS; only allow mesh routers with correct WPA authentication and encryption settings to form WDS links. |
| **authentication shared wep <wep-profile-name> default-key <1-4>** | | Enable WEP authentication for this WDS; only allow routers with the correct WEP key settings to form WDS links. |
| **ip address** *[ip address/mask]* | INTERFACE DOT11RADIO WDS | Configure IP address of WDS interface. |
| **no ip address** | | Remove IP address from WDS interface |
| **mtu** *<256-2274>* | INTERFACE DOT11RADIO WDS | Configure MTU size of WDS interface |
| **no mtu** | | Restore default MTU size (1500)<br><br>***Setting of MTU is optional and should be done with care.*** |
| **qos class** *<class>* | INTERFACE DOT11RADIO WDS | Specify the Quality of Service (QoS) class policy[12] that should be applied for this WDS interface |
| **no qos class** | | Disable QoS on this interface (default) |
| **remote mac** <*HH:HH:HH:HH:HH:HH*> | INTERFACE DOT11RADIO WDS | Specify the MAC address of the remote radio on the other router that this WDS interface will establish a link with |
| **remote node** *<1-255> <0-N>* | | Specify the node ID and the index of the radio on the remote router that this WDS interface will establish a link with<br><br>1-255: The node ID of the other router<br>0-N: The index of the radio on the other router that will form the link. |
| **role** <ap \| station> | INTERFACE DOT11RADIO WDS | Specify the role of this WDS interface in the link; each link |

[12] Please see chapter 9, Quality of Service (QoS), for more information.

| | | |
|---|---|---|
| | | requires a WDS interface as an ap and the other as station. |
| role auto<br>no role | | Allow routers to automatically assign roles to the WDS interface (default, recommended setting) |
| **ssid** <NAME> | INTERFACE DOT11RADIO WDS | Specify the SSID of this WDS link (required for WPA) |
| **no ssid** | | Do not use a SSID (default) |
| **shutdown** | INTERFACE DOT11RADIO WDS | Administratively shutdown this WDS interface; stops the operation of the WDS link |
| **no shutdown** | | Activate this WDS interface so it may establish a link with another router |

### A note regarding WDS configuration:

To set up a manual WDS link between two routers, a backhaul radio interface should be configured on each router. Both radio should use the same wireless mode and channel.

## 802.11 Security Configuration

The 802.11 security standard defines a suite of wireless security protocols and implementations. The MSR series allows each WDS link to use a different 802.11 security profile such as WEP or WPA. Refer to the chapter on 802.11 Security for more information.

### Viewing a list of all interfaces

The "**show interface brief**" command can be used to display a list of all interfaces on the router that includes both physical and logical interfaces.

```
MSR2000# show interface brief
Name                IP address           State
Dot11Radio0         unassigned           up
Dot11Radio1         unassigned           up
Radio0MWds0         10.1.6.2/28          up
Radio0MWds1         10.2.6.2/28          up
Radio1MWds0         10.4.6.1/28          up
Radio1MWds1         10.5.6.1/28          up
FastEthernet0       192.168.1.136/24     up
FastEthernet1       unassigned           administratively down
```

In the above list, two physical radio interfaces and two physical fast-ethernet interfaces were included. In addition, one auto WDS[13] logical interface bound to Dot11Radio0 (Radio0AWds0), two manual WDS interfaces bound to Dot11Radio0 (Radio0MWds0-1), and two manual WDS interfaces bound to Dot11Radio1 (Radio1MWds0-1) were displayed. The prefix of the WDS interface name indicates the radio that the WDS interface uses.

[13] See the next chapter on RFM for information on auto WDS link discovery.

### Viewing WDS Interface information.

```
MSR2000# show run
...
interface dot11radio 0
...
 wds 0
  remote mac 00:17:7b:35:36:bc
  ip address 10.1.6.2/28
  no shutdown
...
interface dot11radio 1
 wds 0
  remote node 5 0
  ip address 10.4.5.1/28
  no shutdown
!
...
MSR2000# show interface dot11radio 0 wds 0
Interface Radio0MWds0
  neighbor specified using: mac address
  remote mac address: 00:17:7b:35:eb:0d, remote node: 152, remote radio: 0
  admin status: up  physical status: up  neighbor ip: 200.151.152.2
  rssi: 69, snr: 69, link quality: 86%, datarate: 60
  role:auto, physical interface:0,
  index 20 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWmode: a, channel: 149, Fragment thr: 2346, RTS thr: 2347
  HWaddr: 00:17:7b:18:18:38
  inet 200.151.152.1/24 broadcast 200.151.152.255
    input packets 280, bytes 46812, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 186, bytes 38728, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

Figure 10 Output of dot11wds interface

# Chapter 5 Access and BSS Configuration

When a Dot11Radio interface is put into Access mode, a BSS configured for that interface becomes a virtual AP that client devices may associate with. Each BSS is bound to a physical dot11radio interface; therefore, BSS is configured within the 'interface dot11radio' mode. The MSR series router supports up to four BSSs on each radio interface.

## Basic BSS configuration

The following table outlines the basic settings for each BSS.

**Table 14** Configuring Basic BSS

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **bss** *<SSID>* | INTERFACE DOT11RADIO | Configure a new or existing BSS on this radio interface |
| **no bss** *<SSID>* | | Remove an existing BSS from this radio interface<br>SSID: The 802.11 Service Set ID (SSID) that identifies a BSS on this radio interface. |
| **ip address A.B.C.D/M** | INTERFACE DOT11RADIO BSS | Configure IP Address for this BSS. |
| **authentication open**<br>**no authentication** | INTERFACE DOT11RADIO BSS | Allow all clients to associate with this BSS |
| **authentication open wep <wep-profile-name> default-key <1-4>** | | Enable WEP encryption for this BSS using the key settings in the WEP profile and the specified default key |
| **authentication open key-management wpa <wpa-profile-name>** | | Enable WPA security for this BSS; only allow clients with correct WPA authentication and encryption settings to associate with this BSS. |
| **authentication open key-management wpa2 <wpa2-profile-name>** | | Enable WPA2 security for this BSS; only allow clients with correct WPA2 authentication and encryption settings to associate with this BSS. |
| **authentication shared wep <wep-profile-name> default-key <1-4>** | | Enable WEP authentication and encryption for this BSS using the key settings in the WEP profile and the specified default key |
| **mac-address accept <mac-list-name>** | INTERFACE DOT11RADIO BSS | Only accept clients with MAC addresses in the specified list; deny all other clients |

| | | |
|---|---|---|
| **mac-address deny <mac-list-name>** | | Only deny clients with MAC addresses in the specified list; allow all other clients. |
| **mac-address accept-all**<br>**no mac-address** | | Restore to default configuration (accept all MAC addresses) |
| **ignore-broadcast-ssid** | INTERFACE DOT11RADIO BSS | Disable broadcasting of this BSS's SSID |
| **no ignore-broadcast-ssid** | | Enable broadcasting of this BSS's SSID (Default) |
| **max-rate** *<rate>* | INTERFACE DOT11RADIO BSS | Select the maximum allowed transmission rate for this BSS in units of 100kbps.<br>Available rates: 10, 20, 55, 110, 60, 90, 120, 180, 240, 360, 480, 540. |
| **no max-rate** | | Allow the maximum transmission rate supported by the client and radio hardware (Default) |
| **max-station-allowed** *<0-240>* | INTERFACE DOT11RADIO BSS | Configure the maximum number of stations allowed to associate with this BSS at the same time. |
| **max-station-allowed 240**<br>**no max-station-allowed** | | Allow up to 240 stations to associate with this BSS at the same time (default). |
| **station-inactivity-limit <**_1-65535_**>** | INTERFACE DOT11RADIO BSS | Configure the maximum amount of time (in seconds) a station is allowed to be inactive before the action specified by the inactivity-policy (see next) is taken |
| **station-inactivity-limit 300**<br>**no station-inactivity-limit** | | Set the inactivity limit to the default value of 300 seconds |
| **station-inactivity-policy** *<0-1>* | INTERFACE DOT11RADIO BSS | Configure the action taken when a station exceeds the inactivity limit. |
| **station-inactivity-policy 0**<br>**no station-inactivity-policy** | | Poll the station and de-authenticate station if it does not respond (default) |
| **station-inactivity-policy 1** | | De-authenticate station immediately |

| | | |
|---|---|---|
| **unicast-rate** <*rate*> | INTERFACE DOT11RADIO BSS | Set the unicast rate of this BSS; once set, the radio interface will attempt to consistently use the specified transmission rate for stations associated with this BSS. Setting this option will also prevent stations that do not support the specified rate from associating with the BSS.<br>The rate is specified in units of 100kbps; the available rates are: 10, 20, 55, 110, 60, 90, 120, 180, 240, 360, 480, 540 |
| **no unicast-rate** | | Disables unicast rate setting for this BSS; radio interfaces will automatically select transmission rates (default setting) |
| **dhcp server**<br>**dhcp relay** | INTERFACE DOT11RADIO BSS | Configure DHCP server or relay for this BSS; for details, please refer to the chapter on DHCP and NAT. |

## 802.11 Security Configuration

The 802.11 security standard defines a suite of wireless security protocols and implementations. It provides open and shared key authentication, is compatible with WPA /WPA2, and interoperates with 802.1x.

The mesh router allows each BSS to use a different 802.11 security profile. Please refer to the chapter on 802.11 Security for more information.

### Viewing BSS of dot11radio interface information.

```
MSR2000# show run
...
interface dot11radio 0
...
 bss demo
  station-inactivity-policy 1
  station-inactivity-limit 300
  max-rate 60
  authentication open wep test-supplicant default-key 1
  mac-address accept AAA
...
!
security-profile wep test-supplicant
 wep-key 1 1234567890
 wep-key 2 2345678901
 wep-key 3 3456789012
 wep-key 4 4567890123
!
mac-list AAA
 mac-addr 22:22:22:bc:22:44
 mac-addr 22:22:22:bc:22:45
 mac-addr 22:22:22:bc:22:08
...
!
MSR2000# show interface dot11radio 0 bss demo
BSS:demo

  ignore broadcast ssid:disable, maxium station allowed:240,
  transmission fail percentage:0, transmission fail check interval:0,
  station inactivity policy:1, station inactivity limit:300,
    maxium  rate  control  rate:60,  authentication:open  wep  test-supplicant
default-key 1,mac authentication:accept AAA,
    HWaddr: 00:17:7b:18:18:40
```

**Figure 11** Output of BSS under dot11radio interface

# Chapter 6 Client Mode Configuration

When a Dot11Radio interface is configured for client mode, an 802.11 client station configured under that interface can associate to any matching 802.11 access points as any other 802.11 client. The access point can be BSSs provided by other MSR seriess or an AP from another vendor. On each MSR series router, only one radio interface can operate in client mode.

## Basic Client Mode configuration

The following table outlines the basic settings for a client station

**Table 15 Configuring Basic Client Mode**

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **station <station name>** | INTERFACE DOT11RADIO | Configure a 802.11 client station on this radio interface |
| **no station <station name>** | | Remove 802.11 client station setting from this radio interface<br>***Note: only one client can be created on a radio interface*** |
| **ip address** *[ip address/mask]* | INTERFACE DOT11RADIO STATION | Set IP address of this client station. |
| **ip address dhcp** | | Set IP address to be automatically obtained by using the DHCP protocol; a DHCP server must be running on the network this station associates to. |
| **no ip address** | | Remove IP address from this client station. |
| **client-authentication open wep <wep-profile-name> default-key <1-4>** | INTERFACE DOT11RADIO STATION | Enable WEP encryption for this client using the key settings in the WEP profile and the specified default key |
| **client-authentication open client-8021x <client-8021x-profile-name>** | | Enable 802.1X authentication for this client, using the authentication settings in the client-8021x profile |
| **client-authentication open key-management wpa client-8021x <client-8021x-profile-name>** | | Enable WPA security for this client; using the authentication settings in the client-8021x |

| | | |
|---|---|---|
| | | profile |
| **client-authentication open key-management wpa2 client-8021x <client-8021x-profile-name>** | | Enable WPA2 security for this client; using the authentication settings in the client-8021x profile |
| **client-authentication open key-management wpa-psk hex <string>** | | Enable WPA PSK on client and configure pre-shared key using hexadecimal format. |
| **client-authentication open key-management wpa-psk ascii <string>** | | Enable WPA PSK on client and configure pre-shared key using ascii format. |
| **client-authentication shared wep <wep-profile-name> default-key <1-4>** | | Enable WEP encryption for this client using the key settings in the WEP profile and the specified default key |
| **no client-authentication** | | Disable authentication for this client interface. |
| **access-point ssid <SSID>** | INTERFACE DOT11RADIO STATION | SSID of the access point that this client station wants to associate with. Default is no SSID. |
| **no access-point ssid** | | Remove access-point SSID configuration.<br>SSID: 802.11 Service Set ID |
| **access-point bssid <***HH:HH:HH:HH:HH:HH***>** | INTERFACE DOT11RADIO STATION | BSSID of the access point that this client station wants to associate with. Default has no BSSID specified. |
| **no access-point bssid** | | Remove the setting of BSSID for an access point. |
| **access-point bssid-filter acceptable prefix <***HH:HH:HH:HH:HH:HH***>** *<HH:HH:HH:HH:HH:HH>* | INTERFACE DOT11RADIO STATION | This command provides a filter when the client is selecting an Access Point during scanning. The first MAC address is the prefix of BSSID you allow the client to associate with. The second MAC address is a mask of the prefix. If configured, only an access point with matching BSSID will be selected. For example, if you want the client |

| | | |
|---|---|---|
| | | to only connect to MSR series routers, you can specify a prefix of 00:17:7b:00:00:00 with mask of ff:ff:ff:00:00:00<br>Multiple filters can be configured if you want to allow multiple BSSID prefix choices.<br>Default allows all BSSIDs. |
| **no access-point bssid-filter acceptable prefix**<br>**<**_HH:HH:HH:HH:HH:HH_><br>_<HH:HH:HH:HH:HH:HH>_ | | Remove a certain BSSID filter |
| **no access-point bssid-filter acceptable-prefix** | | Remove all the BSSID filters |
| **scanning channel-list <channel list>** | INTERFACE DOT11RADIO STATION | Configure a list of channels that you allow the client to look at when doing access point scanning. Only one channel list is allowed.<br>Default has no channel list and it scans in all legal channels of the configured hardware modes. (See "scanning hardware-mdoes" command).<br><channel list>: a list of comma separated channel numbers, no space in between |
| **no scanning channel-list** | | Remove the current configured channel list |
| **scanning hardware-modes <mode string>** | INTERFACE DOT11RADIO STATION | Configure the hardware modes that you allow the client to stay in when doing access point scanning<br><mode string>: a, g, ag<br>It means do scanning only in 802.11a mode, 802.11g mode or in both modes. Default value is both 802.11a and 802.11g. |
| **no scanning hardware-modes** | | Remove the hardware scanning mode setting and return to default. |
| **scanning minimum-interval <seconds>** | INTERFACE DOT11RADIO STATION | Configure the minimum allowed time interval between two consecutive scans.<br><seconds>: a number between 1 and 300, the unit is second. Default value is 60 seconds. |

| | | |
|---|---|---|
| **no scanning minimum-interval** | | Restore default setting of minimum scan interval |
| **scanning threshold rssi <rssi value>** | INTERFACE DOT11RADIO STATION | Configure the RSSI value threshold to trigger a new scan. If the current RSSI is lower than configured threshold, the client will start a new scan.<br><rssi value>: a number between 0 and 100. 0 means no such trigger. Default value is 15.<br>RSSI stands for Received Signal Strength Index |
| **no scanning threshold rssi** | | Restore the default RSSI threshold value. |
| **release-dhcp dot11radio <0-N> station <station name>** | Privileged EXEC | **Release the station's IP address acquired from DHCP server** |
| **renew-dhcp dot11radio <0-N> station <station name>** | | **Renew the station's IP address via DHCP server** |
| **restart-dhcp dot11radio <0-N> station <station name>** | | **Restart DHCP client for the station** |

## . 802.11 Security Configuration

The 802.11 security standard defines a suite of wireless security protocols and implementations. The MSR series allows the client mode to use a specific 802.11 security profile such as WEP or WPA. Refer to the chapter on 802.11 Security for more information.

### Viewing information of a station in a dot11radio interface.

```
MSR2000# show run
...
!
interface dot11radio 0
...
 station demo
  ip address dhcp
  access-point ssid demo

...
MSR2000# sh interface dot11radio 0
  Interface Dot11Radio0
  operation_mode:client, country code:US, channel policy:0, antenna:1,
  cts protection:2,
  distance:0, short retry:7, long retry:4,
  admin status: up  physical status: up
  index 35 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWmode: g, channel: 1, Fragment thr: 2346, RTS thr: 2347
  HWaddr: 00:17:7b:00:27:40
    input packets 823925, bytes 96825419, dropped 0, multicast packets 0
    input errors 88069, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 457, bytes 26006, dropped 0
    output errors 2, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
  Station Information:
   Station demo
    State: Associated
    SSID: "demo", Access Point: 00:17:7b:35:e8:53 RSSI: 55
    Previous Access Point: NA
    IP Address: 172.16.21.249(DHCP acquired)
    Security: None
    Scanning threshold: RSSI 15
    Minimum scan interval: 60 seconds
    scanning in hardware modes: ag
    scanning in channels:
     mode A: 36 40 44 48 52 56 60 64 149 153 157 161 165
     mode G: 1 2 3 4 5 6 7 8 9 10 11
```

**Figure 12** Output of station information under dot11radio interface

# Chapter 7 Radio Frequency Management

Radio Frequency Management (RFM) is an advanced feature of MSR series that allows automatic discovery and quality monitoring of wireless mesh links. RFM automatically scans for compatible mesh routers in the neighboring area and create automatic WDS links to these routers. With RFM, multiple mesh routers can form a mesh network without any manually configured WDS interfaces. In addition, an RFM-aware routing protocol could use the link quality information from RFM to optimize the routing path in the wireless mesh network.

## Auto neighbor discovery and WDS link creation

RFM discovers neighboring mesh routers using ***passive-scanning***, a process that is automatically started when a backhaul radio interface is operating without any manually configured WDS interfaces. Passive-scanning automatically changes the channel of the radio interface and listens for 802.11 beacons from other mesh routers. If one or more routers are heard, RFM selectively attempts to create WDS links with these other routers. Auto WDS interfaces are automatically created and configured if the WDS connection is successfully established.

The configuration commands that controls auto-discovery is **wds auto**, which enables Auto WDS discovery for a radio interface, and **max-auto-wds**, which controls how many automatic WDS links RFM is allowed to create on that interface. If **wds auto** is not set for a radio interface, RFM will not perform any scanning or WDS interface creation on that radio.

Note: As previously mentioned in the chapter on WDS configuration, the MSR series can only form WDS links with other MSR series routers that use the same mesh ID.

## WDS link quality monitoring

RFM could monitor the link quality for all WDS links present on an MSR series router, regardless of whether the link is manually configured or automatically created. The WDS interface for the link must be active[14]. The link quality is displayed in the results of the “show interface dot11radio X wds” command:

```
MSR2000# show interface dot11radio 0 wds 0
Interface Radio0MWds0
  neighbor specified using: mac address
  remote mac address: 00:17:7b:35:eb:0d, remote node: 152, remote radio: 0
  admin status: up  physical status: up  neighbor ip: 200.151.152.2
  rssi: 71, snr: 71, link quality: 87%, datarate: 60
  role:auto, physical interface:0,
  index 20 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWmode: a, channel: 149, Fragment thr: 2346, RTS thr: 2347
  HWaddr: 00:17:7b:18:18:38
  inet 200.151.152.1/24 broadcast 200.151.152.255
    input packets 1046, bytes 164912, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
```

[14] An active WDS interface is one that is bound to an active backhaul radio interface and not administratively shutdown.

```
    output packets 862, bytes 160520, dropped 0
    output errors 4, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
    output packets 6082, bytes 1602424, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

The link quality parameters monitored by RFM include RSSI, SNR, overall quality[15], and data rate.

## RFM related configuration commands

The following table summarizes the commands used to configure RFM's auto-discovery and link monitoring functions:

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **wds auto**<br>**no wds auto** | INTERFACE DOT11RADIO | Enable automatic WDS provisioning on this radio interface and enter the INTERFACE DOT11RADIO WDS AUTO mode for auto WDS configuration; this command is mutually exclusive with the wds <0-5> command.<br>Disable auto WDS on this radio interface. |
| **max-auto-wds** *<1-6>* | INTERFACE DOT11RADIO WDS AUTO | Set the maximum number of auto WDS interfaces that could be created on this RFM |
| **service rf-management** | CONFIGURATION | Start the configuration of the RFM service |
| **enable** | SERVICE RF-MANAGEMENT | Activate the RFM function |
| **debug**<br>**debug none**<br>**debug error**<br>**debug state**<br>**debug information**<br>**debug frame**<br>**debug dump** | SERVICE RF-MANAGEMENT | Set the RFM debug log level<br>Disable RFM debug log<br>Set RFM debug log to record errors<br>Set RFM debug log to record errors & state changes<br>Log error, state, and other detailed information<br>Log error, state, information, and RFM control packet frames<br>Log all RFM debug information |

[15] The link quality percentage measurement is based on the level of RFM control packet loss.

The following commands can be entered at the privileged EXEC prompt to display information about the RFM service:

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **show log rf-management** | Privileged EXEC | Display the debug log of RFM (see debug command above) |
| **show rf-management active-neighbors** | Privileged EXEC | Display a list of neighboring MSR series routers and radios discovered by RFM |
| **show rf-management interface** | Privileged EXEC | Display a list of WDS interfaces currently monitored by RFM; may include both auto and manual WDS interfaces. |
| **show rf-management configuration** | Privileged EXEC | Display the current configuration parameters of RFM |

**Viewing rf-management information.**

```
MSR2000# show rf-management active-neighbors
RF Management active neighbor table:
RFM has 2 active radio interfaces, 2 total WDS interfaces
Dot11Radio0 has 1 active neighbors:
Ngh  1: Mac: 00:00:00:00:00:00 Learned: No
        IP: 10.140.141.1, node_id: 0, radio_idx: 0
        local WDS if: Radio0MWds0, local IP: 10.140.141.2
        admin status: Up, physical status: Down, state: Initial, flag: 0x13
        phytype: IEEE 802.11a, ch: 161, mode: WDS
        link quality: 93%, rssi: 70, snr: 70
Dot11Radio1 has 1 active neighbors:
Ngh  1: Mac: 00:17:7b:36:a3:5b Learned: No
        IP: 10.141.143.2, node_id: 143, radio_idx: 0
        local WDS if: Radio1MWds0, local IP: 10.141.143.1
        admin status: Up, physical status: Up, state: Established, flag: 0x13
        phytype: IEEE 802.11a, ch: 52, mode: WDS
        link quality: 86%, rssi: 69, snr: 69

MSR2000# show rf-management interface
RF Management WDS Interfaces:
Dot11Radio0:    mesh ID: TestMesh, peer capacity: 5
Radio0MWds0:    Radio: Dot11Radio0, node ID: 141
                admin status: Up, physical status: Down
                IP: 10.140.141.2, Netmask: 255.255.255.0, Bcast: 10.140.141.255
                NGH MAC: 00:00:00:00:00:00, NGH node ID: 0, NGH radio_index: 0
                        NGH IP: 10.140.141.1, NGH Netmask: 255.255.255.0, NGH Bcast:
10.140.141.255
                link state: Initial, Link quality: 93%
                RSSI: 70, SNR: 70
Radio1MWds0:    Radio: Dot11Radio1, node ID: 141
                admin status: Up, physical status: Up
                IP: 10.141.143.1, Netmask: 255.255.255.0, Bcast: 10.141.143.255
                NGH MAC: 00:17:7b:36:a3:5b, NGH node ID: 143, NGH radio_idx: 0
                        NGH IP: 10.141.143.2, NGH Netmask: 255.255.255.0, NGH Bcast:
10.141.143.255
                Link State: Established, Link quality: 86%
```

```
              RSSI: 69, SNR: 69
```

**Figure 13** Output of Rf-management

# Chapter 8 Configuring Routing

This chapter contains information on configuring layer-3 routing on the MSR series, it has the following sections:

- Static Routing
- Dynamic Routing through AWR

## Static Routing

Static routing allows the network administrator full control over the layer-3 topology and data forwarding behavior of the network. The administrator constructs the routing table for a router by specifying a route for each destination network.

A configured static route is installed in the routing table only when the route is active; that is, the route's next-hop must be bound to an operational interface. The following table summarizes the command to add/remove static route:

**Table 16** Configuring Static Route

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **ip route** *<A.B.C.D/M> <A.B.C.D> [<1-255>]*<br>**no ip route** *<A.B.C.D/M> <A.B.C.D>* | CONFIGURATION | Add a indirect static route<br>Remove a gateway static route<br>A.B.C.D/M: destination network prefix/mask<br>A.B.C.D: gateway IP address<br>1-255: the distance value for this route, lower is better with 255 being unreachable. (optional, default is 1) |
| **ip route** *<A.B.C.D/M>* **station** <name> *<0-N>*<br>**no ip route** *<A.B.C.D/M>* **station** <name> *<0-N>* | | Add a directly-connected static route that binds to a client mode station<br>Remove a directly-connected route<br>A.B.C.D/M: destination network prefix/mask<br>name: Station name<br>0-N: Index of radio interface the station belongs to |

## Dynamic Routing through the AWR protocol

Dynamic routing is the process through which a router learns and updates routes to the other nodes in the network. For optimal performance in a wireless mesh environment, MSR series supports the intelligent Adaptive Wireless Routing (AWR) protocol. When AWR is activated, each MSR series will automatically maintain a table of optimal routes to the other MSR series nodes in the network, the clients associated to these nodes, and to the internet gateway. AWR ensures high-performance data forwarding in a wireless mesh environment by minimizing the number of hops used in data communication, regardless of whether that communication is within the mesh network itself, or between a host in the network and the internet.

The following table summarizes the configuration commands that control the operation of AWR:

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **router awr**<br>**no router awr** | CONFIGURATION | Start the configuration of the AWR routing protocol<br>Disable AWR and remove its configuration |
| **enable** | ROUTER AWR | Administratively activate the AWR routing protocol[16] |
| **disable** | ROUTER AWR | Administratively disable the AWR routing protocol |
| **debug**<br>**debug none**<br>**debug error**<br>**debug state**<br>**debug information**<br>**debug dump** | ROUTER AWR | Set the AWR debug log level<br>Disable AWR debug log<br>Set AWR debug log to record errors<br>Set AWR debug log to record errors & state changes<br>Log error, state, and other detailed information<br>Log all AWR debug information |

## Displaying current routing status

The following commands can be entered at the privileged EXEC prompt to display information about the system routing table and/or the AWR protocol state:

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **show ip route** | Privileged EXEC | Display the current routing table |
| **show ip forwarding** | Privileged EXEC | Display the current layer-3 forwarding information |
| **show log awr** | Privileged EXEC | Display the debug log of AWR (see |

[16] If AWR is administratively enabled, it should be running as long as it has a valid configuration.

| | | |
|---|---|---|
| | | debug command above) |
| **show ip awr configuration** | Privileged EXEC | Display the current AWR configuration and status |
| **show ip awr database** | Privileged EXEC | Display the routing data currently tracked by the AWR protocol |
| **show ip awr neighbor** | Privileged EXEC | Display the list of IP addresses of neighboring MSR series routers |

### Viewing routing information.

```
MSR2000# show ip route
Codes: K - kernel route, C - connected, S - static, H - host,
       A - AWR, > - selected route, * - FIB route

A>* 0.0.0.0/0 [50/2] via 10.2.6.1, Radio0MWds1, 01:43:57
A>* 10.0.0.0/8 [50/2] via 10.2.6.1, Radio0MWds1, 02:23:46
A>* 10.1.5.1/32 [50/2] via 10.1.6.1, Radio0MWds0, 02:30:56
A>* 10.1.5.2/32 [50/2] via 10.5.6.2, Radio1MWds1, 02:30:44
A>* 10.2.5.1/32 [50/2] via 10.2.6.1, Radio0MWds1, 02:23:37
A>* 10.2.5.2/32 [50/2] via 10.5.6.2, Radio1MWds1, 02:23:37
C>* 10.6.7.0/24 is directly connected, Radio0MWds0
H>* 10.6.7.1/32 [0/0] is directly connected, Radio0MWds0
A   10.6.7.2/32 [50/2] via 10.6.7.2, 02:30:56
C>* 192.168.1.0/24 is directly connected, fast-ethernet 0
H>* 192.168.1.136/32 [0/0] is directly connected, fast-ethernet 0
A>* 192.168.2.131/32 [50/2] via 10.1.6.1, Radio0MWds0, 02:31:01
A>* 192.168.2.132/32 [50/2] via 10.2.6.1, Radio0MWds1, 02:23:46
A>* 192.168.2.134/32 [50/2] via 10.4.6.2, Radio1MWds0, 02:30:56
A>* 192.168.2.135/32 [50/2] via 10.5.6.2, Radio1MWds1, 02:30:56
C>* 192.168.2.136/32 is directly connected, lo:2
A>* 192.168.2.137/32 [50/2] via 10.6.7.2, Radio0MWds0, 02:30:56
A>* 10.1.2.1/32 [50/2] via 10.1.6.1, Radio0MWds0, 02:23:46
A>* 10.1.2.2/32 [50/2] via 10.2.6.1, Radio0MWds1, 02:23:46
C>* 10.1.6.0/28 is directly connected, Radio0MWds0
A   10.1.6.1/32 [50/2] via 10.1.6.1, 02:31:01
H>* 10.1.6.2/32 [0/0] is directly connected, Radio0MWds0
A>* 10.1.7.1/32 [50/2] via 10.1.6.1, Radio0MWds0, 02:31:01
A>* 10.1.7.2/32 [50/2] via 10.6.7.2, Radio0MWds0, 02:30:56
C>* 10.2.6.0/28 is directly connected, Radio0MWds1
H>* 10.4.6.1/32 [0/0] is directly connected, Radio1MWds0
A   10.4.6.2/32 [50/2] via 10.4.6.2, 02:30:56
A>* 10.4.7.1/32 [50/2] via 10.4.6.2, Radio1MWds0, 02:30:56
A>* 10.4.7.2/32 [50/2] via 10.6.7.2, Radio0MWds0, 02:30:56
C>* 10.5.6.0/28 is directly connected, Radio1MWds1
H>* 10.5.6.1/32 [0/0] is directly connected, Radio1MWds1
A   10.5.6.2/32 [50/2] via 10.5.6.2, 02:30:56
A>* 10.5.7.1/32 [50/2] via 10.5.6.2, Radio1MWds1, 02:30:53
A>* 10.5.7.2/32 [50/2] via 10.6.7.2, Radio0MWds0, 02:30:56

MSR2000# show ip awr neighbor
AWR internal neighbor table:
Neighbor IP address=10.2.6.1
Neighbor IP address=10.5.6.2
Neighbor IP address=10.6.7.2
Neighbor IP address=10.4.6.2
Neighbor IP address=10.1.6.1
```

**Figure 14** Output of routing information

# Chapter 9 Configuring Motrix Roaming

This chapter contains information on configuring the Motrix Roaming Service on the MSR series.

## Motrix Protocol Overview

Motrix is the roaming service MSR series provides to support the seamless roaming of wireless clients across different mesh network subnets. Such support is necessary because every MSR series is a layer-3 router and each BSS within the mesh network is associated with a single layer-3 subnet. These subnets are interconnected via IP routing functions of the MSR series. When a client joins the network on one router's BSS, it would have an IP that belongs to that BSS's subnet. If the client subsequently roams to another router's BSS, the Motrix service enables the client to retain its connectivity to the network using its previous IP address (which would actually belong to a different subnet). Without Motrix, the client would have to change its IP address and thus lose all of its existing connections.

To support inter-subnet roaming, each participating access router must enable the Motrix service and have the same BSS settings (SSID, authentication, etc) configured. We emphasize "access router" here because it is not necessary for a MSR series configured only for backhaul or client to enable the Motrix service.

When using the built-in wireless functions of a Centrino® certificated notebook, one is recommended to upgrade the notebook to the latest official driver from the Download/Support webpage of the notebook vendor.

It is highly recommended that the participating clients use dynamic IP addressing (DHCP). If the clients must be configured with static IP addresses, then only one router may act as the gateway for the mesh network and a "Static IP client list" must be specified on the gateway router and each access router. For more information, see the item "Static IP Client List" in the section "Motrix-related configuration information."

## Motrix Configuration

This section covers the following main topics:

- Motrix-related configuration information
- Motrix-related configuration commands
- Show motrix configuration

### Motrix-related configuration information

**1) The roaming gateway**

Motrix requires the specification of a single gateway router on each access router that provides roaming support. Even when there are multiple gateways connected to the same mesh network, one of them needs to be specified as the “roaming gateway” router.

### 2) The MAC-IP mapping of other BSSs

The Motrix service also requires the IP and MAC address of every BSS (or virtual AP) within the mesh network. This information is automatically learned if the AWR routing protocol is enabled. However, if Motrix is to be used while AWR is not running, then the MAC-IP mapping must be configured manually through the **mac-ip-list** command described below. Each entry in the MAC-IP list is a mapping that associates a BSS’s MAC address with its router ID.

***Note: The MAC-IP list is indexed by the BSS MAC address, and each MAC address may be associated with only one IP address.***

### 3) Static IP client list

In some applications, clients use preconfigured static IP addresses. To support such clients, only one wired-gateway router could be present in the mesh network and a station list need to be specified on each participating access router and the gateway router. The station list contains MAC-IP mappings that associate the static IP clients’ IP addresses with their MAC addresses. This information can only be configured manually.

## Configuring Motrix Service

The following table summarizes the configuration commands for Motrix:

| **Command Syntax** | **Command Mode** | **Purpose** |
|---|---|---|
| **service roaming-motrix**<br>**no service roaming-motrix** | CONFIGURATION | Start configuration of the Motrix Roaming Service<br>Disable Motrix Roaming Service and remove its configuration |
| **enable**<br>**disable** | SERVICE ROAMING-MOTRIX | Activate the Motrix roaming service[17]<br>Shutdown the Motrix Roaming service |
| **gateway** A.B.C.D | SERVICE ROAMING-MOTRIX | Specify the IP address of the roaming gateway router |
| **mac-ip-list** *<HH:HH:HH:HH:HH:HH> <A.B.C.D>* | SERVICE ROAMING-MOTRIX | Add an entry to the MAC-IP list |

[17] When enabled, Motrix should be running as long as it has a valid configuration.

| | | |
|---|---|---|
| **no mac-ip-list**<br>**no mac-ip-list** <*HH:HH:HH:HH:HH:HH*> | | Clear all entries of the MAC-IP list<br>Remove an entry from the MAC-IP list<br>HH:HH:HH:HH:HH:HH: The MAC address of a BSS in the network |
| **station-list** <*HH:HH:HH:HH:HH:HH*> <*A.B.C.D/M*><br>**no station-list**<br>**no station-list** <*HH:HH:HH:HH:HH:HH*> | SERVICE ROAMING-MOTRIX | Add an entry to the station list<br>Clear all entries of the station list<br>Remove an entry from the station list<br>HH:HH:HH:HH:HH:HH: The MAC address of a static-IP client in the network |
| **debug**<br>**debug none**<br>**debug error**<br>**debug information**<br>**debug dump** | SERVICE ROAMING-MOTRIX | Set the Motrix debug log level<br>Disable Motrix debug log<br>Set Motrix debug log to record errors<br>Log errors and other important information<br>Log all Motrix debug information |

## Displaying Motrix Configuration and Status

**Table 17** Display roaming status

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **show log motrix** | Privileged EXEC | Display the debug log of Motrix (see debug command above) |
| **show ip mobility motrix** | Privileged EXEC | Display Motrix configuration and status |
| **show ip mobility motrix mac-ip-list** | Privileged EXEC | Display the MAC-IP list used by Motrix |
| **show ip mobility motrix stations** | Privileged EXEC | Display the list of clients/stations that are Home associated or roaming from other MSR seriess |

```
!
!
! Configuration
!
service roaming-motrix
 enable
 debug information
 mac-ip-list  00:00:65:43:21:00 172.16.21.1
 mac-ip-list  00:17:7b:37:ab:53 172.16.20.1
 mac-ip-list  00:17:7b:36:a1:0a 172.16.19.1
 station-list 00:14:bf:c2:09:4c 10.1.1.249/32
 station-list 00:17:7b:00:27:38 10.2.2.99/32
 gateway 192.168.15.97
!

MSR2000# show ip mobility motrix
 <cr>
 mac-ip-list  Display mac-ip table
 stations     Display roaming stations
MSR2000# show ip mobility motrix
 status RUNNING
 enable
 tcp
 debug information
 keepalive on

MSR2000# show ip mobility motrix mac-ip-list
Learned from configuration:
00:17:7b:43:21:00 172.16.21.1
00:17:7b:37:ab:53 172.16.20.1
00:17:7b:36:a1:0a 172.16.19.1
MSR2000# show ip mobility motrix stations
STATIONS:
Total number of stations: 2

  MAC: 00:40:96:a2:be:e3
  IP: 172.16.20.242
  State: Roam Associated
  Time since last (re)association: 448(s)
  Associated interface: Dot11Radio0(00:17:7b:36:a1:0a)
  Previous AP: 00:17:7b:37:ab:53
  Home AP: 00:17:7b:37:ab:53/172.16.20.1
  No tunnel

  MAC: 00:14:78:72:10:01
  IP: 0.0.0.0
  State: Home Associated
  Time since last (re)association: 7(s)
  Associated interface: Dot11Radio0(00:17:7b:36:a1:0a)
  Previous AP: 00:00:00:00:00:00
  No tunnel
  Tunnel from gateway 192.168.15.97 is established
```

Figure 15 Output of Motrix

# Chapter 10 DHCP and NAT

This chapter contains information on configuring the DHCP and NAT services on the MSR series, it has the following sections:

- DHCP Protocol Overview
- Configuring DHCP Server
- Configuring DHCP Relay
- Configuring NAT

## DHCP Protocol Overview

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. DHCP allows devices connecting to a network to automatically obtain an IP address.

In order to ensure that each STA can communicate with external internet and/or between each other, it should be assigned an IP address. The MSR series provides DHCP services such as DHCP server and DHCP Relay to dynamically assign such addresses.

## Configuring DHCP Server

On MSR series, each BSS has its own private subnet. Each STA associated with a BSS obtains an IP address from the DHCP server.

- Configuring DHCP Server Parameters
    - Configuring DHCP pools
    - Attaching DHCP pools to BSSs
- Showing DHCP Information and Status

### Configuring DHCP Server Parameters

DHCP configurations are performed in CONFIGURATION mode.  The following table outlines the general DHCP configuration commands:

**Table 18** Configuring DHCP Server

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **ip dhcp server** | CONFIGURATION | Start configuration of DHCP server |
| **no ip dhcp server** | | Stop the DHCP server and remove its configuration |
| **enable** | IP DHCP SERVER | Enable the DHCP server[18] |

| | | |
|---|---|---|
| **disable** | IP DHCP SERVER | Temporarily disable the DHCP server |
| **default-lease-time** *<0-31536000>* | IP DHCP SERVER | Set the time (in seconds) given to each DHCP lease request that does not specify a lease time. The maximum is 31536000 seconds (one year). |
| **no default-lease-time** | | Set this parameter to the default value of 86400 seconds (1 day) |
| **dns** *[DNS-list]* | IP DHCP SERVER | Enter DNS addresses that will be included in a DHCP lease. Multiple DNS servers may be specified by separating them with commas (,). |
| **no dns** | | Clear the DNS list; no DNS information will be included in leases |
| **max-lease-time** *<0-31536000>* | IP DHCP SERVER | Set the maximum allowed lease time in seconds; can be set as high as 3153600 (one year) |
| **no max-lease-time** | | Set this parameter to the default value of 86400 seconds (one day) |
| **pool [NAME]** | IP DHCP SERVER | Configure a new or existing DHCP pool (see below for details) |
| **no pool [NAME]** | | Remove an existing DHCP pool |
| | | NAME: An alphanumeric string that identifies the DHCP pool |

## Configuring DHCP Pools

The MSR series DHCP server supports multiple DHCP pools. Each DHCP pool is a separate IP address space that the DHCP server uses to respond to lease requests for specific pools. Each pool may be on different networks or uses different gateways and domain-names. The pool-specific configuration controls the IP address, gateway, and domain-name information the client devices would obtain through their DHCP requests.

Usually, pools are bind to specific BSSs and DHCP requests received from clients associated to these BSSs would use different DHCP pools to honor the request. DHCP pools may be configured manually on the MSR series or be automatically created. Automatically created DHCP pools use the IP address prefix 172.16 through 172.31, while manual DHCP pools may use any IP address prefix. ***Note: the DHCP pool IP address prefix must not duplicate any other IP addresses or networks needed by the mesh network.***

The following table outlines the manual DHCP pool configuration commands:

| | | |
|---|---|---|
| **pool [NAME]** | IP DHCP SERVER | Configure a new or existing DHCP pool (see below for details) |

[18] Once enabled, DHCP server will be running as long as it has a valid configuration.

| | | |
|---|---|---|
| **no pool [NAME]** | | Remove an existing DHCP pool<br>NAME: An alphanumeric string that identifies the DHCP pool |
| **domain-name** *[name]*<br>**no domain-name** | IP DHCP SERVER POOL | Set the domain name to be included in DHCP leases for this pool<br>Do not include any domain name information in DHCP leases for this pool<br>name: A domain name such as “azaleanete.com” |
| **gateway** *<A.B.C.D>*<br>**no gateway** *<A.B.C.D>* | IP DHCP SERVER POOL | Set the gateway IP to be included in DHCP leases for this pool<br>Do not include gateway in DHCP leases<br>A.B.C.D: A gateway IP address that should conform to a IPv4 unicast address, where A is 1-223, B & C is 0-254, and D is 1-254. |
| **host** *<HH:HH:HH:HH:HH:HH> <A.B.C.D>*<br>**no host** *<HH:HH:HH:HH:HH:HH>* | IP DHCP SERVER POOL | Add a fixed DHCP IP address entry for a client host<br>Remove a fixed DHCP IP address entry<br>HH:HH:HH:HH:HH:HH: MAC address of the client host<br>A.B.C.D: Fixed IP address to be assigned to the host |
| **network** *{<A.B.C.D Mask> \| <A.B.C.D/M>}* | IP DHCP SERVER POOL | Specify the subnet that this pool belongs to<br><A.B.C.D Mask>: Address and mask of the subnet, e.g. 10.1.1.0 255.255.255.0<br>A.B.C.D/M: Address/mask of the subnet, e.g. 10.1.1.0/24 |
| **range** *<begin IP> <end IP>*<br>**no range** *<begin IP> <end IP>* | IP DHCP SERVER POOL | Add a range of IP addresses to this DHCP pool<br>Remove a range from this DHCP pool<br>Begin IP: The first IP address of the range<br>End IP: The last IP address of the range. |

| | | |
|---|---|---|
| | | Both begin and end IP should be a valid IPv4 unicast address. |

## Attaching DHCP pools to Ethernet interfaces and BSSs

Different BSSs and/or different Ethernet interfaces may use different DHCP pools. You can use the following command in the **BSS** and **INTERFACE DOT11RADIO BSS modes** to attach DHCP pools to BSSs and Ethernet interfaces:

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **dhcp server** *<POOL-NAME>* | INTERFACE DOT11RADIO BSS | Attach a manual DHCP pool to the current BSS[19] |
| **dhcp server automatic** | | Attach an automatic DHCP pool to the current BSS |
| **no dhcp** | | Detach DHCP service from the current BSS |
| **ip address** *[ip address/mask]* | INTERFACE DOT11RADIO BSS | Set IP address of this BSS. This command is required when using a manual DHCP pool. |
| **no ip address** | | Remove IP address from this BSS |

## Show DHCP Server Information and Status

You can use the following commands to show current configuration about DHCP server.

**Table 19** Display DHCP Server Information

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **show dhcp server all** | Privileged EXEC | Show all DHCP server information |
| **show dhcp server default-lease-time** | Privileged EXEC | Show the current value of default lease time |
| **show dhcp server dns** | Privileged EXEC | Show the current dns value |
| **show dhcp server lease** | Privileged EXEC | Show the current IP address assignments |
| **show dhcp server max-lease-time** | Privileged EXEC | Show the current value of maximal lease time |
| **show dhcp server pool** | Privileged EXEC | Show the current DHCP pools |

[19] Only one of DHCP pool and DHCP relay can be used on a BSS, so if this BSS had DHCP relay enabled (see next section), it will be disabled.

### Viewing DHCP Server configuration

```
!
! Configuration
!
router dhcp server
 domain-name azaleanete.com
 dns 10.13.28.12,10.13.31.12
 max-lease-time 100000
!
!
MSR2000# show dhcp server all
domain-name: azaleanete.com
DNS servers: 10.13.28.12,10.13.31.12
default-lease-time: 86400 (unit: seconds)
max-lease-time: 100000 (unit: seconds)
!
!
MSR2000# show dhcp server default-lease-time
default-lease-time: 86400 (unit: seconds)
!
!
MSR2000# show dhcp server dns
DNS servers: 10.13.28.12,10.13.31.12
!
!
MSR2000# show dhcp server max-lease-time
max-lease-time: 86400 (unit: seconds)
!
```

**Figure 16** Output of DHCP Server configuration

## Configuring DHCP Relay

DHCP Relay is responsible for forwarding the DHCP requests and responses sent by the DHCP clients and server. It allows clients associated to BSSs on the MSR series routers to obtain IP address from pools defined on an external DHCP server.

- Configuring DHCP Relay Parameters
    - Enabling DHCP relay on specific BSSs
- Show DHCP Relay Information

### Configuring DHCP Relay Parameters

Configuring DHCP relay has to be in CONFIGURATION mode. The following table summarizes the commands to configure DHCP relay.

**Table 20** Configuring DHCP Relay

| Command Syntax | Command Mode | Purpose |
|---|---|---|

| | | |
|---|---|---|
| **ip dhcp relay** | CONFIGURATION | Start configuration of DHCP relay |
| **no ip dhcp relay** | | Stop DHCP relay service and remove its configuration |
| **enable** | IP DHCP RELAY | Start the DHCP relay service |
| **disable** | IP DHCP RELAY | Temporarily stop the DHCP relay service |
| **dhcp-servers** *[SERVER-list]* | IP DHCP RELAY | Configure a list of DHCP servers to which the DHCP requests would be relayed. Multiple servers may be specified by separating them with commas (,). |
| **no dhcp-servers** | | Clear the DHCP server list |

## Enabling DHCP Relay on specific BSSs

Not all BSSs have to use DHCP relay; some may use DHCP pools or no DHCP service at all. You can use the following command in the “**BSS mode**” to enable DHCP relay for a BSS:

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **dhcp relay** | INTERFACE DOT11RADIO BSS | Enable DHCP relay on this BSS[20] |
| **no dhcp** | | Disable DHCP service from the current BSS |

## Show DHCP Relay Information

You can use the following commands to show current configuration about dhcp relay. Note that it should be in ENABLE mode.

**Table 21** Configuring DHCP Server

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **show dhcp relay dhcp-servers** | Privileged EXEC | Show DHCP servers are used by DHCP relay |

### Viewing DHCP Relay configuration

```
!
!DHCP Relay Configuration
!
router dhcp relay
 dhcp-servers 192.168.1.1,192.168.1.2
```

[20] Only one of DHCP pool and DHCP relay can be used on a BSS, so if this BSS had DHCP pool attached (see previous section), it will be removed.

```
!
!Display DHCP Relay Information
!
MSR2000# show dhcp relay dhcp-servers
dhcp-servers: 192.168.1.1 192.168.1.2
!
```

**Figure 17** Output of DHCP Relay configuration

## Configuring NAT

Network Address Translation (NAT) is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations. This chapter contains the information of configuring NAT on the MSR series.

The service NAT runs only in the mesh gateway. You can use the following commands to configure the NAT service:

**Table 22** Configuring NAT

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **ip nat** | CONFIGURATION | Enter NAT configuration mode |
| **no ip nat** | | Disable NAT and remove NAT configuration |
| **Enable** | IP NAT | Enable NAT service |
| **Disable** | IP NAT | Disable NAT service temporarily |
| **out-interface fast-ethernet** *<0-1>* | IP NAT | Add a FastEthernet interface as external NAT interface |
| **out-interface dot11radio** *<0-N>* **station** *<name>* | | Add a client station as external NAT interface. |
| **no out-interface fast-ethernet** *<0-1>* | | Remove a FastEthernet as the NAT interface. |
| **no out-interface dot11radio** *<0-N>* **station** *<name>* | | Remove a client station as the NAT interface. |

## Show the configuration of NAT

You can use the following commands to show current configuration about NAT.

**Table 23** Display NAT interface and NAT table

| Command Syntax | Command Mode | Purpose |
|---|---|---|

| | | |
|---|---|---|
| **show nat out-interface** | Privileged EXEC | Display NAT Outside interface |
| **show nat table** | Privileged EXEC | Display NAT Table |

# Chapter 11 802.11 Security

This chapter describes how to configure security policies as defined by the 802.11i standard on the MSR series router. It contains the following sections:

- 802.11 security standard overview
- MAC-based access control configuration
- RADIUS AAA Configuration
- Security Profile Configuration
- BSS security
- WDS security

## 802.11 standard overview

The 802.11 security standard defines a suite of wireless security protocols and implementations. It provides open and shared key authentication, is compatible with WPA /WPA2, and interoperates with 802.1x.

## MAC-based Access Control Configuration

MSR series allows MAC address-based access control. For each BSS hosted by the router, one can allow or disallow a list of client MAC addresses proper association with the AP. Creation of the MAC list and the specification of the MAC addresses are performed by the mac-list command under CONFIGURATION TERMINAL mode.

**Table 24** Configuring MAC-List

| **Command Syntax** | **Command Mode** | **Purpose** |
|---|---|---|
| **mac-list** <*listname*><br>**no mac-list** <*listname*> | CONFIGURATION<br>CONFIGURATION | Create or modify a MAC address list with the specified name<br>Remove a MAC address list |
| **mac-addr** <*HH:HH:HH:HH:HH:HH*><br>**no mac-addr** <*HH:HH:HH:HH:HH:HH*> | MAC-LIST<br>MAC-LIST | Add a MAC address to the MAC list<br>Remove a MAC address from MAC list |

## Show the configuration of MAC-List

You can use the following commands to show current configuration about MAC-List.

**Table 25** Display MAC-List and information

| **Command Syntax** | **Command Mode** | **Purpose** |
|---|---|---|
| **show mac-list** | Privileged EXEC | Show all configured MAC address list |

View MAC-List configuration

**Figure 18** Output of MAC-List configuration

```
!
```

```
mac-list aaa
 mac-addr 00:00:11:11:11:11
 mac-addr 00:00:11:11:11:12
 mac-addr 00:00:11:11:11:13
 mac-addr 00:00:11:11:11:14
mac-list bbb
 mac-addr 00:00:22:22:22:22
 mac-addr 00:00:22:22:22:23
 mac-addr 00:00:22:22:22:24
!

MSR2000# show mac-list
mac-list aaa
 mac-addr 00:00:11:11:11:11
 mac-addr 00:00:11:11:11:12
 mac-addr 00:00:11:11:11:13
 mac-addr 00:00:11:11:11:14
mac-list bbb
 mac-addr 00:00:22:22:22:22
 mac-addr 00:00:22:22:22:23
 mac-addr 00:00:22:22:22:24
```

## RADIUS AAA Configuration

This section describes how to enable and configure the RADIUS (Remote Authentication Dial-In User Service), which provide flexible administrative control over authentication and authorization processes. RADIUS is configured with the AAA mode command.

**Table 26** Configuring AAA

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **Aaa** | CONFIGURATION | Configuring AAA parameters, including authentication and accounting servers and ports |
| **radius-server** *<A.B.C.D> auth-port <1-65535> key <string>*<br>**radius server** *<A.B.C.D> auth-port default key <string>*<br>**no radius-server** *<A.B.C.D> auth* | AAA | Add a radius authentication server using the specified port and secret key.<br>Add a radius authentication server using the default port of 1812 and the specified secret key.<br>Remove a radius authentication server |
| **radius-server** *<A.B.C.D>acct-port <1-65535> key <string>*<br>**radius server** *<A.B.C.D> acct-port default key <string>* | AAA | Add a radius accounting server using the specified secret key and authentication port<br>Add a radius accounting server using the default port of 1813 and the specified secret key. |

| | | |
|---|---|---|
| **no radius-server** *<A.B.C.D>* **acct** | | Remove a radius accounting server |
| **server-group**[2] | AAA | Enter server group configuration |
| **server** *<A.B.C.D>* **auth**<br>**no server** *<A.B.C.D>* **auth**<br>**server** *<A.B.C.D>* **acct**<br>**no server** *<A.B.C.D>* **acct** | SERVER GROUP | Add a authentication server to server group<br>Remove authentication server from server group<br>Add a accounting server to server group<br>Remove a accounting server from server group |

**Notes:**

1. The radius-server command defines a radius server; the definition includes the ip address and port of an authentication or the ip address and port of an accounting server, Specifying a radius-server only make it available for use to the MSR series, but would not be used until included by a server group.
2. The server-group contains the radius server information for authentication or accounting, it is the current running-configuration that allow user to configure multiple servers under the server-group. The first authentication and accounting radius server is the primary server, the second server is the backup server, and the second server takes effect only when the first server fail to communicate with MSR series.

**Table 27** Display AAA configuration

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **show aaa** | PRIVILEGE EXEC | show aaa configuration, including radius server and server-group configuration |

View AAA configuration

**Figure 19** Output of AAA configuration

```
!
aaa
 radius-server  192.168.10.69 auth-port 1812 key secret
 radius-server  192.168.20.234 auth-port 1812 key 123456
 server-group
  server 192.168.10.69 auth
  server 192.168.20.234 auth
!
MSR2000# show aaa
!
aaa
 radius-server  192.168.10.69 auth-port 1812 key secret
 radius-server  192.168.20.234 auth-port 1812 key 123456
 server-group
  server 192.168.10.69 auth
  server 192.168.20.234 auth
MSR2000#
```

## *Certificate Configuration*

This section describes how to download and install certificates which are used for authenticating the MSR series as an allowed client for other 802.11 APs.

Table 27 Installing Authentication Certificates

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **install certificate ca  <URL>** | Privilege EXEC | Download and install the CA certificate from the provided URL |
| **install certificate client <URL>** | Privilege EXEC | Download and install the client certificate from the provided URL |
| **install client-key <URL>** | Privilege EXEC | Download and install the client key file from the provided URL |

**Table 28** Displaying Installed Certificates

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **show certificate ca** | Privilege EXEC | Show the information of the installed CA certificate. |
| **show certificate client** | Privilege EXEC | Show the information of the installed client certificate. |

Configuration example:

```
MSR2000# install certificate ca http://192.168.1.1/certs/cert-ca.pem

MSR2000#  install  certificate  client  http://192.168.1.1/certs/cert-clt.pem

MSR2000# install client-key http://192.168.1.1/certs/cert-clt-key.pem

MSR2000# show certificate ca

MSR2000# show certificate client
```

## Security-Profile Configuration

This section describes the authentication types and encryption methods that you can configure on the router. Security profile on MSR series defines all security policy supported by router software. Now router supports WEP, WPA, WPA2 and 8021X security suites. This block is only a definition of security policy, and it will take effect after attached in BSS or WDS. You can add multi profile for the same methods, and that will be flexible to change security policy on router for user.

**Table 29** Configuring Security Profiles

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **security-profile wep <wep-profile-name>**<br>**no security-profile wep <wep-name>** | CONFIGURATION | Create or modify a WEP security profile of the given name<br>Remove a WEP profile |
| **wep-key <1\|2\|3\|4> <key-string>**<br>**no wep-key <1\|2\|3\|4>** | SECURITY-PROFILE WEP | Add a WEP key to the WEP profile<br>Remove a WEP key from WEP profile |
| **security-profile wpa <wpa-profile-name>**<br>**no security-profile wpa <wpa-profile-name>** | CONFIGURATION | Create or modify a WPA security profile of the given name<br>Remove a WPA profile |
| **encryption-mode-cipher tkip**<br>**no encryption-mode-cipher** | SECURITY-PROFILE WPA | Enable TKIP encryption mode for WPA |
| **wpa-type 8021x <8021x-profile-name>**<br>**no wpa-type 8021x** | SECURITY-PROFILE WPA | Enable 8021X authentication for WPA profile<br>Remove 8021X authentication on WPA profile |
| **wpa-type psk hex <string>**<br>**wpa-type psk ascii <string>**<br>**no wpa-type psk** | SECURITY-PROFILE WPA | Enable WPA PSK authentication on WPA profile and configure pre-shared key using hexadecimal format.<br>Enable WPA PSK and configure pre-shared key using ASCII format<br>Remove WPA PSK authentication from WPA profile |
| **security-profile wpa2 <wpa2-profile-name>**<br>**no security-profile wpa2 <wpa2-profile-name>** | CONFIGURATION | Add a WPA2 profile<br>Remove a WPA2 profile from current configuration |
| **encryption-mode-cipher ccmp**<br>**encryption-mode-cipher tkip**<br>**no encryption-mode-cipher** | SECURITY-PROFILE WPA2 | Enable CCMP encryption for WPA2 profile<br>Enable TKIP encryption for WPA2 profile |

| | | |
|---|---|---|
| **wpa2-type 8021x <8021x-profile-name>**<br>**no wpa2-type 8021x** | SECURITY-PROFILE WPA2 | Enable 8021X authentication for WPA2 profile<br>Remove 8021X authentication from WPA2 profile |
| **wpa2-type psk hex <string>**<br>**wpa2-type psk ascii <string>**<br>**no wpa2-type psk** | SECURITY-PROFILE WPA2 | Enable WPA2 PSK authentication on WPA2 profile and configure pre-shared key using hexadecimal format.<br>Enable WPA2 PSK and configure pre-shared key using ASCII format<br>Remove WPA2 PSK authentication from WPA2 profile |
| **security-profile 8021x <8021x-profile-name>**<br>**no security-profile 8021x<8021x-profile-name>** | CONFIGURATION | Add a 8021X authentication profile<br>Remove a 8021X authentication profile |
| **eap-reauth-period <0-65535>**<br>**eap-reauth-period 3600**<br>**no eap-reauth-period** | SECURITY-PROFILE 8021x | Set EAP re-authentication period<br>Restore EAP re-authentication to default value of 3600 seconds |
| **security-profile client-8021x <client-8021x-profile-name>**<br>**no security-profile client-8021x <client-8021x-profile-name>** | CONFIGURATION | Add a client 8021X authentication profile<br>Remove a client 8021X authentication profile |
| **eap-method peap**<br>**eap-method ttls**<br>**eap-method tls**<br>**no eap-method** | SECURITY-PROFILE CLIENT-8021x | Enable PEAP authentication method for client-8021x profile<br>Enable TTLS authentication method for client-8021x profile<br>Enable TLS authentication method for client-8021x profile<br>Remove eap method for client-8021x profile. |

| | | |
|---|---|---|
| **password <string>**<br>**no password** | SECURITY-PROFILE CLIENT-8021x | Set the user password for authentication<br>Remove password for client-8021x profile |
| **user-name <string>**<br>**no user-name** | SECURITY-PROFILE CLIENT-8021x | Set the user name for authentication<br>Remove user name for client-8021x profile |

**Table 30** Display configuration of security profile

| **Command Syntax** | **Command Mode** | **Purpose** |
|---|---|---|
| **show security-profile wep** | Privilege EXEC | Show WEP profile configuration |
| **show security-profile wpa** | Privilege EXEC | Show WPA profile configuration |
| **show security-profile wpa2** | Privilege EXEC | Show WPA2 profile configuration |
| **show security-profile 8021x** | Privilege EXEC | Show 8021x profile configuration |
| **show security-profile client-8021x** | Privilege EXEC | Show client-8021x profile configuration |

**Figure** Output of WEP profile configuration

```
security-profile wep wep1
 wep-key 1 1234567890abcdef1234567890
 wep-key 2 "abcde"
 wep-key 3 "abcdefabcdefa"
 wep-key 4 abcdefabcdefabcdefabcdefabcdefab
security-profile wep wep2
 wep-key 1 "abcde"
 wep-key 2 "1234567890123"
 wep-key 3 "1234567890abcdef"
 wep-key 4 1234567890
security-profile wep wep3
 wep-key 3 abcdefabcdefabcdefabcdefab
security-profile wep wep4

MSR2000#  show security-profile wep
security-profile wep wep1
 wep-key 1 1234567890abcdef1234567890
 wep-key 2 "abcde"
 wep-key 3 "abcdefabcdefa"
 wep-key 4 abcdefabcdefabcdefabcdefabcdefab
security-profile wep wep2
 wep-key 1 "abcde"
 wep-key 2 "1234567890123"
 wep-key 3 "1234567890abcdef"
 wep-key 4 1234567890
security-profile wep wep3
 wep-key 3 abcdefabcdefabcdefabcdefab
security-profile wep wep4
MSR2000#
```

**Figure 20** Output of WPA profile configuration

```
security-profile wpa wpa1
 encryption-mode-cipher tkip
                  wpa-type                   psk                   hex
1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef
security-profile wpa wpa2
 encryption-mode-cipher tkip
 wpa-type 8021x 802.1xprofile
security-profile wpa wpa3
 encryption-mode-cipher tkip
```

**Figure 21** Output of WPA2 profile configuration

```
security-profile wpa2 wpa2-pskprofile
 encryption-mode-cipher ccmp
 wpa2-type 8021x 802.1xprofile
!
```

**Figure 22** Output of 8021x profile configuration

```
!
security-profile 8021x 8021xprofile
 eap-reauth-period 3600
security-profile 8021x 8021x1

MSR2000# show security-profile 8021x
security-profile 8021x 8021xprofile
 eap-reauth-period 3600
security-profile 8021x 8021x1
MSR2000#
```

**Figure23** Output of client-8021x profile configuration

```
security-profile client-8021x client-8021x1
 eap-method tls
 user-name test-tls
security-profile client-8021x client-8021x2
 eap-method peap
 user-name test-peap
 password whatever
security-profile client-8021x client-8021x3
 eap-method ttls
 user-name test-ttls
 user-name ttls
 password whatever
```

## BSS Security Configuration

This section describes how to apply security profiles and MAC lists to the router's BSS configurations.

**Table 31** Configuring BSS Security

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **authentication open**<br>**no authentication** | INTERFACE DOT11RADIO BSS | Allow all clients to associate with this BSS |
| **authentication open wep <wep-profile-name> default-key <1-4>** | | Enable WEP encryption for this BSS using the key settings in the WEP profile and the specified default key |
| **authentication open key-management wpa <wpa-profile-name>** | | Enable WPA security for this BSS; only allow clients with correct WPA authentication and encryption settings to associate with this BSS. |
| **authentication open key-management wpa2 <wpa2-profile-name>** | | Enable WPA2 security for this BSS; only allow clients with correct WPA2 authentication and encryption settings to associate with this BSS. |
| **authentication shared wep <wep-profile-name> default-key <1-4>** | | Enable WEP authentication and encryption for this BSS using the key settings in the WEP profile and the specified default key |
| **mac-address accept <mac-list-name>** | INTERFACE DOT11RADIO BSS | Only accept clients with MAC addresses in the specified list; deny all other clients |
| **mac-address deny <mac-list-name>** | | Only deny clients with MAC addresses in the specified list; allow all other clients. |
| **mac-address accept-all**<br>**no mac-address** | | Restore to default configuration (accept all MAC addresses) |

**Table** Display security configuration on BSS

| | | |
|---|---|---|
| **show interface dot11radio <0\|1> bss <SSID> accept-macs**<br>**show interface dot11radio <0\|1> bss <SSID> deny-macs** | Privileged EXEC<br>Privileged EXEC | Show attached accept macs address on SSID of the Radio<br>Show attached deny macs address on SSID of the Radio |
| **show interface dot11radio0 bss <SSID> wep-keys** | Privileged EXEC | Show BSS WEP configuration |

```
MSR2000# show interface dot11radio 0 bss public accept-macs
accept mac list:
00:00:22:22:22:22, 00:00:22:22:22:23, 00:00:22:22:22:24,

MSR2000# show interface dot11radio 0 bss public1 deny-macs
deny mac list:
00:00:11:11:11:11,        00:00:11:11:11:12,        00:00:11:11:11:13,
00:00:11:11:11:14,


MSR2000# show interface dot11radio 0 bss public wep-keys
  <cr>
MSR2000# show interface dot11radio 0 bss public wep-keys
wep key 1=1234567890abcdef1234567890
wep key 2="abcde"
wep key 3="abcdefabcdefa"
wep key 4=abcdefabcdefabcdefabcdefabcdefab
MSR2000#
```

## WDS Security Configuration

This section describes how to apply security profiles and MAC lists to the router's manual WDS interfaces.

**Table 32** Configuring WDS security

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **authentication open**<br>**no authentication** | INTERFACE DOT11RADIO WDS | Disable authentication for this WDS interface (open system). |
| **authentication open key-management wpa <wpa-profile-name>** | | Enable WPA security for this WDS interface using the specified profile settings. |
| **authentication shared wep <wep-profile-name> default-key <1-4>** | | Enable WEP security for this WDS interface using the key settings in the WEP profile and the specified default key |

## CLIENT Security Configuration

This section describes how to apply security profiles and WEP key to the router's configured clients.

**Table 33** Configuring client-mode security

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **client-authentication open wep <wep-profile-name> default-key <1-4>** | INTERFACE DOT11RADIO STATION | Enable WEP encryption for this client using the key settings in the WEP profile and the specified default key |
| **client-authentication open client-8021x <client-8021x-profile-name>** | | Enable 802.1X authentication for this client, using the authentication settings in the client-8021x profile |
| **client-authentication open key-management wpa client-8021x <client-8021x-profile-name>** | | Enable WPA security for this CLIENT, using the authentication settings in the client-8021x profile |
| **client-authentication open key-management wpa2 client-8021x <client-8021x-profile-name>** | | Enable WPA2 security for this CLIENT, using the authentication settings in the client-8021x profile |
| **client-authentication open key-management wpa-psk hex <string>** | | Enable WPA PSK on client and configure pre-shared key using hexadecimal format. |
| **client-authentication open key-management wpa-psk ascii <string>** | | Enable WPA PSK on client and configure pre-shared key using ascii format. |
| **client-authentication shared wep <wep-profile-name> default-key <1-4>** | | Enable WEP encryption for this client using the key settings in the WEP profile and the specified default key |
| **no client-authentication** | | Disable authentication for this client interface. |

**Notes:**

1. Open: Open authentication allows any clients to authenticate and then attempts to communicate with the router.
2. Shared-key :
   a) Shared Key authentication seeks to authenticate clients as either a member of those who know a shared secret key or a member of those who do not.
   b) Shared Key authentication can be used if and only if WEP has been selected.
   c) Not recommended because of known security flaws.
3. WEP: Wired Equivalent Privacy
   a) WEP have three keys, 64bits, 128bits and 152bits, and based on RC4 algorithm.
   b) WEP was defined as a means of protecting the confidentiality of data exchanged among authorized users of a wireless LAN from casual eavesdropping.
4. WPA :
   a) Wi-Fi Protected Access (WPA) is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems.
   b) WPA leverages TKIP (Temporal Key Integrity Protocol) for data protection and 802.1X for authenticated key management.
   c) WPA key management supports two mutually exclusive management types: WPA(802.1X) and WPA-Pre-shared key (WPA-PSK)
5. WPA2: WPA version 2, add AES encryption algorithm than WPA.
6. 802.1X:
   a) Port-Based Networks Access Control;
   b) 8021X is consisting of supplicant, authenticator and server.
   c) After clients associate to BSS successful, clients start authentication process of 8021X. IEEE 8021X think an associate to be a controlled port.

# Chapter 12 QoS Configuration

Traffic over-subscription is a common cause for the instability of network links; if many links in the mesh network is over-subscribed, the performance of the overall network becomes unstable. In order to avoid over-subscribing any individual WDS link, we strongly recommend enabling QoS to control and limit the traffic flows injected into the network. This chapter contains information on defining and configuring QoS on MSR series.

- Enable/Disable QoS Service
- Configuring QoS over ManualWDS Interface
    - Configuring QoS class
    - Attaching QoS class to ManualWDS
- Configuring QoS over AutoWDS Interface
- Showing Qos Information and Status

## Enable/Disable QoS Service

By default, QoS doesn't take effect on MSR series. Use the following commands to start or stop the QoS in CONFIGURATION mode.

Table **34** Enable/Disable QoS

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **qos** | CONFIGURATION | Enter QOS configuration mode |
| **enable** | QOS | Enable QoS, start QoS service and all QoS classes attached to WDS interface will take effect |
| **disable** | QOS | Disable QoS, stop QoS service and all QoS classes attached to WDS interface will be disabled |

When enable QoS globally, user should attach QoS to WDS Interface. There are two kinds of WDS interfaces, ManualWDS interface created by users and AutoWDS interface created by RF-Management service. Correspondingly, for ManualWDS interface, user should manually configure QoS settings. On the other hand, for AutoWDS interface, it will automatically configure QoS settings if QoS service is enabled.

## Configuring QoS over ManualWDS Interface

There are two steps to run QoS service over one ManualWDS interface: creating one QoS class and attaching it to ManualWDS interface. First, user should configure one QoS class which specifies the maximal and minimal bandwidth of this ManualWDS interface. After creating one specific QoS class, user should attach this QoS class to ManualWDS interface.

### Configuring QoS Classes

The QoS class is targeted to let user specify acceptable bandwidth of one WDS link. For each QoS class, user must specify one maximal bandwidth value and one minimal bandwidth value. Use the following commands to configure QoS classes.

Table 35 Configuring QoS Classes

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **class <name>** | QOS | Create/configure one QoS class. The class name is unique identifier for all QoS classes. Meanwhile, user enters the CLASS configuration mode to configure the QoS class |
| **no class <name>** | QOS | Delete the QoS class with specific name |
| **maxbw <1-500>** | QOS CLASS | Specify the maximal bandwidth that this QoS class can obtain. (Unit: 100kbps) |
| **no maxbw** | | Set the maximal bandwidth to default value (30Mbps). |
| **minbw <1-200>** | QOS CLASS | Specify the minimal bandwidth guarantee to this class. (Unit: 100kbps) |
| **no minbw** | | Set the minimal bandwidth to default value (5Mbps) |

### Attaching QoS Class to ManualWDS Interface

After configuring one preferable QoS class, user should indicate which ManualWDS interface to use this specific QoS class. Use the following commands to attached one specific QoS class to one ManualWDS interface.

Table 36 Attaching QoS Class to ManualWDS

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **qos class <*classname*>** | INTERFACE DOT11RADIO WDS | Attach one specific QoS class with *classname* to this ManualWDS Interface. Correspondingly, start QoS service over this interface if QoS serive is enabled on router. |
| **no qos class** | INTERFACE DOT11RADIO WDS | Deattach QoS class from this ManualWDS interface. Furthermore, one default QoS class will take effect on this interface if enable QoS globally. |

Note that one QoS class can be attached to multiple different ManualWDS interfaces. It must ensure that user is in the WDS configuration mode for attaching one QoS classe to ManualWDS interface.

Additionally, one default QoS class will be automatically created once QoS service is enabled on router. For the ManualWDS interfaces to which a QoS class doesn't be attached, it will automatically apply the default QoS class to these ManualWDS interfaces. But, it needs to further note that all of the special ManualWDS interface share the maximal and minimal bandwidth indicated by the default QoS class. **Max** bandwidth of the default class is **30/(wdsnumber+1) Mbps** and and **Min** bandwidth is minimal value of **2M** and **30/(wdsnumber+1)*25%Mbp**s, where wdsnumber is the number of WDS interfaces on the radio over which .QoS service is started.

### Configuring QoS over Auto WDS Interface

By default, for all AutoWDS interfaces, QoS service will be automatically take effect on them once QoS service is enabled on router. The QoS class for auto WDS interfaces is created based on the following rules:

a. Each AutoWDS's max bandwidth is 30Mbps;
b. Each AutoWDS's min bandwidth is 30/(wdsnumber+1) Mbps;
c. If wds-unicast-rate of the radio to which this auto WDS interface is attached has been specified, the maximal bandwidth of one auto WDS interface will be set to wds-unicast-rate.value (under the condition that this value is smaller than 30Mbps).

### Showing QOS Information and Status

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **show qos configuration** | Privileged EXEC | Show configuration of QoS |
| **show qos dot11radio <*Radio*> class** | Privileged EXEC | Show class rules on specific radio |
| **show qos dot11radio <*Radio*> qdisc** | Privileged EXEC | Show queue discipline rules on specific radio |
| **show qos interface** | Privileged EXEC | Show class name applied on interfaces and running state |

### View QOS configuration

```
MSR2000# show running-config
!
node-id 54
router-id 192.168.15.54
!
……
interface dot11radio 0
 wireless-mode a 136 DK
 antenna 1
 mode backhaul
 max-auto-wds 5
 wds 0
  remote mac 00:17:7b:37:a0:00
  ip address 10.53.54.2/24
  qos class band1
  no shutdown
 wds 1
  remote mac 00:17:7b:37:a1:00
  ip address 10.52.54.2/24
  qos class band2
  no shutdown
```

```
!
……
!
qos
 enable
 class band1
  maxbw 200
  minbw 100
 class band2
  maxbw 150
  minbw 60
 class band3
  maxbw 100
  minbw 40
!
```

# Chapter 13 Configuring SNMP

This section describes commands used to configure the Simple Network Management Protocol (SNMP) Agent on the MSR2000 for the purposes of network monitoring and management.

## Configuring SNMP Community

To set the community string for controlling access to the Management Information Base (MIB) on the SNMP Agent, use the **snmp-server community** command. The **no** form of this command removes the specified community string.

**Table 37** Configuring snmp-server community

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **snmp-server community** *[community] [ro\|rw]* | CONFIGURATION | Add an SNMP community string that identifies an access control domain for the SNMP agent.<br>**ro:** Specifies read-only access. Authorized management stations are able to retrieve, but not modify, MIB objects.<br>**rw:** Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects. |
| **no snmp-server community** *[community]* | | Remove SNMP community string |
| **show snmp-server community** | Privileged EXEC | Display all configured community strings |

## Configuring SNMP Trap

To specify the recipient of a SNMP trap (a mechanism used to notify Network Management Servers of a change in the network device state), use the snmp-server host configuration command. To remove the specified host, use the no form of this command.

**Table 38** Configuring snmp-server host

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **snmp-server host** *[ip-address] [community] [udp-port]*<br>**no snmp-server host** *[ip-addres]* | CONFIGURATION | Configure IP address of SNMP host to receive traps using the specified community string and SNMP port. |
| **show snmp-server host** | Privileged EXEC | Display all SNMP trap hosts with associated community strings and ports |

## Configuring SNMPv3 users

MSR series also supports SNMPv3, which introduces the concept of users. The following commands controls the SNMPv3 user database on each MSR series router:

**Table 39** Configuring SNMPv3 users

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **snmp-server v3user** *<name> <ro\|rw> <MD5 pass> <DES pass> <user-type>* | CONFIGURATION | Configure a new or existing SNMPv3 user account. |
| **no snmp-server v3 user <name>** | | Remove an existing SNMPv3 user account<br>name: SNMPv3 user name<br>ro\|rw: whether the user is read-only or read-write<br>MD5 pass: Authentication password<br>DES pass: Encryption password<br>user-type:<br>auth auth, no priv<br>noauth no auth, no priv<br>priv auth, priv |
| **show snmp-server v3user** | Privileged EXEC | Display all configured SNMP V3 user accounts |

### Viewing the snmp-server information

```
MSR2000# show snmp-server community
community string                 access mode
public                           read-only
private                          read-write
!
MSR2000# show snmp-server host
host                             community string                 port
192.168.10.55                    public                           162
192.168.10.10                    trap                             162
192.168.10.64                    trap                             162
192.168.10.130                   trap                             162
192.168.10.44                    public                           162
MSR2000# show snmp-server v3user
user             access      usm-level  auth-pass        priv-pass
read             read-only   noauth     12345678         12345678
```

Figure 23 Output of snmp-server configuration

# Chapter 14 Other commands and utilities

This chapter contains other commands and troubleshooting utilities on the MSR series, it has the following sections:

- Save & Reboot
- Ping & Traceroute
- Telnet Client & Server
- Auto Recovery

## Save & Reboot

### Save

Azalea recommends that you save your configuration often.

To save a configuration file, use either of the following commands in the Privileged EXEC mode:

**Table 40** Save the running configuration to startup configuration

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **copy running-config startup-config** | Privileged EXEC | Save the current running configuration to the startup-config file. |
| **write memory** | Privileged EXEC | Save the current running configuration to the startup-config file. (old way to save configuration) |

### Reboot

Azalea provides command **reboot** to hot restart MSR series.  After upgraded, user can use command **reboot** to restart MSR series, then the new image takes effects.

**Table 41** Reboot configuration

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **reboot** | Privileged EXEC | Restart MSR series without turning off power. |

## Ping & Traceroute

Commands **ping** and **traceroute** are very helpful utilities to troubleshoot network access problems.

### Ping

Command **ping** a very common method for troubleshooting the accessibility of devices. It uses a series of Internet Control Message Protocol (ICMP) Echo messages to determine:

- Whether a remote host is active or inactive.
- The round-trip delay in communicating with the host.
- Packet loss.

Command **ping** first sends an echo request packet to an address, then waits for a reply, the reply will be recorded with latency. The default **ping** packet is 6, **Ctrl+c** can terminate **ping**.

### Traceroute

Command **traceroute** is used to discover the routes that packets actually take when traveling to their destination. The network device sends out a sequence of User Datagram Protocol (UDP) datagrams to an invalid port address at the remote host.

Three datagrams are sent, each with a Time-To-Live (TTL) field value set to one. The TTL value of 1 causes the datagram to "timeout" as soon as it hits the first router in the path; this router then responds with an ICMP Time Exceeded Message (TEM) indicating that the datagram has expired.

Another three UDP messages are now sent, each with the TTL value set to 2, which causes the second router to return ICMP TEMs. This process continues until the packets actually reach the other destination. Since these datagrams are trying to access an invalid port at the destination host, ICMP Port Unreachable Messages are returned, indicating an unreachable port; this event signals the Traceroute program that it is finished.

The purpose behind this is to record the source of each ICMP Time Exceeded Message to provide a trace of the path the packet took to reach the destination.

**Table 42** ping & traceroute configuration

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **ping { *<A.B.C.D>* \| *<hostname>* }** | Privileged EXEC | Detect remote device accessibility or not. |
| **traceroute { *<A.B.C.D>* \| *<hostname>* }** | Privileged EXEC | Trace the path of the packet to destination. |

```
MSR2000# ping 192.168.15.126
PING 192.168.15.126 (192.168.15.126): 56 data bytes
84 bytes from 192.168.15.126: icmp_seq=0 ttl=64 time=8.7 ms
84 bytes from 192.168.15.126: icmp_seq=1 ttl=64 time=0.8 ms
84 bytes from 192.168.15.126: icmp_seq=2 ttl=64 time=1.0 ms
84 bytes from 192.168.15.126: icmp_seq=3 ttl=64 time=0.9 ms
84 bytes from 192.168.15.126: icmp_seq=4 ttl=64 time=1.0 ms
84 bytes from 192.168.15.126: icmp_seq=5 ttl=64 time=0.9 ms

--- 192.168.15.126 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.8/2.2/8.7 ms

MSR2000# ping 192.168.15.11
```

```
PING 192.168.15.11 (192.168.15.11): 56 data bytes

--- 192.168.15.11 ping statistics ---
6 packets transmitted, 0 packets received, 100% packet loss


MSR2000# traceroute 192.168.15.126
traceroute to 192.168.15.126 (192.168.15.126), 30 hops max, 40 byte packets
 1  192.168.15.126 (192.168.15.126)  7.134 ms  1.323 ms  0.821 ms
MSR2000#
```

**Figure 24** Output of ping & traceroute information

## Telnet Client & Server

MSR series can play role as Telnet Client and Telnet Server.

### Telnet Client

When MSR series acts as Telnet client, you can use command **telnet** to access other device.

### Telnet Server

When MSR series acts as Telnet server, you should use command **ip telnet server** to enable the service. Telnet Server disable by default.

**Table 43** Telnet Client & Server configuration

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **telnet { *<A.B.C.D>* \| *<hostname>* } [port]** | Privileged EXEC | Access remote device through Telnet. |
| **ip telnet server**<br>**no ip telnet server** | Configuration | Enable telnet server.<br>Disable telnet server |

### Viewing Telnet Server configuration

```
!
ip telnet server
!
```

## Auto Recovery

Auto Recovery is an advanced feature provided by MSR series, When enabled, Auto Recovery will automatically detect and recover from system fault. When configured with a portal IP, auto recovery would also monitor its connectivity with the portal node. If the connectivity is lost and auto recovery believes it is due to a local problem, it will automatically reboot the router as an attempt to restore its normal working state.

**Table 44** Auto Recovery configuration

| Command Syntax | Command Mode | Purpose |
|---|---|---|
| **service recovery** | CONFIGURATION | Enter Auto Recovery configuration mode |
| **enable** | SERVICE RECOVERY | Administratively activate Auto Recovery |
| **disable** | SERVICE RECOVERY | Administratively disable Auto Recovery |
| **portal ip <*A.B.C.D*>**<br>**no portal ip <*A.B.C.D*>** | SERVICE RECOVERY | Set an IP address for the device to check the state of connection wire network<br>Delete portal IP address |

## Viewing Auto Recovery configuration

```
!
service recovery
 enable
!
```

# Chapter 15 MIBs and RFCs

## Supported MIBs

The following is a list of Management Information Bases (MIBs) supported by MSR series.

- RFC 1213 Network Management of TCP/IP-based internet: MIB-II
- RFC 1157 Simple Network Management Protocol
- RFC 1573 Interfaces Group MIB
- RFC 2012 SNMPv2 Management Information Base for the TCP
- RFC 2013 SNMPv2 Management Information Base for the User Datagram Protocol
- RFC 2271 An Architecture for Describing SNMP Management Frameworks
- RFC 1901 Introduction to Community-based SNMPv2
- RFC 1902 Structure of Management Information for Version 2 of the SNMPv2
- RFC 1903 Textual Conventions for SNMPv2
- RFC 1904 Conformance Statements for SNMPv2
- RFC 1905 Protocol Operations for SNMPv2
- RFC 1906 Transport Mappings for SNMPv2
- RFC 1907 Management Information Base for SNMPv2
- RFC 2571 Architecture for SNMP Frameworks
- RFC 2572 Message Processing and Dispatching
- RFC 2573 SNMP Applications
- RFC 2574 User-based Security Model (USM) for SNMPv3
- RFC 2575 View-based Access Control Model (VACM) for SNMP
- RFC 2578 Structure of Management Information Version 2 (SMIv2).
- RFC 2579 Textual Conventions for SMIv2
- RFC 2580 Conformance Statements for SMIv2
- MIB II
- IF-MIB
- IP-MIB,TCP-MIB,UDP-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-TARGET-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-USM-MIB
- SNMP-VACM-MIB
- AZALEA-REF-MIB
- AZALEA-DOT11-IF-MIB
- AZALEA-ROUTER-MIB

# Chapter 16 List of Commands

```
     <cr>
A    aaa
     Accept-point bssid HH:HH:HH:HH:HH:HH
     access-point bssid-filter acceptable-prefix HH:HH:HH:HH:HH:HH HH:HH:HH:HH:HH:HH
     access-point ssid WORD
     antenna {0|1|2}
     authentication-algorithm {open|shared-key}
     authentication open [{wep WEP-LIST-NAME default-key <1-4> | key-management {wpa|wpa2} PROFILE-NAME}]
B    bss WORD
C    class NAME
     clear counters interface dot11radio INDEX
     clear counters interface dot11radio INDEX (wdsauto|wdsmanu) <0-5>
     clear counters interface fast-ethernet  INDEX
     clear log {awr|cli|hostapd|rf-management|motrix}
     clear log {awr|cli|hostapd|rf-management|motrix|station}
     client-authentication (open|shared) wep PROFILE-NAME default-key  <1-4>
     client-authentication open client-8021x PROFILE-NAME
     client-authentication open key-management (wpa|wpa2) client-8021x PROFILE-NAME
     client-authentication open key-management wpa-psk (hex|ascii) WORD
     configure terminal
     copy running-config startup-config
     cts-protection {0|1|2|3}
D    debug {hap|cli) {dump|error|frame|info|none|state}
     debug rf-management ping
     debug dot11radio <0-N> distance [{default<a|b|g> |timout VALUE}]
     debug dot11radio <0-N> scan [{bssid HH:HH:HH:HH:HH:HH|channel N}]
     debug phm (error|info|dump)
     default-lease-time <0-31536000>
     dhcp relay
     dhcp server {<POOL-NAME> | automatic}
     dhcp-servers SERVER-list
     disable
     dns DNS-list
     domain-name NAME
E    eap-method (peap|ttls) phase2 (md5|mschapv2|tls)
     eap-method tls
     eap-reauth-period <0-65535>
     enable
```

```
       encryption-mode-cipher {tkip|ccmp}
       encryption-mode-cipher tkip ccmp
       end
       exit
G      gateway A.B.C.D
H      help
       hostname WORD
       host HH:HH:HH:HH:HH A.B.C.D
I      ignore-broadcast-ssid
       interface dot11radio <0-N>
       interface fast-ethernet <0-1>
       install certificate ca URL
       install certificate client URL
       install client-key URL
       install client-key URL password PRIVATE-KEY-PASSWORD
       ip address  A.B.C.D/M
       ip address dhcp
       ip address STANAME A.B.C.D A.B.C.D
       ip dhcp {relay|server}
       ip nat
       ip route A.B.C.D/M A.B.C.D [<1-255>]
       ip route A.B.C.D/M station <name> <0-N>
       ip telnet server
L      List
M      mac-addr HH:HH:HH:HH:HH:HH
       mac-address {deny|accept} MAC-LIST-NAME
       mac-address accept-all
       mac-list WORD
       max-auto-wds <1-6>
       max-lease-time <0-31536000>
       max-rate RATE
       max-station-allowed <0-240>
       mode {access|backhaul|client}
       Mode backhaul WORD
       mode {access|gateway A.B.C.D/M|none}
       mtu <256-1500>
       mtu <256-2274>
N      network {A.B.C.D|A.B.C.D/M}
       no access-point bssid
       no access-point bssid-filter acceptable-prefix
              no    access-point    bssid-filter    acceptable-prefix
     HH:HH:HH:HH:HH:HH HH:HH:HH:HH:HH:HH
       no access-point ssid
       no antenna
       no authentication
       no authentication-algorithm
       no bss WORD
       no class NAME
```

```
  no client-authentication
  no cts-protection
  no default-lease-time
  no dhcp
  no dhcp-servers
  no dns
  no domain-name
  no eap-method
  no eap-reauth-period
  no encryption-mode-cipher
  no gateway A.B.C.D
  no hostname [HOSTNAME]
  no host HH:HH:HH:HH:HH:HH
  no ignore-broadcast-ssid
  no ip address
  no ip dhcp {relay|server}
  no ip nat
  no ip route A.B.C.D/M {A.B.C.D|station WORD <0-N>}
  no ip telnet server
  no mac-address
  No mac-addr HH:HH:HH:HH:HH:HH
  no mac-list WORD
  no mac-ip-list
  no mac-ip-list HH:HH:HH:HH:HH:HH
  no max-lease-time
  no max-rate
  no max-station-allowed
  no mode
  no mtu
  no out-interface dot11radio  INDEX station WORD
  no out-interface fast-ethernet <0-1>
  no pool [NAME]
  no password
  no profile mesh <WORD>
  no qos class
  no radius-server A.B.C.D (auth_acct)
  no range A.B.C.D A.B.C.D
  no retry
  no role
  no router awr
   no  scanning  {channel-list|  hardware-modes|  mininum-interval|
threshold rssi}
  no security-profile {8021x|client-8021x|wep|wepa|wpa2} WORD
  no service roaming-motrix
  no server A.B.C.D
  no shutdown
  no snmp-server community COMMUNITY
  no snmp-server host A.B.C.D
```

```
      no snmp-server v3user USERNAME
      no ssid
      no station WORD
      no station-inactivity-limit
      no station-inactivity-policy
      no station-isolation
      no station-list
      no station-list HH:HH:HH:HH:HH:HH
      no tx-power-reduction
      no unicast-rate
      no user-name
      no wds {<0-5>|auto}
      no wds-unicast-rate
      no wep-key <1-4>
      no wireless-mode
      no wpa-type {8021x|psk}
      no wpa2-type {8021x|psk}
      node-id <1-255>
O     out-interface dot11radio  INDEX station WORD
      out-interface fast-ethernet <0-1>
P     password PASSWORD-STRING
      ping WORD
      pool [NAME]
      profile mesh <WORD>
Q     qos
      qos class NAME
      quit
        radius-server  A.B.C.D  {auth-port  {<1-65535>|default}|acct-
R    port{<1-65535>|default} key <string>
      range A.B.C.D A.B.C.D
      reboot
      remote-mac HH:HH:HH:HH:HH:HH
       release-dhcp {dot11radio <0-N> station WORD |fast-ethernet<0-
     1>}
      remote node <1-255>  INDEX
      renew-dhcp {dot11radio <0-N> station WORD |fast-ethernet<0-1>}
       restart-dhcp {dot11radio <0-N> station WORD| fast-ethernet<0-
     1>}
      retry <1-32> <1-32>
      role (ap|station|auto)
      router awr
      router-id A.B.C.D
      router-password
S     scanning automatic
      scanning hardware-modes WORD
      scanning mininum-interval <1-300>
      scanning threshold rssi <0-100>
      security-profile {8021x|client-8021x|wep|wpa|wpa2}
```

```
  server-group
  server A.B.C.D
  service recovery
  service rf-management
  service roaming-motrix
  setup ap {US|CN|JP} <1-255> A.B.C.D A.B.C.D/M  WORD WORD
  setup factory
  setup point (US|CN|JP} <1-255> A.B.C.D A.B.C.D/M
   setup portal (US|CN|JP} <1-255> A.B.C.D A.B.C.D/M SSID DNS-
SERVER-LIST
   setup portal (US|CN|JP) <1-255> A.B.C.D A.B.C.D/M SSID DNS-
SERVER-LIST nat-off
   setup portal (US|CN|JP) <1-255> A.B.C.D dhcp SSID DNS-SERVER-
LIST
   setup portal (US|CN|JP) <1-255> A.B.C.D dhcp SSID DNS-SERVER-
LIST nat-off
  show aaa
   show arp [<A.B.C.D>|interface {dot11radio <0-N>| dot11wds <0-
31>| fast-ethernet <0-1>}]
   show arp count [interface {dot11radio <0-N>| dot11wds <0-31>|
fast-ethernet <0-1>}]
  show certificate (ca|client)
  show clock
  show cpu
  show dhcp relay dhcp-servers
  show dhcp server  {all| default-lease-time|dns|lease|max-lease-
time|pool|pool POOL-NAME}
  show dot11radio <0-N> stations
  show hardware
  show hostname
  show interface brief
  show interface dot11radio <0-N> [{stations|states|txpower|node-
database}]
   show interface dot11radio <0-N>  [<ssid> {accept-macs| deny-
macs| stations| wep-keys}]
  show interface dot11radio <0-N> {wds|wdsauto} <0-5>
  show interface fast-ethernet <0-1>
  show ip awr {configuration|database|neighbor}
  show ip forwarding
  show ip mobility motrix {mac-ip-list|stations}
    show ip route [{awr|connected|static| A.B.C.D| A.B.C.D/M|
A.B.C.D/M longer-prefixes|fib|summary}]
  show log {awr|cli|hostapd|rf-management|motrix|station|phm}
  Show mac-list
  show nat {out-interface|configuration|table}
  show node-id
  show process
  Show profile mesh
  show qos dot11radio <0-N> {class|qdisc}
  show qos {configuration|interface}
  show recovery configuration
```

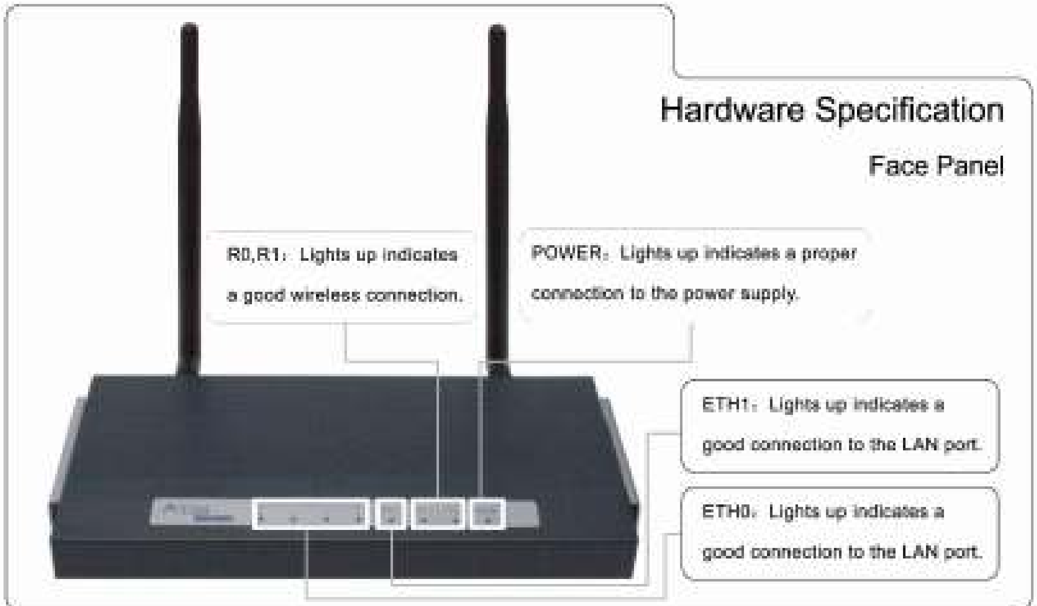
```
      show rf-management {active-neighbors|interface|configuration}
      show router id
      show running-config
      show security-profile (wep|wpa|wpa2|8021x|client-8021x)
      show snmp-server {community|host|v3user}
      show startup-config
      show version
      ssh HOST {USER|USER PORT}
      Shutdown
      snmp-server community COMMUNITY {rw|ro}
      snmp-server host A.B.C.D COMMUNITY <1-65535>
      snmp-server v3user USERNAME {ro|rw} MD5PWD DESPWD {noauth|auth|
    priv}
      ssh HOST {USER|USER PORT}
      ssid <WORD>
      station <WORD>
      station-inactivity-limit <1-65535>
      station-inactivity-policy {0|1}
      station-isolation
      switch image
T     telnet WORD [PORT]
      time <2005-2008> <1-12> <1-31> <0-23> <0-59> <0-59>
      traceroute WORD
      tx-power-reduction <0-65535>
U     unicast-rate RATE
      upgrade ftp A.B.C.D FILENAME USERNAME PASSWORD [reboot]
      upgrade url URL [reboot]
      user-name NAME-STRING
W     wds-unicast-rate RATE
      wep-key <1-4> (ascii|hex) WORD
      wds <0-5>
      wds auto
      wireless-mode (a|g|b) CHANNEL [country-name] <0|1|2>
      wireless-mode {a|g|b} <channel> [country-name]
      write {file|memory|terminal}
      wpa-type 8021x NAME
      wpa-type psk (hex|ascii) WORD
      wpa2-type 8021x NAME
      wpa2-type psk (hex|ascii) WORD
```

# MSR1000 Wireless Mesh Router

## —— Hardware Installation Flyer

### Hardware Specification

#### Face Panel



R0,R1：Lights up indicates a good wireless connection.

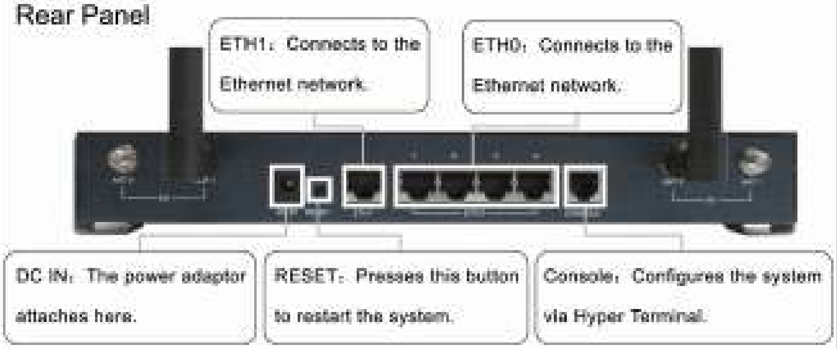
POWER：Lights up indicates a proper connection to the power supply.

ETH1：Lights up indicates a good connection to the LAN port.

ETH0：Lights up indicates a good connection to the LAN port.

www.azaleanet.com

#### Rear Panel



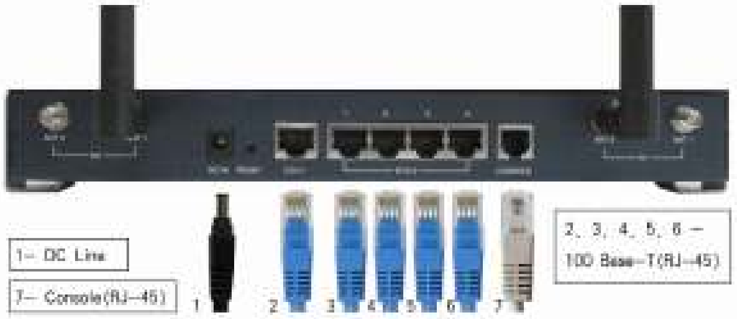
ETH1：Connects to the Ethernet network.

ETH0：Connects to the Ethernet network.

DC IN：The power adaptor attaches here.

RESET：Presses this button to restart the system.

Console：Configures the system via Hyper Terminal.



1– DC Line

7– Console(RJ–45)

2、3、4、5、6 — 100 Base–T(RJ–45)

1. Connect the DC power adapter to the power connector socket on the rear panel. The Power LED should be on to indicate a proper connection.
2. Connect an Ethernet cable to the ETH1 port on the rear panel. Connect the other end of the Ethernet cable to a switch/hub. The LED of this WAN port should be on to indicate a proper connection.
3. Connect an Ethernet cable to one of ETH0 ports on the rear panel. Connect the other end of the Ethernet cable to a switch/hub, pc or AP. The LED of ETH0 should be on to indicate a proper connection.

www.azaleanet.com

## FCC Statement:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the
following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

## FCC Caution:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

## IMPORTANT NOTICE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.