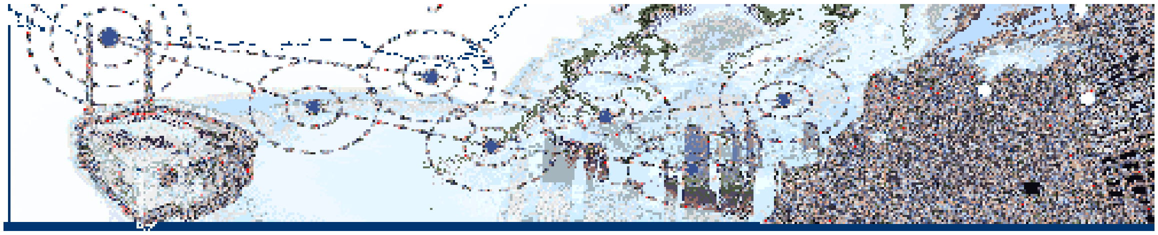
MSR 2000 Wireless Mesh Router CLI Configuration Guide

Version AOS-1.3.0   November 3, 2006



Copyright 2006 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.

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 the MSR2000 outdoor wireless mesh router. It contains information on current features and protocols supported by MSR2000.

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 provides CLI mode to configure MSR2000, not including HTTP GUI based configuration, see related documents.

Audience

This document is intended for system/IT or network administrator who is responsible for configuring or maintaining MSR2000, this guide is also assumed the user is knowledgeable in wireless/wire Layer2 and Layer 3 networking technologies.

Related Documents

For more information about MSR2000, please refer to the following documents:

- MSR2000 Quick Start Guide
- MSR2000 Web-based Configuration Guide
- Release Notes for MSR2000 hardware and software

Chapter 2 Configuration Fundamentals

This section covers the following main topics:

- Azalea CLI Modes
- Basic Configuration Information
- Software Image Upgrade

Azalea CLI Modes

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

CLI Modes

Azalea 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 Azalea CLI.

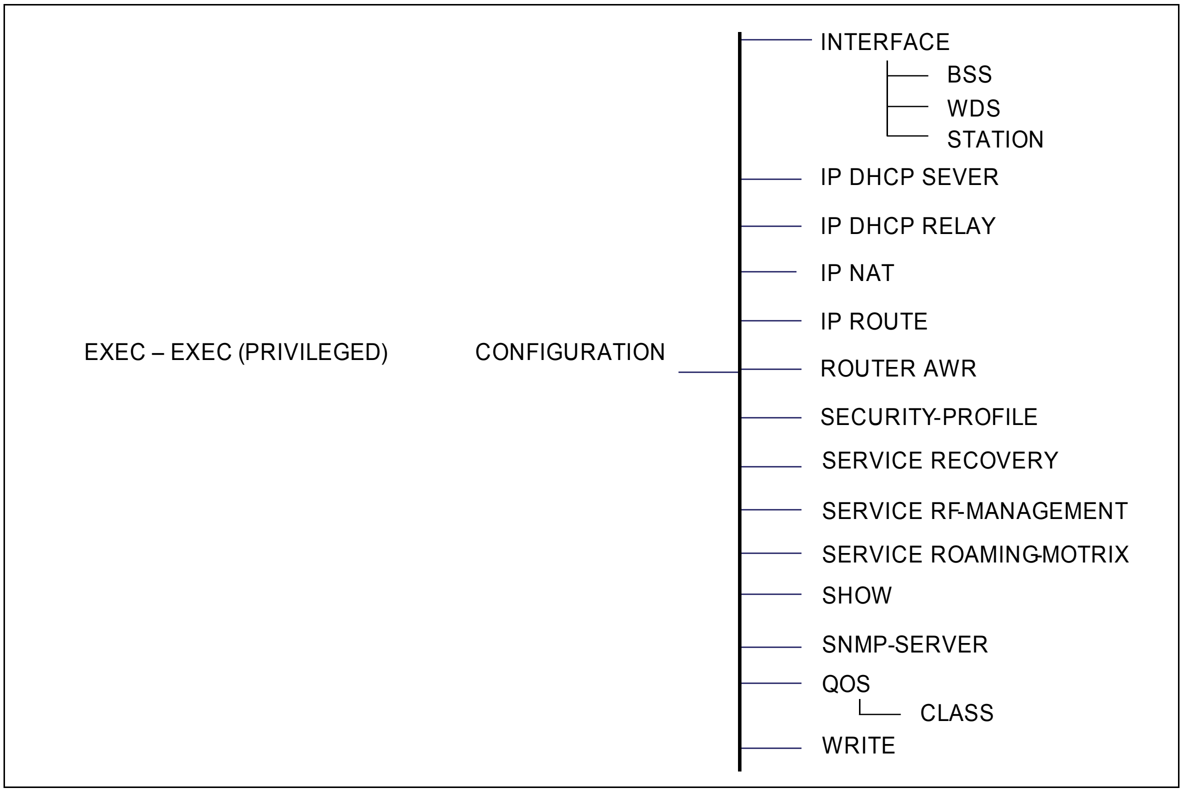


Figure 1 CLI Modes in Azalea Image

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 Azalea MSR2000, 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.

INTERFACE mode enables you to configure layer 2 and layer 2 protocols and IP services specific to that interface only.

IP DHCP RELAY mode enables you to configure DHCP RELAY globally for the Azalea MSR2000. You may configure multiple DHCP Servers by IP addresses.

IP DHCP SERVER mode enables you to configure DHCP SERVER globally for Azalea MSR2000. You may configure the DNS, Domain name, lease time.

IP NAT mode enables you to configure NAT globally for Azalea MSR2000. You may configure NAT the out interface associated with the physical interface.

ROUTER AWR mode enables you to configure the Adaptive Wireless Routing (AWR) protocol. You may enable or disable the protocol.

SECURITY PROFILE mode enables you to configure the SECURITY profile globally for Azalea MSR2000. You may configure 802.1X, WEP, WPA, WPA2 profile.

SERVICE RECOVERY mode enables RECOVRY globally for Azalea MSR2000. You may configure portal IP address.

SERVICE ROAMING-MOTRIX mode enables you to configure MOTRIX globally for Azalea MSR2000. You may configure MAC, IP, and IAPP settings.

SERVICE RF-MANAGEMENT mode enables you to configure RFM globally for Azalea MSR2000. You may configure debug level.

QOS mode enables you to configure QOS globally for Azalea MSR2000. You may configure multiple classes and define maximum and minimum bandwidth for each class.

*** PASSWORD FUNCTION IS RESERVED FOR NEXT RELEASE**

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
  end
  exit
  help
  interface fast-ethernet <0-1>
  ip address A.B.C.D/M
  ip address dhcp
  list
  mode access
  mode gateway
  mode gateway A.B.C.D
  mtu <256-1500>
  no ip address
  no mode access
  no mode gateway
  no mtu
  no shutdown
  quit
  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	**Pro**		
Mode	**mpt**	**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. 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**	Use the either the **exit** or **end** command.

commands.
From every other modes except the EXEC and Privileged EXEC modes, use the **exit** command.

Table 1 CLI Mode Information (continued)

CLI Command Mode	Prompt	To Enter Mode	To Exit Mode
INTERFACE	MSR20 00(config-if-ethernet)#	From the CONFIGURATION mode, use the **interface** command.	Use the **exit** commands to return to **CONFIGURATION** mode, except of **bss, wds, station** and **class** Use the **end** to return to Privileged EXEC mode.
BSS	MSR2000(config-if-dot11radio-bss)#	From the INTERFACE mode, use the **bss** command.	
WDS	MSR2000(config-if-dot11radio-wds)# MSR2000(config-if-dot11radio-wds-auto)#	From the INTERFACE mode, use the **wds or wds auto** command.	
STATION	MSR2000(config-if-dot11radio-sta)#	From the INTERFACE mode, use the **station** command.	
IP NAT	MSR2000(config-nat)#	From the CONFIGURATION mode, use the **ip nat** 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.	
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-MOTRIX	MSR2000(config-roaming)#	From the CONFIGURATION mode, use the **service roaming-motrix** command.	
QOS	MSR2000(config-qos)#	From the CONFIGURATION mode, use the **qos** command.	
CLASS	MSR2000(config-qos-class)#	From the CONFIGURATION mode, use the **class <name>** command.	

Deleting Command Lines in the Configuration File

Each command enters a command line in the Azalea MSR2000 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 Azalea 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
Azalea VTY provides advanced help feature. 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)# ?
  end                 End current mode and change to enable 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 mtu of interface
  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
MSR2000(config-if-ethernet)#
```

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
  service                     immediately by a ?. All keywords that begin with
  show                        "s" in the CONFIGURATION mode are listed.
  snmp-server
MSR2000(config)#
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 in Azalea Image.

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 MSR2000, the system configuration program is not implemented automatically, user has to configure MSR2000 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 MSR2000. Enter a new host name in the form of an alphanumeric string.
Router-password	Default password is **public**, it can be change by using this CLI command
Management port IP address	By default, IP address 192.168.0.1/24 is configured on FastEthernet 0, user can change it if need.
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 MSR2000 mesh network.

Host Name Configuration

The host name appears in the prompt. The default host name is MSR2000. 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 MSR2000. Enter a new host name in the form of an alphanumeric string.
no hostname		Remove the hostname, it goes back to default. Default hostname = MSR2000

Password Configuration

MSR2000 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

Azalea Networks recommends 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
show startup-config	CONFIGURATION	Display the configuration information stored in the internal memory
node-id	CONFIGURATION	Set node ID, should be value between 1 and 255.
router-id	CONFIGURATION	Set router ID 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 MSR2000. 1.) dot11radio 2.) fast-ethernet
show running-config	CONFIGURATION	Display current configuration information on the system.

Software Image Upgrade

MSR2000 is shipped with an Azalea firmware; however, you may upgrade the firmware or load a different version of Azalea firmware.

Table 10 Upgrade firmware

Command Syntax	Command Mode	Purpose
upgrade [FTP | URL]	Privileged EXEC mode	Upgrade operation has two methods to upgrade image to MSR2000

For best result, use **upgrade** command to transfer the system firmware to MSR2000

```
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 MSR2000, it has the following sections:

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

Interface Modes

The MSR2000 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

MSR2000 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
mode access	INTERFACE FAST-ETHERNET	Set this fast-ethernet interface as a LAN interface, for connecting with client

[1] On some MSR2000 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.

		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 ***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
release-dhcp fast-ethernet <0-1>	Privileged EXEC	Release the fast-ethernet interface's IP address acquired from DHCP Server
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

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
  mode: gateway   gateway ip: 192.168.1.1
  admin status: up  physical status: up
```

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

```
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 clients 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 act as an 802.11 client itself to connect to any BSS 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 *<0-1>*	CONFIGURATION	Configure one of the dot11radio interfaces.
mode access	INTERFACE DOT11RADIO	Configure radio interface for client access, allowing BSS association Radio 0 is configured as mode access by default
mode backhaul		Configure radio interface for backhaul operation, allowing connection with other MSR2000 routers
mode client		Configure radio interface to work as a 802.11 client, allowing connection with a generic 802.11 Access Point including other MSR2000 routers' interfaces working in Access Mode. A router may

		only have one radio in client mode.

Common settings

Radio Interface supports two type of hard-ware mode: 802.11a and 802.11g (backward-compatible with 802.11b) and 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. mode: a or g a: Use 802.11a g: Use 802.11b/g channel: Mode and country-specific channel number Mode g and US: 1-11 Mode g and JP: 1-14; Mode g and CN: 1-13; Mode a and US: 149, 153, 157, 161, 165; Mode a and JP: 36, 40, 44, 48 Mode a and CN: 149, 153, 157, 161, 165 country-code: US, CN, or JP US: United States CN: P.R. China 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 **no antenna**		Automatically choose the best antenna (default)
antenna 1		Always use antenna 1
antenna 2		Always use antenna 2

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 **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] ***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 ***Setting of radio MTU is not recommended and should be done 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.

Operation-mode specific settings

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

Command Syntax	Command Mode	Purpose
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];
no wds *<0-5>*		Remove an existing manual WDS

[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

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

interface from this radio

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]
no wds auto		Disable auto WDS on this radio interface.
wds-unicast-rate [*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. The rate is specified in units of 100kbps; the available rates are: 10, 20, 55, 110, 60, 90, 120, 180, 240, 360, 480, 540 **(Example: if choose 20, then RATE=20*100kbps=2Mbps)**
no wds-unicast-rate [rate]		Disables unicast rate setting; WDS links will automatically select the transmission rate and may dynamically vary depending on link quality (default setting)

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]
no bss <*SSID*>		Remove an existing BSS from this radio interface SSID: The 802.11 Service Set ID (SSID) that identifies a BSS on this radio interface

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 Note: currently only one station is allowed on each router

[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.

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

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 48 US
 mode backhaul
 max-auto-wds 5
 wds-unicast-rate 60
!
...
MSR2000# show interface dot11radio 1
Interface Dot11Radio0
  operation_mode:backhaul, country code:US, channel policy:0, antenna:0,
  cts protection:0,  max auto wds:5,
  admin status: up  physical status: up
  index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWmode: a, channel: 48, Fragment thr: 2346, RTS thr: 2347
  HWaddr: 00:0b:6b:35:e8:5d
    input packets 2683950, bytes 175569398, dropped 0, multicast packets 0
    input errors 34844, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 115532, bytes 11644226, dropped 0
    output errors 2, 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 MSR2000 routers to communicate each other 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 through 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 when the radio interface is in backhaul mode.

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.
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]
ip address *[ip address/mask]*	INTERFACE DOT11RADIO WDS	Configure IP address of WDS interface.
no ip address		Remove IP address from WDS interface

[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.

mtu *<256-2274>*	INTERFACE DOT11RADIO WDS	Configure MTU size of WDS interface
no mtu		Restore default MTU size (1500) ***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> <0-1>*		Specify the node ID and the index of the radio on the remote router that this WDS interface will establish a link with 1-255: The node ID of the other router 0-1: A radio on the other router, Dot11Radio0 or Dot11Radio1
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.

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
```

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

```
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.

Viewing WDS Interface information.

```
MSR2000# show run
...
interface dot11radio 0
...
 wds 0
  remote mac 00:0b:6b: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
  admin status: up  physical status: up  neighbor ip: 10.1.6.1/28
  rssi: 79, snr: 79, link quality: 91%, datarate: 60
  remote mac address:00:0b:6b:35:36:bc, physical interface:0,
  index 20 metric 1 mtu 2100 <UP,BROADCAST,RUNNING,MULTICAST>
  HWmode: a, channel: 48, Fragment thr: 2346, RTS thr: 2347
  HWaddr: 00:0b:6b:35:e8:5d
  inet 10.1.6.2/28 broadcast 10.1.6.15
    input packets 6077, bytes 1429442, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 6082, bytes 1602424, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

Figure 10 Output of dot11wds interface

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

Chapter 5 Access and BSS Configuration

When a Dot11Radio interface is put into Access mode, BSSs configured for that interface becomes virtual APs that client devices may associate with. Each BSS is bound to a physical dot11radio interface; therefore, BSSs are configured within the 'interface dot11radio' mode. The MSR2000 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 SSID: The 802.11 Service Set ID (SSID) that identifies a BSS on this radio interface
authentication open **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

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

	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)

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 MSR2000 allows each BSS to use a different 802.11 security profile. For more information regarding 802.11 security, please refer to Chapter 11.

Viewing BSS of dot11radio interface information.

```
MSR2000# show run
...
!
interface dot11radio 0
...
 bss azalea_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 azalea_demo
BSS:azalea_demo

  ignore broadcast ssid:0, 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 MSR2000s or an AP from other vendors. On each MSR2000 router, only one radio interface can operate in client mode and have station configured.

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
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.
authentication-algorithm open	INTERFACE DOT11RADIO STATION	Configure authentication algorithm as open (default)
authentication-algorithm shared-key		Configure authentication algorithm as shared key
wep-key <1 | 2 | 3 | 4> <key-string>	INTERFACE DOT11RADIO STATION	Add a WEP key to the client station
no wep-key <1 | 2 | 3 | 4 >		Remove a WEP key from the client station
wep-default-key <1 | 2 | 3 | 4>		Specify the key index for default WEP key to use at transmission (default is WEP key 1)
no wep-default-key		Remove default WEP key configuration

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. 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. This configuration is only needed when automatic scanning (see later part of this section) is not enabled. And if automatic scanning is enabled, this configuration will be ignored. 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 only consider Azalea's MSR2000s to connect, you can specify a prefix of 00:17:7b:00:00:00 with mask of ff:ff:ff:00:00:00 Multiple filters can be configured if you want to allow multiple BSSID prefix choices. Default allows all BSSIDs.
no access-point bssid-filter acceptable prefix <*HH:HH:HH:HH:HH:HH*> *<HH:HH:HH:HH:HH:HH>*		Remove a certain BSSID filter
scanning automatic	INTERFACE DOT11RADIO STATION	Configure the station to do automatic scanning for access point. Without this configuration, you need to specify an Access Point's BSSID (using the "access-point bssid" command) to instruct it to associate to it.

		With automatic scanning configured, the client will automatically search for an AP with matching criteria. The search criteria include SSID, BSSID prefix. And the search will start after it is first started or after an existing connection is discontinued. Default is no scanning.
no scanning automatic		Disable automatic scanning
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. Default has no channel list and it scans in all legal channels of the configured hardware modes. (See “scanning hardware-mdoes” command). <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 <mode string>: a, g, ag 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. <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. <rssi value>: a number between 0 and 100. 0 means no such trigger. Default value is 15. RSSI stands for Received Signal Strength Index
no scanning threshold rssi		Restore the default RSSI threshold value.
release-dhcp dot11radio <0-1> station <station name>	Privileged EXEC	**Release the station's IP address acquired from DHCP server**
renew-dhcp dot11radio <0-1> station <station name>		**Renew the station's IP address via DHCP server**
restart-dhcp dot11radio <0-1> station <station name>		**Restart DHCP client for the station**

.

Viewing information of a station in a dot11radio interface.

```
MSR2000# show run
...
!
interface dot11radio 0
...
 station demo
  ip address dhcp
  access-point ssid demo
  scanning automatic
...
MSR2000# sh interface dot11radio 1 stations
Station test
 State: Associated
 Access Point SSID: AzaleaTest1
 Access Point BSSID: 00:17:7b:18:18:40
 Previous Access Point BSSID: NA
 IP Address: 172.16.44.200(DHCP acquired)
 WEP disabled
 Automatic scanning: enabled
  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 MSR2000 that allows automatic discovery and quality monitoring of wireless mesh links. RFM automatically scans for neighboring MSR2000 routers and create automatic WDS interfaces. With RFM, multiple MSR2000 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 MSR2000 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 MSR2000 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.

WDS link quality monitoring

RFM could monitor the link quality for all WDS links present on an MSR2000 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
  admin status: up  physical status: up  neighbor ip: 10.1.6.1/28
  rssi: 79, snr: 79, link quality: 91%, datarate: 60
  remote mac address:00:0b:6b:35:36:bc, physical interface:0,
  index 20 metric 1 mtu 2100 <UP,BROADCAST,RUNNING,MULTICAST>
  HWmode: a, channel: 48, Fragment thr: 2346, RTS thr: 2347
  HWaddr: 00:0b:6b:35:e8:5d
  inet 10.1.6.2/28 broadcast 10.1.6.15
    input packets 6077, bytes 1429442, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 6082, bytes 1602424, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

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

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 **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. 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 **debug none** **debug error** **debug state** **debug information** **debug frame** **debug dump**	SERVICE RF-MANAGEMENT	Set the RFM debug log level Disable RFM debug log Set RFM debug log to record errors Set RFM debug log to record errors & state changes Log error, state, and other detailed information Log error, state, information, and RFM control packet frames Log all RFM debug information

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

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

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 MSR2000 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: Up, physical: Down, state: Initial, flag: 0x13
        phytype: IEEE 802.11a, ch: 161, mode: WDS
        link quality: 0%, rssi: 0, snr: 0
Dot11Radio1 has 1 active neighbors:
Ngh  1: Mac: 00:0b:6b: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: Up, physical: 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:
Radio0MWds0:    Radio: Dot11Radio0, NID: 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 NID: 0, Ngh Radio_idx: 0
                Ngh IP: 10.140.141.1, Netmask: 255.255.255.0, Bcast: 10.140.141.255
                Link State: Initial, Linke quality: 93%
                RSSI: 0, SNR: 0
Radio1MWds0:    Radio: Dot11Radio1, NID: 141
                Admin status: Up, Physical status: Up
                IP: 10.141.143.1, Netmask: 255.255.255.0, Bcast: 10.141.143.255
                Ngh MAC: 00:0b:6b:36:a3:5b, Ngh NID: 143, Ngh Radio_idx: 0
                Ngh IP: 10.141.143.2, Netmask: 255.255.255.0, Bcast: 10.141.143.255
                Link State: Established, Linke quality: 86%
                RSSI: 69, SNR: 69
```

Figure 13 Output of Rf-management

Chapter 8 Configuring Routing

This chapter contains information on configuring Static Routing and AWR on the MSR2000, it has the following sections:

- Static Routing
- AWR

Static Routing

Static routing allows the network administrator full control over the 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>* **no ip route** *<A.B.C.D/M> <A.B.C.D>*	CONFIGURATION	Add a indirect static route Remove a gateway static route <A.B.C.D/M>: destination network prefix/mask <A.B.C.D>: gateway IP address
ip route *<A.B.C.D/M>* **station** <name> *<0-1>* **no ip route** *<A.B.C.D/M>* **station** <name> *<0-1>*		Add a directly-connected static route that binds to a client mode station Remove a directly-connected route <A.B.C.D/M>: destination network prefix/mask <0-1>: The 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, MSR2000 supports the intelligent Adaptive Wireless Routing (AWR) protocol. When AWR is activated, each MSR2000 will automatically maintain a table of optimal routes to the other MSR2000 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 **no router awr**	CONFIGURATION	Start the configuration of the AWR routing protocol 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 **debug none** **debug error** **debug state** **debug information** **debug dump**	ROUTER AWR	Set the AWR debug log level Disable AWR debug log Set AWR debug log to record errors Set AWR debug log to record errors & state changes Log error, state, and other detailed information 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 debug command above)
show ip awr configuration	Privileged EXEC	Display the current AWR configuration and status

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

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 MSR2000 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 MSR2000.

Motrix Protocol Overview

Motrix is the roaming service MSR2000 provides to support the seamless roaming of wireless clients across different mesh network subnets. Such support is necessary because every MSR2000 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 MSR2000. 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 MSR2000 configured only for backhaul or client to enable the Motrix service.

Motrix is designed to function with all 802.11-conforming clients without special client-side support. When a client decides to leave its currently associated router and attempts to associate with a new router, it sends to the new router an IEEE802.11 re-association request to make roaming succeed. Upon observing the request, the Motrix service on the new router will communicate with the Motrix service running on other participating routers and set up the roaming support that routes the client traffic through the new router.

Note: There are some clients that do not send re-association requests as according to the 802.11 standard. These non-conforming clients always send association requests regardless of whether they are first associating to an AP when they switch from one AP to another. Motrix currently can not provide roaming support for these clients without additional configurations (see the following section "Support for non-conforming or static IP clients"). The appendix section of this manual contains a list of clients that have verified to be 802.11-conforming clients as well as a list of non-conforming clients.

It is also highly recommended that the participating clients use dynamic IP addressing (DHCP). If the clients must be configured with static IP addresses or the client it is non-conforming, (see above) please refer to the following section "Support for non-conforming or static IP clients"

Motrix Configuration

This section covers the following main topics:

- Configuring motrix service
- Show motrix configuration

1) The MAC-IP list

The most important configuration information needed by the Motrix service is a list that tracks the MAC address of every virtual AP (or BSS) within the mesh network. Each list entry is a mapping that associates the BSS's MAC address with its router loopback IP address. The MAC-IP list may be populated manually (through the **mac-ip-list** command described below) as well as automatically (by enabling the AWR protocol together with Motrix). ***Note: The MAC-IP list is indexed by the BSS MAC address, and each MAC address may be associated with only one IP address.***

2) Support for non-conforming or static IP clients

Not every type of card from the market implements the full 802.11 standard (i.e., it may not send re-association requests). Also in some applications, it is preferable that clients use static IP addresses assigned by an administrator. In each of these cases, we need the following additional configurations. Each participating access router and the gateway router need to have these configurations. At the same time, please make sure there is only one router working as gateway in the roaming-domain network.

- station-list

Every station-list entry is a mapping that associates the participating client's MAC address with its static IP address. We should configure it manually.

- gateway AP

A Gateway AP is the AP that serves as the gateway of the network. The big assumption here is that all traffic destined to the client goes through the gateway.

Configuring Motrix Service

The following table summarizes the configuration commands for Motrix:

Command Syntax	Command Mode	Purpose
service roaming-motrix **no service roaming-motrix**	CONFIGURATION	Start configuration of the Motrix Roaming Service Disable Motrix Roaming Service

		and remove its configuration
enable **disable**	SERVICE ROAMING-MOTRIX	Activate the Motrix roaming service[17] Temporarily disable the Motrix Roaming service
mac-ip-list <*HH:HH:HH:HH:HH:HH*> <*A.B.C.D*> **no mac-ip-list** **no mac-ip-list** <*HH:HH:HH:HH:HH:HH*>	SERVICE ROAMING-MOTRIX	Add an entry to the MAC-IP list Clear all entries of the MAC-IP list Remove an entry from the MAC-IP list 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*> **no station-list** **no station-list** <*HH:HH:HH:HH:HH:HH*>	SERVICE ROAMING-MOTRIX	Add an entry to the station list Clear all entries of the MAC-IP list Remove an entry from the station list HH:HH:HH:HH:HH:HH: The MAC address of a participating client in the network
gateway A.B.C.D	SERVICE ROAMING-MOTRIX	Set the gateway router's IP address for Motrix
debug **debug none** **debug error** **debug information** **debug dump**	SERVICE ROAMING-MOTRIX	Set the Motrix debug log level Disable Motrix debug log Set Motrix debug log to record errors Log errors and other important information Log all Motrix debug information

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

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 stations	Privileged EXEC	Display the list of clients/stations that are Home associated or roaming from other MSR2000s

```
!
!
! Configuration
!
service roaming-motrix
 enable
 debug information
 mac-ip-list  00:00:65:43:21:00 172.16.21.1
 mac-ip-list  00:0b:6b:37:ab:53 172.16.20.1
 mac-ip-list  00:0b:6b: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:
00:00:65:43:21:00 172.16.21.1
00:0b:6b:37:ab:53 172.16.20.1
00:0b:6b: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(00:0b:6b:36:a1:0a)
  Previous AP: 00:0b:6b:37:ab:53
  Home AP: 00:0b:6b: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(00:0b:6b: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 MSR2000, 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 MSR2000 provides DHCP services such as DHCP server and DHCP Relay to dynamically assign such addresses.

Configuring DHCP Server

On MSR2000, 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 MSR2000 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 MSR2000 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 NAME: An alphanumeric string that identifies the DHCP pool
domain-name *[name]* **no domain-name**	IP DHCP SERVER POOL	Set the domain name to be included in DHCP leases for this pool Do not include any domain name information in DHCP leases for this pool name: A domain name such as “azaleanet.com”
gateway *<A.B.C.D>* **no gateway** *<A.B.C.D>*	IP DHCP SERVER POOL	Set the gateway IP to be included in DHCP leases for this pool Do not include gateway in DHCP leases 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>* **no host** *<HH:HH:HH:HH:HH:HH>*	IP DHCP SERVER POOL	Add a fixed DHCP IP address entry for a client host Remove a fixed DHCP IP address entry HH:HH:HH:HH:HH:HH: MAC address of the client host 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 <A.B.C.D Mask>: Address and mask of the subnet, e.g. 10.1.1.0 255.255.255.0 A.B.C.D/M: Address/mask of the subnet, e.g. 10.1.1.0/24
range *<begin IP> <end IP>* **no range** *<begin IP> <end IP>*	IP DHCP SERVER POOL	Add a range of IP addresses to this DHCP pool Remove a range from this DHCP pool Begin IP: The first IP address of the range 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 BSSs

Different BSSs may use different DHCP pools. You can use the following command in the “**BSS mode**” to attach DHCP pool to BSSs:

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

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

Viewing DHCP Server configuration

```
!
! Configuration
!
router dhcp server
```

[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.

```
 domain-name azaleanet.com
 dns 10.13.28.12,10.13.31.12
 max-lease-time 100000
!
!
MSR2000# show dhcp server all
domain-name: azaleanet.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 MSR2000 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
!
!Display DHCP Relay Information
!
MSR2000# show dhcp relay dhcp-servers
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.

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 MSR2000.

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 **no ip nat**	CONFIGURATION	Enter NAT configuration mode 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>* **out-interface dot11radio** *<0-1>* **station** *<name>* **no out-interface fast-ethernet** *<0-1>* **no out-interface dot11radio** *<0-1>* **station** *<name>*	IP NAT	Add a FastEthernet interface as external NAT interface Add a client station as external NAT interface. Remove a FastEthernet as the NAT interface. 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 MSR2000 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

MSR2000 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>*	CONFIGURATION	Create or modify a MAC address list with the specified name
no mac-list *<listname>*	CONFIGURATION	Remove a MAC address list
mac-addr *<HH:HH:HH:HH:HH:HH>*	MAC-LIST	Add a MAC address to the MAC list
no mac-addr *<HH:HH:HH:HH:HH:HH>*	MAC-LIST	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[1] *<A.B.C.D> key <string> auth-port <1-65535>* **no radius-server** *<A.B.C.D>* **auth**	AAA AAA	Add a radius authentication server, and configure the corresponding secret key and authentication port Remove a radius authentication server
radius-server *<A.B.C.D> key <string> acct-port <1-65535>* **no radius-server** *<A.B.C.D>* **acct**	AAA AAA	Add a radius accounting server, and configure the corresponding secret key and authentication port Remove a radius accounting server
server-group[2]	AAA	Enter server group configuration

server *<A.B.C.D>* **auth**	SERVER GROUP	Add a authentication server to server group
no server *<A.B.C.D>* **auth**		Remove authentication server from server group
server *<A.B.C.D>* **acct**		Add a accounting server to server group
no server *<A.B.C.D>* **acct**		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 MSR2000, 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.

Table 27 Display AAA configuration

Command Syntax	Command Mode	Purpose
show aaa	CONFIGURATION	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 azalea
 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 azalea
 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#
```

Security-Profile Configuration

This section describes the authentication types and encryption methods that you can configure on the router. Security profile on MSR 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 28 Configuring Security Profiles

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

security-profile wpa2 <wpa2-profile-name> **no security-profile wpa2 <wpa2-profile-name>**	CONFIGURATION	Add a WPA2 profile Remove a WPA2 profile from current configuration
encryption-mode-cipher ccmp **encryption-mode-cipher tkip** **no encryption-mode-cipher**	SECURITY-PROFILE WPA2	Enable CCMP encryption for WPA2 profile Enable TKIP encryption for WPA2 profile
wpa2-type 8021x <8021x-profile-name> **no wpa2-type 8021x**	SECURITY-PROFILE WPA2	Enable 8021X authentication for WPA2 profile Remove 8021X authentication from WPA2 profile
security-profile 8021x <8021x-profile-name> **no security-profile 8021x<8021x-profile-name>**	CONFIGURATION	Add a 8021X authentication profile Remove a 8021X authentication profile
eap-reauth-period <0-65535> **eap-reauth-period 3600** **no eap-reauth-period**	SECURITY-PROFILE 8021x	Set EAP re-authentication period Restore EAP re-authentication to default value of 3600 seconds

Table 29 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 WPA profile configuration
show security-profile 8021x	Privilege EXEC	Show 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#
```

BSS Security Configuration

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

Table 30 Configuring BSS Security

Command Syntax	Command Mode	Purpose
authentication open **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 **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 **show interface dot11radio <0|1> bss <SSID> deny-macs**	Privileged EXEC Privileged EXEC	Show attached accept macs address on SSID of the Radio 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 Azalea 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 Azalea1 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 Azalea wep-keys
  <cr>
MSR2000# show interface dot11radio 0 bss Azalea 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 31 Configuring WDS security

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

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 MSR2000.

- 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 MSR2000. Use the following commands to start or stop the QoS in CONFIGURATION mode.

Table **32** 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 33 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 34 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 amount of auto WDS interfaces and ManualWDS interfaces 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 00:0b:6b:37:a0:00
  ip address 10.53.54.2/24
  qos class band1
  no shutdown
 wds 1
  remote mac 00:0b:6b: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 35 Configuring snmp-server community

Command Syntax	Command Mode	Purpose
snmp-server community *[community] [ro|rw]* **no snmp-server community** *[community]*	CONFIGURATION	Add an SNMP community string that identifies an access control domain for the SNMP agent. **ro:** Specifies read-only access. Authorized management stations are able to retrieve, but not modify, MIB objects. **rw:** Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects. 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 36 Configuring snmp-server host

Command Syntax	Command Mode	Purpose
snmp-server host *[ip-address] [community] [udp-port]* **no snmp-server host** *[ip-addres]*	CONFIGURATION	Configure IP address of SNMP host to receive traps using the specified community string and SNMP port (162 is required for Azalea NMS).
show snmp-server host	Privileged EXEC	Display all SNMP trap hosts with associated community strings and ports

Configuring SNMPv3 users

MSR2000 also supports SNMPv3, which introduces the concept of users. The following commands controls the SNMPv3 user database on each MSR2000 router:

Table 37 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 name: SNMPv3 user name ro|rw: whether the user is read-only or read-write MD5 pass: Authentication password DES pass: Encryption password user-type: auth auth, no priv noauth no auth, no priv 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
azalear                          read-only
private                          read-write
azaleaw                          read-write
!
MSR2000# show snmp-server host
host                             community string                 port
192.168.10.55                    public                           162
192.168.10.10                    azalea                           162
192.168.10.64                    azalea                           162
192.168.10.130                   azalea                           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 MSR2000, it has the following sections:

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

Save & Reboot

Save

Azalea Networks recommends that you save your configuration often.

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

Table 38 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 Networks provides command **reboot** to hot restart MSR2000. After upgraded, user can use command **reboot** to restart MSR2000, then the new image takes effects.

Table 39 Reboot configuration

Command Syntax	Command Mode	Purpose
reboot	Privileged EXEC	Restart MSR2000 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 40 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

MSR2000 can play role as Telnet Client and Telnet Server.

Telnet Client

When MSR2000 acts as Telnet client, you can use command **telnet** to access other device.

Telnet Server

When MSR2000 acts as Telnet server, you should use command **ip telnet server** to enable the service. Telnet Server disable by default.

Table 41 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 **no ip telnet server**	Configuration	Enable telnet server. Disable telnet server

Viewing Telnet Server configuration

```
!
ip telnet server
!
```

Auto Recovery

Auto Recovery is an advanced feature provided by MSR2000, 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 42 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*> **no portal ip <*A.B.C.D*>**	SERVICE RECOVERY	Set an IP address for the device to check the state of connection wire network 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 Azalea Firmware

- 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
       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
       clear counters interface {dot11radio<0-1> {wdsauto|wdsmanu} <0-
C    5>|fast-ethernet <0-1>}
       clear log {awr|cli|hostapd|rf-management|motrix}
       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<0-1> scan [{bssid HH:HH:HH:HH:HH:HH|channel
     N}]
       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-reauth-period <0-65535>
       enable
       end
       exit
G      gateway A.B.C.D
H      help
       hostname WORD
I      ignore-broadcast-ssid
       interface dot11radio <0-1>
       interface fast-ethernet <0-1>
       ip address  A.B.C.D/M
       ip address dhcp
       ip dhcp {relay|server}
       ip nat
       ip route A.B.C.D/M A.B.C.D
       ip route A.B.C.D/M fast-ethernet <0-1>
       ip telnet server
```

```
L      List
M      mac-add HH:HH:HH:HH:HH:HH
       mac-access-control-type {deny|accept|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 {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
     HH:HH:HH:HH:HH:HH
       no antenna
       no authentication
       no authentication-algorithm
       no bss WORD
       no cts-protection
       no default-lease-time
       no dhcp
       no dhcp-servers
       no dns
       no domain-name
       no eap-reauth-period
       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 <0-1>}
       no ip telnet server
       no mac-address
       no mac-list WORD
       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 pool [NAME]
       no radius-server A.B.C.D
       no range A.B.C.D
       no router awr
       no scanning {automatic| channel-list| hardware-modes| mininum-
```

```
      interval| threshold rssi}
        no security-profile {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 station WORD
        no station-isolation
        no station-inactivity-limit
        no station-inactivity-policy
        no tx-power-reduction
        no unicast-rate
        no wds {<0-5>|auto}
        no wds-unicast-rate
        no wep-default-key
        no wep-key <1-4>
        no wireless-mode
        node-id <1-255>
P       ping A.B.C.D [<1-10>]
        pool [NAME]
Q       Qos
        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
        Reboot
        remote-mac HH:HH:HH:HH:HH:HH
        release-dhcp {dot11radio<0-1> station WORD |fast-ethernet<0-1>}
        renew-dhcp {dot11radio<0-1> station WORD |fast-ethernet<0-1>}
        restart-dhcp {dot11radio<0-1> station WORD| fast-ethernet<0-1>}
        remote-node <1-255>
        router awr
        router-id A.B.C.D
        router-password
S       scanning automatic
        scanning channel-list WORD
        scanning hardware-modes WORD
        scanning mininum-interval <1-300>
        scanning threshold rssi <0-100>
        security-profile {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> <router-loopback-ip>
{A.B.C.D/M|dhcp} <ssid> <dns-server-list> [nat-off]
  show aaa
  show arp [<A.B.C.D>|interface {dot11radio <0-1>| dot11wds <0-
31>| fast-ethernet <0-1>}]
  show arp count [interface {dot11radio <0-1>| dot11wds <0-31>|
fast-ethernet <0-1>}]
  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 <0-1> stations
  show hardware
  show hostname
  show interface brief
  show interface dot11radio <0-1> [{stations|states|txpower|node-
database}]
  show interface dot11radio <0-1>  [<ssid> {accept-macs| deny-
macs| stations| wep-keys}]
  show interface dot11radio <0-1> {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|scanning}
  show nat {out-interface|configuration|table}
  show node-id
  show process
  show qos dot11radio <0-1> {class|qdisc}
  show qos {configuration|interface}
  show recovery configuration
  show rf-management {active-neighbors|interface|configuration}
  show router id
  show running-config
  show snmp-server {community|host|v3user}
  show startup-config
  show version
  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}
  station-inactivity-limit <1-65535>
  station-inactivity-policy {0|1}
```

```
       switch image
T      telnet WORD [PORT]
       time <2005-2008> <1-12> <1-31> <0-23> <0-59> <0-59>
       traceroute WORD
U      unicast-rate RATE
       upgrade ftp A.B.C.D FILENAME USERNAME PASSWORD [reboot]
       upgrade url URL [reboot]
W      wds-unicast-rate RATE
       Wep-default-key <1-4>
       wep-key <1-4> WORD
       wds <0-5>
       wireless-mode {a|g} <channel> [coutry-name]
       write {file|memory|terminal}
```

Chapter 17 Roaming Client Compatibility

This chapter contains a list of 802.11 clients that have been verified to be 802.11-conforming clients (send re-association request when roaming) as well as a list of non-conforming-clients (always send association request when roaming). For details on the Motrix roaming service, please refer to Chapter 9.

Client hardware verified to be 802.11-conforming clients

TP-LINK TL-WN510G	chipset: Atheros AR5212 (recommended[21])
Cisco AIR-CB21AG-A-K9	chipset: Atheros AR5212 (recommended)
NetGear WG511U	chipset: Atheros AR5004X
D-LINK DWL-G650+A	chipset: Atheros AR5212
D-LINK DWL-G630	chipset: Atheros AR5212
BELKIN F5D7011A	chipset: Broadcom

Client hardware of non-conforming clients

HUAWEI Aolynk WCB300g	chipset: Unknown
Hawking HWC54D	chipset: Ralink
Linksys WPC54G	chipset: Broadcom
Linksys WPC54GX	chipset: Airgo
NetGear WG511v2	chipset: Marvell
AirLink AWLC3026	chipset: Texas Instrument
Thinkpad T42/43 built-in MiniPCI	chipset: Intel 2200BG

Notes:

The above lists do not encompass all available client hardware in the market. Moreover, due to minor variations in implementation of the 802.11 standard (such as scanning algorithm, the speed of rate negotiations, etc), the roaming speeds may vary from one supported client to another. Most clients, however, should have a roaming delay of less than 50ms.

[21] Recommended clients are verified to offer the most consistent performance with MSR2000's Motrix Roaming service.