

Wireless Broadband anytime & anywhere.



Azalea Networks MST200 Multi-Service Terminal Device CLI Configuration Guide

AOS-v2.6



Copyright 2005-2009 by Azalea Networks, USA. All rights reserved.

Statement of Conditions

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

Contact

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

info@azaleanet.com
<http://www.azaleanet.com>

Table of Contents

1.	About This Guide	5
1.1.	Audience	5
1.2.	Related Documents	5
1.3.	Software Version	5
2.	Overview	6
2.1.	CLI Modes	6
2.2.	CLI Navigation	8
2.3.	Obtaining Help	9
2.4.	Entering and Editing Commands	10
2.5.	Filter Output	11
3.	Basic Configuration	12
3.1.	System Information	12
3.2.	Host Name Configuration	12
3.3.	Root Password Configuration	13
3.3.	Configuration Code	13
3.4.	Saving and Viewing Configuration File Information	14
3.5.	Setting CONFIGURATION Mode Parameters	14
4.	Software Image Upgrade	15
5.	Physical Interfaces	17
5.1.	Interface Modes	17
5.2.	Viewing Fast-Ethernet Interface Information	18
5.3.	Configuring Dot11Radio Interfaces (Layer-2 Interfaces)	19
5.4.	Viewing The Dot11radio Interface Information	20
6.	Client Mode Configuration	22
6.1.	Basic Client Mode Configuration	22
6.2.	Viewing Information of a Station in a Dot11Radio Interface	26
7.	Video Friendly Network	27
7.1.	AVT Configuration	27
7.2.	AVT Parameter Configuration	27
8.	Configuring Routing	29
8.1.	Static Routing	29
9.	NAT	30

10.	802.11 Security	31
10.1.	802.11 Standard Overview	31
10.2.	Certificate Configuration	32
10.3.	Security-Profile Configuration	33
10.4.	Client Security Configuration	37
11.	WME Configuration	40
11.1.	Basic functions of WME (802.11e)	40
12.	Other Commands and Utilities	42
12.1.	Save and Reboot	42
12.2.	Ping & Traceroute	42
12.3.	Telnet Client & Server	44
12.4.	Auto Recovery	44

1. About This Guide

This document provides information about how to configure the MST200 using the Command Line Interface or CLI.

This document provides the configuration instructions and examples for the MST200, also called the “router”. It contains information on current features and protocols supported by the MST series.

Note: The command examples and outputs are created with an MST200 and are for demonstration purposes only. The exact output of the commands may vary depending on the router model and its firmware version.

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

1.1. Audience

This document is intended for the system/IT or network administrator who is responsible for configuring or maintaining the MST series; this guide assumes the user is knowledgeable in wireless/wired Layer-2 and Layer-3 networking technologies.

1.2. Related Documents

For more information about the MST series, please refer to the following documents:
MST series Web-based Configuration Guide

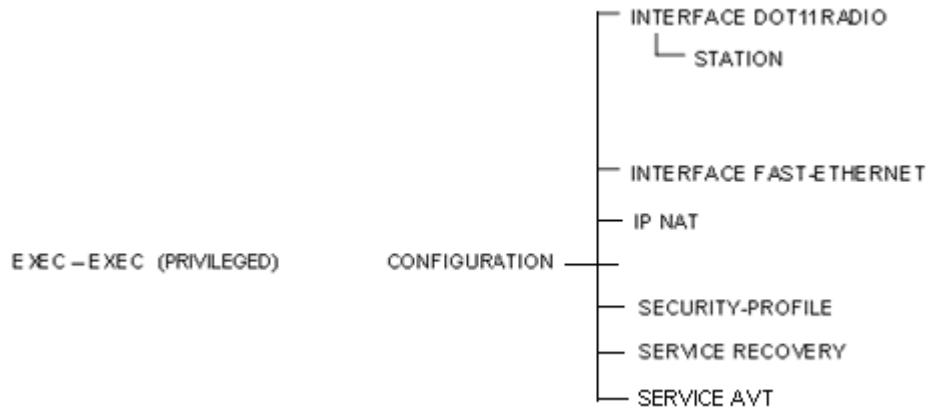
1.3. Software Version

This document pertains to Version 2.6

2. Overview

2.1. CLI Modes

The CLI is organized into multiple modes that allow navigation between different protocols and interfaces. The diagram below displays the CLI modes and CLI structures that are available if you have full access to the CLI:



User EXEC Mode

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 cannot create or change any configuration. You can only view system information or execute limited commands. In User EXEC mode, the enable command prompts you for your password to allow you into Privileged EXEC mode.

Privileged EXEC Mode

Privileged EXEC mode has commands to view configuration, manage configuration files, run diagnostics, enable or disable debug operations, and reboot the router.

CONFIGURATION Mode

From the Privileged EXEC mode, use the configure terminal command to enter the CONFIGURATION mode. CONFIGURATION mode enables you to configure security features, setup various services and configure static route. You can also enter protocol, interfaces, and line CLI modes to configure settings, and save the configuration.

INTERFACE DOT11RADIO Mode

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

INTERFACE FAST ETHERNET Mode

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

IP NAT Mode

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

SECURITY PROFILE Mode

SECURITY PROFILE mode enables you to configure security profiles to be used on the MST. You may configure 802.1x, WEP, WPA and WPA2 profiles.

SERVICE RECOVERY Mode

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

SERVICE RF MANAGEMENT Mode

SERVICE RF-MANAGEMENT mode enables you to configure the intelligent radio-frequency management service provided by the MST and the adjustment level.

SERVICE AVT Mode

SERVICE AVT mode enables you to configure AVT services for the MST.

The LIST Command

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

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

The following example demonstrates the use of the list command.

```
MST200(config)# interface fast-ethernet 0
MST200(config-if-ethernet)# list
end
exit
help
ip address A.B.C.D/M
ip address dhcp
list
mtu <256-1500>
no ip address
no mtu
no shutdown
quit
show config
show config | (grep|begin) PATTERN
show running-config
show running-config | (grep|begin) PATTERN
shutdown
write memory
write terminal
```

2.2. CLI Navigation

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

CLI Command Mode	Prompt	To Enter Mode *	To Exit mode
User EXEC	MST200>	Access the router through Telnet and successfully log in.	Use the exit commands.
PRIVILEGED EXEC	MST200#	From the User EXEC mode, use the enable command. From any other mode, use the end command.	Use the exit command.
CONFIGURATION	MST200(config)#	From the PRIVILEGED EXEC mode, use the configure terminal command. From any other modes except the User EXEC and Privileged EXEC modes, use the exit command.	Use either the exit or end command.
INTERFACE DOT11RADIO	MST200(config-if-dot11radio)#	From the CONFIGURATION mode, use the interface dot11radio command.	Use either the exit or end command.
STATION	MST200(config-if-dot11radio-sta)#	From the INTERFACE DOT11RADIO mode, use the station command.	
INTERFACE FAST-ETHERNET	MST200(config-if-ethernet)#	From the CONFIGURATION mode, use the interface fast-ethernet command.	Use either the exit or end command.
IP NAT	MST200(config-nat)#	From the CONFIGURATION mode, use the profile mesh command.	
SERVICE RECOVERY	MST200(config-recovery)#	From the CONFIGURATION mode, use the service rf-management	

CLI Command Mode	Prompt	To Enter Mode *	To Exit mode
		command.	
SERVICE AVT	MST200(config-avt)#	From the CONFIGURATION mode, use avt command.	

* See the relevant sections in this document for more information about each of the recommended commands.

2.3 Obtaining Help

CLI mode provides several ways for you to obtain help, and to list the available command keywords for a given CLI mode.

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

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

Help command

The sample text below illustrates the output that appears when you type help at any mode's prompt. The output tells you how to use ? to get help.

The following example demonstrates the use of the help command.

```
MST200(config)# help
When you need help, anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
command argument (e.g. 'show ?') and describes each possible
argument.
2. Partial help is provided when an abbreviated argument is entered
and you want to know what arguments match the input
(e.g. 'show me?'.)
```

? command

Type ? to list all keywords on the left with a brief description of the commands on the right.

The following example demonstrates the use of the ? command.

```
MST200(config-if-ethernet)# ?
end      End current mode and return to privilege EXEC mode
exit     Exit current mode and down to previous mode
help     Description of the interactive help system
ip       Interface Internet Protocol config commands
list     Print command list
mtu      Set the interface's Maximum Transmission Unit (MTU)
no       Negate a command or set its defaults
quit     Exit current mode and down to previous mode
show     Show running system information
shutdown Shutdown this interface
write    Write running configuration to file or terminal
```

2.4 Entering and Editing Commands

The following rules apply to entering and editing CLI 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.

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 one character.
CTRL-D	Deletes character to left of 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 from 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 CTRL-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.

Key Combinations	Action
Esc D	Deletes all characters from the cursor to the end of the word.

2.5 Filter Output

Reduce outputs by configuring the filter rules. Support grep and begin mode.

Grep command

[Command] | grep [mode]

Output lines accord with specified mode.

The following example demonstrates the use of the grep command.

```
MST200 (config)# show running-config | grep service
service recovery
service avt
```

Begin command

[Command] | begin [mode]

Output contents begin with specified mode.

The following example demonstrates the use of the begin command.

```
MST200 (config)# show running-config | begin qos
qos
  disable
  class DEFAULT
    maxbw 300
    minbw 50
```

3. Basic Configuration

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](#)
- Root [Password configuration](#)
- Code configuration
- [Viewing configuration file information](#)
- [Setting CONFIGURATION mode parameters](#)

3.1 System Information

When booting up the MST, the system is pre-configured. Use the CLI commands to configure the router and to enable and manage the system.

System Information	Purpose
Hostname	Allows you to set the host name of the MSR (MST?) series routers. Enter a new host name in the form of an alphanumeric string.
Router-password	Default password is public; it can be changed by using the router-password command.
Management port IP address	IP address 192.168.0.1/24 is configured on FastEthernet 0 by default, and if FastEthernet 0 is configured to be the DHCP client mode, user can automatically get the address from DHCP server.
Regulatory Domain Code	Default regulatory domain code is US by system. The configuration can be changed using the country code command.

3.2 Host Name Configuration

The host name appears in the prompt. The default host name is the MST device name, e.g. MST200. 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 CONFIGURATION mode:

Command Syntax	Command Mode	Purpose
hostname <name>	CONFIGURATION	Set the host name of the MST series. Enter a new host name in the form of a character string which must begin with a letter. The length should be no more than 32 characters.

no hostname		Remove the hostname, go back to default. Default hostname is MST200
-------------	--	---

3.3 Root Password Configuration

The MST series default password is public.

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

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

The following example demonstrates changing the login password.

```
MST200# router-password
  root Set login password for root

MST200# 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.
```

3.3 Configuration Code

The default country/regulatory domain code for the MST series is: US.

In PRIVILEGED EXEC mode, configure the country/regulatory domain code through the command below

Command Syntax	Command Mode	Purpose
country-code (AU CN EU JP KR LA NA PS SG TW US)	PRIVILEGED EXEC	Configure country/regulatory domain code manually.
no country-code		Cancel the manual configured country/regulatory domain code back to default: US.

The following example demonstrates changing the regulatory domain.

```
MST200(config)# country-code
  AU Set code for Australia
  CN Set code for China
  EU Set code for Denmark, Germany, Iceland, Finland, Netherlands, Norway, Sweden,
  Poland, Slovenia, Luxembourg, and South Africa
  JP Set code for Japan
  KR Set code for Korea
  LA Set code for Latin America
  NA Set code for North America (USA and Canada)
  PS Set code for US Public Safety 4.9G
  SG Set code for Singapore
  TW Set code for Taiwan
```

US Set code for USA

```
MST200 (config)# country-code CN
% regulatory domain code will be set to 'CN' at the next router reboot.
% If any radio is configured to use a channel incompatible with the new regulatory domain code,
% it will be reset to the first legal channel of the configured mode.
```

3.4 Saving and Viewing Configuration File Information

The configuration should be saved frequently.

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

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.

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

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.

3.5 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:

Command Syntax	Command Mode	Purpose
Interface <interface>	CONFIGURATION	Configure a physical or logical interface on MSR series. dot11radio fast-ethernet vlan tunnel
show running-config	CONFIGURATION	Display current configuration information on the system.

5. Physical Interfaces

This chapter contains information on defining and configuring and physical interfaces on the MST, the fast Ethernet and the dot11radio..

5.1 Interface Modes

The MST contains physical and logical interfaces in both Layer-2 and Layer-3 modes.

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

Configuring Fast-ethernet Interfaces

The MST device has two physical fast-ethernet interfaces¹ 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.

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	INTERFACE FAST-ETHERNET	Set IP address of fast-ethernet interface by dhcp.
no ip address		Remove IP address from Fast-ethernet interface
mtu <256-1500>	INTERFACE FAST-ETHERNET	Set Maximum Transmission Unit (MTU) ² size, 1500 is default. <i>Setting of MTU is optional and should be done with care.</i>
no mtu		Reset the MTU to the default value.
shutdown	INTERFACE FAST-ETHERNET	Administratively shut down the interface.

¹ On some MST models, two Ethernet port (FastEthernet 0, 1) are usable. The default IP address is 192.168.0.1/24 for Fast-Ethernet Port0, and 192.168.1.1/24 for Fast-Ethernet Port1.

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

Command Syntax	Command Mode	Purpose
no shutdown		Administratively activate the interface (Default).
exit, end, or quit	INTERFACE FAST-ETHERNET	Leave Interface mode and commit the change.

5.2 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.

The following example demonstrates using the show command to view fast-ethernet information.

```
MST200# show running-config
hostname MST200
!
country-code CN
!
...
!
interface fast-ethernet 0
 ip address 192.168.12.12/24
 mtu 256
!
service recovery
 disable
!
service avt
 disable
!
!
```

5.3 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:

Radio Operation Mode

When configured for Client mode, the router can connect as a Wi-Fi client to other APs.

Command Syntax	Command Mode	Purpose
Interface dot11radio <0-1>	CONFIGURATION	Configure one of the dot11radio interfaces

Common settings

MST200-A supports 802.11a and MST200-C supports 802.11g. 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 be configured on each radio interface.

Command Syntax	Command Mode	Purpose
shutdown	INTERFACE DOT11RADIO	Administratively shut down this radio; all existing operations on this radio will stop.
no shutdown		Activate the interface.
packet-loss-ratio	INTERFACE DOT11RADIO	Choose the packet loss ratio of the current environment; the rate algorithm will adjust based on the packet loss ratio value.
packet-loss-ratio low		The packet loss ratio is high under the current environment.
packet-loss-ratio very-low		The packet loss ratio is common under the current environment.
packet-loss-ratio lowest		The packet loss ratio is low under the current environment.
no packet-loss-ratio		Back to the default value of common packet loss ratio.
force-rate-control-algorithm [data video]	INTERFACE DOT11RADIO	Enforce a particular algorithm, no auto configuration.
force-rate-control-algorithm data		Enforce the data transmission algorithm.
force-rate-control-algorithm video		Enforce the video transmission algorithm.

Command Syntax	Command Mode	Purpose
no force-rate-control -algorithm		Select a rate algorithm automatically according to the QoS.
Distance <1-50000> No distance	INTERFACE DOT11RADIO	Set the transmission distance, default: 0, unit: meter. Delete the setting of transmission distance, back to the default 0.
mtu <256-2274> no mtu	INTERFACE DOT11RADIO	Set the layer-3 MTU of this radio interface. Reset the MTU to the default value. <i>Setting of radio MTU is not recommended and should be done with extreme caution.</i>

Client mode settings

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

Command Syntax	Command Mode	Purpose
station <station name> no station <station name>	INTERFACE DOT11RADIO	Configure a 802.11 client station on this radio interface ³ . Remove 802.11 client station setting from this radio interface. Note: currently only one station is allowed on each router.

5.4 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.

The following example demonstrates using the show command to view the dot11radio information.

```
MST200# show running-config
hostname MST200
!
country-code CN
!
!
!
interface dot11radio 0
mtu 256
distance 1
force-rate-control-algorithm data
packet-loss ratio very-low
station 0
```

³ Please see the later chapter on client mode for more information.

```
ip address dhcp
access-point ssid radio 1
!
interface fast-ethernet 0
ip address 192.168.12.12/24
mtu 256
!
service recovery
disable
!
service avt
disable
!
!
ip nat
disable
out-interface fast-ethernet 0
!
```

6. Client Mode Configuration

6.1. Basic Client Mode Configuration

The following table outlines the basic settings for a client station.

Command Syntax	Command Mode	Purpose
station <station name> no station <station name>	INTERFACE DOT11RADIO	Configure a 802.11 client station on this radio interface. Remove 802.11 client station setting from this radio interface.
ip address [<i>ip address/mask</i>] ip address dhcp no ip address	INTERFACE DOT11RADIO STATION	Set IP address of this client station. Set IP address to be automatically obtained by using the DHCP protocol; a DHCP server must be running on the network to which this station associates. Remove IP address from this client station.
client-authentication open wep <wep-profile-name> default-key <1-4> client-authentication open key-management wpa client-8021x <client-8021x-profile-name> client-authentication open key-management wpa2 client-8021x <client-8021x-profile-name> client-authentication open key-management wpa-psk hex <string> client-authentication open key-management wpa-psk ascii <string> client-authentication open key-management wpa2-psk hex <string>	INTERFACE DOT11RADIO STATION	Enable WEP encryption for this client using the key settings in the WEP profile and the specified default key. Enable WPA security for this client; using the authentication settings in the client-8021x profile. Enable WPA2 security for this client; using the authentication settings in the client-8021x profile. Enable WPA PSK on client and configure pre-shared key using hexadecimal format. Enable WPA PSK on client and configure pre-shared key using ascii format. Enable WPA2 PSK on client and configure pre-shared key using hexadecimal format.

Command Syntax	Command Mode	Purpose
client-authentication open key-management wpa2-psk ascii <string> client-authentication shared wep <wep-profile-name> default-key <1-4> no client-authentication		Enable WPA2 PSK on client and configure pre-shared key using ascii format. Enable WEP encryption for this client using the key settings in the WEP profile and the specified default key. Disable authentication for this client interface.
access-point ssid <SSID> no access-point ssid	INTERFACE DOT11RADIO STATION	SSID of the access point that this client station wants to associate with. Default is no SSID. Remove access-point SSID configuration. SSID: 802.11 Service Set ID.
access-point bssid <HH:HH:HH:HH:HH:HH> no access-point bssid	INTERFACE DOT11RADIO STATION	BSSID of the access point that this client station wants to associate with. Default has no BSSID specified. 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> no access-point bssid-filter acceptable prefix <HH:HH:HH:HH:HH:HH> <HH:HH:HH:HH:HH:HH> no access-point bssid-filter acceptable-prefix	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 the 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 a matching BSSID will be selected. For example, if you want the client to only connect to MSR (MST?) series routers, 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. Remove a certain BSSID filter. Remove all the BSSID filters.

Command Syntax	Command Mode	Purpose
<p>scanning hardware-modes <mode string></p> <p>scanning hardware-modes <mode string> channel-list <channel list></p> <p>no scanning hardware-modes</p>	<p>INTERFACE DOT11RADIO STATION</p>	<p>Configure the hardware modes that you allow the client to stay in when doing access point scanning.</p> <p><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.</p> <p>Channel-list is optionally provided to permit you specifying which channels the client will scan in. Only one channel list is allowed. Default has no channel list and it scans in all legal channels of the configured hardware modes.</p> <p><channel-list>: a list of comma-separated channel numbers, no space in between.</p> <p>Remove the hardware scanning mode and channel-list setting and return to default.</p>
<p>scanning minimum-interval <seconds></p> <p>no scanning minimum-interval</p>	<p>INTERFACE DOT11RADIOSTATION</p>	<p>Configure the minimum allowed time interval between two consecutive scans.</p> <p><seconds>: a number between 1 and 300, the unit is second. Default value is 60 seconds.</p> <p>Restore default setting of minimum scan interval.</p>
<p>scanning threshold rssi <rssi value></p> <p>no scanning threshold rssi</p>	<p>INTERFACE DOT11RADIO STATION</p>	<p>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.</p> <p><rssi value>: a number between 0 and 100. 0 means no such trigger. Default value is 15.</p> <p>RSSI stands for Received Signal Strength Index.</p> <p>Restore the default RSSI threshold value.</p>
<p>release-dhcp dot11radio <0-N> station <station name></p>	<p>PRIVILEGED EXEC</p>	<p>Release the station's IP address acquired from DHCP server.</p>

Command Syntax	Command Mode	Purpose
renew-dhcp dot11 radio <0-N> station <station name>		Renew the station's IP address via DHCP server.
restart-dhcp dot11 radio <0-N> station <station name>		Restart DHCP client for the station.

Supporting Client-list

In client mode, the MST200 supports client-list to make the network aware of multiple IP devices daisy-chained to MST Ethernet interface. The MST200 acts as the extension of Azalea mesh connecting attached devices like a video camera, and enables non-interrupting access between attached devices and mesh network while roaming.

The following table demonstrates how to configure the basic client-list:

Command Syntax	Command Mode	Purpose
client-list <HH:HH:HH:HH:HH:HH> <HH:HH:HH:HH:HH:HH> <A.B.C.D/M>	INTERFACE DOT11RADIO	Add entry into the client list. One MAC address can configure up to 4 IP addresses.
no client-list <HH:HH:HH:HH:HH:HH>		Remove the specific entry with designated MAC address from station list. HH:HH:HH:HH:HH:HH: the MAC address of the interface in client mode that connecting to the network.

Under client mode, in the client-list, one MAC address can configure up to four IP addresses to create four client-list entries. The MAC address of the station needs to be the same as the MAC address of the radio interface. The IP address is the IP address of the video camera or other device. If the station itself needs network-side management while roaming, it should be assigned a static IP address, and that IP address should be added to the client-list. When using a static IP address for the station, manually add the default routing of the station interface.

802.11 Security Configuration

The 802.11 security standard defines a suite of wireless security protocols and implementations. The MST200 allows the client mode to use a specific 802.11 security profile such as WEP or WPA. Refer to the chapter on 802.11 Security for more information.

6.2. Viewing Information of a Station in a Dot11Radio Interface

The following example shows the output of station information under Dot11radio interface.

```
MST200# show run
...
!
interface dot11radio 0
...
station 0
ip address dhcp
access-point ssid demo
...
MST200# sh interface dot11radio 0
Interface Dot11Radio0
operation_mode:client, country code:US, channel policy:0, antenna:1,
cts protection:2,
distance:0, short retry:7, long retry:4,
admin status: up physical status: up
index 35 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
HWmode: g, channel: 1, Fragment thr: 2346, RTS thr: 2347
HWaddr: 00:17:7b:00:27:40
input packets 823925, bytes 96825419, dropped 0, multicast packets 0
input errors 88069, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 457, bytes 26006, dropped 0
output errors 2, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
Station Information:
Station 0
State: Associated
SSID: "demo", Access Point: 00:17:7b:35:e8:53 RSSI: 55
Previous Access Point: NA
IP Address: 172.16.21.249(DHCP acquired)
Security: None
Scanning threshold: RSSI 15
Minimum scan interval: 60 seconds
scanning in hardware modes: ag
scanning in channels:
mode A: 36 40 44 48 52 56 60 64 149 153 157 161 165
mode G: 1 2 3 4 5 6 7 8 9 10 11
```

7. Video Friendly Network

Video Friendly Network is a network transmission optimization technology specially designed by Azalea for mobile video service. It includes three parts: Active Video Transport (AVT), video friendly MAC technology, and virtual video distribution layer.

AVT is a specially designed network transmission optimization technology for soft video transmission with a typical application of fixed or mobile video surveillance. Through the data delay configured by users in a mesh network, AVT can effectively reduce or resolve the problems of packet loss, delivery disorder, and packet jitter caused by wireless transmission, so as to provide smooth and stable multi-channel video traffic transmission. In video surveillance, by providing in-network cache, AVT can resolve the problems that impact the quality of video transport in WMN to achieve the best transmission result.

7.1. AVT Configuration

Below is a video surveillance network topology:



The MST is at the ingress port, directly connecting to the video server (camera/encoder). The video flow enters the mesh network through the MST.

7.2. AVT Parameter Configuration

Necessary Parameters

Parameters needed to configure in ingress:

- Encoder: choose the type of video server.
- Buffer-time at the ingress port. The default buffer time is 4 seconds for ingress.

- Ingress-IP: configure the IP address of the video server.

At present, one ingress MST can support four video servers at the same time.

Optional Parameters

A different network delay in different applications may help to achieve a more satisfactory video transmission. In general, the longer the network delay, the fewer problems occur that impact video transmission, such as packet loss; the shorter the network delay, the better the real-time capability.

CLI Command

The following commands are used to configure AVT mode and parameters:

Command Syntax	Command Mode	Purpose
service AVT	CONFIGURATION	Enable AVT service configuration
enable/disable	SERVICE AVT	Enable/disable AVT service
encoder <generic tycosun visiondigi > no encoder	SERVICE AVT	Set the encoder type (video server). This would be "Generic" (default) for most of the encoders such as Hiklif and AVINFO; use tycosun for Tycosun encoder; use visiondigi for Visiondigi encoder. Remove the type of encoder, get back to the default: generic.
ingress-ip A.B.C.D no ingress-ip A.B.C.D	SERVICE AVT	Set ingress IP (up to 4). Remove the IP address of encoder at ingress.
buffer-time<1-5> no buffer-time	SERVICE AVT	Set the buffer time as 1-5 seconds. Default second for ingress is 3. Remove the buffer time, restore to the default value.

The following commands show AVT running status and statistics:

Command Syntax	Command Mode	Purpose
show avt status	PRIVILEGED EXEC	Display the runtime statistics of AVT.
show avt configuration	PRIVILEGED EXEC	Display the running configuration of AVT.

8. Configuring Routing

This chapter contains information on configuring Layer-3 routing on the MST.

8.1. Static Routing

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

A configured static route is installed in the routing table only when the route is active; that is, the route's next hop must be bound to an operational interface.

The following table summarizes the command to add/remove the static route:

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

9. NAT

Network Address Translation (NAT) is an Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. An NAT box located where the LAN meets the Internet manages all necessary IP address translations. This chapter contains the information for configuring NAT on the MST.

You can use the following commands to configure the NAT service:

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.
mapping static A.B.C.D/M A.B.C.D no mapping static A.B.C.D/M no mapping static all	IP NAT	Mapping rules to a certain IP address. Disable mapping rules and IP address. Disable all mapping rules and IP address.
out-interface fast-ethernet <0-1> out-interface dot11radio <0-N> station <name> no out-interface fast-ethernet <0-1> no out-interface dot11radio <0-N> 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.

10. 802.11 Security

This chapter describes how to configure security policies as defined by the 802.11i standard on the MST series router.

10.1. 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.

Open

Open authentication allows any client authentication and tries to connect with the router.

Shared-key (WEP)

- Shared Key Authentication verifies that the clients know the sharing key.
- Shared Key only applies to WEP.
- Shared key is not a secure method and is not recommended.

WEP (wired equivalent privacy) is the wireless security solution based on symmetric encryption using the RC4 encryption algorithm.

To enhance the WEP security, WEP adopts the 4 different sequence keys and enhances the key strength with: 40 bits, 104 bits and 128 bits.

WPA

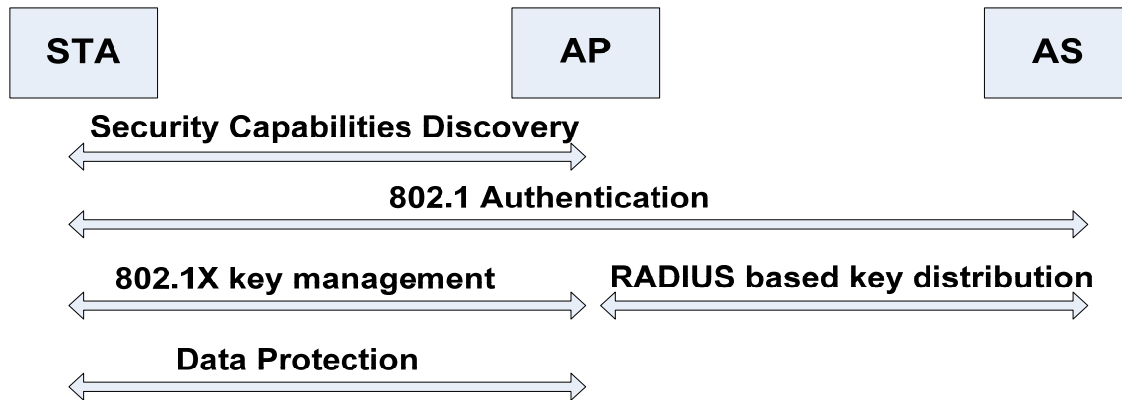
WPA (Wifi protected access) and WPA2 can achieve wireless security through pre-shared key and 802.1x. The only difference between WPA and WPA2 are the different encryption algorithms; WPA achieves data security using TKIP (RC4), while WPA2 through CCMP (AES).

Pre-shared key is the encryption which achieves data communications through a symmetric approach.

WPA and WPA2 also combined 802.1x to strengthen the wireless data communications security.

802.1x

The basic 802.1x authentication model:



In the MST200 system, the MSR is the AP and the MST is the STA.

802.1 x-based certification processes:

The certification process follows the authenticating sequence described below:

- 1 Access point (AP) announces security suites in Beacon and Probe Response frame.
- 2 Station (STA) chooses the correct security suite and password connecting to the access point.
- 3 Establish a Layer-2 link between station and access point.
- 4 Use EAP for 802.1x authentication:
 - a. Station and AS (Authentication Server) have the similar PMK (Pairwise Master Key); access point gets the PMK from AS.
 - b. Access point and AS create a PTK (Pairwise Transient Key).
 - c. Access point distributes GTK (Group Transient Key) using PTK's KCK (EAPOL-Key confirmation Key) and KEK (EAPOL-Key Encryption Key).
 - d. Station and access point shake hands four times creating a group of keys to protect data during network transmission.
- 5 Disconnect link.

10.2. Certificate Configuration

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

The following commands are used to install authentication certificates:

Command Syntax	Command Mode	Purpose
install certificate ca <URL>	PRIVILEGED EXEC	Download and install the Certificate Authority (CA) certificate from the provided URL.
install certificate client <URL>		Download and install the client certificate from the provided URL.
install client-key <URL>		Download and install the client key file from the provided URL.

Installed certificates may be displayed with these commands:

Command Syntax	Command Mode	Purpose
show certificate ca	PRIVILEGED EXEC	Show the information of the installed CA certificate.
show certificate client		Show the information of the installed client certificate.

The following example shows the output of a configuration.

```
MST200# install certificate ca http://192.168.1.1/certs/cert-ca.pem
MST200# install certificate client http://192.168.1.1/certs/cert-clt.pem
MST200# install client-key http://192.168.1.1/certs/cert-clt-key.pem
MST200# show certificate ca
MST200# show certificate client
```

10.3. Security-Profile Configuration

This section describes the authentication types and encryption methods that you can configure on the router. Security profile on the MST series defines all security policy supported by router software. The router supports WEP, WPA, WPA2 and 8021x security suites. This block is only a definition of security policy, and it will take effect after connection to the BSS or WDS. Users can add or delete configuration files according to the actual application; interface can switch security policy flexibly through different configuration facilities.

The following table demonstrates the configuring of security profiles:

Command Syntax	Command Mode	Purpose
security-profile wep <wep-profile-name>	CONFIGURATION	Create or modify a WEP security profile of the given name.
no security-profile wep <wep-name>		Remove a WEP profile.
wep-key <1 2 3 4> <key-string>	SECURITY-PROFILE WEP	Add a WEP key to the WEP security profile.
no wep-key <1 2 3 4>		Remove a WEP key from WEP security profile.

Command Syntax	Command Mode	Purpose
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	Designate TKIP encryption mode for WPA security policy. Remove the encryption mode configuration.
wpa-type 8021x <8021x-profile-name> no wpa-type 8021x	SECURITY-PROFILE WPA	Designate WPA security policy using 802.1x authentication. Remove 8021X authentication.
wpa-type psk hex <string> wpa-type psk ascii <string> no wpa-type psk	SECURITY-PROFILE WPA	Designate WPA PSK authentication on WPA policy and pre-configure hexadecimal key. Designate 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	Designate CCMP encryption for WPA2 security policy. Designate TKIP encryption for WPA2 security policy. Remove WPA2 encryption type setting.
wpa2-type 8021x <8021x-profile-name> no wpa2-type 8021x	SECURITY-PROFILE WPA2	Designate 8021X authentication for WPA2 profile. Remove 8021X authentication from WPA2 profile.
wpa2-type psk hex <string> wpa2-type psk ascii <string> no wpa2-type psk	SECURITY-PROFILE WPA2	Designate WPA2 PSK for WPA2 security policy, pre-configured hex key. Designate WPA2 PSK for WPA2 security policy, pre-configured ASCII code key. Remove WPA2 PSK authentication setting.
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	SECURITY-PROFILE	Set EAP re-authentication period.

Command Syntax	Command Mode	Purpose
<0-65535> eap-reauth-period 3600 no eap-reauth-period	E 8021x	Restore EAP re-authentication to default value of 3600 seconds.
security-profile client-8021x <client-8021x-profile-name> e> no security-profile client-8021x <client-8021x-profile-name> e>	CONFIGURATION	Add 802.1 x security policy profile and client authentication profile that client mode use. Remove the 802.1x and client authentication policy profiles.
eap-method peap eap-method ttls eap-method tls no eap-method	SECURITY-PROFILE E CLIENT-8021x	Set EAP to PEAP. Set EAP to TTLS. Set EAP to TLS. Remove EAP setting.
password <string> no password	SECURITY-PROFILE E CLIENT- 8021x	Set authentication user password Remove authentication user password setting.
user-name <string> no user-name	SECURITY-PROFILE E CLIENT-8021x	Set authentication user name. Remove authentication user name.

The following table provides commands to display the security profile configuration:

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

The following example shows the 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

MST200# show security-profile wep
security-profile wep wep1
wep-key 1 1234567890abcdef1234567890
wep-key 2 "abcde"
wep-key 3 "abcdefabcdefa"
wep-key 4 abcdefabcdefabcdefabcdefab
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
MST200#
```

The following example shows the 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
```

The following example shows the output of WPA2 profile configuration:

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

The following example shows the output of 8021x profile configuration:

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

MST200# show security-profile 8021x
security-profile 8021x 8021xprofile
eap-reauth-period 3600
security-profile 8021x 8021x1
MST200#
```

The following example shows the output of client-8021x profile configuration:

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

10.4. Client Security Configuration

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

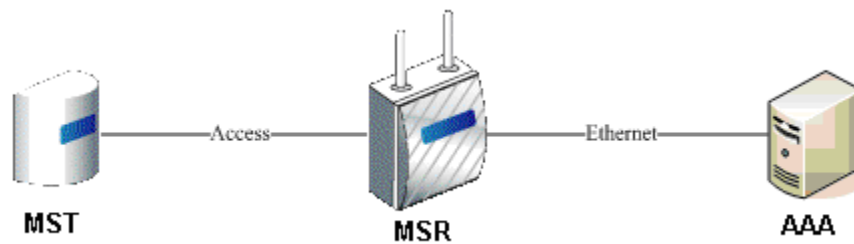
The following table displays configuring client-mode security:

Command Syntax	Command Mode	Purpose
client-authentication open wep <wep-profile-name> default-key <1-4>	INTERFACE DOT11RADIO STATION	Enable WEP encryption for this client using the key settings in the WEP profile and the specified default key.
client-authentication open client-8021x <client-8021x-profile-name>		Enable 802.1X security for this CLIENT, using the authentication settings in the client-8021x profile.
client-authentication open key-management wpa client-8021x <client-8021x-profile-name>		Enable WPA security for this CLIENT, using the authentication settings in the client-8021x profile.
client-authentication open key-management wpa2 client-8021x <client-8021x-profile-name>		Enable WPA2 security for this CLIENT, using the authentication settings in the client-8021x profile.
client-authentication open key-management wpa-psk hex <string>		Enable WPA PSK on client and configure pre-shared key using hexadecimal format.
client-authentication open key-management wpa-psk ascii <string>		Enable WPA PSK on client and configure pre-shared key using ascii format.
client-authentication open key-management wpa-psk ascii <string>		Enable WPA2 PSK on client and configure pre-shared key using ascii format.

Command Syntax	Command Mode	Purpose
client-authentication shared wep <wep-profile-name> default-key <1-4> no client-authentication		Enable WEP encryption for this client using the key settings in the WEP profile and the specified default key. Disable authentication for this client interface.

802.1x Typical Configuration

Network Topology:



Topology Note

- AAA represents Authentication Server
- MSR opens WPA2+802.1x authentication
- Client can access MSR and have the right to visit AAA

The following example demonstrates the MSR and MST Configuration display:

```

MSR

aaa
 radius-server 192.168.10.69 auth-port 1812 key 123456
 server-group
  server 192.168.10.69 auth

security-profile 8021x 8021x
security-profile wpa2 wpa2-8021x
 encryption-mode-cipher ccmp
 wpa2-type 8021x 8021x

interface dot11radio 0
 wireless-mode g 1
 antenna 1
 mode access
 bss Azalea
  authentication open key-management wpa2 wpa2-8021x
  dhcp server automatic
  
```

MST

```
security-profile client-8021x client-8021x
user-name hzhang
password whatever
eap-method peap phase2 mschapv2

interface dot11radio 0
station 0
ip address dhcp
client-authentication open key-management wpa2 client-8021x client-8021x
access-point ssid Azalea
```

802.11 Security Configuration Troubleshooting

If you encounter difficulty when configuring the security protocol, do the following:

- 1 Determine whether Station and access point have the same security strategy.
- 2 When using WEP security strategy, note the following:
 - a. The same serial key at both ends of the key list should be consistent.
 - b. Whether they have the same authentication method, open or shared-key.
 - c. Whether they have the same default key.
- 3 For the PSK security of WPA and WPA2:
 - a. If client sets two security policies with an option, it must determine whether it uses the same encryption algorithm with the AP.
 - b. When the key is HEX, and the allowed key length may not be 63, it must ensure whether the complemented key is the same.
- 4 For the 802.1x clients:
 - a. Determine if MST can scan the wireless signal of AP.
 - b. Determine if MST configures the correct encryption.
 - c. For the certificate authentication, it must install correctly and configure the correct user name and password.

11. WME Configuration

WME (Wireless multimedia enhanced protocol), as a transitional standard, supports 802.11e and also provides a 2-layer QoS guarantee for the mesh network. When the network is overloaded or congested, QoS can ensure that critical traffic volume is not delayed or discarded, so as to maintain efficient operation of the network. The traditional 802.11 protocol provides service using the best effort to deliver the data traffic, which makes the real-time service operation un-guaranteed.

Azalea MSR series routers use the Service differentiation mechanism of 802.11e to divide the data transmission queue into six priorities, which can ensure the priority transmission of voice, video and other business. When WME is enabled, data with different priorities will be entered into different queues. The end-to-end QoS in the protocol ensures that the high-priority transmission and receive requests will be handled first.

11.1. Basic functions of WME (802.11e)

Transmission queue (AP-STA traffic)



In the MST200 system, the MSR is the AP and the MST is the STA.

There are 6 transmission queues in the AP: 4 queues for data flow, 1 queue for the transmission of beacon frames, 1 queue for the transmission of the "beacon after" packet (such as management frame transmission should follow by the beacon frame). The last two queues cannot be configured by users.

- If 802.11e (wme) is disabled, the AP will transmit data by the default queue (make the best effort to deliver).
- If 802.11e (wme) is enabled, but the linking STA does not support 802.11, then the AP will transmit data by the default queue (make the best effort to deliver).
- If 802.11 e (wme) is enabled, and the linking STA also supports 802.11e, then the AP will transmit data in different queues based on the priority label of VLAN 802.11p or the DHCP of the IP header.

QoS broadcast (STA-to-AP traffic)

The AP can broadcast QoS parameters through the beacon frame. QoS parameters can be acquired when 802.11e clients are connected to the AP, which will be the basis of Client transmitting communication flow.

The following table shows the queue comparison between DSCP value and Terms of Service (TOS) value:

DSCP		TOS	Priority
HEX	Binary	Decimal	

0x40	01000000	16	Background
0x20	00100000	8	Background
Any other value			Best Effort
0x60	0110 0000	24	Video
0x80	1000 0000	32	Video
0xa0	1010 0000	40	Video
0xc0	1100 0000	48	Voice
0xe0	1110 0000	56	Voice

Note: Running WME requires that both points support WME at the same time, i.e.: If the AP and Station enable WME, then they both must support WME. WME is enabled under the default backhaul mode.

WME Configuration Command

The following table displays the WME command configuration:

Command Syntax	Command Mode	Purpose
wme	INTERFACE DOT11RADIO	Enable WME service.
no wme		Disable WME service.

The following example demonstrates a typical WME configuration:

```
MST200(config-if-dot11radio)# wme
MST200(config-if-dot11radio)# no wme
```

The following example demonstrates how the WME configuration is shown:

```
MST200 # show running-config
....
interface dot11radio 0
wme
```

12. Other Commands and Utilities

This chapter contains other commands and troubleshooting utilities on the MST device. It contains the following sections:

12.1. Save and Reboot

Save

Azalea recommends that you save your configuration frequently.

To save a configuration file, use the following command in the Privileged EXEC mode:

Command Syntax	Command Mode	Purpose
copy running-config startup-config	PRIVILEGED EXEC	Save the current running configuration to the startup-config file.

Reboot

Azalea provides the reboot command to hot restart the MSR (MST?) series. After image upgrade, you can use the reboot command to restart the MST200. The new image will then take effect.

The following table displays the reboot configuration:

Command Syntax	Command Mode	Purpose
Reboot	PRIVILEGED EXEC	Restart MSR

12.2. Ping & Traceroute

The ping and traceroute commands are helpful utilities for troubleshooting network access problems.

Ping

The ping command is the most 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.

The ping command 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

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

Three datagrams are sent, each with a Time-To-Live (TTL) field value set to 1. 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 destination host. 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.

The following table shows the 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.

The following example demonstrates output of ping & traceroute information

```
MST200# 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

MST200# 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

MST200# 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
```

MST200#

12.3. Telnet Client & Server

The MST200 can function as a Telnet Client and Telnet Server.

Telnet Client

When the MST acts as a Telnet Client, you can use the command telnet to access other devices.

Telnet Server

When the MST acts as a Telnet Server, you can use the command IP telnet server to enable the service. Telnet Server is disabled by default.

The following table shows the 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	CONFIGURATION	Enable telnet server.
no ip telnet server		Disable telnet server.

The following example demonstrates enabling the Telnet server.

```
!
ip telnet server
!
```

12.4. Auto Recovery

Auto Recovery is an advanced feature provided by the MST. When enabled, Auto Recovery will automatically detect and recover from a 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 in an attempt to restore its normal working state.

The following table displays the 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.

The following example demonstrates activating Auto Recovery.

```
!  
service recovery  
  enable  
!
```