MP1800 SERIES Multi-Operation Access Router

Maipu Communication Technology Co., Ltd
No. 16, Jiuxing Avenue
Hi-Tech Park
Chengdu, Sichuan Province
P. R. China
610041
Tel: (86) 28-85148850, 85148041
Fax: (86) 28-85146848, 85148139
URL: http:// www.maipu.com
Mail: overseas@maipu.com

Maipu Communication Technology Co., Ltd
No. 16, JiuXing Avenue, Hi-Tech Park
Chengdu, Sichuan Province
P. R. China
610041
Tel: (86) 28-85148850, 85148041
Fax: (86) 28-85146848, 85148139
URL: http:// www.maipu.com
Mail: overseas@maipu.com

NOTE1:

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

NOTE2:

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

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

Contents

WLAN Configuration

Main contents:

- Introduction to WLAN
- Wireless interface parameter configuration
- Virtual AP parameter configuration
- Wireless security profile configuration
- WLAN typical configuration

Introduction to WLAN

WLAN (Wireless Local Area Networks) is developed from the earliest 802.11 standard to the later 802.11b/g, which makes WLAN bandwidth be improved greatly. 802.11i standard ensures the WLAN security; 802.11f/r/s standard makes the WLAN removable and deployable.

WLAN consists of Independent BSS, Infrastructure BSS and ESS. This chapter describes the configuration and debugging of the access point in Infrastructure BSS. The virtual AP mentioned in the following text refers to multiple access points on the same wireless interface and they have the same physical parameters, but the protocol parameters in the security policy can be different.

Wireless Interface Parameter Configuration

Main contents:

- Introduction to wireless interface parameter
- Basic commands of wireless interface parameter
- Application instance of wireless interface parameter
- Monitoring and debugging of wireless interface parameter

Introduction

Wireless interface has some configurable parameters, including antenna, channel, power, mode, rate, re-transmission times, country code, preamble length, SLOT length, beacon period and so on. The parameters of all virtual APs are the same.

Basic Commands

Command	Description	Configuration Mode
antenna {rx | tx} {left | right | diversity}	Select antenna. The receiving and sending antennas can be selected separately. You can select fixed or auto.	config-if-dot11radio0
beacon {period | dtim-period} *time*	The beacon period and DTIM period	config-if-dot11radio0
channel *number* **channel auto** **channel auto** *time*	Select channel	config-if-dot11radio0
packet {long | short} **retry** *1-15*	Set the times of re-transmitting packets	config-if-dot11radio0
power {100 | 50 | 25 | 12 | min}	Set the power; set according to the percentage of the maximum power	config-if-dot11radio0
preamble {short | long}	Set long and short preamble	config-if-dot11radio0
radioMode {11b | 11g | mixed}	Set wireless mode	config-if-dot11radio0
radioSpeed {**basic-**x.x | x.x}	Set the wireless rate	config-if-dot11radio0
rts {retry | threshold} *count*	Set the RTS threshold and re-transmission times	config-if-dot11radio0

slot {short | long}	Set the slot length of the conflict window	config-if-dot11radio0
shutdown	Close the wireless interface	config-if-dot11radio0
worldwide countrycode *code*	Set the country code	config-if-dot11radio0

Note

The command description with * means that the command has the configuration instance to describe.

- **antenna**

The antenna has two antennas. You can select one or auto.

antenna {rx | tx} {left | right | diversity}

no antenna {rx | tx}

Syntax	Description
rx left	Select the left antenna for receiving
rx right	Select the right antenna for receiving
rx diversity	The receiving selects the antenna according to the signal intensity automatically.
tx left	Select the left antenna for sending
tx right	Select the right antenna for sending
tx diversity	The receiving selects the antenna according to the signal intensity automatically.

Default status: By default, select antenna automatically for sending and receiving.

Note

The receiving antenna on MP1800 SERIES router can take effect only when being set as auto.

- **beacon**

The command is used to set the beacon period and DTIM period.

beacon {period | dtim-period} *time*

no beacon {period | dtim-period}

Syntax	Description

period *100-3000*	Set the period of sending the beacon packets and the unit is 1024us
dtim-period *1-30*	Set the period of sending buffered broadcast packets and the unit is beacon periods

Default status: The default beacon period is 300 and the period of sending the buffer packets is 6.

- **channel**

You can select the fixed channel or set to search the idle channels automatically.

channel *number*

channel auto

channel auto *time*

no channel

Syntax	Description
1-14	Set the specified channel. The channel is the wireless center channel. In fact, after expanding, it may occupy the center channel left two and right two channels. Therefore, the enter channels without overlapping are 1, 6, and 11. In fact, the configurable channel range is related with the set country code.
auto	Automatically detect the idle channel for one time.
auto *1-6000*	Automatically detect the idle channels with the configured minutes as the period. The auto detection affects the normal communication, so the period cannot be set too small.

Default status: By default, automatically detect the idle channel for one time.

- **packet**

The command is used to set the times of re-transmitting the packets.

packet {long | short} **retry** *1-15*

no packet {long | short} **retry**

Syntax	Description
short retry *count*	Set the times of re-transmitting the packet with the length smaller than RTS threshold
long retry *count*	Set the times of re-transmitting the packet with the length larger than RTS threshold

Default status: By default, the re-transmission times is 10.

- **power**

The command is used to set the percentage of the maximum wireless power.

power {100 | 50 | 25 | 12 | min}

no power

Syntax	Description
100	Set the wireless sending power as 100% of the maximum power
50	Set the wireless sending power as 50% of the maximum power
25	Set the wireless sending power as 25% of the maximum power
12	Set the wireless sending power as 12% of the maximum power
min	Set the wireless sending power as the minimum power

Default status: By default, the wireless sending power is 100% of the maximum power.

- **preamble**

The command is used to set the length of the preamble.

preamble {short | long}

no preamble

Syntax	Description
short	Set the preamble as the short preamble
long	Set the preamble as the long preamble

Default status: By default, it is the short preamble.

- **radioMode**

The command is used to set the wireless mode.

radioMode {11b | 11g | mixed}

no radioMode

Syntax	Description
11b	Set the wireless mode as 802.11b
11g	Set the wireless mode as 802.11g
mixed	Set the wireless mode as 802.11b/g mixed

Default status: By default, the wireless mode is 802.11b/g mixed.

🕮 Note

Set the wireless mode to affect the rate configuration. When being set as 802.11b, the rate can only be set as 1.0, 2.0, 5.5, 11.0; when being set as 802.11g, the rate can only be set as 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, and 54.0; when being set as mixed, you can set all rates.

- **radioSpeed**

You can select multiple wireless rates. Meanwhile, you need to specify whether each rate is the basic rate (the basic rate is the rate that all associated stations must support).

radioSpeed {**basic-**x.x | x.x}

no radioSpeed

Syntax	Description
basic-x.x ...	Set the wireless basic rate
x.x ...	Set the wireless extended rate

Default status: All 802.11b/g rates: basic-1.0 2.0 5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0.

🕮 Note

1. The wireless rate means the rate that must be supported when the wires access node is associated with the stations. At least one basic rate must be set.
2. You can set multiple rates, such as radioSpeed basic-1.0 basic-2.0 48.0 54.0.
3. During the actual running, the program selects from the rate setting range according to the signal.

4. The no format of the command selects the appropriate rate according to the current wireless mode.

- **rts**

The command is used to set the RTS threshold and retransmission times.

rts {retry | threshold} *count*

no rts {retry | threshold}

Syntax	Description
threshold *256-2346*	Set the packet size threshold of using the RTS/CTS mechanism. When the unicast packet is larger than the threshold, use RTS/CTS to interact.
retry *1-15*	Set the re-transmission times of RTS

Default status: By default, the RTS threshold is 2346 bytes and the RTS re-transmission times is 10.

- **shutdown**

The command is used to disable the wireless interface.

shutdown

no shutdown

Default status: By default, the wireless interface is enabled.

- **slot**

The command is used to set the length of the conflicting window slot.

slot {short | long}

no slot

Syntax	Description
short	Set the conflicting window as short slot, that is, 9us.
long	Set the conflicting window as long slot, that is, 20us.

Default status: By default, it is the short slot.

■ **worldwide**

The command is used to set the country code of the wireless interface. Each country may have different limitation for wireless signal.

worldwide countrycode *code*

no worldwide countrycode

Syntax	Description
code	Use two capital letters to express the ISO country code. For example, CN is for China and US is for America.

Default status: CN

Note

1. The setting of the country code affects the available wireless channel and the maximum sending power.

2. The configurable country codes:

Country code	Country name
AR	ARGENTINA
AT	AUSTRIA
AU	AUSTRALIA
BE	BELGIUM
BG	BULGARIA
BR	BRAZIL
CA	CANADA
CH	SWITZERLAND
CL	CHILE
CN	CHINA (Default)
CO	COLOMBIA
CY	CYPRUS
CZ	CZECH REPUBLIC
DE	GERMANY
DK	DENMARK
EE	ESTONIA
ES	SPAIN
FI	FINLAND
FR	FRANCE
GB	UNITED KINGDOM
GR	GREECE
HK	HONGKONG

HR	CROATIA
HU	HUNGARY
ID	INDONESIA
IE	IRELAND
IL	ISRAEL
IN	INDIA
IS	ICELAND
IT	ITALY
JP	JAPAN
KR	KOREA
LI	LIECHTENSTEIN
LT	LITHUANIA
LU	LUXEMBOURG
LV	LATVIA
MA	MOROCCO
MT	MALTA
MX	MEXICO
MY	MALAYSIA
NL	NETHERLANDS
NO	NORWAY
NZ	NEW ZEALAND
PE	PERU
PH	PHILIPPINES
PL	POLAND
PT	PORTUGAL
RO	ROMANIA
RU	RUSSIAN FEDERATION
SA	SAUDI ARABIA
SE	SWEDEN
SG	SINGAPORE
SI	SLOVENIA
SK	SLOVAKIA
TH	THAILAND
TR	TURKEY
TW	TAIWAN,PROVINCE OF CHINA
US	UNITED STATES
UY	URUGUAY
ZA	SOUTH AFRICA

Application Instance

Application Instance 1

WLAN application network topology

Illustration

One router with the WLAN module and one PC with the wireless adapter are interconnected.

ROUTER configuration:

Command	Description
router(config)#interface dot11radio0	Enter the wireless interface mode
router(config-if-dot11radio0)#beacon period 100	Configure beacon period as 100ms
router(config-if-dot11radio0)#channel auto	Configure selecting channel automatically
router(config-if-dot11radio0)#radioSpeed basic-1.0 basic-2.0 54.0	Configure the basic rate and extended rate
router(config-if-dot11radio0)# worldwide countrycode CN	Configure the country code as CN
router(config-if-dot11radio0)#exit	Exit the wireless interface mode

Monitoring and Debugging

Monitoring Command

Command	Description
show dot11radio *unit*	Display the running parameter and status of the wireless interface

Monitoring Command Instance

router#**show dot11radio 0**

Displayed result:

```
dot11radio 0:
  LinkStatus        : Up
  Mac Address       : 0001.7a12.3456
  Current SSIDs     : 2              MAX SSIDs : 4
  ********************************************************************************
  SSID(network name)  LinkStatus     VLAN      Stations   Privilege
  maipu               Up             1         1          No
  CPE                 Up             2         0          No
  ********************************************************************************

  Country Code      : 156            RadioMode        : 11b/g mixed
  Allowed Channels  : 1 2 3 4 5 6 7 8 9 10 11 12 13
  Auto Channel      : Yes            Auto ReChannel   : Disable
  Current Channel   : 4 [AUTO]       Power            : 100%
  Recv Antenna      : diversity      Transmit Antenna : diversity
  Allowed Rates     : [1] 2 5.5 6 9 11 12 18 24 36 48 54
  Broadcast rate    : 1              Need Protection  : No
  Beacon Period     : 300            Short Time Slot  : Yes
  Dtim Period       : 6              Short Preamble   : No
  RTS Threshold     : 2346           Packet Short Retry: 10
  RTS Retry         : 10             Packet Long Retry : 10

  Fragment Input    : 1026           Fragment Output  : 139
  Bytes Input       : 90704          Bytes Output     : 24162
  Frame Input       : 3104           Frame Output     : 139
  Multicast Input   : 2923           Multicast Output : 136
  Duplicates Rcvd   : 0              Exceeded Retries : 0
  Decrypt Failed    : 5              Data Retries     : 0
  MIC Failed        : 0              RTS Retries      : 0
 FCS Failed         : 138

   Associate Request  : 1            Associate Response: 1
  Associate Success  : 1            Diassociate      : 0
```

Description and analysis:

The above information includes three parts:

1. The current wireless interface status, including the Link status of the wireless interface, the information about all virtual APs under the wireless interface and so on;
2. The running parameters of the current wireless interface;
3. The statistics information of the current wireless interface;

Virtual AP Parameter Configuration

Main contents:

- Overview
- Basic commands of virtual AP parameters
- Application instance of virtual AP parameters
- Monitoring and debugging of virtual AP parameters

Overview

Virtual AP refers to the multiple virtual logical wireless access point (AP) on the same wireless interface. The parameters of the virtual APs can be different and can be bound to different security policies.

Basic Commands

Command	Description	Configuration Mode
ssid *name*	Enter the virtual AP configuration mode or create a new virtual AP	config-if-dot11radio0 config-dot11radio0-ssid-xxx
clientlimit *1-56*	Set the maximum number of the access clients of the virtual AP	config-dot11radio0-ssid-xxx
encapsulation {802.1h | rfc1042}	Select the LLC encapsulation format	config-dot11radio0-ssid-xxx
fragment *256-2346*	Set the fragment threshold	config-dot11radio0-ssid-xxx

idle-timeout *0-60*	Set the idle timeout	config-dot11radio0-ssid-xxx
maclist *2001-3000*	Bind the access list of the MAC address	config-dot11radio0-ssid-xxx
regroup time *1-30*	Re-calculate the period of the multicast key	config-dot11radio0-ssid-xxx
security *name*	Bind the security profile	config-dot11radio0-ssid-xxx
shutdown	Disable the virtual AP	config-dot11radio0-ssid-xxx
ssidIe {enable | disable}	Enable and disable the SSID advertisement of virtual AP	config-dot11radio0-ssid-xxx
vlan *1-4094*	Configure the vlan ID of the virtual AP	config-dot11radio0-ssid-xxx
privilege {enable | disable}	Configure the privilege attribute of the virtual AP	config-dot11radio0-ssid-xxx
station isolate {enable | disable}	Configure whether the AP isolates the station	config-dot11radio0-ssid-xxx
interface dot11radio0.x	Create one the wireless sub interface and enter the configuration mode of the wireless sub interface	config config-if
encapsulation dot1q *1-4094*	Encapsulate the wireless sub interface with the VLAN ID	config-if-dot11radio0.x

🕮 Note

The command description with * means that the command has the configuration instance to describe.

- **ssid**

The command is used to create a new virtual AP or enter the existing virtual AP, with ssid as ID.

ssid *name*

no ssid *name*

Syntax	Description
ssid *name*	If virtual AP identified by *name* does not exist, first create a new virtual AP and enter the virtual AP configuration mode, that is, the ssid configuration mode
no ssid *name*	Delete the virtual AP identified by *name*

Default status: none

🕮 Note

At most four virtual APs can be configured.

- **clientlimit**

The command is used to limit the maximum number of the stations of the virtual AP.

clientlimit *1-56*

no clientlimit

Syntax	Description
1-56	The maximum number of the access stations of the virtual AP

Default status: By default, up to 14 access stations are permitted.

🕮 Note

1. Each virtual AP can be configured with up to 56 access stations, but the total number of the associated stations of all virtual APs of one wireless interface cannot exceed 56. Therefore, the total number of the stations of all virtual APs exceeds 56, the system prints the prompt information.

2. The encrypted policy affects the maximum number of the associated stations of the wireless interface. If the encrypted policy is TKIP, one station occupies two resources. Therefore, the wireless interface can associates with 56 stations at most. If all associated stations use TKIP, the maximum number of the stations that can be associated with the wireless interface changes to 28.

- **encapsulation**

The command is used to set the OUI encapsulation format of the link layer LLC/SNAP.

encapsulation {802.1h | rfc1042}

no encapsulation

Syntax	Description
rfc1042	Encapsulate LLC/SNAP (aa-aa-03-00-00-00) by RFC1042
802.1h	Encapsulate LLC/SNAP (aa-aa-03-00-00-f8) by 802.1H.

Default status: Encapsulate by rfc1042.

Note

1. The command is invalid for the IPX and AppleTalk protocol packets. The IPX and AppleTalk packets are encapsulated by 802.1h.
2. The command does not affect the de-encapsulating of the encapsulated packet and the device processes according to IEEE 802.1H-1997 standard.

- **fragment**

The command is used to set the fragment threshold. The packet that exceeds the threshold is fragmented.

fragment *256-2346*

no fragment

Syntax	Description
256-2346	Set the bytes of the packet fragment

Default status: The threshold of the packet fragment is 2346 bytes.

- **idle-timeout**

The command is used to set the idle timeout of the station.

idle-timeout *0-60*

no idle-timeout

Syntax	Description
0-60	0 means no timeout forever. The remaining means 1-60-minute timeout.

Default status: By default, the timeout is 5 minutes.

- **maclist**

The command is used to bind the MAC access list.

maclist *2001-3000*

no maclist

Syntax	Description
2001-3000	Bind the created MAC access list, which is used for the basic authentication of 802.11.

Default status: By default, no MAC access list is bound.

- **regroup**

The command is used to set re-calculating the multicast key period.

regroup time *1-30*

no regroup time

Syntax	Description
1-30	Set re-calculating the period of the multicast key, in the unit of minute.

Default status: By default, do not re-calculate the multicast key.

Note

The setting is valid only when the security policy is WPA1 or WPA2.

- **security**

The command is used to bind the configured security profile.

security *name*

no security

Syntax	Description
name	Bind the configured security profile. Check the contents of the security profile during binding. If there is conflicting project, the system prompts error.

Default status: No security profile is bound.

- **shutdown**

The command is used to disable the virtual AP.

shutdown

no shutdown

Default status: Enable the virtual AP.

- **ssidIe**

The command is used to set whether to broadcast SSID of the virtual AP.

ssidIe {enable | disable}

no ssidIe

Syntax	Description
enable	Broadcast the SSID of the virtual AP.
disable	Do not broadcast SSID of the virtual AP.

Default status: Broadcast the SSID of the virtual AP.

- **vlan**

The command is used to set the VLAN ID of the virtual AP.

vlan *1-4094*

no vlan

Syntax	Description
1-4094	Set the VLAN of the virtual AP. The vlan number corresponds to the VLAN number of the wireless sub interface, so the wireless packets of the virtual AP can be submitted to the IP protocol stack.

Default status: no vlan attribute

Note

Modifying the configuration results in the disconnection of all stations.

- **privilege**

The command is used to set the privilege attribute of the virtual AP.

privilege {enable | disable}

no privilege

Syntax	Description
enable	Set the virtual AP as the privilege virtual AP. Once the attribute is set, only the privilege user on the web interface can view and configure the virtual AP.
disable	Set the virtual AP as the common virtual AP and all users can view and configure.

Default status: No privilege attribute

- **station isolate**

The command is used to set the privilege attribute of the virtual AP.

station isolate {enable | disable}

no station isolate

Syntax	Description
enable	Set the virtual AP to isolate all associated stations. All stations cannot communicate with each other, but they can only communicate with the wireless sub interface.
disable	Set the virtual AP not to isolate stations. All stations in the virtual AP can communicate with each other and the wireless sub interface.

Default status: Do not isolate the stations.

- **interface dot11radio0.x**

The command is used to create the wireless sub interface or enter the wireless sub interface configuration mode.

interface dot11radio0.x

Default status: No sub interface

🕮 Note

1. Wireless sub interface is the channel of the virtual AP connecting the DS system. You can configure the IP address, NAT, ACL, route protocol and bridge group on the wireless sub interface.

2. The wireless main interface can only be configured with the wireless parameters and SSID, but cannot be configured with the IP address or run the IP protocol stack. It can only serve as one console interface.

- **encapsulation dot1q**

The command is used to configure the VLAN number of the wireless sub interface.

encapsulation dot1q *1-4094*

Syntax	Description
1-4094	Set the VLAN number of the wireless sub interface. The vlan number corresponds to the VLAN number of the wireless sub interface, so the wireless packets of the virtual AP can be submitted to the IP protocol stack.

Default status: No vlan attribute

Application Instance

Application Instance 1

Refer to Figure 1-1.

Router configuration:

Command	Description
router(config)#interface dot11radio0	Enter the wireless interface mode
router(config-if-dot11radio0)#ssid test	Enter the virtual AP configuration mode
router(config-if-dot11radio0-ssid-test)#clientlimit 10	Configure the limitation for the clients of the virtual AP
router(config-if-dot11radio0-ssid-test)#fragment 2000	Configure the fragment threshold of the virtual AP
router(config-if-dot11radio0-ssid-test)#idle-timeout 60	Configure the client idle timeout of the virtual AP
router(config-if-dot11radio0-ssid-test)#security wpa	Bind the security profile of the virtual AP
router(config-if-dot11radio0-ssid-test)#vlan 1	Configure the VLAN attribute of the virtual AP
router(config-if-dot11radio0-ssid-test)#exit	Exit the virtual AP configuration mode

Monitoring and Debugging

Monitoring Commands

For example:

Command	Description
show dot11radio *unit* **ssid** name	Display the running parameters and status of the virtual AP
show dot11radio *unit* **ssid** *name* **station** *mac-address*	Display the running status of the access station

Monitoring Command Instance

router# **show dot11radio 0 ssid maipu**

Displayed result:

SSID [maipu]:
LinkStatus : Up
Mac Address : 0201.7a12.3456
Current Stations : 1 MAX Stations : 14
****
MAC Address IP Address Authenticated Associated WPA1/2-PSK EAP-802.1X
00b0.8c51.0327 192.168.119.40 Yes Yes - -
****

Vlan : 1 Security Profile :
Hidden SSID : No RegroupTime : 0
Encapsulation : RFC1042 MacList :
Fragment Threshold : 2346 Privilege : No

Fragment Input : 437 Fragment Output : 100
Bytes Input : 60351 Bytes Output : 18539
Frame Input : 437 Frame Output : 100
Multicast Input : 255 Multicast Output : 96
Duplicates Rcvd : 0 Exceeded Retries : 0
Decrypt Failed : 0 Data Retries : 0
MIC Failed : 0 RTS Retries : 0

Associate Request : 1 Associate Response: 1
Associate Success : 1 Diassociate : 0

Description and analysis:

The above information includes three parts:

1. The current virtual AP status, including the Link status of the virtual AP, the information about all associated stations of the virtual AP;
2. The running parameters of the current virtual AP;
3. The statistics information of the current virtual AP;

router#**show dot11radio 0 ssid maipu station 00b0.8c51.0327**

Displayed result:

Station [00b0.8c51.0327]:

MAC Address	: 00b0.8c51.0327	IP Address	: 192.168.119.40
SSID	: maipu	Vlan	: 1
SecPol	: -	Authenticated	: Yes
AuthPol:	: -	Associated	: Yes
CiphPol:	: -	AID	: 1
Supported Rates	: [1] 2 5.5 6 9 11 12 18 24 36 48 54		
Receive Rate	: 54	Transmit Rate	: 54
Signal Strength	: -70dBm	Connected For	: 490 seconds
Signal Quality	: 41%	Activity Timeout	: 120 seconds
Power-save	: Off	Last Activity	: 26 seconds ago
Fragment Input	: 71	Fragment Output	: 1
Bytes Input	: 4704	Bytes Output	: 360
Frame Input	: 71	Frame Output	: 1
Duplicates Rcvd	: 0	Exceeded Retries	: 0
Decrypt Failed	: 0	Data Retries	: 0
MIC Failed	: 0	RTS Retries	: 0

Description and analysis:

The above information includes two parts:

1. The running parameters of the associated station
2. The statistics information of the associated station

Debugging Commands

Command	Description
debug dot11radio pro assoc	Debug the association of the station
debug dot11radio pro auth	Debug the basic authentication of the station
debug dot11radio pro data	Debug all packets received and sent by the wireless interface
debug dot11radio pro datanull	Debug the datanull packets received by the wireless interface
debug dot11radio pro deauth	Debug the de-authentication of the station
debug dot11radio pro disassoc	Debug the dis-association of the station
debug dot11radio pro dperx	Debug the packets received by the wireless interface
debug dot11radio pro dpetx	Debug the packets sent by the wireless interface
debug dot11radio pro pm	Debug the converting of the mode of saving energy of the station
debug dot11radio pro probe	Debug the detection frames received by the wireless interface and the response
debug dot11radio pro pspoll	Debug the pspoll frame received by the wireless interface
debug dot11radio pro ratectrl	Debug the rate adjusting of the wireless interface
debug dot11radio pro reassoc	Debug the re-association of the station
debug dot11radio pro scan	Debug the process of the wireless interface of detecting the idle channel automatically
debug dot11radio rsn	Debug the process of the wireless interface expanding security

Debugging Command Instance

For environment, refer to Figure 1.1.

1. A complete process of connecting the station

The following debugging switches need to be enabled:

debug dot11radio pro auth

debug dot11radio pro assoc

debug dot11radio rsn

Information and analysis:

00:03:53: DOT11->AUTH: from 00:b0:8c:51:03:27 to 02:e0:4c:fb:76:a7

The authentication packet is sent from the station 00:b0:8c:51:03:27 to the virtual AP 02:e0:4c:fb:76:a7

00:03:53: DOT11->Update Sta:00:b0:8c:51:03:27 Start

Update the status of the station 00:b0:8c:51:03:27.

00:03:53: DOT11->Sta:00:b0:8c:51:03:27 is already here

Find that the station 00:b0:8c:51:03:27 already exists.

00:03:53: DOT11->Update Sta:00:b0:8c:51:03:27 End

00:03:53: DOT11->Auth Recv Start

Start to process the authentication packet.

00:03:53: DOT11->OPEN-SYSTEM-SEQ-1

The authentication mode opensystem, the first frame (reques)

00:03:53: DOT11->Auth Send Start

00:03:53: DOT11->Sta:00:b0:8c:51:03:27

Send the authentication response packet.

00:03:53: DOT11->Auth Send End

00:03:53: DOT11->Open-System Authentication success!

Pass the opensystem basic authentication.

00:03:53: DOT11->Auth Recv End

00:03:53: DOT11->ASSOC: from 00:b0:8c:51:03:27 to 02:e0:4c:fb:76:a7

Receive the association packet sent from the station 00:b0:8c:51:03:27 to virtual **AP 02:e0:4c:fb:76:a7.**

00:03:53: DOT11->Assoc Recv Start

00:03:53: DOT11->Asso Rsp Send Start

00:03:53: DOT11->Sta:00:b0:8c:51:03:27

Send the association response packet to the station 00:b0:**8c:51:03:27.**

00:03:53: DOT11->Asso Rsp Send End

00:03:53: DOT11->Association success

The association succeeds.

00:03:53: DOT11->Sta's negAuthPol is PSK

The authentication mode of the station is PSK.

00:03:53: DOT11->Send uniCast MSG A to 00:b0:8c:51:03:27

Start to perform the RSN authentication and send the first packet to the station**.**

00:03:53: DOT11->Received uniCast MSG B from 00:b0:8c:51:03:27

Receive the second response packet RSN of the station.

00:03:53: DOT11->Key data added!

00:03:53: DOT11->Send uniCast MSG C/RSN to 00:b0:8c:51:03:27

Send the RNS third packet to the station.

00:03:53: DOT11->Received uniCast MSG D from 00:b0:8c:51:03:27

Receive the RSN fourth response packet of the station.

2. The debugging of power saving mode

The following debugging switches need to be enabled:

debug dot11radio pro pm

debug dot11radio pro pspoll

debug dot11radio pro datanull

The process of AP buffering the packers of the station in the power saving mode and TIM advertising:

ROUTER#ping 192.168.119.40

The station is already in the power saving mode, so it is necessary to send packets from the AP to the station actively, buffer them and use the TIM advertising**:**

Press key (ctrl + shift + 6) interrupt it.

Sending 5, 76-byte ICMP Echos to 192.168.119.40 , timeout is 2 seconds:

00:11:57: DOT11->Enqueue to Sta's PM Queue

The station is in the power saving state, so the packets sent to the station is buffered in the PM queue.

00:11:57: DOT11->enough space in Sta's PM Queue

The PM buffer queue still has space.

00:11:57: DOT11->Started to SET AID 5. Byte = 0, bit = 5 (oldStart = 0, oldStop=1)

Set the fields from AID 5 to TIM of the station, so as to inform the station that there are packets for it via beacon.

00:11:57: DOT11->Bit 5 set in byte 0 (newStart=0 newStop = 1)

00:11:58: DOT11->PSPOLL: from 00:b0:8c:51:03:27 to 02:e0:4c:fb:76:a7

After receiving the beacon advertisement, the station sends the pspoll packets to require receiving the buffered data.

00:11:58: DOT11->PsPoll Recv Start

00:11:58: DOT11->PmFlush Start:ONE,SEND

Send one packet in the PM buffer queue at once.

00:11:58: DOT11->Sta:00:b0:8c:51:03:27

The destination station is 00:b0:8c:51:03:27.

00:11:58: DOT11->Packet Send Start

00:11:58: DOT11->Send to Driver Start

00:11:58: DOT11->Send to Driver End

00:11:58: DOT11->Packet Send End

Sending packets is complete.

00:11:58: DOT11->No More Packets In Queue

The PM buffer queue of the station is empty.

00:11:58: DOT11->Started to CLEAR AID 5. Byte = 0, bit = 5 (oldStart = 0, oldStop=1)

Clear up the AID 5 of the TIM field and inform the station that there is no buffered packet.

00:11:58: DOT11->Byte 0 after clear Bit 5 is zero(oldStart=0 oldStop=1)

00:11:58: DOT11->Bit 5 clear in byte 0 (newStart=0 newStop=1)

The process of converting the power saving state of the station:

00:31:30: DOT11->DATA-NULL: from 00:b0:8c:51:03:27 to 02:e0:4c:fb:76:a7

Receive the datanull packet from the station.

00:31:30: DOT11->DataNull Recv Start

00:31:30: DOT11->PM from FALSE to TRUE

The PM information in the datanull packet means that the station changes from the normal state to the power saving state.

00:31:51: DOT11->DataNull Recv End

Here, the station pings the wireless sub interface **actively, so the station actively changes to the normal state for communicating.**

00:31:48: DOT11->PM from TRUE to FALSE

Receive the ping packet from the station and the PM field in the packet means that the status changes to normal.

00:31:48: DOT11->PmFlush Start:ALL,SEND

The power saving state of the station changes **to normal, so it is necessary to send all buffered packets to the station.**

00:31:48: DOT11->Sta:00:b0:8c:51:03:27

00:31:48: DOT11->No packets in queue

The buffer queue is already empty.

00:31:48: DOT11->Started to CLEAR AID 5. Byte = 0, bit = 5 (oldStart = 0, oldStop=1)

00:31:48: DOT11->Bit 5 already cleared in byte 0 (oldStart=0 oldStop=1)

There are no buffered packets of the station, so modify the AID of the TIM field.

00:31:51: DOT11->DATA-NULL: from 00:b0:8c:51:03:27 to 02:e0:4c:fb:76:a7

Receive the datanull packets from the station (because there is no communication for a period of time, the station enters the power saving state.)

00:31:51: DOT11->DataNull Recv Start

00:31:51: DOT11->PM from FALSE to TRUE

The PM information in the datanull packet means **that the station changes from the normal state to the power saving state.**

00:31:51: DOT11->DataNull Recv End

Wireless Security Profile Configuration

Main contents:

- Overview
- Basic commands of wireless security profile
- Application instance of wireless security profile
- Monitoring and debugging of wireless security profile

Overview

Wireless security profile means to configure the authentication, encryption and password of the wireless security to one profile and then bind the profile to any virtual AP. One virtual AP can only be bound to one security profile, but multiple virtual APs can be bound to one security profile. After the security profile is bound to the virtual AP, it cannot be modified, but should be un-bound first.

Basic Commands

Command	Description	Configuration Mode
ssid-security-profile *name*	Create one wireless security profile and enter the security profile configuration mode	**config** **config-dot11radio0-ssid-xxx** **config-ssid-secprofile-xxx**

authpol {opensystem|sharekey|psk|802.1x}	Set the authentication policy	**config-ssid-secprofile-xxx**
ciphpol {none | wep40 | wep104 | aes | tkip}	Set the encryption policy	**config-ssid-secprofile-xxx**
secpol {none | wep | wpa1 | wpa2}	Set the security policy	**config-ssid-secprofile-xxx**

Note

The command description with * means that the command has the configuration instance to describe.

- **ssid-security-profile**

The command is used to create one new security profile or enter the configuration mode of the existing security profile.

ssid-security-profile *name*

no ssid-security-profile *name*

Syntax	Description
ssid-security-profile *name*	Create one new security profile or enter the configuration mode of the existing security profile
no ssid-security-profile *name*	Delete the existing security profile

Default status: none

- **authpol**

The command is used to set the authentication policy.

authpol {opensystem|sharekey|psk|802.1x}

Syntax	Description
opensystem	Set the 802.11 basic authentication as open; no extended authentication mode
sharekey	Set the 802.11 basic authentication as share; no extended authentication mode
psk ascii *string*	Set the 802.11 basic authentication as open and the extended authentication mode is PSK; set the key with a length of 8-63 bytes.
psk hex *hex-string*	Set the 802.11 basic authentication as open and the extended authentication mode is PSK; set the hex number of the key with a length of 64 characters (that is, 32-byte hex number)
802.1x default 802.1x *name*	Set the 802.11 basic authentication as open and the extended authentication mode is 802.1x; set the 802.1x authentication server list name (by default, it is default).

Default status: opensystem

- **ciphpol**

The command is used to set the encryption policy.

ciphpol {none | wep40 | wep104 | aes | tkip}

Syntax	Description
none	Set no encryption policy
wep40 key-slot *1-4* key hex *hex-string*	Set the encryption policy as wep, use the 40-bit key and set the hex number of the key index and key, with a length of 10 characters (that is, 5-byte hex number)
wep40 key-slot *1-4* key ascii *string*	Set the encryption policy as wep, use the 40-bit key and set the ascii character string of the key index and key, with a length of 5 characters (that is, 5-byte hex number)
wep104 key-slot *1-4* key hex *hex-string*	Set the encryption policy as wep, use the 104-bit key and set the hex number of the key index and key, with a length of 26 characters (that is, 13-byte hex number)
wep104 key-slot *1-4* key ascii *string*	Set the encryption policy as wep, use the 104-bit key and set the ascii character string of the key index and key, with a length of 13 characters (that is, 13-byte hex number)
tkip	Set the encryption policy as TKIP (only WPA1 and WPA2 can set the encryption policy)
aes	Set the encryption policy as AES (that is, CCMP; only WPA1 and WPA2 can set the encryption policy)

Default status: none

Note

Encryption policy affects the maximum number of the associated stations of the wireless interface. If the encryption policy is TKIP, one station occupies two resources. Therefore, the wireless interface can be associated with 56 stations at most. If all associated stations use TKIP, the maximum number of the associated stations of the wireless interface changes to 28.

- **secpol**

The command is used to set the security policy.

secpol {none | wep | wpa1 | wpa2}

Syntax	Description
none	Set non security policy
wep	Set the security policy as WEP
wpa1	Set the security policy as WPA1
wpa2	Set the security policy as WPA2

Default status: none

Application Instance

Application Instance 1

There are the following typical wireless security profiles:

- **WEP**

The configuration of the security profile:

Syntax	Description
secpol wep	Set the security policy as wep
authpol {opensystem | sharekey}	Set the authentication policy as opensystem or sharekey
ciphpol {wep40 | wep104} **key-slot** *1-4* **key** {ascii | hex} *string*	Set the encryption policy as wep40 or wep104

- **WPA1-PSK**

The configuration of the security profile:

Syntax	Description
secpol wpa1	Set the security policy as wpa1
authpol psk {ascii | hex} *string*	Set the authentication policy as PSK and set the key value
ciphpol {tkip | aes}	Set the encryption policy as TKIP or AES

- **WPA1-EAP**

The configuration of the security profile:

Syntax	Description

secpol wpa1	Set the security policy as wpa1
authpol 802.1x *name*	Set the authentication policy as 802.1x and set the authentication server list name
ciphpol {tkip | aes}	Set the encryption policy as TKIP or AES

- **WPA2-PSK**

The configuration of the security profile:

Syntax	Description
secpol wpa2	Set the security policy as wpa2
authpol psk {ascii | hex} *string*	Set the authentication policy as PSK and set the key value
ciphpol {tkip | aes}	Set the encryption policy as TKIP or AES

- **WPA2-EAP**

The configuration of the security profile:

Syntax	Description
secpol wpa2	Set the security policy as wpa2
authpol 802.1x *name*	Set the authentication policy as 802.1x and set the authentication server list name
ciphpol {tkip | aes}	Set the encryption policy as TKIP or AES

Monitoring and Debugging

Monitoring Command

Command	Description
show ssid-security-profile *name*	Display the contents of the security profile

Monitoring Command Instance

router# **show ssid-security-profile wpa2**

Displayed result:

ssid-security-profile wpa2

secpol wpa2

authpol psk ascii abcdefgh

ciphpol aes

Description and analysis:

The displayed result includes the security policy, authentication policy and encryption of the security profile.

WLAN Typical Configuration

Command	Description
router#**configure terminal**	Enter global configuration mode
router(config)#**ssid-security-profile wpa2**	Create the security profile wpa2 and enter the security profile configuration mode
router(config-ssid-secprofile-wpa2)#**secpol wpa2**	Set the security policy as wpa2
router(config-ssid-secprofile-wpa2)#**authpol psk ascii 12345678**	Set the authentication policy as psk and configure the key value
router(config-ssid-secprofile-wpa2)#**ciphpol aes**	Set the encryption policy as aes
router(config-ssid-secprofile-wpa2)#**exit**	Return to the global configuration mode
router(config)#**int dot11radio 0**	Enter the wireless interface configuration mode
router(config-if-dot11radio0)#**ssid test**	Create one virtual AP, whose SSID is test, and enter the SSID configuration mode
router(config-dot11radio0-ssid-test)#**security wpa2**	Bind the security profile wpa2 to the virtual AP
router(config-dot11radio0-ssid-test)#**vlan 1**	Set the VLAN ID of the virtual AP as 1, corresponding to the later wireless sub interface
router(config-dot11radio0-ssid-test)#**exit**	Return to the wireless interface configuration mode
router(config-if-dot11radio0)#**int dot11radio 0.1**	Create the wireless sub interface dot11radio0.1 and enter the wireless sub interface configuration mode
router(config-if-dot11radio0.1)#**encapsulation dot1q 1**	Configure the VLAN ID of the wireless sub interface as 1, corresponding to the

	VLAN ID of the previous virtual AP
router(config-if-dot11radio0.1)#**ip address 192.168.1.1 255.255.255.0**	Configure the IP address of the wireless sub interface
router(config-if-dot11radio0.1)#**exit**	Return to the global configuration mode; up to now, the WLAN configuration is complete, but WLAN should cooperate with DHCP to complete the access function, so the following describe the DHCP configuration.
router(config)#**ip dhcp pool wlan**	Create the DHCP pool named wlan
router(dhcp-config)#**range 192.168.1.100 192.168.1.200 255.255.255.0**	Configure the distributable IP address pool of DHCP
router(dhcp-config)#**default-router 192.168.1.1**	Configure the default gateway distributed by DHCP
router(dhcp-config)#**dns-server 61.139.2.69**	Configure the DNS server distributed by DHCP

Software & Hardware Version

Hardware version: MP1800 SERIES H020

Software version: rp8-i-6.1.XX(RL09-70).bin