Content

Chapter 1 RFPing

1.1 Introduction to RFPing

For monitoring the wireless link communication quality between the AP and the associated client, the system administrator may need to get the wireless link connection information such as signal strength, packets retransmissions, RTT (Round-trip Time) and etc. We develop the RFping for monitoring the wireless link communication quality between the wireless terminals. This function can issue the link monitoring command to AP on the AC to make the AP send the empty data frame to the client with all the rates which are supported by that appointed client. And then the AP collects the signal strength of the response packets and the average time and sends then to AC.

1.2 Basic RFPing Configuration

1) Enable the RFPing function

Command	Explanation
Admin Mode	
wireless link-test <client-MAC> (count <1-100>|) (timeout <1000-5000>|)	Enable the RFPing function. <client-MAC>: the mac address of client is needed to be tested and only the associated wireless clients are allowed being tested. count <1-100>: the number of the ping packets that the radio interface sends with each kind of rate. timeout <1000-5000>: the maximum timeout value that the radio interface waits the respond of ping packet, the unit is ms.

2) Disable the RFPing function

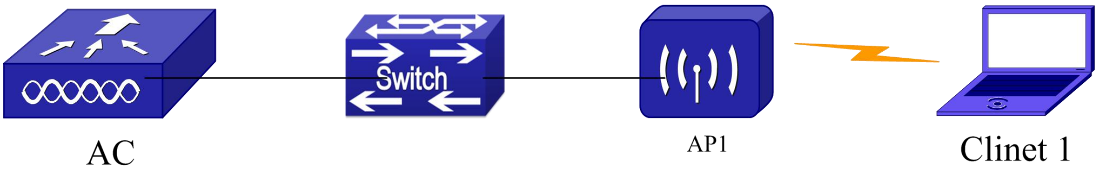
Command	Explanation
Admin Mode	
ctrl+c	Disable the RFPing function to stop the link testing.

3) RFPing debugging

Command	Explanation
Admin Mode	

debug wireless link-test msg **no debug wireless link-test msg**	Enable/disable the RFPing debugging, the communication and information exchange can be seen between ac and ap including issuing commands, reporting information and stopping testing message.

1.3 RFPing Example



Create the environment. AC is connected to AP through the switch or poe, AP is managed successfully. Client1 is associated with ap1.

Basic configuration of AC:

```
AC#wireless link-test e0-46-9a-b1-fa-ef count 5 timeout 3000
```

The client is associated with ap1 and the client is associated successfully on ac. Configure the number of sending packets of each kind of client rate as 5 and configure the timeout value as 3000ms. Click “enter” to start the test and the result is as below:

```
AC#wireless link-test e0-46-9a-b1-fa-ef count 5 timeout 3000
Testing link to client e0-46-9a-b1-fa-ef, press CTRL_C to break......
                              link Status
 RTT:Round trip time
-------------------------------------------------------------------------
 Client MAC Address:e0-46-9a-b1-fa-ef
-------------------------------------------------------------------------
 No./MCS    Rate(Mbps)    Txcnt    RxCnt    RSSI    Retries    RTT(ms)
-------------------------------------------------------------------------
       6            12        5        5      54          0          0
       7            18        5        5      53          0          0
       8            24        5        5      53          0          0
       9            36        5        5      53          0          0
      10            48        5        5      53          0          0
      11            54        5        5      52          0          0
    MCS-0          6.5        5        5      52          0          0
    MCS-1           13        5        5      53          0          0
    MCS-2         19.5        5        5      53          0          0
    MCS-3           26        5        5      53          0          0
```

```
   MCS-4          39        5        5      53         0         0
   MCS-5          52        5        5      53         0         0
   MCS-6        58.5        5        5      53         0         0
   MCS-7          65        5        5      53         0         0
   MCS-8          13        5        5      53         0         0
   MCS-9          26        5        5      53         0         0
  MCS-10          39        5        5      52         0         0
  MCS-11          52        5        5      52         0         0
  MCS-12          78        5        5      52         0         0
  MCS-13         104        5        5      52         0         0
  MCS-14         117        5        5      52         0         0
  MCS-15         130        5        5      52         0         0
No more Rate, link-test complete!
AC#
```

1.4 RFPing Troubleshooting

☞ In the test, there may be the situation that the configured radio mode is bandwidth of 40M, GI=400, but the bandwidth is shown as 20M, GI=800 in the test rate. The reason is that the high rate is compatible to the low rate because of the link quality problems in the consultation between the client and ap. And it is consulted as the low rate.

☞ If the link test is still running after the sudden power off of client, the reason is that the client on the ap is not deleted.

Chapter 2 Wireless Packet Capture

2.1 Introduction to the Wireless Packet Capture

In the actual network, there is often the problem about single interference and packet collision. These problems are hard to be located through the debug or show information on the wireless device. For locating these problems quickly, the AP can be as the packet capturing tool to monitor, capture and record the wireless packets. The captured packets will be saved in the file whose type is ".pcap". The administrator can locate the problems through the packets. As shown as below, enable the wireless packet capture function on capture AP to capture the wireless packets including other APs, Rouge AP and client. At the same time, the wired packets passing through the capture AP can be also captured through configuring the wired port.

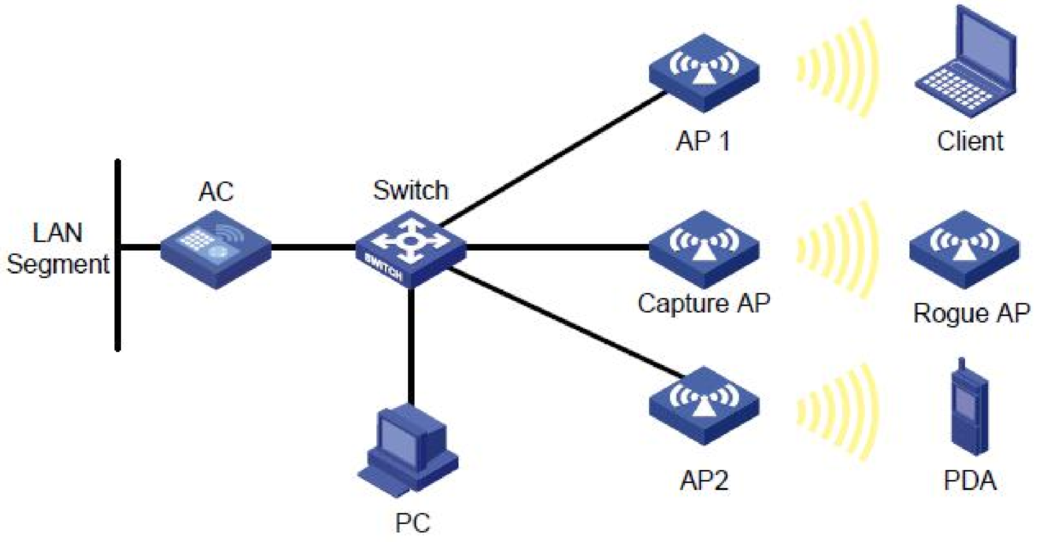
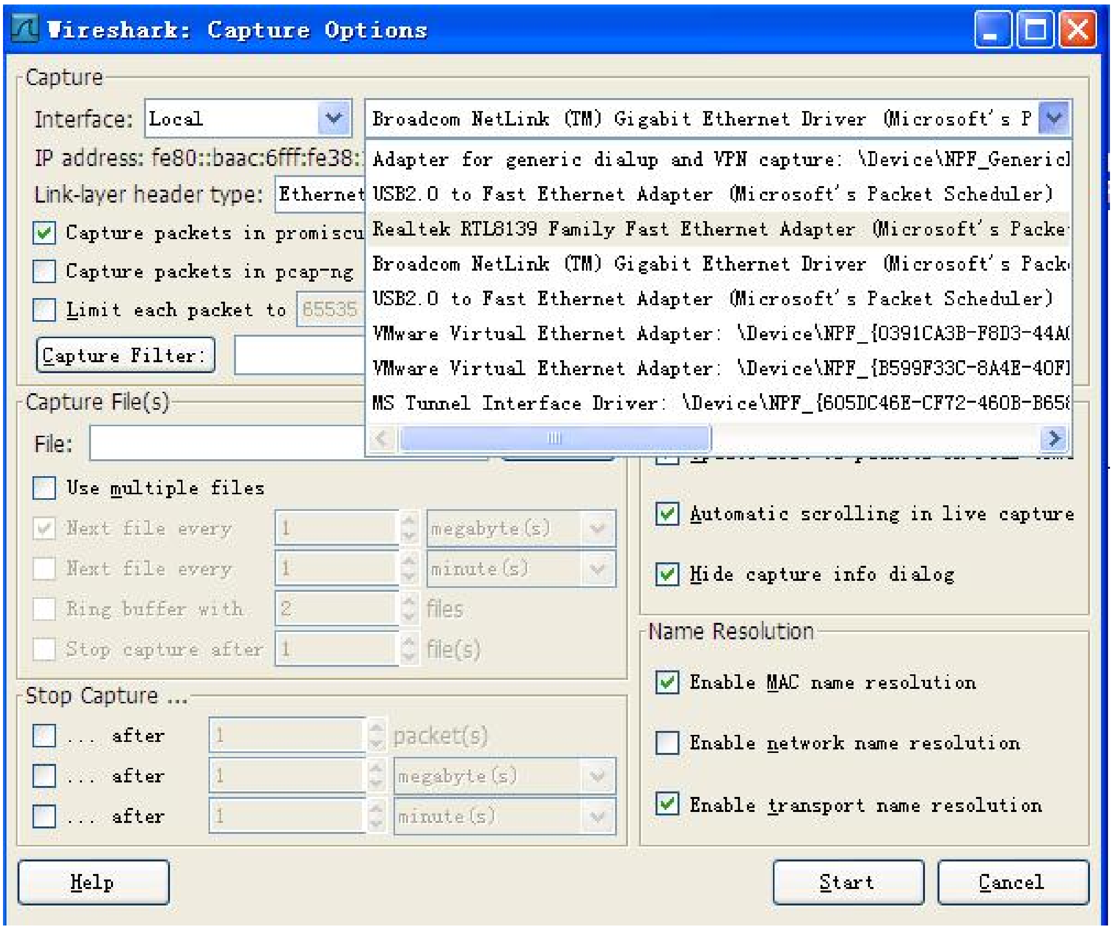


Fig 2- 1 wireless packet capture network

The wireless packet capture process includes command enabling, packet capturing, packet transferring, packet dealing. The wireless packet capture is under two modes: file mode and remote mode.

Under the file mode, the administrator can configure the parameters about the wireless packet capture module on AC. AC sends the commands and parameters to capture AP and the wireless packet capture function is enabled. The captured packets are saved in one file of capture AP. After the capture AP captured the packet, it will send the packet with the frame of pacp file to AC. The administrator downloads the file to local and uses some tools to analyze the packet such as Wireshark and OmniPeek.

Under the remote mode, the captured packet can be redirected to the external PC which is running the Wireshark. The remote wireless packet capture is applicable to work together with the Wireshark tool of Windows. One wireless packet capture server is running on the AP and sends the captured packet to Wireshark through the TCP connection. When using the remote mode, the Capture AP does not save any captured data to local file system. The capture AP uses the parameters issued by AC to start the packet capturing. And it will send the captured data to the monitoring software; the common monitoring software is Wireshark. The capture AP cannot save the captured data. Enable the monitoring software on PC, such as Wireshark (version 1.6.0.37592). Enable the software, choose Capture -> Option, and then the dialog is as below:



Wireshark: Capture Options

Capture

Interface: Local

Broadcom NetLink (TM) Gigabit Ethernet Driver (Microsoft's P

IP address: fe80::baac:6fff:fe38:

Link-layer header type: Ethernet

☑ Capture packets in promiscu

☐ Capture packets in pcap-ng

☐ Limit each packet to 65535

Capture File(s)

File:

☐ Use multiple files

☑ Next file every 1 megabyte(s)

☐ Next file every 1 minute(s)

☐ Ring buffer with 2 files

☐ Stop capture after 1 file(s)

Stop Capture ...

☐ ... after 1 packet(s)

☐ ... after 1 megabyte(s)

☐ ... after 1 minute(s)

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

Name Resolution

☑ Enable MAC name resolution

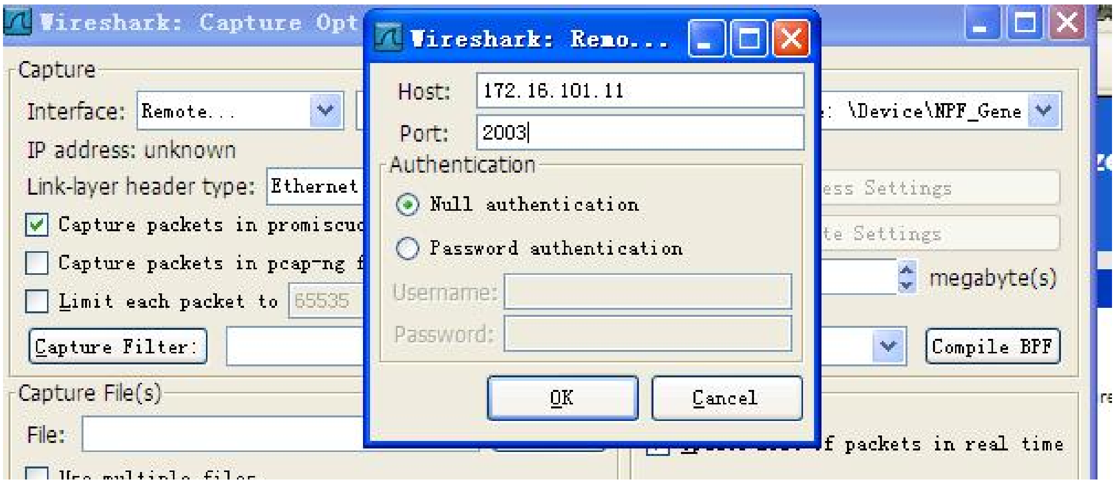
☐ Enable network name resolution

☑ Enable transport name resolution

Adapter for generic dialup and VPN capture: \Device\NPF_Generic
USB2.0 to Fast Ethernet Adapter (Microsoft's Packet Scheduler)
Realtek RTL8139 Family Fast Ethernet Adapter (Microsoft's Packe
Broadcom NetLink (TM) Gigabit Ethernet Driver (Microsoft's Pack
USB2.0 to Fast Ethernet Adapter (Microsoft's Packet Scheduler)
VMware Virtual Ethernet Adapter: \Device\NPF_{0391CA3B-F8D3-44A
VMware Virtual Ethernet Adapter: \Device\NPF_{B599F33C-8A4E-40F
MS Tunnel Interface Driver: \Device\NPF_{605DC46E-CF72-460B-B65
Capture Filter:
Help
Start
Cancel

Fig 2- 2 options page

The dialog after choosing the interface as remote is as below:



Capture

Interface: Remote...

IP address: unknown

Link-layer header type: Ethernet

☑ Capture packets in promiscuo

☐ Capture packets in pcap-ng f

☐ Limit each packet to 65535

Capture Filter:

Capture File(s)

File:

Host: 172.16.101.11

Port: 2003

Authentication

● Null authentication

○ Password authentication

Username:

Password:

Fig 2-3 the page after choosing the remote mode

The capture AP sends the captured data to Wireshark directly. For Wireshark, the IP address of capture AP should be input in Host and they should communicate each other. Because the configured port of the remote wireless packet capture is 2003, 2003 should be input in Port. After configured the above parameters, click OK to go back to the dialog of options page. Choose the wireless packet capture type from the drop-down list of interface and click Start button, and then the capturing result can be shown on Wireshark.

2.2 Wireless Packet Capture Configuration

The configuration task list of wireless packet capture is as below:

1. Configure the packet capturing mode
2. Configure the parameters of packet capturing
    1) Configure the promiscuous mode
    2) Configure the duration of packet capturing under the file mode
    3) Configure the number of captured packets under the file mode
    4) Configure the mac address filtration condition
3. Control the AP to enable the wireless packet capture

1. Configure the packet capturing mode

Command	Explanation
Admin Mode	
wireless capture mode {file | remote [<*2002-2006*>]} **no wireless capture mode**	Configure the wireless packet capturing mode of AP. The no command clears this configuration.

2. Configure the parameters of packet capturing

1) Configure the promiscuous mode

Command	Explanation
Admin Mode	
wireless capture promiscuous-mode **no wireless capture promiscuous-mode**	Enable the promiscuous mode of packet capturing. The no command disables this mode.

2) Configure the duration of packet capturing under the file mode

Command	Explanation
Admin Mode	
wireless capture duration <*60-3600*> **no wireless capture duration**	Configure the duration of packet capturing under the file capturing mode. The no command recovers it to be the default value.

3) Configure the number of captured packets under the file mode

Command	Explanation
Admin Mode	
wireless capture packet-num <*1-10000*> **no wireless capture packet-num**	Under the file capturing mode, configure the maximum value of the captured packets. The no command recovers it to be the default value.

4) Configure the mac address filtration condition

Command	Explanation
Admin Mode	
wireless capture filter-mac <*macaddr*> **no wireless capture filter-mac**	Configure the filtration conditions of MAC address of the packet capturing. The no command clears the configuration.

3. Control the AP to enable the wireless packet capture

Command	Explanation
Admin Mode	
wireless capture start ap <*macaddr*>	Configure the MAC address of the capture

interface {radio <1|2>|ethernet }	AP and the interface of the packet capturing. At the same time, control the AP to capture the packets.

2.3 Wireless Packet Capture Examples

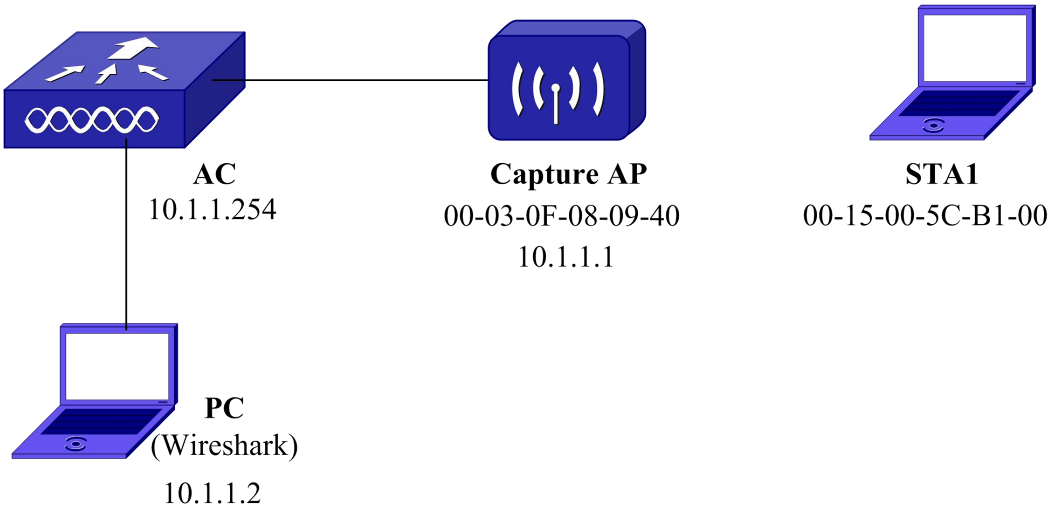


Fig 2-4 topology of wireless packet capture

Introduction:

In the above figure, the Capture AP is managed by AC and it is in the same network segment with the PC whose address is 10.1.1.2. STA1 is associated with capture AP and it can control the capture AP to capture packets through AC.

Application 1: Adopt the file mode and control the capture AP to capture all the packets including STA1 mac address in radio1. Configure the duration as 2min and configure the packet number as the default value.

Configure the file mode.

```
AC#wireless capture mode file
```

Enable the promiscuous mode.

```
AC#wireless capture promiscuous-mode
```

Configure the duration of capturing as 120s.

```
AC#wireless capture duration 120
```

Configure the filtration STA1 mac address condition.

```
AC#wireless capture filter-mac 00-15-00-5c-b1-00
```

Configure the capture AP to capture in radio1.

```
AC#wireless capture start ap 00-03-0f-08-09-40 interface radio 1
```

View the capturing status after starting the capturing.

```
AC#show wireless capture status
wireless capture status........................ Enable
Capture ap MAC................................ 00-03-0f-08-09-40
wireless capture running status................ wireless capture in progress
wireless download status....................... -----
wireless capture mode.......................... file
wireless capture interface..................... radio 1
wireless capture duration...................... 120
wireless capture packet number................. 10000
wireless capture filter mac.................... 00-15-00-5c-b1-00
wireless capture promiscuous mode.............. Enable
```

The packet capturing can be stopped manually; it can also stop automatically after 120s or after the packets number achieves 10000. AP will upload the file to AC after stopping the capturing and the file name is file_capture.pcap. the file can be uploaded to PC later and the Wireshark and Omnipeek can be used for analysis.

Application 2: Adopt the remote mode and control the capture AP to capture the wired packets.

```
AC#wireless capture mode remote 2003
```

In remote mode, the capture duration and packet numbers parameters will be ignored by Capture AP.

```
AC#wireless capture start ap   00-03-0f-09-51-30 interface ethernet
AC#show wireless capture status
wireless capture status........................ Enable
Capture ap MAC................................ 00-03-0f-08-09-40
wireless capture running status................ wireless capture in progress
wireless download status....................... -----
wireless capture mode.......................... remote
Remote port................................... 2003
wireless capture interface..................... ethernet
wireless capture duration...................... 3600
wireless capture packet number................. 10000
wireless capture filter mac.................... -----
wireless capture promiscuous mode.............. Enable
```

After started the packet capturing, enable the remote port of 10.1.1.1:2003 on Wireshark on PC, and the captured packets can be shown.

2.4 Wireless Packet Capture Troubleshooting

When there are problems in using the AP capturing function, please check the following reasons:

- ☞ Please ensure the promiscuous mode is enabled when capturing the packets of other AP or client interaction.
- ☞ Please ensure the capture AP is in the same channel with the AP or client when capturing the packets of the AP or client interaction.
- ☞ In the file mode, please ensure there are enough flash space on AC for saving the capturing files (AP can limit the number of packets according to the space. If the space is too small, the captured packets will be very few.)
- ☞ In wireless packet capture, if the packet is not captured, please ensure the radio of capture AP is not down.

Chapter 3 SMTP

3.1 Introduction to SMTP

With the further development of technology, there are many mobile email terminals currently and more and more people can send or receive emails through the mobile email terminals.

We can send the syslog of the device to the network administrator at the same time. Then the administrator can view the operation of the device any time and anywhere. For the unusual circumstance, they can discover and solve it in time to reduce the loss. So the SMTP function has significance for the network maintaining.

Except for the syslog information, other important information can be also sent to the administrator through the mail. The smtp function provides the common interface for sending mails on AC, any information can notice the administrator according to the mails through the interface.

3.2 SMTP Configuration

The basic configuration task list of SMTP function is as below:

1. Enable the smtp function
2. Create and configure the receiver rules
3. Configure the parameters of smtp server
4. Show the configuration of smtp function
5. Test the configuration of smtp

1. Enable/disable the smtp function

Command	Explanation
Global Mode	
smtp **no smtp**	Enter into the SMTP configuration mode and enable the global SMTP on-off. The no command disables this on-off and does not provide the function of sending emails any more.

2. Create/delete and configure the receiver rules

Command	Explanation
smtp Configuration Mode	

receiver rule <rule-id> **no receiver rule <rule-id>**	Create the SMTP receiver rule and enter into the SMTP receiver rule configuration mode. The no command deletes the SMTP receiver rule.
smtp Receiver Rule Configuration Mode	
receiver description <desc> **no receiver description**	Configure the description information for the current receiver rule. The no command recovers to be default.
receiver address <email-addr> **no receiver address <email-addr>**	Add the receiver in the current receiver rule. The no command deletes the configured receiver.
receiver severity [critical| warnings| informational |dubugging] **no receiver severity**	Configure the severity level of the SMTP receiver rule. Only when the mail's severity level is the configured level or higher than it, this mail needs to be sent to the configured receiver in the rule. The no command recovers to be the default value of critical.
receiver time-range from <start-time> to <end-time> [monday| tuesday| wednesday| thursday| friday| saturday| sunday| weekend| weekday| everyday] **no receiver time-range [monday| tuesday| wednesday| thursday| friday| saturday| sunday| weekend| weekday| everyday]**	Configure the time-range of receiving mails for the receiver in the current rule. Out of the time-range, AC will not send mails to receiver. The no command recovers to be default.

3. Configure the parameters of smtp server

Command	Explanation
smtp Configuration Mode	
smtp server ipv4 <ipaddr> [port <port-num>] **no smtp server**	Configure or update the address and port of the smtp serverty; the no command deletes the configuration.
smtp sender address <email-addr> **no smtp sender address**	Appoint the sender. The no command deletes the sender.
smtp server authentication username <username> password <password> **no smtp server authentication**	Configure the authentication user name and password for smtp server. The no command recovers to be default.

smtp server source-ipv4 <ipaddr> **no smtp server source-ipv4**	Appoint a source IP address for AC. AC will adopt this IP address as the source IP to create TCP connection to the server. The no command deletes the source IP address.

4. Show the configuration of smtp function

Command	Explanation
Admin Mode	
show smtp status	Show the configuration of smtp including smtp status, server address, port number, server connection status, sender's address, source IP address of sender, server authentication user name and password.
show smtp receiver rule [<rule-id>] status	Show the configuration of smtp receiver rule.

5. Test the configuration of smtp

Command	Explanation
Admin Mode	
smtp test-mail-send	Test if the SMTP can send the mail to receiver successfully according to the current configuration. The theme and content of the mail are both "test".

3.3 SMTP Examples

Typical case:

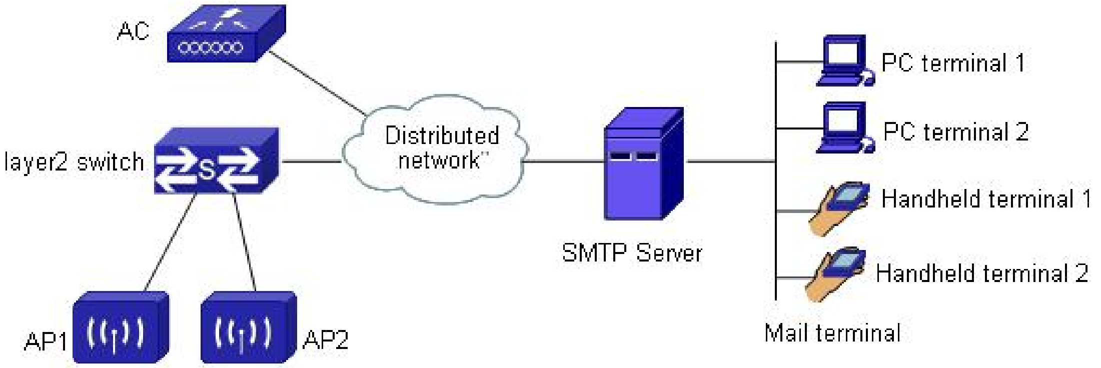


Fig 4- 1 typical case of smtp

As shown above, AP1 and AP2 are connected to the network through the layer2 switch and managed by AC; they provide the access server for the clients. There is a mail server, it sends the mail. For the local user, the mails can be sent to the user; for the non-local user, the mails should be relayed in the mail server that the user is in (the relayed part is not shown in the above figure, AC is the client that needs to achieve the smtp, the server and relaying server are not cared.). the mail terminal can show the mails through POP3, IMAP protocols.

AC is the smtp client. If there are some unusual events in the network, for example, AP is offline; user can send a mail to the administrator through the smtp server in the network to notice the PC or handheld terminals. The administrator can check the mail that AC sent to it through the mail terminal reminder, and then know the unusual event and deal with it to reduce the loss.

The configuration is as below:

Parameters of smtp server:

SMTP server type: smtp server of Windows2003
SMTP server address: 192.168.1.200
SMTP server port: 25
Supported authentication: LOGIN
Authentication user name: admin@domain.com
Authentication password: domain_123456

Requirements of sending mails:

A. The mails should be sent through the sender of admin@domain.com.
B. The ordinary administrator of zhangsan@domain.com needs to monitor the network status all day and focus on the network events with the level of warnings and above it. The administrator can handle the serious events in time.
C. The department manager of lisi@domain.com only focuses on the network events with the level of critical and above it. They can receive the mails from 8 am to 11 pm and they do not want to receive the mails when they are at rest.

The configuration of AC smtp is as below:

Enable the smtp function and enter into the smtp configuration mode.

```
AC(config)#smtp
```

Configure the smtp server address and port: 192.168.1.200:25.

```
AC(config-smtp)#smtp server ipv4 192.168.1.200 port 25
```

Configure the parameters of smtp server authentication: user name is admin@domain.com; password is domain_123456.

```
AC(config-smtp)#smtp server authentication username admin@domain.com password
```

```
domain_123456
```

Configure the sender address.

```
AC(config-smtp)#smtp sender address admin@domain.com
```

Configure a receiver rule and the receivers in this rule monitor the network events with the level of warning and above it all day.

```
AC(config-smtp)#receiver rule 1
```

Configure the description of this rule: general staff - any time receive warnning email.

```
AC(config-smtp-rule)#receiver description general staff - any time receive warnning email
```

Configure the receiver address in the rule as zhangsan@domain.com.

```
AC(config-smtp-rule)#receiver address zhangsan@domain.com
```

Configure the event level that the receiver focuses on.

```
AC(config-smtp-rule)#receiver severity warnings
```

The interval of receiving mails does not need to be configured, they are received all day as default.

The above rule is completely configured and quit the receiver rule configuration mode.

```
AC(config-smtp-rule)#exit
```

Configure another receiver rule, the receiver only focuses on the event with the level of critical and above it and does not receive any mail when he is at rest.

```
AC(config-smtp)#receiver rule 2
```

Configure the description information of this rule: department manager - working time receive critical email

```
AC(config-smtp-rule)#receiver description department manager - working time receive critical email
```

Configure the receiver address in the rule as lisi@domain.com.

```
AC(config-smtp-rule)#receiver address lisi@domain.com
```

Configure the event level that the receiver focuses on.

```
AC(config-smtp-rule)#receiver severity critical
```

Configure the interval that the receiver receives the mails.

```
AC(config-smtp-rule)#receiver time-range from 8:00 to 23:00 everyday
```

The configuration is completed.

3.4 SMTP Troubleshooting

Please adopt the following steps when there is problem in using SMTP function:

- Input the command of **smtp test-mail-send** under the admin mode and judge the problem according to the printed information of the console controller.
- Check if the smtp receiver mail is configured correctly.
- Check if the smtp receiver time is configured correctly.

- ☞ Check if the smtp mail sending level is configured correctly.
- ☞ Check if the AC smtp server address and port configuration are consistent to the server configuration.
- ☞ If the above configurations are all correct, but the mail sending failed, please check if the AC router is configured correctly and can reach the smtp server.

Chapter 4 Local AP Configuration

4.1 Introduction to Local AP Configuration

The wireless cluster management adopts AC+Fit AP mode. AP can be configured and managed on AC. The configuration includes adding AP to Valided AP table, configuring position information of AP, configuring authentication code between AP and AC, appointing files for AP etc.

AP should run the authentication to AC when it gets online. AP is allowed online when the authentication is successful; if the authentication fails, AP cannot get online. There are some methods of AP authentication including mac, none, pass-phrase and serial-num. The method of serial-num means to authenticate based on the serial number of AP. This serial number is carried from factory, and it can be shown through using the command of **get system** under the console mode of AP. When AP sends the serial number to AC in authenticating, AC finds the serial number of that AP in the configuration for comparing, if they are same, the authentication is successful, and otherwise, it fails.

4.2 Basic Local AP Configuration

Local AP task list:

1. Add AP record to Valid AP list
2. Configure position information of AP
3. Configure management mode of AP
4. Configure authentication code between AP and AC
5. Configure AP authentication mode
6. Configure the serial-num of AP on AC
7. Appoint authentication method of AP
8. Configure the management ip address of ap
9. Issue the configuration parameter to the associated AP

1. Add AP record to Valid AP list

Command	Explanation
Wireless Global Mode	
ap database <*macaddr*> **no ap database <*macaddr*>**	Add a log to the table of Valid AP and enter the configuration mode of AP. The no command deletes the appointed AP from the table of Valid AP.

2. Configure position information of AP

Command	Explanation
AP Configuration Mode	
location <*value*> **no location**	Add the position description for AP. The no command deletes the current position information of AP.

3. Configure management mode of AP

Command	Explanation
AP Configuration Mode	
mode {ws-managed | standalone | rogue}	Configure the managed mode for AP. The default managed mode is ws-managed.

4. Configure authentication code between AP and AC

Command	Explanation
AP Configuration Mode	
password plain <*word*> **no password**	Add/cancel code for AP authenticated with AC. The code format is plantext password.
password encrypted **no password**	Appoint a cryptography password for AP.

5. Configure AP authentication mode

Command	Explanation
Wireless Global Mode	
ap authentication {none | mac | pass-phrase}	Configure AP authentication mode
ap authentication serial-num	Configure the authentication method of AP on AC as serial-num.

6. Configure the serial-num of AP on AC

Command	Explanation
AP database Mode	
serial-num **no serial-num**	Configure the serial-num of AP on AC, the no command deletes the serial-num.

7. Appoint authentication method of AP

Command	Explanation
Wireless Global Mode	
ap validation {local | radius}	Designate the authentication for AP adopting local authentication or throughing the server of RADIUS. The default authentication mode is local authentication.

8. Configure the management ip address of ap

Command	Explanation
AP Configuration Mode	

management {ip A.B.C.D/M|ipv6 X:X::X:X/M}
no management {ip|ipv6}
	Configure the management ip address of ap. The no command deletes this ip address.

9. Issue the configuration parameter to the associated AP

Command	Explanation
Admin Mode	
wireless ap eth-parameter apply [macaddr | profile<1-1024>]	Issue the configuration parameter to the associated AP.

4.3 Local AP Configuration Examples

Typical Scenario1:

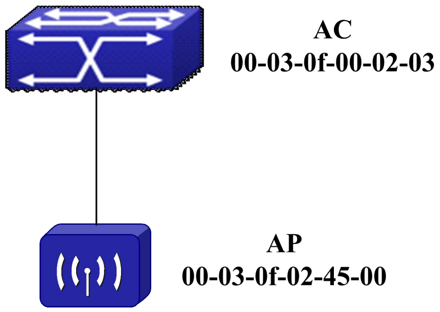


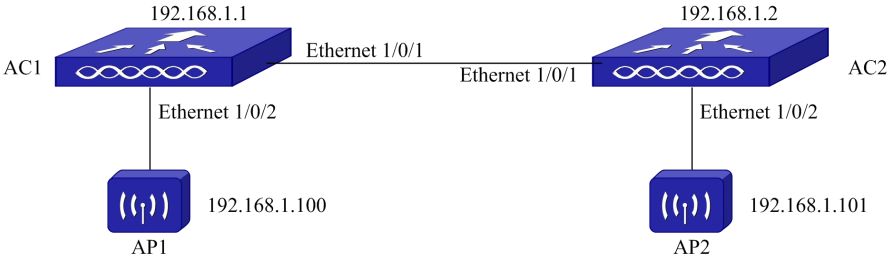
Fig 1-1 Typical scenario of Local AP

As shown in Fig 1-1, configure AP which is associated with AC. Configure position information of AP as “here” and profile id is 2.

The configuration sequence of AC is as below:

```
AC#config
AC(config)#wireless
AC(config-wireless)#ap database 00-03-0f-02-45-00
AC(config-ap)#location here
AC(config-ap)#profile 2
AC(config-ap)#exit
AC(config-wireless)#exit
AC(config)#
```

Typical Scenario2:



AC1 manages AP1. The cluster is created between AC1 and AC2. As default, the TLS protocol connection is adopted between AC1 and AC2, and between AC1 and AP1. The following configuration is for the serial-num authentication of AP1:

First, enable the serial-num authentication of AP on AC1:

```
AC#config
AC(config)#wireless
AC(config-wireless)# ap authentication serial-num
```

Ensure to adopt the TCP connection, there will be the prompt that it will cause network disconnection:

View the authentication method of the current AP:

```
AC#show wireless

Administrative Mode........................... Enable
Operational Status............................ Enabled
WS IP Address................................. 172.20.32.2
WS IPv6 Address............................... -----
WS Auto IP Assign Mode ....................... Disable
WS Switch Static IP .......................... 172.20.32.2
WS Switch Static IPv6 ........................ -----
AP Authentication Mode........................ Serial-Num
AP Auto Upgrade Mode.......................... Disable
AP Validation Method.......................... Local
Client Roam Timeout (secs).................... 30
Country Code.................................. CN - China
```

```
Peer Group ID................................. 1
Cluster Priority.............................. 1
Cluster Controller............................ Yes
Cluster Controller IP Address................. 172.20.32.2
Cluster Controller IPv6 Address................ -----
Wireless System IP control port................ 57775
Wireless Management Protocol................... TCP
AP Client QoS Mode............................ Enable
AP Igmp Snooping Mode.......................... Disable
Switch Provisioning........................... Enable
Network Mutual Authentication Mode............. Enable
Unmanaged AP Re-provisioning Mode.............. Enable
Network Mutual Authentication Status........... Not Started
Regenerate X.509 Certificate Status............ Not In Progress
Keep Alive Interval(ms)........................ 10000
Keep Alive Max Count.......................... 3
Force Wifi Compatible.......................... Disable
Statistics Interval(secs)..................... Auto(5)
Rf Scan Report Interval(secs)................. Auto(30)
```

Configure the serial-num of AP1 on AC1. We assume the database of AP1 is 00-01-02-03-04-05, and the serial-num is 112233. The configuration is as below:

```
AC#config
AC(config)#wireless
AC(config-wireless)# ap database 00-01-02-03-04-05
AC(config-ap)#serial-num 112233
```

4.4 Local AP Troubleshooting

- If the configuration for AP is invalid, please check if AP is at managed status. If AP is at managed status, AP should be reset, then the configuration will be effective.
- When there is problem in using the serial number authentication, please check the following reasons:

  (1) Whether the AP has the serial-num. The command of **get system** can be used under the console mode of AP to view the serial-num.

  (2) Wether the serial-num of AP is configured on AC.

  (3) Wether the serial-num of AP authentication is enabled on AC, the default authentication method is mac.

Chapter 5 Enabling and Disabling Wireless Feature

5.1 Introduction to Enabling and Disabling Wireless Feature

Wireless feature allows enabling and disabling functions manually as one important function of controller. In the process of enabling wireless feature, it is a process of the whole WLAN module initialization. It is responsible for applying for resources and enabling the sub functions; the disabling function is responsible for releasing resources and disabling the sub functions.

5.2 Wireless Feature Enabling and Disabling Configuration

Wireless feature enabling and disabling task list is as below:

1. Enter wireless global mode
2. Enable/disable wireless feature of AC
3. Configure automatical appointing IP address function of wireless feature (recommend to configure Loopback interface and layer 3 interface address to ensure the stability of automatic appointed wireless IP address)
4. Bind static IP for wireless feature

1. Enter wireless global mode

Command	Explanation
Global Mode	
wireless	Enter the wireless global mode of AC.

2. Enable/disable wireless feature of AC

Command	Explanation
Wireless Global Mode	
enable **no enable**	Enable/disable the wireless feature on AC.

3. Configure automatical appointing IP address function of wireless feature

(recommend to configure Loopback interface and layer 3 interface address to ensure the stability of automatic appointed wireless IP address)

Command	Explanation
Wireless Global Mode	
auto-ip-assign **no auto-ip-assign**	Enable/disable automatical appointing IP address function of wireless feature.

4. Bind static IP for wireless feature

Command	Explanation
Wireless Global Mode	
static-ip <*ipaddr*> **no static-ip**	Bind IP to the wireless characteristic of AC. The no command deletes the wireless characteristic IP address which is bond in static state.
static-ipv6 <*ipv6addr*> **no static-ipv6**	Bind IPv6 to the wireless characteristic of AC. The no command deletes the wireless characteristic IPv6 address which is bond in static state.

5.3 Wireless Feature Enabling and Disabling Troubleshooting

If it is fail to enable wireless feature of AC, please check if it is wrong with the following reasons:

- ☞ If there is layer3 interface or loopback interface existing on AC.
- ☞ If the layer3 interface or loopback interface of AC is configured IP address correctly.