Troubleshooting MAC-authentication

杨逢君 2006-05-15 发表

Troubleshooting MAC-authentication

(Author：Fengjun Yang)

Revision Records

Revision No.	Revision Date	Revision Content
V1	2006/03/09	
V2	2006/04/23	Supplement R&Ds' solutions for Case 2 &3

Key Words

MAC-authentication;RADIUS

Introduction

MAC-authentication is an alternative to 802.1X that allows network access to devices (such as PCs, especially printers and IP phones) that do not have the 802.1X supplicant capability.

At present, only S3900 series and S5600 series switches can support MAC-authentication in Huawei-3Com.

Switch which supports MAC-authentication initiates authentication session once it detects a new MAC address of a device for the first time.

Two MAC-authentication modes are available:

l MAC address mode: switch sends access-request with the detected MAC address as the username and password to the RADIUS server.

l Fixed mode: switch sends access-request with the preconfigured username and password to the RADIUS server. In this mode, all logon devices share the same username and password.

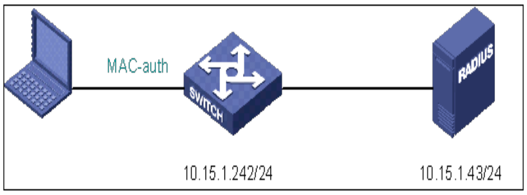
MAC-authentication of fixed mode is not popular because of its low security. So this document only focuses on MAC-authentication of MAC address mode.

Some unforeseen trouble will happen to you just because the configuration of MAC-authentication is as very simple as the one of 802.1X.

This document will help you avoid these trouble by three troubleshooting cases.

Case 1: Failure from laziness

Network Topology



Related Configuration

```
#
radius scheme radius-eps          /* Create a RADIUS scheme */
 server-type standard        /* Set the Supported Type of RADIUS Server */

 primary authentication 10.15.1.43 1812 /* Set IP address and port number of
                                       primary RADIUS authentication & authorization server
*/
 accounting optional   /* Enable the selection of RADIUS accounting option */

 key authentication networld           /* Set RADIUS authentication & authorization
                                                           packet encryption key
*/
 user-name-format without-domain /* Set Username Format Transmitted to
                                                              RADIUS Server */
```

```
#
domain test.networld.co.jp  /* Create an ISP domain */
 scheme radius-scheme radius-eps /* Configure a RADIUS scheme for the
                                                                                  domain */

#
 MAC-authentication  /* Enable MAC-authentication globally */
 MAC-authentication domain test.networld.co.jp   /* Configure the ISP domain used
                                                          by MAC-authentication users */

#
interface Ethernet1/0/1
 MAC-authentication  /* Enable MAC-authentication on a specific port */

#
interface Ethernet1/0/2
 MAC-authentication  /* Enable MAC-authentication on a specific port
*/
#
interface Vlan-interface1
 ip address 10.15.1.242 255.255.255.0        /* Configure IP address for a VLAN
                                                                                  interface
*/
#
 ip route-static 0.0.0.0 0.0.0.0 10.15.1.254 preference 60         /* Configure a default
                                                                                   route */
#
```

Notice: Configuration on RADIUS server is omitted.

Problem

PC access Failed!

Troubleshooting

The results of **debugging MAC-authentication event** and **debugging radius packet** are as follows:

```
*0.1605000 Quidway MACAUTH/8/EVENT:- 1 -Port:0,MAC authentication new MAC is: 0
00f-1fc6-d777
*0.1605095 Quidway MACAUTH/8/EVENT:- 1 -Port:0,MAC authenticaiton: excute MAC_A
ddressLearn...
*0.1605211 Quidway MACAUTH/8/EVENT:- 1 -Port:0,new MAC address 000f-1fc6-d777
*0.1605311 Quidway MACAUTH/8/EVENT:- 1 -Auth:12,Processing  InitTrans!
*0.1605395 Quidway MACAUTH/8/EVENT:- 1 -Auth:12,Processing node CONNECTING...
*0.1605478 Quidway MACAUTH/8/EVENT:- 1 -Port:0,MAC authentication new MAC is: 0
00f-1fc6-d777
*0.1605578 Quidway MACAUTH/8/EVENT:- 1 -Port:0,MAC authenticaiton: excute MAC_A
ddressLearn...
*0.1605695 Quidway MACAUTH/8/EVENT:- 1 -Port:0,new MAC address 000f-1fc6-d777
*0.1605795 Quidway MACAUTH/8/EVENT:- 1 -Auth:12,Processing CONNECTING Trans!
*0.1605878 Quidway RDS/8/DEBUG:- 1 -Recv MSG,[MsgType=Normal auth request Index
= 12, ulParam3=2185876916]
*0.1606012 Quidway RDS/8/DEBUG:- 1 -Send attribute list:
*0.1606078 Quidway RDS/8/DEBUG:- 1 -
[1  User-name                 ] [14] [000f1fc6d777]
*0.1606178 Quidway RDS/8/DEBUG:- 1 -
[2  Password                  ] [18] [7279FFFF432A5D2FFF0EFF43FF43FFFFFFFFC5]
[4  NAS-IP-Address            ] [6 ] [10.15.1.242]
[32 NAS-Identifier            ] [14] [00e0fc59b050]
[5  NAS-Port                  ] [6 ] [268443649]
[61 NAS-Port-Type             ] [6 ] [15]
*0.2769141 NAS RDS/8/DEBUG:- 1 -
[6  Service-Type              ] [6 ] [2]
[7  Framed-Protocol           ] [6 ] [1]
[31 Caller-ID                 ] [16] [303030662D316663362D64373737]
*0.1607195 Quidway RDS/8/DEBUG:- 1 -Send: IP=[10.15.1.43], UserIndex=[12], ID=[12
], RetryTimes=[0], Code=[1], Length=[195]
*0.1607345 Quidway RDS/8/DEBUG:- 1 -Send Raw Pakcet is:
```

```
*0.1607412 Quidway RDS/8/DEBUG:- 1 -
 01 0c 00 fff00 6c 00 00 3a 3d 00 00 2e 72 00 00
 fff3b 00 00 01 0e 30 30 30 66 31 66 63 36 64 37
 37 37 02 12 72 79 ffffff43 2a 5d 2f fff0e fff43
 fff43 ffffff04 06 7f 00 00 01 20 09 51 75 69 64
 77 61 79 05 06 10 01 fff14 57 24 73 6c 6f 74 3d
 30 3b 73 75 62 73 6c 6f 74 3d 30 3b 70 6f 72 74
 3d 32 34 3b 76 6c 61 6e 69 64 3d 32 30 3d 06 00
 00 00 0f 06 06 00 00 00 02 07 06 00 00 00 01 1f
 10 30 30 30 66 2d 31 66 63 36 2d 64 37 37 37 1a
 34 00 00 07 fff1a 06 00 00 00 0c fff07 53 33 39
 30 30 3c 1b 30 2e 30 2e 30 2e 30 20 30 30 3a 30
 66 3a 31 66 3a 63 36 3a 64 37 3a 37 37 3b 06 38
 ffffff5d

*0.1608228 Quidway RDS/8/DEBUG:- 1 -Recv MSG,[MsgType=PKT response Index = 20, u
lParam3=16777343]
*0.1608345 Quidway RDS/8/DEBUG:- 1 -Receive Raw Packet is:
*0.1608428 Quidway RDS/8/DEBUG:- 1 -
 03 0c 00 14 5c fff74 fff07 52 29 fff25 fff20 fff
 ffffffffffff

*0.1608545 Quidway RDS/8/DEBUG:- 1 -Receive:IP=[10.15.1.242],Code=[3],Length=[20]
*0.1608645 Quidway RDS/8/DEBUG:- 1 -NULL
*0.1608695 Quidway RDS/8/DEBUG:- 1 -RejectMsg=[password incorrect ]

*0.1608811 Quidway MACAUTH/8/EVENT:- 1 -Auth:12,Processing CONNECTING Trans!
*0.1608895 Quidway MACAUTH/8/EVENT:- 1 -Auth:12,Processing node FAILURE...
```

From debugging information (red mark), I know that the password which switch sends to RADIUS server and the one which RADIUS server maintains in the database do not match each other.

I just copied the MAC address from the display of ipconfig/all in PC to RADIUS server without all hyphens included. Why?

From debugging information (red mark), I find that username which switch sends to RADIUS server is the MAC address without Caps, but copied MAC address is the one with Caps.

PC can access successfully after modification.

Case 2: Failure from Format of MAC Address

Network Topology

Same as case 1.

Related Configuration

Same as case 1.

Problem

PC access Failed!

Troubleshooting

The results of **debugging radius packet** are as follows:

```
*0.310903 Quidway RDS/8/DEBUG:- 1 -Recv MSG,[MsgType=Normal auth request Index =
 0, ulParam3=2181282068]
*0.311015 Quidway RDS/8/DEBUG:- 1 -Send attribute list:
*0.311082 Quidway RDS/8/DEBUG:- 1 -
[1  User-name                ] [19] [00-0f-1f-c6-d7-77]
[2  Password                 ] [34] [4A3D4A1862CD56D644449DBAD709491F35E04976
B167B35FAA726389CF8B2160]
[4  NAS-IP-Address           ] [6 ] [10.15.1.242]
[32 NAS-Identifier           ] [14] [00e0fc7da05c]
[5  NAS-Port                 ] [6 ] [268439553]
[61 NAS-Port-Type            ] [6 ] [15]
*0.311582 Quidway RDS/8/DEBUG:- 1 -
[6  Service-Type             ] [6 ] [2]
[7  Framed-Protocol          ] [6 ] [1]
[31 Caller-ID                ] [16] [303030662D316663362D64373737]
*0.311815 Quidway RDS/8/DEBUG:- 1 -Send: IP=[10.15.1.43], UserIndex=[0], ID=[0],
 RetryTimes=[0], Code=[1], Length=[133]
*0.311965 Quidway RDS/8/DEBUG:- 1 -Send Raw Packet is:
*0.312032 Quidway RDS/8/DEBUG:- 1 -
 01 00 00 85 98 52 00 00 3c 3c 00 00 71 1a 00 00
```

```
47 0b 00 00 01 13 30 30 2d 30 66 2d 31 66 2d 63
36 2d 64 37 2d 37 37 02 22 4a 3d 4a 18 62 cd 56
d6 44 44 9d ba d7 09 49 1f 35 e0 49 76 b1 67 b3
5f aa 72 63 89 cf 8b 21 60 04 06 0a 0f 01 f2 20
0e 30 30 65 30 66 63 37 64 61 30 35 63 05 06 10
00 10 01 3d 06 00 00 00 0f 06 06 00 00 00 02 07
06 00 00 00 01 1f 10 30 30 30 66 2d 31 66 63 36
2d 64 37 37 37
```

```
*0.313900 Quidway RDS/8/DEBUG:- 1 -Recv MSG,[MsgType=PKT auth timeout Index = 0,
 ulParam3=0]
*0.313999 Quidway RDS/8/DEBUG:- 1 -Send: IP=[10.15.1.43], UserIndex=[0], ID=[0],
 RetryTimes=[1], Code=[1], Length=[133]
*0.316900 Quidway RDS/8/DEBUG:- 1 -Recv MSG,[MsgType=PKT auth timeout Index = 0,
 ulParam3=0]
*0.316999 Quidway RDS/8/DEBUG:- 1 -Send: IP=[10.15.1.43], UserIndex=[0], ID=[0],
 RetryTimes=[2], Code=[1], Length=[133]
*0.319900 Quidway RDS/8/DEBUG:- 1 -Recv MSG,[MsgType=PKT auth timeout Index = 0,
 ulParam3=0]
*0.320000 Quidway RDS/8/DEBUG:- 1 -RADIUS Server No Response
```

From debugging information (red mark), I know that RADIUS server just discards the access-request from switch silently, which in fact RADIUS server already received. Why? RADIUS server and switch have already known each other with IP address and key. Maybe there is no such a user in the database of RADIUS server at all? After checking the debugging information again, I find that username which switch sends is the MAC address with five hyphens like "-" , but the corresponding username and password which RADIUS server maintains are the ones without any hyphens.

When I contact R&D, I get the answer as follows:

MAC address userd as username and password adopts the format of "HHHHHHHHHHHH" in the basic version of S39/56, but format of "HH-HH-HH-HH-HH-HH" in the enhanced version.

In this case, just enhanced version of S39 is used.

PC can access successfully after modification.

From version of E1508 of both S3900 and S5600, the following command is added in order to switch format of MAC address as username and password sent to RADIUS server.

Syntax:

mac-authentication authmode usernameasmacaddress usernameformat

View:

system view

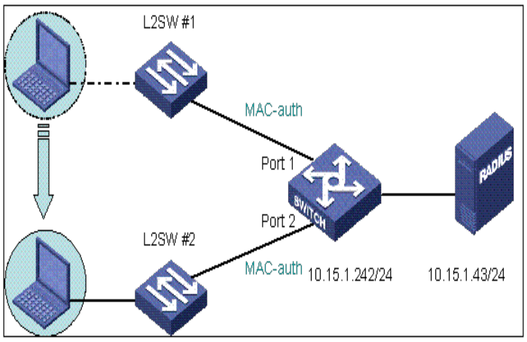
Parameter:

with-hyphen: the format of the username and password is HH-HH-HH-HH-HH-HH.

without-hyphen: the format of the username and password is HHHHHHHHHHHH.

Case 3: Failure from Port Shift indirectly

Network Topology



Related Configuration

Same as case 1.

Problem

As shown in the figure above, After PC which has passed MAC-authentication is moved from port1 to port2 indirectly with constant PINGing, PING is not OK all the time, namely PC can not access again as if MAC aging mechanism of switch does not work.

Troubleshooting

There are no output as **debugging MAC-authentication event** and **debugging radius packet** are inputted, and result of **display connection** also shows no logon user.

Result of **display MAC-address dynamic** shows that PC's MAC address is learned and kept at port 1, and is never aged.

When I contact R&D, I get the answer as follows:

As we know, switch is unable to know PC's leave unless PC connects it directly, there is no handshake between PC and switch with present chip, the only mechanism is MAC aging.

When PC accesses again from another port, if switch detects its MAC address existing already, then switch just ignores and rejects its access for the sake of security (avoid attack from simulating MAC address) during aging time.

It is very necessary to emphasize the mechanism of MAC aging here.

There is a bit (hit) for every MAC address to indicate whether traffic has been passed with this MAC during a period. when aging timer is expired, if the mark is valid (hit =1),then switch will clear it (hit=0); if the mark is invalid (hit=0), then switch will remove this MAC.

Aging time setting is only to configure the value of aging timer. MAC address with invalid mark (hit=0) will be removed when aging timer is expired next time. So it will take 1~2 aging times to remove a MAC address.

In this case, with constant PINGing, switch detects the MAC mark of PC keeping valid (hit=1) all the time , so switch will never remove this MAC resulting in rejecting re-access of the same MAC address from another port.

So if PC is moved from one port to another indirectly, no traffic must be ensured with its MAC within 2 aging times.

Notice: Our R&Ds are planning to publish a new release to solve this issue of realtime detection for MAC-authentication just at cost of no security in the future. That is to say if switch detects a new access of the same MAC address, it will remove the old MAC immediately to admit the new connection.

Version of E1508 of both S3900 and S5600 had modified this issue.

Summary

From the above three cases, we can draw some conclusions as follows:

I. Both username and password which switch sends to RADIUS server are the MAC address without Caps;

II. MAC address userd as username and password adopts the format of "HHHHHHHHHHHH" in the basic version of S39/56, but format of "HH-HH-HH-HH-HH-HH" in the enhanced version. But from version of E1508 of both S3900 and S5600, a command is added in order to switch format of MAC address as username and password sent to RADIUS server;

III. If PC is moved from one port of S39/56 to another indirectly (namely MAC-authentication with AP, HUB or Layer 2 switch in the middle), no traffic must be ensured with its MAC within 2 aging times to re-initiate a new connection.But from version of E1508 of both S3900 and S5600, such condition is ensured no longer.