

MAC Authentication

Ethernet Switch

ZyNOS 3.8

Support Notes

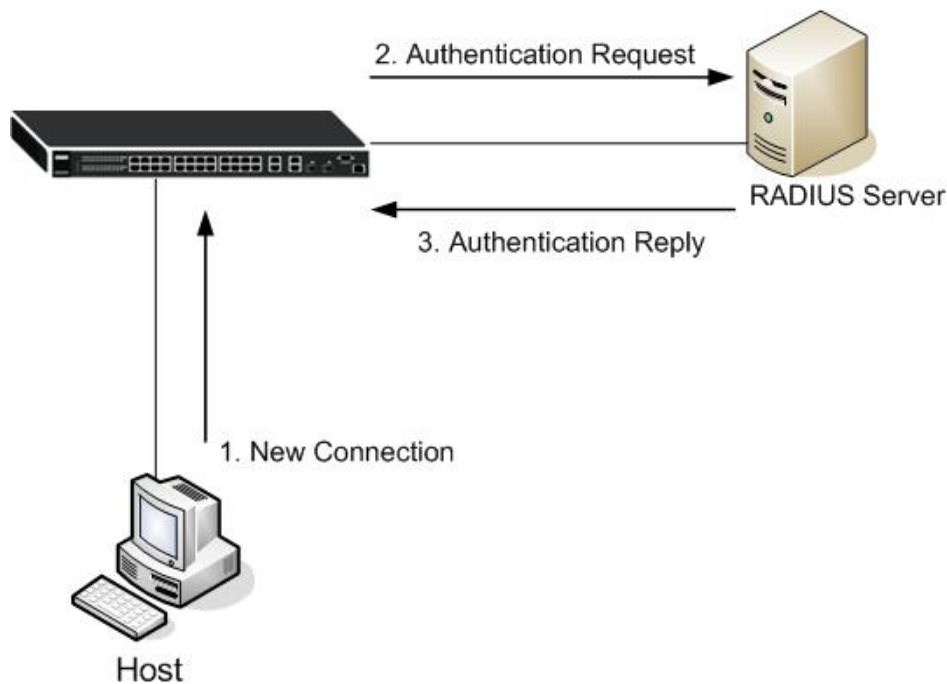
Version 3.80

August 2007



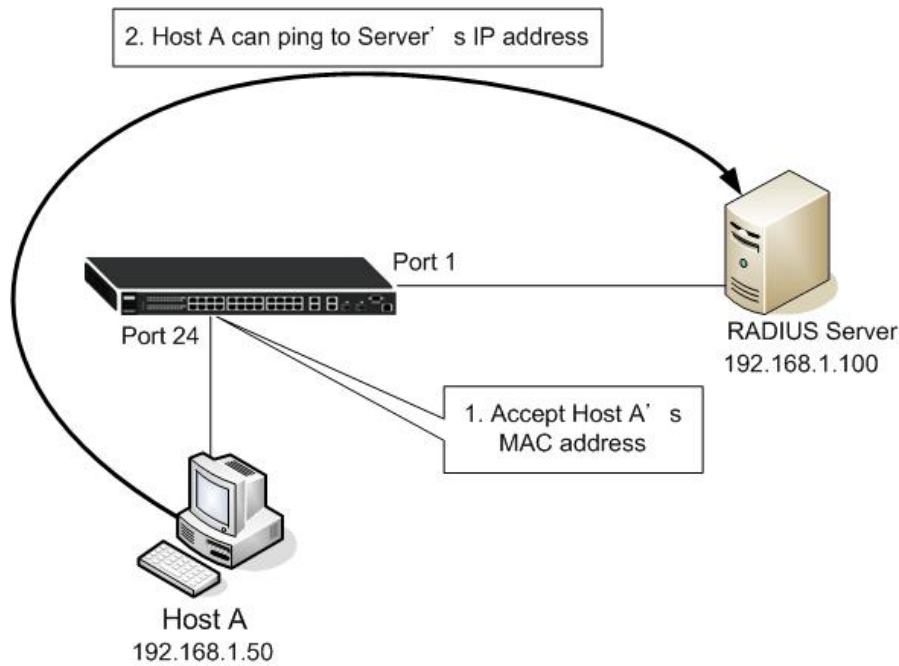
Overview of MAC Authentication

MAC Authentication is an authenticate method that allow the Switch to use client's MAC address to do authentication automatically. When the host MAC address mismatches with the MAC address defined in the database, the switch will reject this link.

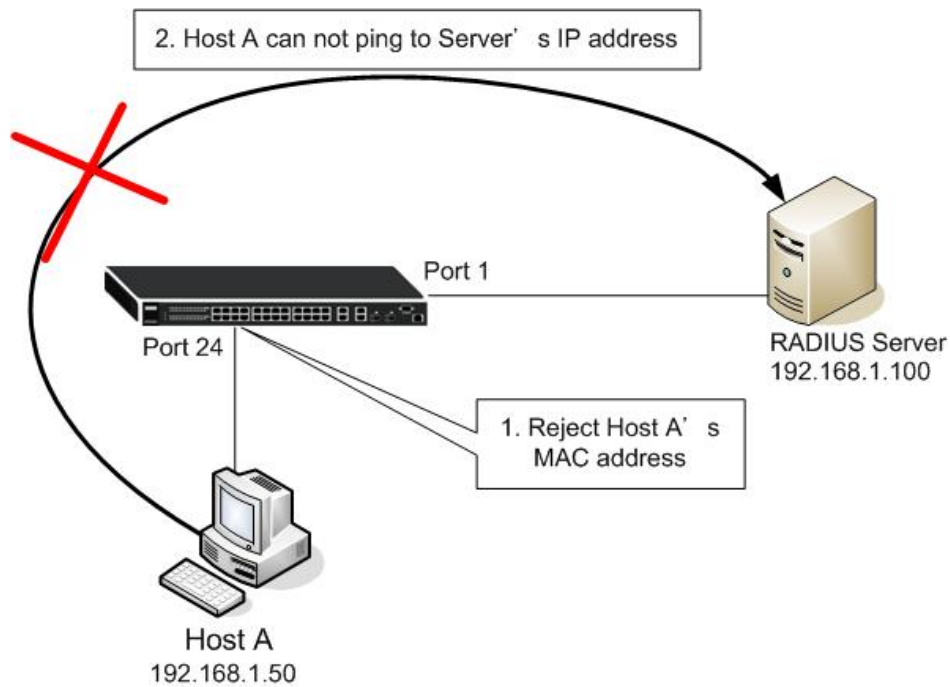


Scenario:

Consider following topology. The Host A's MAC address is authenticated by the RADIUS server , thus the packets from Host A to the connected port will be forwarded.



If the MAC address is rejected by the RADIUS server during authenticating, packets from Host A on that port will be dropped by the switch.



Configuration using the Web GUI

1. Connect MGMT port with a PC or Notebook via the RJ45 Cable.
2. By default, the MGMT IP of the out-band port is 192.168.0.1/24
3. Set your NIC to 192.168.0.100/24
4. Open an Internet browser (e.g. IE) and enter <http://192.168.0.1> in the URL field.
5. By default, the username for the administrator is “admin” and the corresponding password is “1234”.
6. After successful login you will see a screen similar to the one on the screenshot below.

Port	Name	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1		100M/F	FORWARDING	Disabled	214	1044	0	0.0	0.130	0:05:31
2		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
3		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
4		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
5		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
6		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
7		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
8		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
9		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
10		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
11		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
12		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
13		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
14		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
15		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
16		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
17		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
18		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
19		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
20		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

☒ Any
☐ Port

Clear Counter

7. First of all, we need to specify where the RADIUS server is. Click “**Advanced Application**” → “**Auth and Acct**” → “**RADIUS Server Setup**” to go to the “**RADIUS Server Setup**” page.

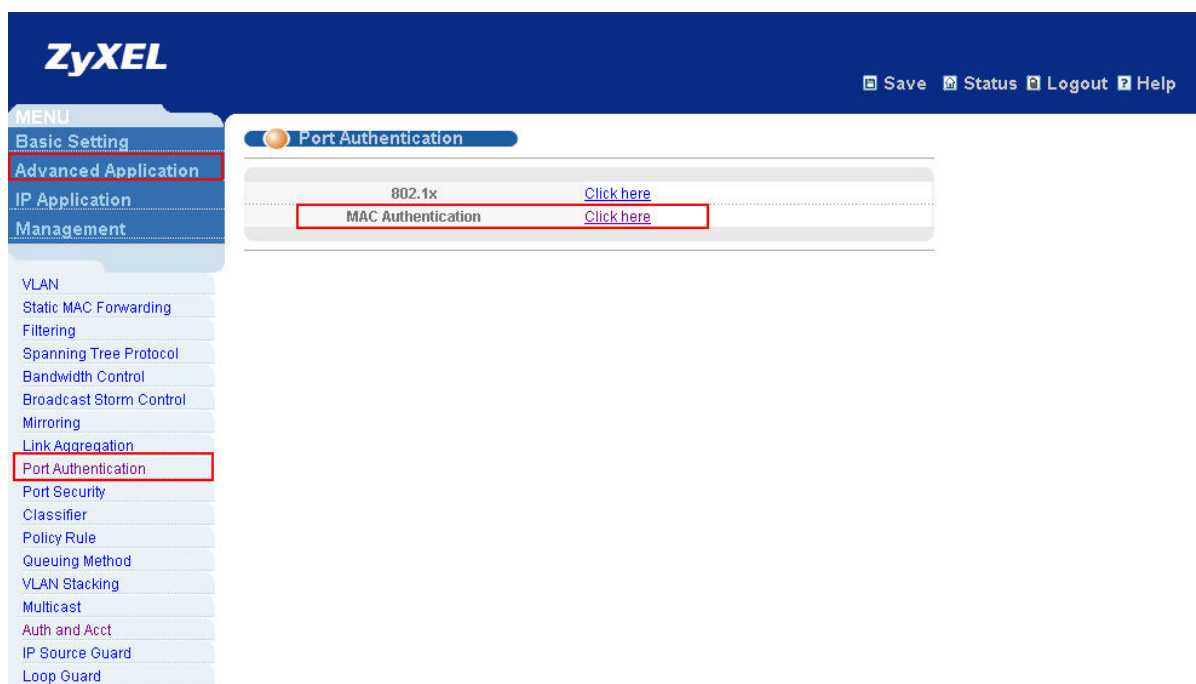
The screenshot shows the ZyXEL web management interface. The top navigation bar includes 'Save', 'Status', 'Logout', and 'Help'. The left sidebar contains a 'MENU' with categories: 'Basic Setting', 'Advanced Application' (highlighted), 'IP Application', and 'Management'. Under 'Advanced Application', 'Auth and Acct' is highlighted. The main content area is titled 'Authentication and Accounting' and contains three links: 'RADIUS Server Setup' (highlighted), 'TACACS+ Server Setup', and 'Auth and Acct Setup'. Each link has a 'Click Here' text next to it.

8. Configure RADIUS server ip address from “**RADIUS Server Setup**” page.

The screenshot shows the 'RADIUS Server Setup' page. The title bar includes 'RADIUS Server Setup' and 'Auth and Acct'. The page is divided into two sections: 'Authentication Server' and 'Accounting Server'. The 'Authentication Server' section contains a 'Mode' dropdown set to 'index-priority' and a 'Timeout' field set to '30' seconds. Below this is a table with columns: 'Index', 'IP Address', 'UDP Port', 'Shared Secret', and 'Delete'. The table has two rows: Row 1 has Index 1, IP Address 192.168.1.100, UDP Port 1812, and Shared Secret 1234; Row 2 has Index 2, IP Address 0.0.0.0, UDP Port 1812, and Shared Secret 0.0.0.0. At the bottom of the page are 'Apply' and 'Cancel' buttons.

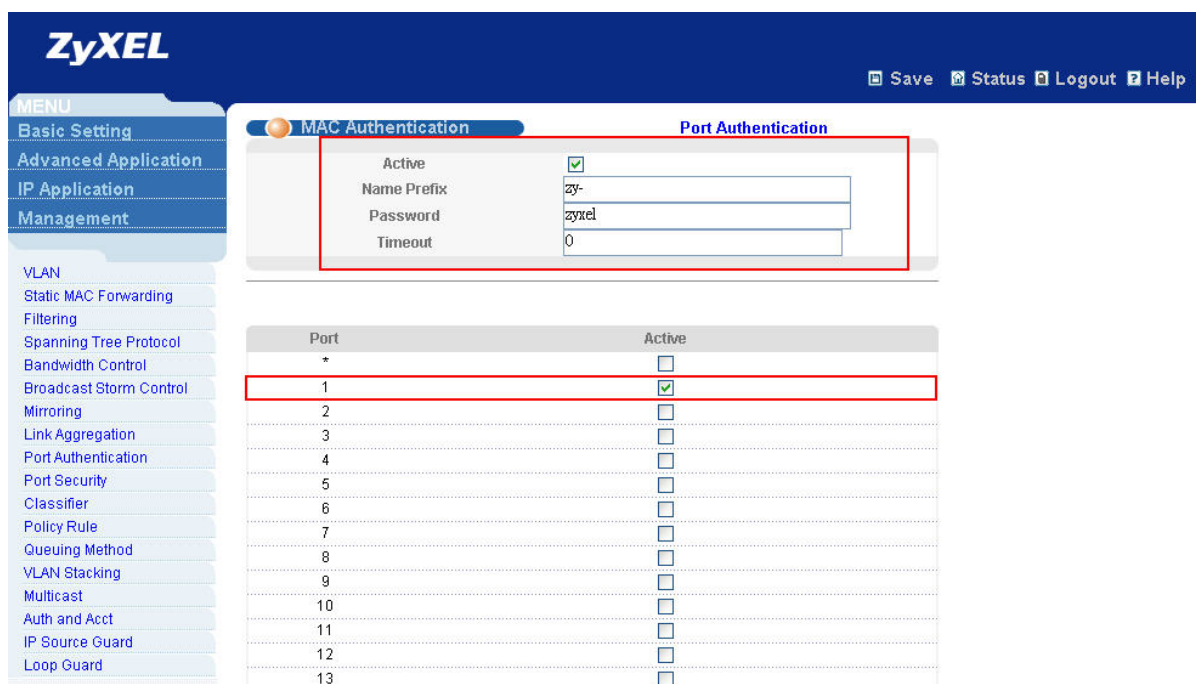
Index	IP Address	UDP Port	Shared Secret	Delete
1	192.168.1.100	1812	1234	<input type="checkbox"/>
2	0.0.0.0	1812	0.0.0.0	<input type="checkbox"/>

9. After specifying the RADIUS server, now we go to the “**MAC Authentication**” page.



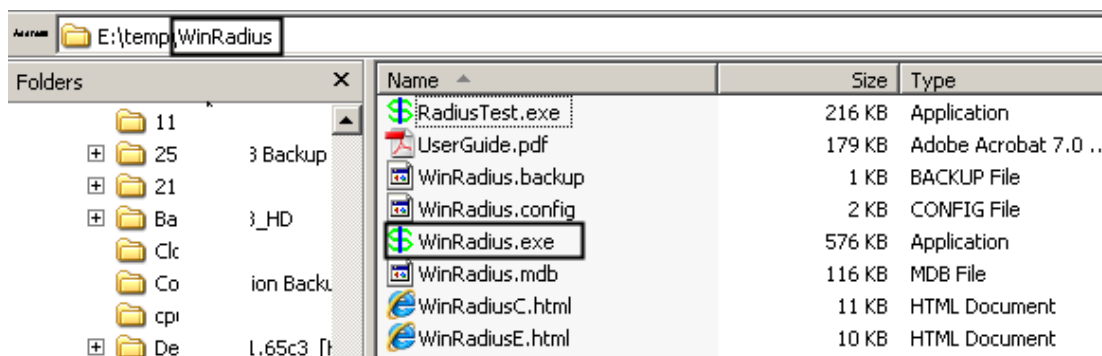
10. To enable MAC Authentication, we check the “**Active**” checkbox and put name prefix and password here. For example, if we use “zy-” as the name prefix and the host’s MAC address was “00-16-01-44-19-12”. During authentication procedure, the switch will send “zy-00-16-01-44-19-12” as the name for authentication to the RADIUS server.

11. Select the switch port which you want to enable MAC Authentication function and click Apply.

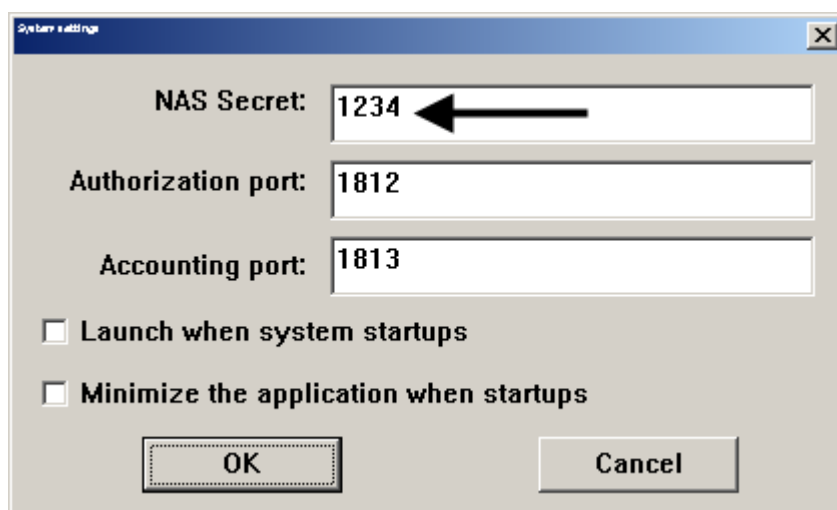
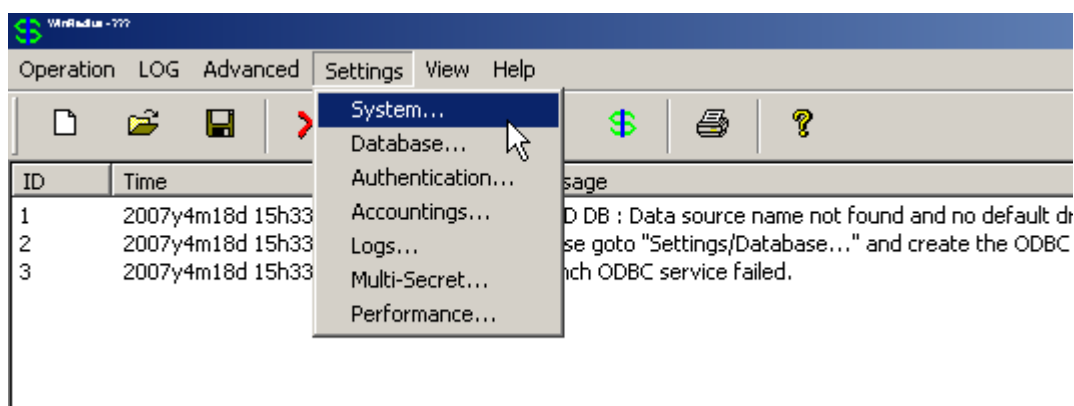


12. After configuring MAC Authentication. Now you need to configure the RADIUS Server. Here we use WINRADIUS as an example.

13. Download and unzip the file (WinRadius) on Radius Server 1. Then double click the file "WinRadius.exe" to run the Radius.

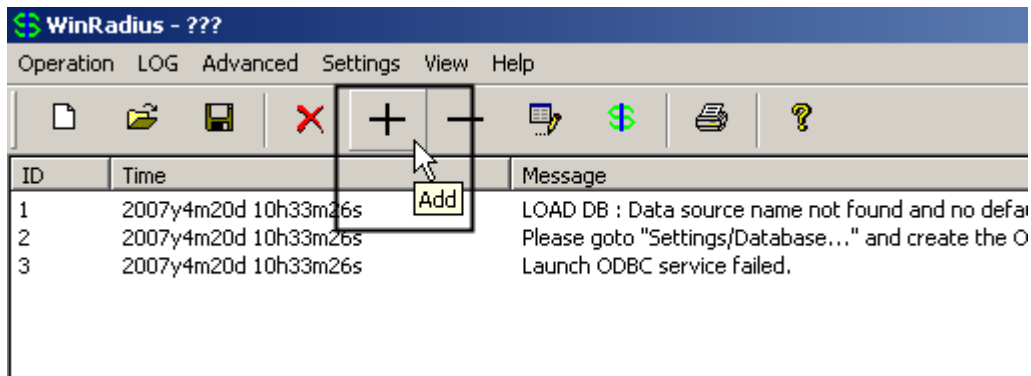


14. When the program shows up, click "Setting" → "System" to apply our shared secret "1234" and leave others unchanged.



15. Now, we need to create our test accounts based on the MAC address of the client

notebook. To do so, click the “+” sign of the GUI of the WinRadius to add an account.



16. Find your MAC address by using the DOS command “ipconfig /all” on the client notebook and put it here with the prefix “zy-” in front of it. Also, please put the password as what you have set in the Switch. In this example, the password is “zyxel”.
[IMPORTANT: Please use the actual MAC of your client instead of the one used in this example]

The screenshot shows the 'Add user' dialog box. It has fields for 'User name:', 'Password:', 'Group:', 'Address:', 'Cash prepaid:', 'Expiry date:', and 'Others:'. The 'User name' field contains 'zy-00-0A-E4-13-7F-D3'. The 'Password' field contains 'zyxel'. The 'Group' field is empty. The 'Address' field is empty. The 'Cash prepaid' field has a value of '0' and a unit of 'Cents'. The 'Expiry date' field is empty. Below the fields is a note: 'Note: yyyy/mm/dd means expiry date; digit means valid days since first login; empty means never expired.' At the bottom, there are radio buttons for 'Prepaid user' and 'Postpaid user', with 'Postpaid user' selected. There is also a dropdown menu for 'Accounting method' set to 'Based on Time'. At the bottom are 'OK' and 'Cancel' buttons.

17. Click “OK” to save the setting. You will see that there is a log saying that your user has been added successfully.

ID	Time	Message
1	2007y4m20d 10h33m26s	LOAD DB : Data source name not found and no default driver specified
2	2007y4m20d 10h33m26s	Please goto "Settings/Database..." and create the ODBC for your RADIUS database.
3	2007y4m20d 10h33m26s	Launch ODBC service failed.
4	2007y4m20d 10h54m58s	Add user successfully.

18. Now connect the client notebook to the Switch at port 15 and do a PING test to the RADIUS Server at "192.168.1.100". You should see PING is able to get through in the very second you launch it since it just takes a very small amount of time to do the MAC authentication. In the log of the RADIUS Software you will see that user authentication was successful.

ID	Time	Message
1	2007y4m20d 10h33m26s	LOAD DB : Data source name not found and no default driver specified
2	2007y4m20d 10h33m26s	Please goto "Settings/Database..." and create the ODBC for your RADIUS database.
3	2007y4m20d 10h33m26s	Launch ODBC service failed.
4	2007y4m20d 10h54m58s	Add user successfully.
5	2007y4m20d 11h27m7s	User (zy-00-0A-E4-13-7F-D3) authenticate OK.

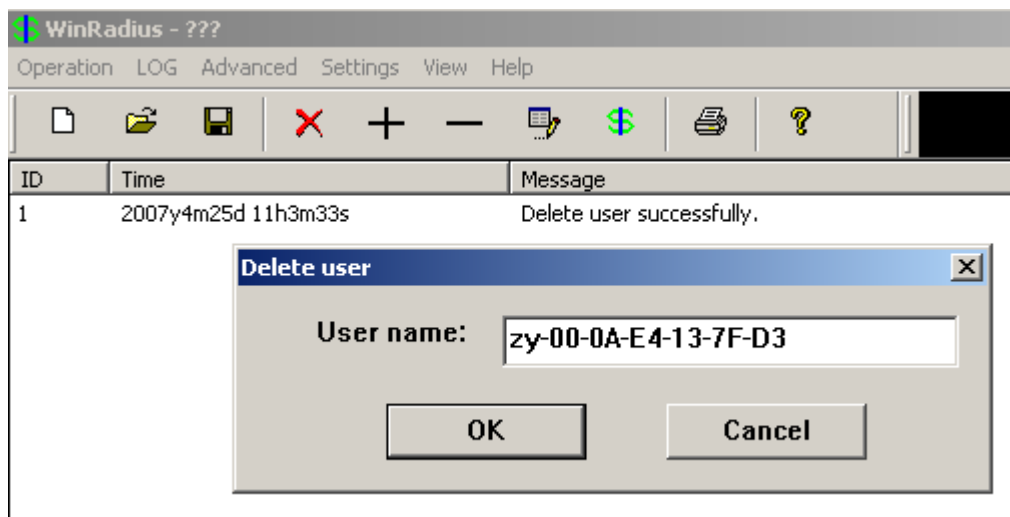
```
C:\Documents and Settings\Zeta>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

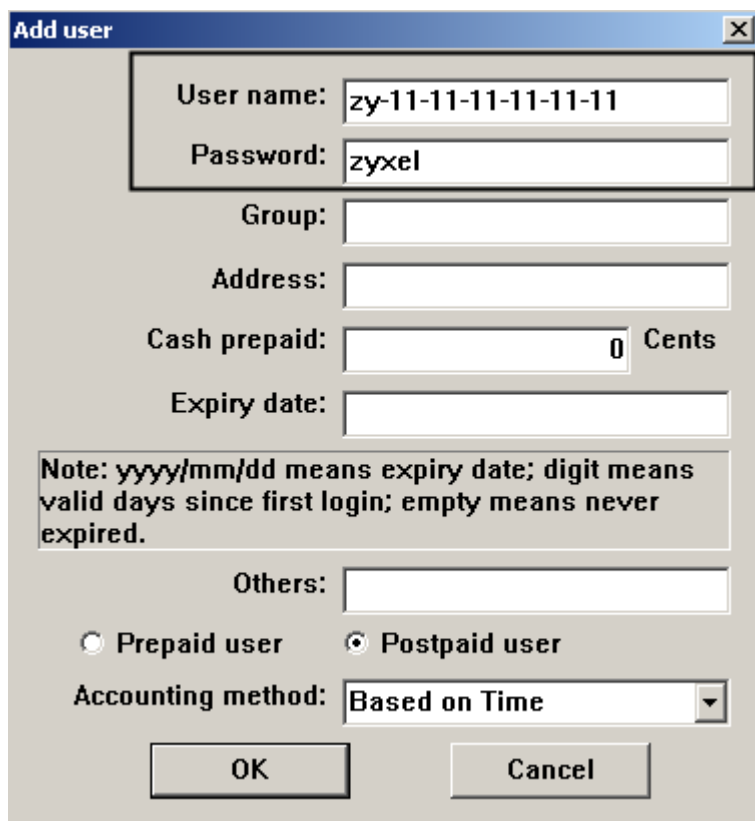
Reply from 192.168.1.100: bytes=32 time=1ms TTL=254
Reply from 192.168.1.100: bytes=32 time=1ms TTL=254
Reply from 192.168.1.100: bytes=32 time=1ms TTL=254
Reply from 192.168.1.100: bytes=32 time=3ms TTL=254

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

19. Now let us do another test to see if this feature really works by changing the MAC to a fake one. Since the username cannot be changed in WinRadius, we need to delete the old one and create a new username (a fake MAC) on the WinRadius. To delete an account, click on the "-" icon and input the username that you want to delete. You should see a log for the confirmation of the account deletion. Now disconnect the client PC.



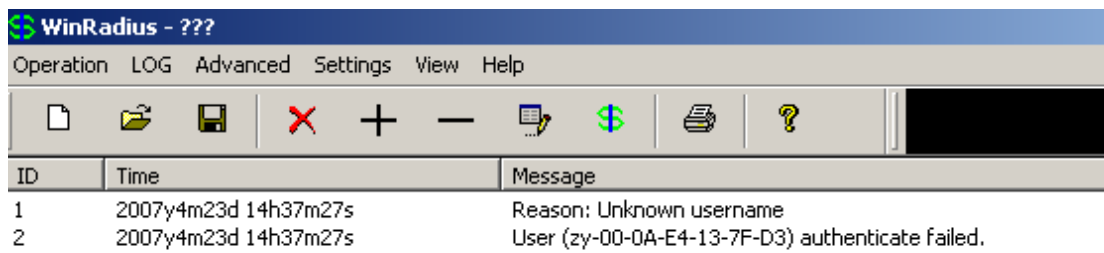
20. Now, as we mentioned before, we create a user account based on a fake MAC address. In this example, please put zy-11-11-11-11-11-11.



21. Now it is the time to verify whether MAC authentication is really working on the Switch. The authentication should fail this time.

22. Connect the Client PC back to the Switch at port 15. Do a PING test to the server at 192.168.1.100 and it should fail in every attempt. Check the WinRADIUS log and

you should see an authentication failure message.



The screenshot shows the WinRadius application window. The title bar reads "WinRadius - ???". The menu bar includes "Operation", "LOG", "Advanced", "Settings", "View", and "Help". Below the menu bar is a toolbar with icons for file operations (new, open, save, delete, add, subtract, print, find, help) and a search icon. The main area displays a log table with three columns: ID, Time, and Message.

ID	Time	Message
1	2007y4m23d 14h37m27s	Reason: Unknown username
2	2007y4m23d 14h37m27s	User (zy-00-0A-E4-13-7F-D3) authenticate failed.

Configuration using the CLI

```
vlan 1
  name 1
  normal ""
  fixed 1-28
  forbidden ""
  untagged 1-28
  ip address 192.168.1.1 255.255.255.0
exit
interface port-channel 1
  mac-authentication
exit
interface route-domain 192.168.1.1/24
exit
ip address 192.168.0.1 255.255.255.0
radius-server host 1 192.168.1.100 key 1234
mac-authentication
mac-authentication nameprefix zy-
```