How To | Configure MAC-based port authentication

Introduction

This document describes how to configure MAC-based port authentication both with and without VLAN assignment.

MAC-based port authentication is an alternative approach to 802.1x for authenticating hosts connected to a port. By authenticating based on the host's source MAC address, the host is not required to run a user for the 802.1x protocol. The RADIUS server that performs the authentication can also return the VLAN ID that the host should be attached to. This allows the switch to add the port as an untagged member of the appropriate VLAN, thereby separating traffic on VLANs for hosts of different security levels.

What information will you find in this document?

This document provides information on:

- configuring MAC-based port authentication without VLAN assignment on page 2
- configuring MAC-based port authentication with VLAN assignment on page 7

Which product and software version does this information apply to?

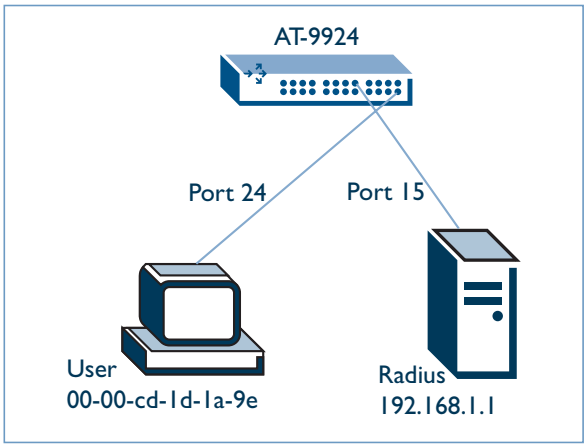
The information provided in this document applies to the following products:

- AT-8600, AT-8900, AT-9900, and Rapier series switches.

running software release 2.7.3 or later.

Configuring MAC-based port authentication without VLAN assignment

First, we will consider a simple scenario, where no VLAN assignment is being performed, using the setup shown in the illustration below.



Configuring the switch

Use the following commands to configure the switch and enable MAC-based authentication on port 24 of the switch.

```
enable ip
add ip interface=vlan1 ip=192.168.1.254

add radius server=192.168.1.1 secret="macbased" port=1812

enable portauth=macbased
enable portauth=macbased port=24 vlanassignment=disabled
```

Note: *MAC authentication MUST NOT be enabled on the port that connects the switch to the RADIUS server.*

This configuration only enables the MAC-based authentication on port 24. The switch will not try to assign a VLAN to this MAC address and will write the MAC address to its forwarding database corresponding to port 24's own VLAN (which is the default, VLAN 1, for this example).

Configuring the RADIUS Server

When you send a packet from the user, the switch asks the RADIUS Server if this user is in its database or not. The username and password that the switch passes to RADIUS Server are **both** the MAC address of the user. So, the only parameters that you need to define on the RADIUS Server for the user are:

```
username = 00-00-cd-1d-1a-9e

Auth-type = Local

User-password = "00-00-cd-1d-1a-9e"
```

The parameters that you need to define on the RADIUS server for the RADIUS client are:

```
secret=macbased
```

Verifying the setup

To check that the switch can reach the RADIUS Server, use the command **show radius**. The status of the server should be **Alive**.

```
RADIUS Server Parameters
--------------------------------------------------------------------------------
  Server Retransmit Count....... 3
  Server Timeout................ 6 sec
  Server Dead Time.............. 0 min
--------------------------------------------------------------------------------
  Server           Port  AccPort  Secret  LocalInterface  Status
  ------------------------------------------------------------------------
  192.168.1.1      1812     1646  ******  Not set         Alive
  ------------------------------------------------------------------------
```

An example of an authentication exchange

The communication between the switch and the RADIUS Server can be seen by turning on debugging with the command:

```
enable radius debug=decode
```

(You can use the command **disable radius debug=decode** to turn off debugging.)

In the example debug output below, you can see that the switch is sending an Access-Request to the RADIUS Server, and the RADIUS Server is sending the switch an Access-Accept packet. After receiving this packet, the switch will add the user's MAC address to its forwarding database.

```
RADIUS DECODE PKT Tx: Server:192.168.1.1
  Code  ...................Access-Request
  Identifier  .............0x05
  Length  .................110
  Authenticator  ..........0x30FFE89C 710072E5 54775258 65BF3ABA
  Attribute type  .........User-Name
  Attribute length  .......19
  Attribute value  ........00-00-cd-1d-1a-9e
  Attribute type  .........NAS-Port
  Attribute length  .......6
  Attribute value  ........0x00000018
  Attribute type  .........NAS-Port-Type
  Attribute length  .......6
  Attribute value  ........0x0000000F
  Attribute type  .........User-Password
  Attribute length  .......34
  Attribute value  ........0xA0E33DC8 2FA49091 5BEED2D4 448A8728 5EDA53FB
0B9901
BA 5A22565B 1CB582A5
  Attribute type  .........NAS-IP-Address
  Attribute length  .......6
  Attribute value  ........192.168.1.254
  Attribute type  .........Calling-Station-Id
  Attribute length  .......19
  Attribute value  ........0x30302D30 302D4344 2D31442D 31412D39 45

RADIUS DECODE PKT Rx: Server:192.168.1.1
  Code  ...................Access-Accept
  Identifier  .............0x05
  Length  .................20
  Authenticator  ..........0x42C6533B ED88F66C 298F7599 10CA1984
```

After receiving the authentication reply, you can check the switch's authenticating port and the switch's forwarding database using the commands:

```
show portauth=mac port=24
show switch fdb
```

These will show details similar to those shown in the output below:

show portauth=mac port=24

```
MAC Based Authentication Configuration
--------------------------------------------------------------------------------
Interface: port24
  PAE Status.............. Enabled
  Number of Supplicants.... 1
  Default Settings
        AuthControlPortControl........ Auto
        quietPeriod................... 60
        reAuthPeriod.................. 3600
        reAuthEnabled................. False
        secureVlan.................... On
        trap.......................... None
        mibReset...................... Enabled
        vlanAssignment................ Disabled

  Attached Supplicant(s)
    MAC Address..................... 00-00-cd-1d-1a-9e
        Authenticator PAE State....... AUTHENTICATED
        Port Status................... authorised
        Backend Authenticator State... IDLE
        AuthControlPortControl........ Auto
        quietPeriod................... 60
        reAuthPeriod.................. 3600
        reAuthEnabled................. False
        secureVlan.................... On
        trap.......................... None
        mibReset...................... Enabled
        vlanAssignment................ Disabled
```

show switch fdb

```
Switch Forwarding Database (software)
  Total number of entries = 3
--------------------------------------------------------------------------------
  VLAN MAC Address        Port/Vidx Status       daRoute
--------------------------------------------------------------------------------
  1    00-00-cd-1d-1a-9e  24        dynamic      0
  1    00-00-cd-24-02-50  CPU       static       1
  1    00-03-47-6b-a7-59  15        dynamic      0
```

An example of authentication failure

Lets check what happens if you do not configure the user and password correctly on the RADIUS Server. The easiest way to see the result is again by enabling RADIUS debugging on the switch, using the command:

```
enable radius debug=decode
```

```
RADIUS DECODE PKT Tx: Server:192.168.1.1
  Code  ...................Access-Request
  Identifier  .............0x06
  Length  .................110
  Authenticator  ..........0x297C170D 11CD6BC2 455D96AF 034FDEBD
  Attribute type  .........User-Name
  Attribute length  .......19
  Attribute value  ........00-00-cd-1d-1a-9e
  Attribute type  .........NAS-Port
  Attribute length  .......6
  Attribute value  ........0x00000018
  Attribute type  .........NAS-Port-Type
  Attribute length  .......6
  Attribute value  ........0x0000000F
  Attribute type  .........User-Password
  Attribute length  .......34
  Attribute value  ........0x46C976C6 D0C74536 F0B08F24 A3AD00FD 8517E851
07ADF92C E40483EB 84A63518
  Attribute type  .........NAS-IP-Address
  Attribute length  .......6
  Attribute value  ........192.168.1.254
  Attribute type  .........Calling-Station-Id
  Attribute length  .......19
  Attribute value  ........0x30302D30 302D4344 2D31442D 31412D39 45

RADIUS DECODE PKT Rx: Server:192.168.1.1
  Code  ...................Access-Reject
  Identifier  .............0x06
  Length  .................20
  Authenticator  ..........0x2DAD4D1A 6096E40E C2F30932 AFAC8408
```

The RADIUS Server sends an Access-Reject message to the switch when the username/password is NOT correctly configured on the RADIUS Server.

Note: *When the switch receives a Reject message, it will not add the user's MAC address to its forwarding database.*

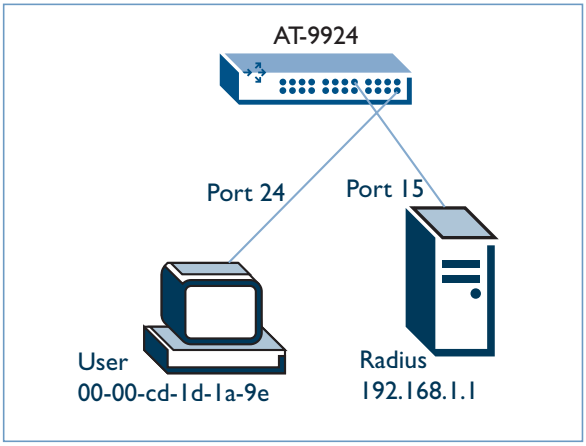
After receiving a Reject message, the switch then drops all the packets received from the rejected MAC address for a specified time period. This time period is called the **QUIETPeriod**, and can be configured using the command:

```
set portauth=mac port=x quietperiod=value
```

The default is 60 seconds. After the quiet timer expires, if another packet is received from the supplicant, the switch will try to authenticate the packet again.

Configuring MAC-based port authentication with VLAN assignment

In this configuration we consider the more advanced scenario, where VLAN assignment is being performed, using the setup shown in the illustration below.



Configuring the switch

Use the following commands to configure the switch, authenticate the MAC address of the user, and assign it to VLAN2.

```
create vlan="testusers" vid=2
add radius server=192.168.1.1 secret="macbased" port=1812
enable portauth=macbased
enable portauth=macbased port=24
```

Our aim is to authenticate the MAC address of the user and assign it to VLAN 2. Note that in the configuration above, port 24 is not a configured member of VLAN2.

Configuring the RADIUS server

When you send a packet from the user, the switch asks the RADIUS Server if this user is in its database or not. The username and password that the switch passes to the RADIUS Server are both the MAC address of the user. The parameters that you need to define on RADIUS Server for the user are:

```
username = 00-00-cd-1d-1a-9e
Auth-type = Local
User-password = "00-00-cd-1d-1a-9e"
Tunnel-Type = "VLAN"
Tunnel-Medium-Type = 6 (Note: 6 means "all 802-type packets)
Tunnel-Private-Group-ID = "testusers"
```

The parameters that you need to define on the RADIUS server for the RADIUS client are:

```
secret=macbased
```

An example of an authentication exchange

The communication between the switch and the RADIUS Server can be seen by turning on debugging using the command:

```
enable radius debug=decode
```

(You can use the command **disable radius debug=decode** to turn off debugging.)

In the example debug output below, you can see that the switch is sending an Access-Request to the RADIUS Server, and the RADIUS Server is sending the switch an Access-Accept packet with the details of the VLAN that the switch should add this MAC address to. After receiving this packet, the switch will add the port to the "testusers" VLAN and add the user's MAC address to its forwarding database and mark it as VLAN 2.

```
RADIUS DECODE PKT Tx: Server:192.168.1.1
  Code  ...................Access-Request
  Identifier  .............0x10
  Length  .................110
  Authenticator  ..........0x48AAF7D1 5073DF9C 675DA407 34BBFC95
  Attribute type  .........User-Name
  Attribute length  .......19
  Attribute value  ........00-00-cd-1d-1a-9e
  Attribute type  .........NAS-Port
  Attribute length  .......6
  Attribute value  ........0x00000018
  Attribute type  .........NAS-Port-Type
  Attribute length  .......6
  Attribute value  ........0x0000000F
  Attribute type  .........User-Password
  Attribute length  .......34
  Attribute value  ........0x834EEBE7 2C23322D 984820A4 2535AA49 567118A1 6EB13A
B9 48788507 CC35591F
  Attribute type  .........NAS-IP-Address
  Attribute length  .......6
  Attribute value  ........192.168.1.254
  Attribute type  .........Calling-Station-Id
  Attribute length  .......19
  Attribute value  ........0x30302D30 302D4344 2D31442D 31412D39 45

RADIUS DECODE PKT Rx: Server:192.168.1.1
  Code  ...................Access-Accept
  Identifier  .............0x10
  Length  .................43
  Authenticator  ..........0xAF9EEF99 81241E67 B77BEEA8 4D89E8BC
  Attribute type  .........Tunnel-Type
  Attribute length  .......6
  Attribute value  ........0x0000000D
  Attribute type  .........Tunnel-Medium-Type
  Attribute length  .......6
  Attribute value  ........0x00000006
  Attribute type  .........Tunnel-Private-Group-Id
  Attribute length  .......11
  Attribute value  ........0x74657374 75736572 73
```

After receiving the authentication reply, you can check the switch's authenticating port and the switch's forwarding database using the commands:

```
show portauth=mac port=24

show switch port=24

show switch fdb
```

show portauth=mac port=24

```
MAC Based Authentication Configuration
--------------------------------------------------------------------------------
Interface: port24
  PAE Status.............. Enabled
  Number of Supplicants.... 1
  Default Settings
        AuthControlPortControl........ Auto
        quietPeriod................... 60
        reAuthPeriod.................. 3600
        reAuthEnabled................. False
        secureVlan.................... On
        trap.......................... None
        mibReset...................... Enabled
        vlanAssignment................ Enabled

  Attached Supplicant(s)
    MAC Address..................... 00-00-cd-1d-1a-9e
        Authenticator PAE State....... AUTHENTICATED
        Port Status................... authorised
        Backend Authenticator State... IDLE
        AuthControlPortControl........ Auto
        quietPeriod................... 60
        reAuthPeriod.................. 3600
        reAuthEnabled................. False
        secureVlan.................... On
        trap.......................... None
        mibReset...................... Enabled
        vlanAssignment................ Enabled
```

show switch port=24

```
 Switch Port Information
--------------------------------------------------------------------------------
 Port ........................ 24
   Description ................ -
   Status ..................... ENABLED
   Link State ................. Up
   UpTime ..................... 00:00:38
   Port Media Type ............ ISO8802-3 CSMACD
   Configured speed/duplex .... Autonegotiate
   Actual speed/duplex ........ 100 Mbps, full duplex
   MDI Configuration (Polarity) .. Automatic (MDI)
   Loopback ................... Off
   Configured master/slave mode .. Not applicable
   Actual master/slave mode ..... Not applicable
   Acceptable Frames Type ..... Admit All Frames
   Disabled Egress Queues ..... -
   BCast & MCast rate limit ..... -
   BCSC rate Limiting ......... disabled
   Egress rate limit .......... -
   Learn limit ................ -
   Intrusion action ........... Discard
   Current learned, lock state ... -, not locked
   Address learn thrash limit .... 8192 (8192 max, 1024 per second)
   Relearn .................... OFF
   Mirroring .................. Disabled
   Is this port mirror port ..... No
   VLAN(s) .................... testusers (2)
   Ingress Filtering .......... Off
   Trunk Group ................ -
   STP ........................ default
   Cable Length ............... -
--------------------------------------------------------------------------------
```

show switch fdb

```
Switch Forwarding Database (software)
  Total number of entries = 3
--------------------------------------------------------------------------------
  VLAN MAC Address        Port/Vidx Status       daRoute
--------------------------------------------------------------------------------
  2    00-00-cd-1d-1a-9e  24        dynamic      0 <--
  1    00-00-cd-24-02-50  CPU       static       1
  1    00-03-47-6b-a7-59  15        dynamic      0
```

You can see now that port 24 belongs to VLAN 2, even though you did not assign that port manually to that VLAN.

Subsequent hosts, downstream of that same switch port, that require authentication will follow the same process, however, the VLAN returned by the RADIUS Server **must match** the VLAN that was assigned for the first host, otherwise **access for the new host will be denied**.

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesyn.com

C613-16053-00 REV A