

LAB GUIDE

# Local MAC Match Authentication

**IMPORTANT! THIS GUIDE ASSUMES THAT THE AOS-CX OVA HAS BEEN INSTALLED AND WORKS IN GNS3 OR EVE-NG. PLEASE REFER TO GNS3/EVE-NG INITIAL SETUP LABS IF REQUIRED.**

## TABLE OF CONTENTS

Lab Objective .....	1
Lab Overview .....	1
Lab Network Layout .....	2
Lab Tasks .....	2
Task 1 - Lab setup .....	2
Task 2 - Lab setup: Local mac match .....	3
Task 3 - Lab setup: Validation .....	4
Task 4 – Running Configuration .....	6

### LAB OBJECTIVE

At the end of this workshop, you will be able to implement the basic configuration to enable local mac match and also understand local role and device-profile. The main goal in to ensure a successful deployment of local mac match authentication.

### LAB OVERVIEW

Mac-Match provides dynamic attribute assignment (e.g., VLAN and QoS) through the use of locally configured authentication repository. The most common use model for LMA is to automatically assign VLAN to IP phones.

Mac-Match solves dynamic assignment of per client (mac-address) attributes without having to create RADIUS infrastructure

When aaa dot1x, Mac-Auth fails, MAC match can be used as fallback

- match mac b2:c3:44:12:78:11
- match mac-oui 1a:2b:3c
- match mac-mask 71:14:89:f3/32

## LAB NETWORK LAYOUT

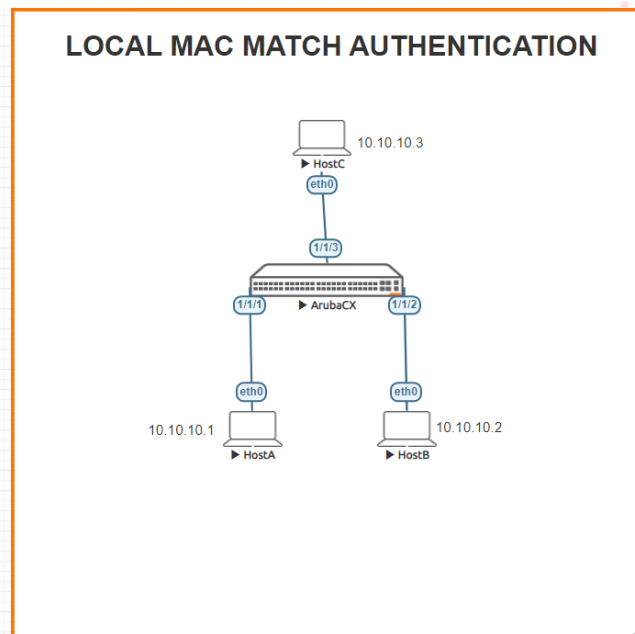


Figure 1. Lab topology and addresses

## LAB TASKS

### Task 1 - Lab setup

For this lab refer to Figure 1 for topology.

- Configure hostname, note that this feature is applicable to only 6xxx platforms.
- Enable interfaces on client connected ports as below:

```
CX6000# show running-config interface 1/1/1
interface 1/1/1
  no shutdown
  no routing
  vlan access 1
exit
```

```
CX6000#
CX6000# sh running-config interface 1/1/2
interface 1/1/2
  no shutdown
  no routing
  vlan access 1
exit
```

```
CX6000# sh running-config interface 1/1/3
interface 1/1/3
  no shutdown
  no routing
  vlan access 1
exit
```

CX6000#

- Please make sure to set ip address on connected host as below:

```
VPCS> ip 10.10.10.1/24
Checking for duplicate address...
PC1 : 10.10.10.1 255.255.255.0

VPCS> ping 10.10.10.10

84 bytes from 10.10.10.10 icmp_seq=1 ttl=64 time=0.593 ms
84 bytes from 10.10.10.10 icmp_seq=2 ttl=64 time=0.908 ms
84 bytes from 10.10.10.10 icmp_seq=3 ttl=64 time=1.420 ms
84 bytes from 10.10.10.10 icmp_seq=4 ttl=64 time=0.885 ms
84 bytes from 10.10.10.10 icmp_seq=5 ttl=64 time=1.117 ms

VPCS> █
```

- **Verify client mac is learned on connected port.**

CX6000# show mac-address-table detail

```
MAC age-time           : 300 seconds
Number of MAC addresses : 3
```

MAC Address	VLAN	Type	Port	Age	Denied	never_	ageout
00:50:79:66:68:05	1	dynamic	1/1/1	300	false	false	
00:50:79:66:68:02	1	dynamic	1/1/2	300	false	false	
00:50:79:66:68:03	1	dynamic	1/1/3	300	false	false	

CX6000#

## Task 2 - Lab setup: Local mac match

For this lab refer to Figure 1 for topology.

- Configure local mac match, local user role and device profile as below:

### Local mac match global configuration

```
mac-group localmacmatch
  seq 10 match mac 00:50:79:66:68:05
  seq 20 match mac 00:50:79:66:68:02
  seq 30 match mac 00:50:79:66:68:03

port-access role localrole
  mtu 1600
  reauth-period 100
  vlan access 1

port-access device-profile localdp
  enable
  associate role localrole
  associate mac-group localmacmatch
```

### Local mac match apply to client connected interfaces

```
interface 1/1/1
  no shutdown
  no routing
```

```
vlan access 1
port-access device-profile
mode block-until-profile-applied
interface 1/1/2
no shutdown
no routing
vlan access 1
port-access device-profile
mode block-until-profile-applied
interface 1/1/3
no shutdown
no routing
vlan access 1
port-access device-profile
mode block-until-profile-applied
```

### Task 3 - Lab setup: Validation

```
CX6000# show port-access clients detail
```

Port Access Client Status Details:

Client 00:50:79:66:68:05

=====

#### Session Details

-----

Port : 1/1/1  
Session Time : 12s  
IPv4 Address :  
IPv6 Address :

#### Authentication Details

-----

Status : Authenticated  
Auth Precedence : dot1x - Not attempted, mac-auth - Not attempted

#### Authorization Details

-----

Role : localrole  
Status : Applied

#### Role Information:

Name : localrole  
Type : local

-----

Reauthentication Period : 100 secs  
Cached Reauthentication Period :  
Authentication Mode :  
Session Timeout :  
Client Inactivity Timeout :  
Description :  
Gateway Zone :  
UBT Gateway Role :  
UBT Gateway Clearpass Role :  
Access VLAN : 1  
Native VLAN :

```
switch# show mac-address-table detail
MAC age-time : 300 seconds
Number of MAC addresses : 3
MAC Address      VLAN   Type                Port    Age    Denied never_ageout
-----
00:50:79:66:68:05 1      port-access-security 1/1/1   300    false false
00:50:79:66:68:02 1      port-access-security 1/1/2   300    false false
00:50:79:66:68:03 1      port-access-security 1/1/3   300    false false
switch#
```

```
Allowed Trunk VLANs      :  
Access VLAN Name       :  
Native VLAN Name       :  
VLAN Group Name        :  
MTU                    : 1600  
QOS Trust Mode         :  
STP Administrative Edge Port :  
PoE Priority           :  
Captive Portal Profile :  
Policy                 :
```

Port Access Client Status Details:

Client 00:50:79:66:68:02

=====

Session Details

-----

```
Port      : 1/1/2  
Session Time : 7s  
IPv4 Address :  
IPv6 Address :
```

Authentication Details

-----

```
Status      : Authenticated  
Auth Precedence : dot1x - Not attempted, mac-auth - Not attempted
```

Authorization Details

-----

```
Role      : localrole  
Status    : Applied
```

Role Information:

Name : localrole

Type : local

-----

```
Reauthentication Period      : 100 secs  
Cached Reauthentication Period :  
Authentication Mode         :  
Session Timeout             :  
Client Inactivity Timeout   :  
Description                  :  
Gateway Zone                 :  
UBT Gateway Role            :  
UBT Gateway Clearpass Role  :  
Access VLAN                  : 1  
Native VLAN                  :  
Allowed Trunk VLANs         :  
Access VLAN Name           :  
Native VLAN Name           :  
Allowed Trunk VLAN Names    :  
VLAN Group Name             :  
MTU                          : 1600  
QOS Trust Mode              :  
STP Administrative Edge Port :  
PoE Priority                 :  
Captive Portal Profile      :  
Policy                       :
```

Port Access Client Status Details:

Client 00:50:79:66:68:03

=====

Session Details

-----  
Port : 1/1/3  
Session Time : 10s  
IPv4 Address :  
IPv6 Address :

Authentication Details

-----  
Status : Authenticated  
Auth Precedence : dot1x - Not attempted, mac-auth - Not attempted

Authorization Details

-----  
Role : localrole  
Status : Applied

Role Information:

Name : localrole  
Type : local

-----  
Reauthentication Period : 100 secs  
Cached Reauthentication Period :  
Authentication Mode :  
Session Timeout :  
Client Inactivity Timeout :  
Description :  
Gateway Zone :  
UBT Gateway Role :  
UBT Gateway Clearpass Role :  
Access VLAN : 1  
Native VLAN :  
Allowed Trunk VLANs :  
Access VLAN Name :  
Native VLAN Name :  
Allowed Trunk VLAN Names :  
VLAN Group Name :  
MTU : 1600  
QOS Trust Mode :  
STP Administrative Edge Port :  
PoE Priority :  
Captive Portal Profile :  
Policy :

CX6000# show port-access clients

Port Access Clients

Status codes: d device-mode

Port	MAC-Address	Onboarding Method	Status	Role
1/1/1	00:50:79:66:68:05	device-profile	Success	localrole
1/1/2	00:50:79:66:68:02	device-profile	Success	localrole
1/1/3	00:50:79:66:68:03	device-profile	Success	localrole

**Task 4 – Running Configuration**

CX6000# show running-config  
Current configuration:

```
!  
!Version ArubaOS-CX Virtual.10.06.0001  
!export-password: default  
hostname CX6000  
user admin group administrators password ciphertext  
AQBapf/xKnYUClo+U49rs88SOqFdHLWKqsWtYjAkdjZP3OvtYgAAALYkSeFOBPlKBQLnuj5P0sGM4rld+KCNgy12HDGx  
adASxpcRFueUx8+yecstQhPNTGHxAP1YwFzT9ka+sqC  
/JGUjdy3BTb0IQbSvwpBpWSBrsLFSPzzyKp/P3TE/N8uP/zy5  
led locator on  
ntp server pool.ntp.org minpoll 4 maxpoll 4 iburst  
ntp enable  
!  
!  
!  
!  
ssh server vrf mgmt  
vlan 1  
interface mgmt  
    no shutdown  
    ip dhcp  
mac-group localmacmatch  
    seq 10 match mac 00:50:79:66:68:05  
    seq 20 match mac 00:50:79:66:68:02  
    seq 30 match mac 00:50:79:66:68:03  
port-access role localrole  
    mtu 1600  
    reauth-period 100  
    vlan access 1  
port-access device-profile localdp  
    enable  
    associate role localrole  
    associate mac-group localmacmatch  
aaa authentication port-access mac-auth  
    enable  
interface 1/1/1  
    no shutdown  
    no routing  
    vlan access 1  
    port-access device-profile  
        mode block-until-profile-applied  
interface 1/1/2  
    no shutdown  
    no routing  
    vlan access 1  
    port-access device-profile  
        mode block-until-profile-applie  
interface 1/1/3  
    no shutdown  
    no routing  
    vlan access 1  
    port-access device-profile  
        mode block-until-profile-applied  
interface vlan 1  
    ip address 10.10.10.10/24  
!  
!  
!  
!  
!  
https-server vrf mgmt
```

