a Hewlett Packard Enterprise company

Aruba 动手实验手册

Aruba OS8 基本配置

V 2.0.4

孙继虎/李磊/刘豪

目录

修订历史记录

下表列出了这个文档的修订历史记录

版本	日期	变更说明
2.0.0	2020/03/21	最初发布 1、删除 cppm 相关配置 2、添加 MD 初始化步骤 3、添加 AP 断电方法
2.0.1	2020/3/30	1、修正错误 2、修正格式
2.0.2	2020/4/07	1、更新 Client IP
2.0.3	2020/06/10	1、更新拓扑、修正错误
2.0.4	2020/07/28	1、修正部分错误 2、VMC 替换 7010

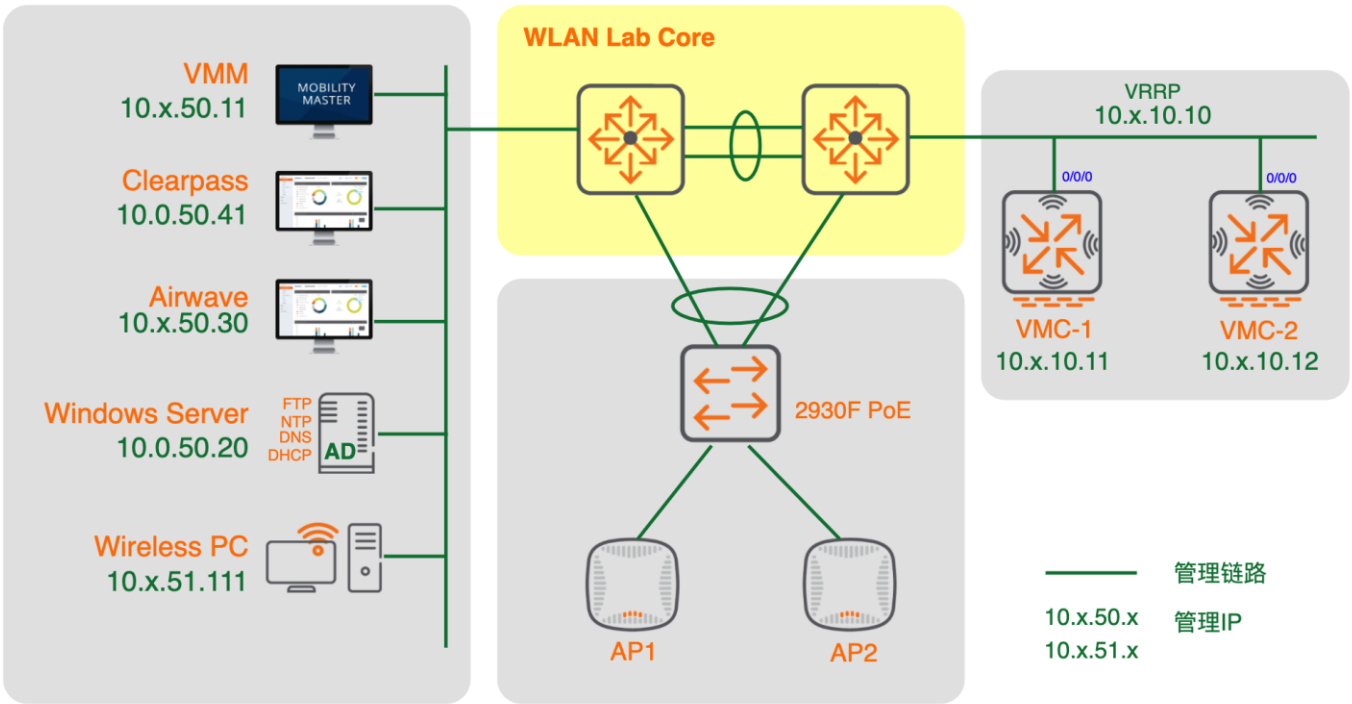
1 LAB 拓扑环境和设备登录信息

1.1 Lab 内容简介

本lab所有内容为远程操作，涉及配置Aruba MM、Controller产品，给初步接触ArubaOS 8产品的人员熟悉基本操作。

1.2 Lab 设备及拓扑

- 6台Mobility Master （每组1台MM）
- 12台Mobility Controller （每组2台MC）
- 1套ClearPass （共用1套CPPM，已提前调试好，AOS handson无需配置CPPM，可查看）
- 6套Airwave （每组1套AMP）
- 12颗Access Point （每组2颗AP）
- 6台无线客户端 （每组1台无线客户端）
- 6台有线客户端 （每组1台有线客户端）



1.3 Lab 设备 VLAN 和 IP 信息

设备信息				
Device	VLAN	IP	Mask	Default GTW
MM-1	X50	10.X.50.11	255.255.255.0	10.X.50.250
MM-2	X50	N/A	N/A	N/A
MD-1	X10	10.X.10.11	255.255.255.0	10.X.10.250
MD-2	X10	10.X.10.12	255.255.255.0	10.X.10.250
MD-VRRP	X10	10.X.10.10	255.255.255.0	10.X.10.250
MD1-COA	X10	10.X.10.21	255.255.255.0	10.X.10.250
MD2-COA	X10	10.X.10.22	255.255.255.0	10.X.10.250
Wireless User	X20			
Wired User 1	X21			
Wired User 2	X22			
ClearPass-Demo		10.0.50.41	255.255.255.0	
Wired Client		10.X.51.101/102	255.255.255.0	
Wireless Client		10.X.51.111/112	255.255.255.0	

1.4 Lab 设备登录账号和密码

默认所有设备用户名：admin，密码：aruba123，各种对接key：aruba123，特殊情况如下：

Device	Method	IP Address	Account	Password
ClearPass-Demo	https	10.0.50.41	readonly	readonly
AirWave	https	10.X.50.30	admin	admin
MM-1	https/ssh	10.X.50.11	admin	aruba123

1.5 设备操作方式

所有设备的console已在web界面设置好，可直接右键点击设备访问。

1.6 AP 重启操作方式

直接右键点击AP操作重启。

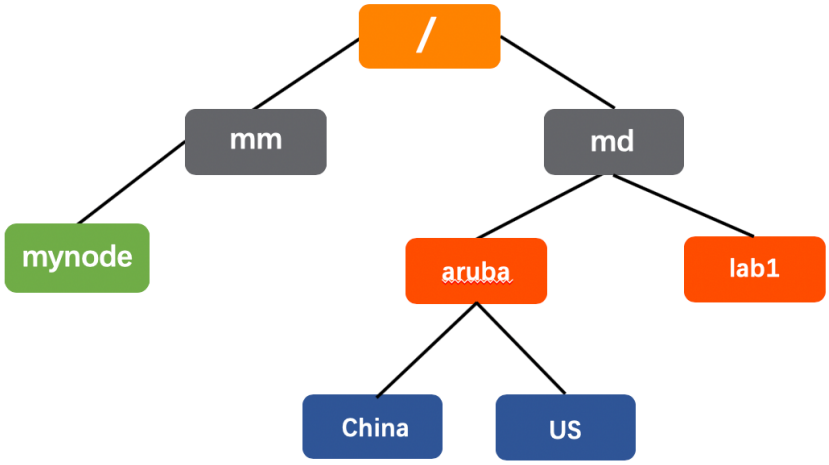
2 AOS8 分层配置(NODE HIERARCHY)

2.1 用户需求

在这个lab中我们需要按照以下需求创建节点层次结构

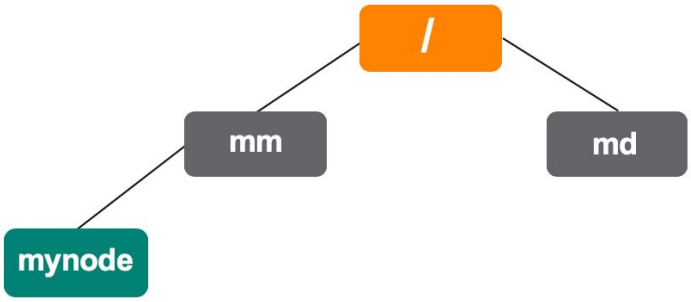
✓ 在/md节点下面创建两个用户配置节点（分组）：aruba和labX <- 这里的X代表lab分组[1…6]

✓ 在/aruba节点下面创建两个用户配置节点（分组）：China和US



2.2 实现思路

ArubaOS 8 中引入了分层配置，以便增强在多控制器网络中应用配置的方式。



/ —— 根节点，MM 及其受管设备通用的配置。

/md —— 所有受管设备通用的配置。 用户可以在此节点下创建其他节点。

/mm —— 主和备 MM（VRRP）通用的配置。

/mm/mynode —— 特定于 MM 的配置。 这只能在相应的 MM 上进行编辑。

NOTE

在可在 Managed Network（/md）节点下创建最多四个嵌套子节点，

例如：/md/Aruba/Aruba-China/Beijing/Building1

2.3 熟悉 AOS8 常用的 CLI 命令

2.3.1 查看 MM 所有配置节点（配置路径）

✓ 方法一：show configuration node-hierarchy

```
(LabX-MM-1) [mynode] #show configuration node-hierarchy <- 这里的 X 代表 lab 分组[1…6]
Default-node is not configured. Autopark is disabled.
Configuration node hierarchy
----------------------------
Config Node              Type    Name
-----------              ----    ----
/                        System
/md                      System
/md/aruba                Group
/md/aruba/China          Group
/md/aruba/US             Group
/md/labX                 Group
/md/labX/00:0b:86:9a:af:37  Device  labX-md1
/md/labX/00:0b:86:dd:2f:00  Device  labX-md2
/mm                      System
/mm/mynode               System
```

✓ 方法二：cd + <Table>键

```
(LabX-MM-1) [mynode] #cd
/
/md
```

```
/md/aruba
/md/aruba/China
/md/aruba/US
/md/labX
/mm
/mm/mynode
labX-md1          Alias for /md/labX/00:0b:86:9a:af:37
labX-md2          Alias for /md/labX/00:0b:86:dd:2f:00
<node-path>       Path of config node
```

2.3.2 更改配置节点

✓ 方法一：通过cd命令

```
(LabX-MM-1) [mynode] #cd /md/
(LabX-MM-1) [md] #
```

✓ 方法二：通过change-config-node命令

```
(LabX-MM-1) [mynode] #change-config-node /md/labX
(LabX-MM-1) [labX] #
```

2.3.3 进入设备（控制器/MD）配置节点

✓ 方法一：通过cd命令，输入完整的设备节点路径

```
(LabX-MM-1) [mynode] #cd /md/labX/00:0b:86:9a:af:37
(LabX-MM-1) [00:0b:86:9a:af:37] #
```

✓ 方法二：通过change-config-node命令，输入完整的设备节点路径

```
(LabX-MM-1) [mynode] #change-config-node /md/labX/00:0b:86:9a:af:37
(LabX-MM-1) [00:0b:86:9a:af:37] #
```

✓ 方法三：通过cd命令，输入设备的别名（hostname）

```
(LabX-MM-1) [mynode] #cd labX-md1
(LabX-MM-1) [00:0b:86:9a:af:37] #
```

✓ 方法三：通过change-config-node命令，输入设备的别名（hostname）

```
(LabX-MM-1) [mynode] #change-config-node labX-md1
(LabX-MM-1) [00:0b:86:9a:af:37] #
```

2.3.4 远程登录 MD（控制器）的方法

✓ 方法一：通过传统的SSH软件登录

```
aruba-MacBook-Pro:~ aruba$ ssh admin@10.1.10.11
The authenticity of host '10.1.10.11 (10.1.10.11)' can't be established.
RSA key fingerprint is SHA256:iuzitYPE12u3w0rt0acWk/zmNOM/p/cyCAhazTs7cxI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.1.10.11' (RSA) to the list of known hosts.
admin@10.1.10.11's password: aruba123


(labX-md1) #
```

✓ 方法二：AOS8中MM提供对接管MD（控制器）免用户名密码的快捷登录控制器的方法

- 快捷登录方法一：通过MM里的mdconnect工具登录

```
(LabX-MM-1) [mynode] #cd labX-md1
(LabX-MM-1) [00:0b:86:9a:af:37] #mdconnect
 Redirecting to Managed Device Shell
(labX-md1) [MDC] #
```

- 快捷登录方法二：通过MM里的logon工具登录，你可以在任意的配置节点使用logon命令。

```
(LabX-MM-1) [mynode] #logon 10.1.10.11
(labX-md1) [MDC] #
```

2.3.5 查看配置的方法

✓ 在AOS8中，配置是有层级关系的，要查看每个层级（节点）的配置，需要用一下命令查看

```
(LabX-MM-1) [labX] #show configuration committed
vlan 120
!
control-plane-security
   auto-cert-prov
!
```

✓ 同时在AOS8中，为了防止误操作，有一个新的功能，配置缓冲机制。你所输入的配置不是立刻生效，需要确认提交后才会下发给设备节点(控制器)

- 查看未提交的配置

通过show configuration pending查看

```
(LabX-MM-1) [labX] (config) #vlan 1000
(LabX-MM-1) ^[labX] (config-submode)#!
(LabX-MM-1) ^[labX] (config) #show configuration pending
vlan 1000
```

- 未提交配置清除

如果我们发现配置错误，但还未提交，不需要传统的no命令一条一条删除，通过以下命令一次性删除

```
(LabX-MM-1) ^[labX] (config) #configuration purge-pending-config
(LabX-MM-1) [labX] (config) #
```

2.3.6 配置提示符

有两种提示符如 『^』和『*』。你可能已经注意到这些符号。

- ✓ ^ 表示MM的当前配置节点或者其他配置节点有未保存的配置，如果要保存并应用该配置，可以执行“show configuration pending”以查看待处理的内容并执行“write memory”提交配置
- ✓ * 表示控制器或者AP产生了crash信息。 可能在本实验中不会出现这一点。 但请记住这一点。可执行“tar crash”来收集crash信息，并将crash文件保存在flash中。 执行命令后 * 会消失，详细的Crash原因需要将保存在flash中的文件发给aruba TAC处理。

```
(labX-md1) *[MDC] #tar crash

(labX-md1) [MDC] #
```

2.4 MM 配置（CLI）

第1步: SSH 登录到 MM（10.X.50.11）<- 这里的 X 代表 lab 分组[1…6]

```
(LabX-MM-1) [mynode] #cd mm

(LabX-MM-1) [mm] #configure terminal
```

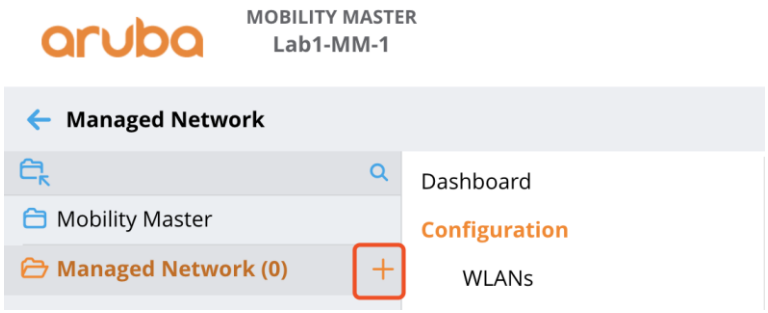
第2步: 创建用户节点（Node Hierarchy），如下:

```
(LabX-MM-1) [mm] (config) #configuration node /md/labX     <- X[1…6]

(LabX-MM-1) [mm] (config) #configuration node /md/aruba

(LabX-MM-1) [mm] (config) #configuration node /md/aruba/China

(LabX-MM-1) [mm] (config) #configuration node /md/aruba/US

(LabX-MM-1) [mm] (config) #exit
```

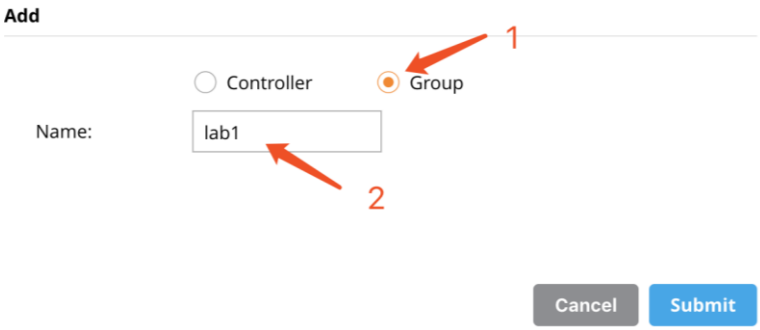
2.5 MM 配置（GUI）

第1步: Web 页面登录到 MM：https://10.X.50.11:4343，用户名：admin，密码：aruba123。点击 ☰ 图标可以看到 MM 的分层配置架构。 （这里的 X 代表 lab 分组[1…6]）

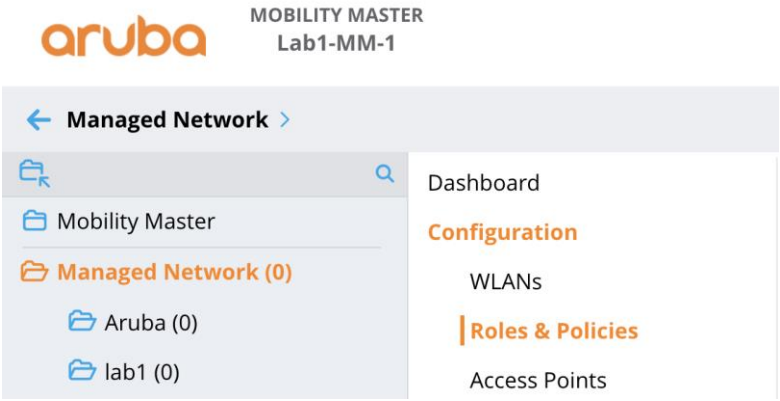
第2步: 点击 Managed Network 右边的“+”



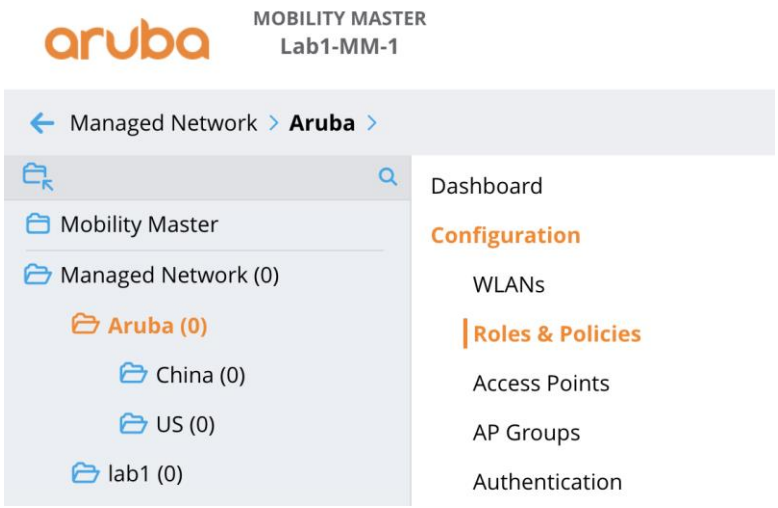
第3步：在弹出到选项卡中，选中 Group（对应 cli 里的 node），在 Name 中输入“labX”，然后点击“Submit” （<- 这里的 X 代表 lab 分组[1…6]）



第4步：重复第 2 步和第 3 步，在 Managed Network 下面创建另一个 Group“Aruba”



第5步：点击“Aruba”节点右边的“+”，创建两个子节点（Group）：“China”和“US”如下图：

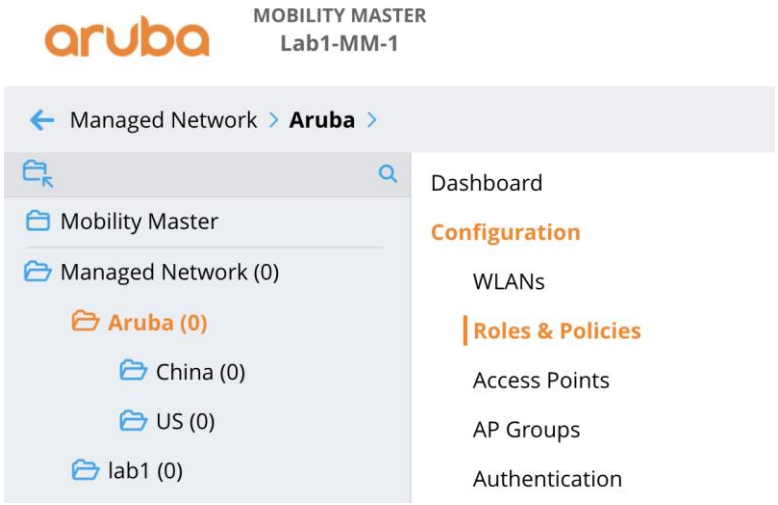


2.6 验证结果

第1步：CLI 查看分层结构，验证创建的用户节点（Node Hierarchy）

```
(LabX-MM-1) [mm] #show configuration node-hierarchy

Default-node is not configured. Autopark is disabled.

Configuration node hierarchy

----------------------------

Config Node              Type    Name

-----------              ----    ----

/                    System

/md                  System

/md/aruba              Group

/md/aruba/China          Group

/md/aruba/US           Group

/md/labX               Group   <- 这里的 X 代表 lab 分组[1…6]

/mm                  System

/mm/mynode             System
```

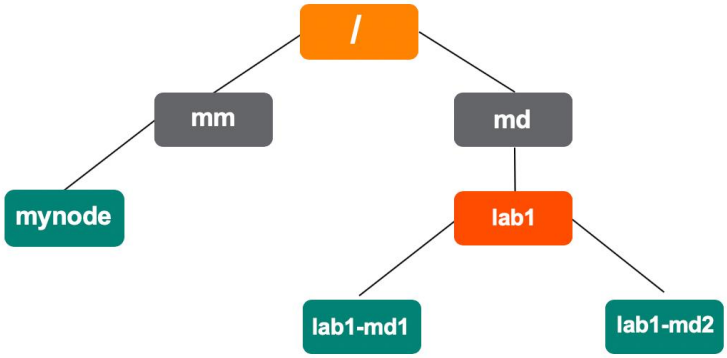
第2步：WEB 页面查看分层结构，验证创建的用户节点（Node Hierarchy）



3 MM 接收管理 MD

3.1 用户需求

- ✓ 根据提供的IP地址信息，对lab环境里的两台7010控制器进行初始化操作。
- ✓ 配置MM接管两台MD，并停靠在配置节点（分组）：/md/labX



3.2 控制器配置

3.2.1 通过 Console 初始化 VMC-1（MD1）

第1步：连接到 VMC-1 后，通过用户密码 admin/aruba123 登录，输入以下命令初始化：

```
(labX-md1) #write erase all

Controller will be factory defaulted. All the configuration and databases will be deleted. Controller will be reloaded. Pres s 'y' to proceed : [y/n]: y

Write Erase successful


System will now restart!
```

第2步：等待系统启动。看到初始化提示，就可以对设备进行初始化操作，配置如下

```
Auto-provisioning is in progress. It requires DHCP and Activate servers

Choose one of the following options to override or debug auto-provisioning...

  'enable-debug'     : Enable auto-provisioning debug logs

  'disable-debug'    : Disable auto-provisioning debug logs

  'mini-setup'       : Start mini setup dialog. Provides minimal customization and requires DHCP server

  'full-setup'       : Start full setup dialog. Provides full customization
```

'static-activate' : Provides customization for static or PPPOE ip assignment. Uses activate for master information

Enter Option (partial string is acceptable): full-setup

Are you sure that you want to stop auto-provisioning and start full setup dialog? (yes/no): yes

Enter System name [Aruba7010_9A_AF_37]: labX-md1 <- 这里的 X 代表 lab 分组[1…6]

Enter Switch Role (standalone|md) [md]:

Enter IP type to terminate IPSec tunnel or secured websocket connection (ipv4|ipv6) [ipv4]:

Enter Master switch IP address/FQDN or ACP IP address/FQDN: 10.X.50.11 <- X[1…6]

Enter Master switch Type? (MM|ACP) [MM]:

Is this a VPN concentrator for managed device to reach Master switch (yes|no) [no]:

This device connects to Master switch via VPN concentrator (yes|no) [no]:

Is Master switch Virtual Mobility Master? (yes|no) [yes]:

Master switch Authentication method (PSKwithIP|PSKwithMAC) [PSKwithIP]:

Enter IPSec Pre-shared Key: aruba123

Re-enter IPSec Pre-shared Key: aruba123

Do you want to enable L3 Redundancy (yes|no) [no]:

Enter Uplink Vlan ID [1]: X10 <- X[1…6]

Enter Uplink port [GE 0/0/0]:

Enter Uplink port mode (access|trunk) [access]: trunk

Enter Native VLAN ID [1]:

Enter Uplink Vlan IP assignment method (dhcp|static|pppoe) [static]:

Enter Uplink Vlan Static IP address [172.16.0.254]: 10.X.10.11 <- X[1…6]

Enter Uplink Vlan Static IP netmask [255.255.255.0]:

Enter IP default gateway [none]: 10.X.10.250 <- X[1…6]

Enter DNS IP address [none]: 114.114.114.114

Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no

Do you want to configure dynamic port-channel (yes|no) [no]:

Enter Country code (ISO-3166), <ctrl-I> for supported list: cn

You have chosen Country code CN for China (yes|no)?: yes

Enter the controller's IANA Time zone [America/Los_Angeles]: Asia/Shanghai

Enter Time in UTC [22:43:08]: （备注：设置当前时间）

Enter Date (MM/DD/YYYY) [11/18/2019]: （备注：设置当前日期）

Do you want to create admin account (yes|no) [yes]:

Enter Password for admin login (up to 32 chars): aruba123

Re-type Password for admin login: aruba123

第3步：确认初始化配置，输入“yes”完成初始化设置，MD1 将会自动重启。

Current choices are:

System name: labX-md1 <- 这里的 X 代表 lab 分组[1…6]

Switch Role: md

IP type to terminate IPSec tunnel or secured websocket connection: ipv4

Master switch IP address or FQDN: 10.1.50.11

Is this VPN concentrator: no

Connect via VPN concentrator: no

IPSec authentication method: PSKwithIP

Vlan id for uplink interface: 110

Uplink port: GE 0/0/0

Uplink port mode: trunk

Native VLAN id: 1

Uplink Vlan IP assignment method: static

Uplink Vlan static IP Address: 10.1.10.11

```
Uplink Vlan static IP net-mask: 255.255.255.0

Uplink Vlan IP default gateway: 10.1.10.250

Domain Name Server to resolve FQDN: 114.114.114.114

Option to configure VLAN interface IPV6 address: no

Country code: cn

IANA Time Zone: Asia/Shanghai

Admin account created: yes


Note: These settings require IP-Based-PSK configuration on Master switch


If you accept the changes the switch will restart!

Type <ctrl-P> to go back and change answer for any question

Do you wish to accept the changes (yes|no)yes
```

NOTE 如果发现初始化时，输入错误配置，可以通过输入 <ctrl-P>更改，输入<ctrl-X>从头开始。

3.2.2 通过 Console 初始化 VMC-2（MD2）

第1步：连接到 VMC-2 后，通过用户密码 admin/aruba123 登录，输入以下命令初始化：

```
(labX-md2) #write erase all

Controller will be factory defaulted. All the configuration and databases will be deleted. Controller will be reloaded. Pres
s 'y' to proceed : [y/n]: y

Write Erase successful


System will now restart!
```

第2步：等待启动，看到初始化提示，就可以对设备进行初始化操作，配置如下

```
Auto-provisioning is in progress. It requires DHCP and Activate servers

Choose one of the following options to override or debug auto-provisioning...
```

'enable-debug' : Enable auto-provisioning debug logs

'disable-debug' : Disable auto-provisioning debug logs

'mini-setup' : Start mini setup dialog. Provides minimal customization and requires DHCP server

'full-setup' : Start full setup dialog. Provides full customization

'static-activate' : Provides customization for static or PPPOE ip assignment. Uses activate for master information

Enter Option (partial string is acceptable): full-setup

Are you sure that you want to stop auto-provisioning and start full setup dialog? (yes/no): yes

Enter System name [Aruba7010_DD_2F_00]: labX-md2 <- 这里的 X 代表 lab 分组[1…6]

Enter Switch Role (standalone|md) [md]:

Enter IP type to terminate IPSec tunnel or secured websocket connection (ipv4|ipv6) [ipv4]:

Enter Master switch IP address/FQDN or ACP IP address/FQDN: 10.X.50.11 <- X[1…6]

Enter Master switch Type? (MM|ACP) [MM]:

Is this a VPN concentrator for managed device to reach Master switch (yes|no) [no]:

This device connects to Master switch via VPN concentrator (yes|no) [no]:

Is Master switch Virtual Mobility Master? (yes|no) [yes]:

Master switch Authentication method (PSKwithIP|PSKwithMAC) [PSKwithIP]:

Enter IPSec Pre-shared Key: aruba123

Re-enter IPSec Pre-shared Key: aruba123

Do you want to enable L3 Redundancy (yes|no) [no]:

Enter Uplink Vlan ID [1]: X10 <- X[1…6]

Enter Uplink port [GE 0/0/0]:

Enter Uplink port mode (access|trunk) [access]: trunk

Enter Native VLAN ID [1]:

Enter Uplink Vlan IP assignment method (dhcp|static|pppoe) [static]:

```
Enter Uplink Vlan Static IP address [172.16.0.254]: 10.X.10.12     <- X[1…6]
Enter Uplink Vlan Static IP netmask [255.255.255.0]:
Enter IP default gateway [none]: 10.X.10.250     <- X[1…6]
Enter DNS IP address [none]: 114.114.114.114
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
Do you want to configure dynamic port-channel (yes|no) [no]:
Enter Country code (ISO-3166), <ctrl-I> for supported list: cn
You have chosen Country code CN for China (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los_Angeles]: Asia/Shanghai
Enter Time in UTC [11:38:10]:
Enter Date (MM/DD/YYYY) [11/19/2019]:
Do you want to create admin account (yes|no) [yes]:
Enter Password for admin login (up to 32 chars): aruba123
Re-type Password for admin login: aruba123
```

第3步：确认初始化配置，输入“yes”完成初始化设置，MD2 将会自动重启。

```
Current choices are:


System name: labX-md2.       <- 这里的 X 代表 lab 分组[1…6]
Switch Role: md
IP type to terminate IPSec tunnel or secured websocket connection: ipv4
Master switch IP address or FQDN: 10.X.50.11     <- X[1…6]
Is this VPN concentrator: no
Connect via VPN concentrator: no
IPSec authentication method: PSKwithIP
Vlan id for uplink interface: X10     <- X[1…6]
Uplink port: GE 0/0/0
```

```
Uplink port mode: trunk
Native VLAN id: 1
Uplink Vlan IP assignment method: static
Uplink Vlan static IP Address: 10.X.10.12     <- X[1…6]
Uplink Vlan static IP net-mask: 255.255.255.0
Uplink Vlan IP default gateway: 10.X.10.250   <- X[1…6]
Domain Name Server to resolve FQDN: 114.114.114.114
Option to configure VLAN interface IPV6 address: no
Country code: cn
IANA Time Zone: Asia/Shanghai
Admin account created: yes
Note: These settings require IP-Based-PSK configuration on Master switch
If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no)yes
```

3.3 MM 配置（CLI）

第1步：添加 MD 到 MM 的 local 控制器列表

```
(LabX-MM-1) [mynode] #cd mm
(LabX-MM-1) [mm] #configure terminal
(LabX-MM-1) [mm] (config) #localip 10.X.10.11 ipsec aruba123   <- X[1…6]
(LabX-MM-1) ^[mm] (config) #localip 10.X.10.12 ipsec aruba123  <- X[1…6]
(LabX-MM-1) ^[mm] (config) #write memory
Saving Configuration...
Configuration Saved.
```

第2步：验证添加的控制器

```
(LabX-MM-1) [mm] (config) #show switches

All Switches

------------

IP Address  IPv6 Address  Name      Location        Type    Model      Version      Status  Configuration State     Config S
ync Time (sec)  Config ID

----------  ------------  ----      --------        ----    -----      -------      ------  -------------------     ---------------------  --
-------

10.1.50.11  None          LabX-MM-1  Building1.floor1  master  ArubaMM-VA  8.4.0.0_68230  up      UPDATE SUCCESSFUL
     0                2

10.1.10.11  None          labX-md1   Building1.floor1  MD      ArubaMC-VA   8.4.0.0_68230  up      UNK(00:0b:86:9a:af:37)
N/A                 N/A

10.1.10.12  None          labX-md2   Building1.floor1  MD      ArubaMC-VA   8.4.0.0_68230  up      UNK(00:0b:86:dd:2f:00)
N/A                 N/A


Total Switches:3
```

第3步：添加 MD 到用户节点/md/labX　<- 这里的 X 代表 lab 分组[1…6]

方法一：手动添加（mac 地址为第 2 步中看到的标记为 UNK 的控制器 mac 地址）

```
(LabX-MM-1) [mm] (config) #configuration device 00:0b:86:9a:af:37 device-model MC-VA /md/labX

(LabX-MM-1) [mm] (config) #configuration device 00:0b:86:dd:2f:00 device-model MC-VA /md/labX
```

NOTE　这里的 device-model 参数一定要和 md 的实际型号一致，否则会导致 md 无法正常上线

方法二：自动停靠

```
(LabX-MM-1) [mm] (config) #configuration device default-node /md/labX    <- X[1…6]
```

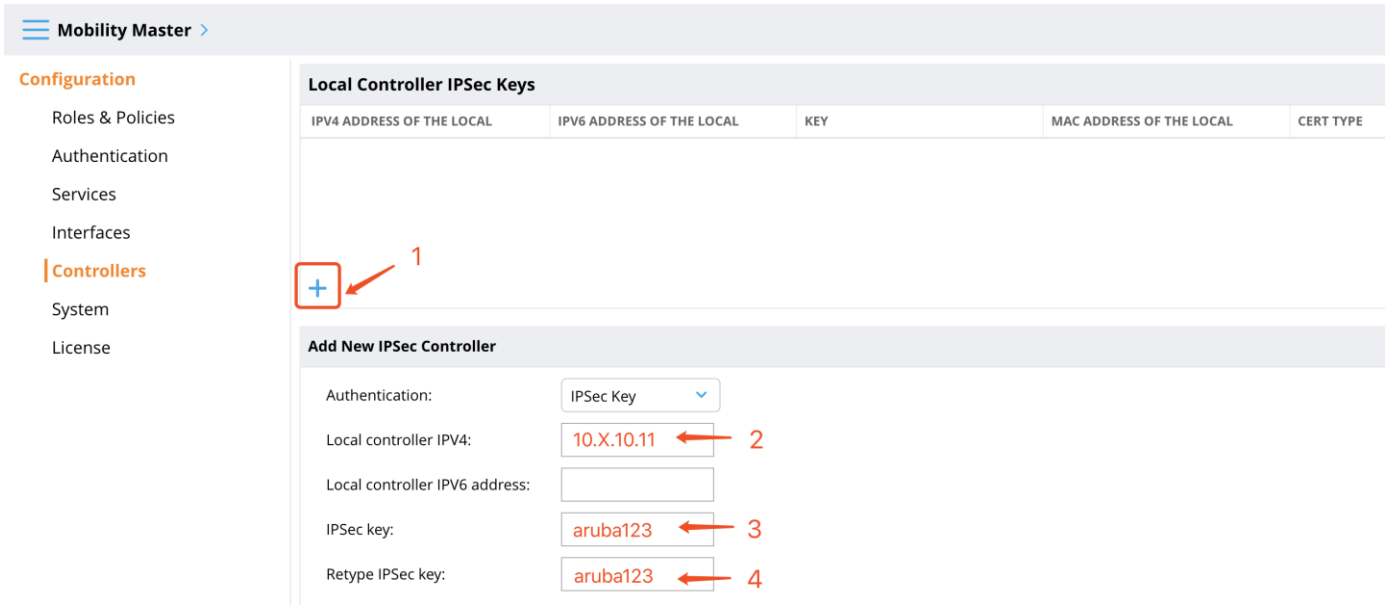
NOTE 自动停靠功能使 MM 接收管理 MD 变得更加容易，特别是有需要引入多个 MD 的情况。 用户可以启用自动停靠并可以灵活选择 /md 下的任何节点作为默认节点来接收管理 MD。

3.4 MM 配置（GUI）

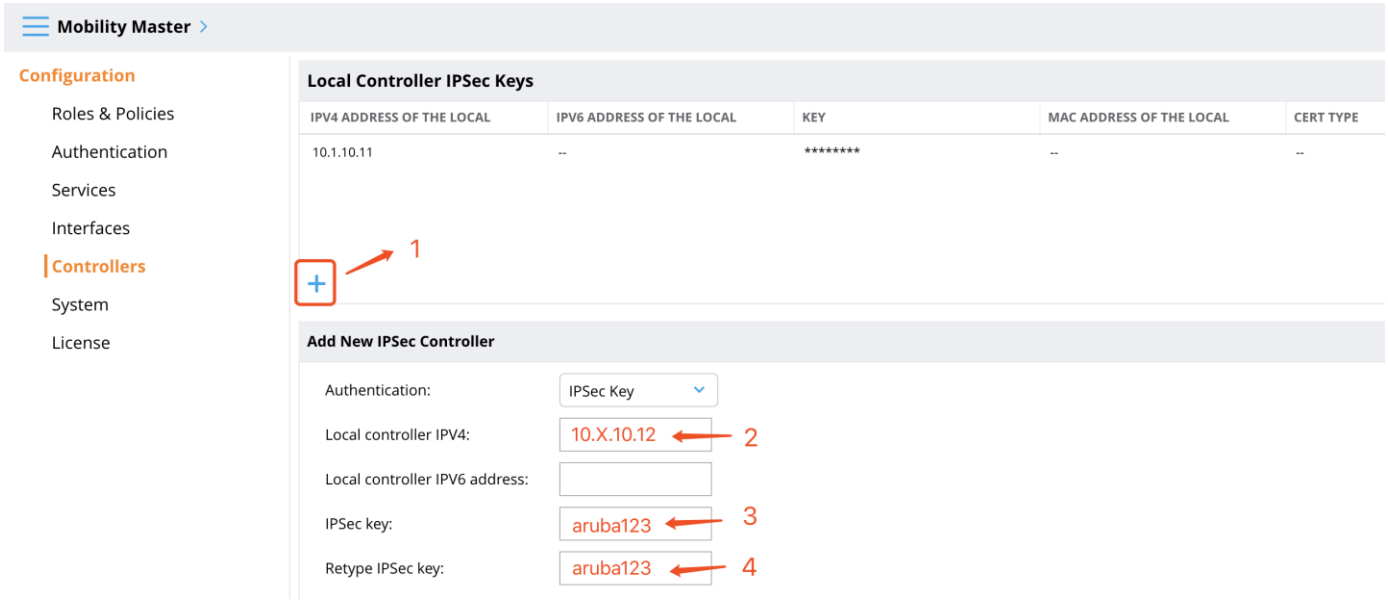
第1步: 登录到 MM 的 Web UI: https://10.X.50.11 <- 这里的 X 代表 lab 分组[1…6]

第2步: 找到 Mobility Master - > Configuration -> Controllers，点击“+”添加 MD 到 MM 的 local 控制器列表，如下图所示

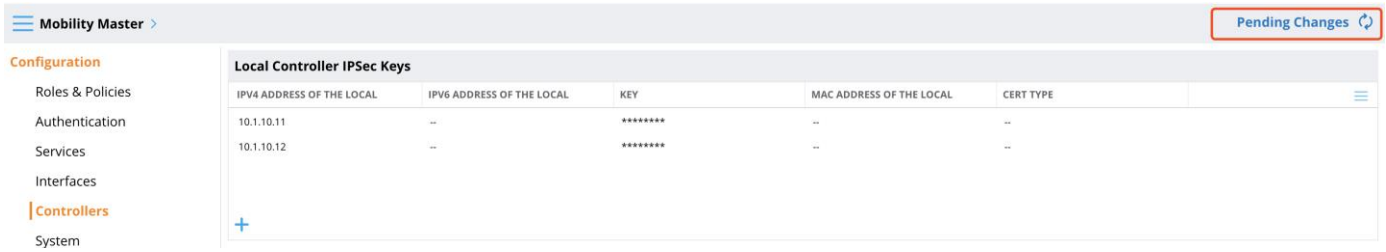
✓ 添加 MD1



✓ 添加 MD2



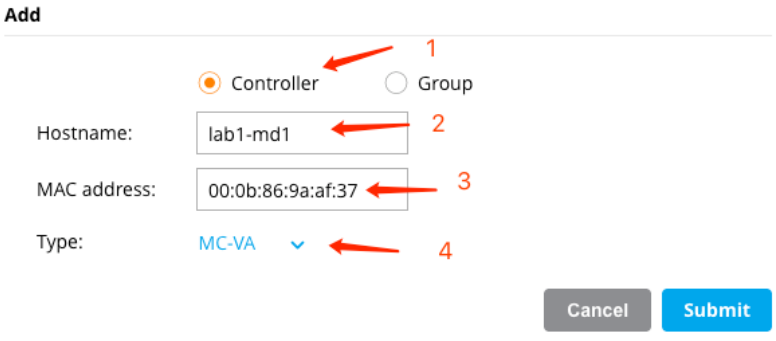
第3步：点击右上角 Pending Changes，完成配置提交

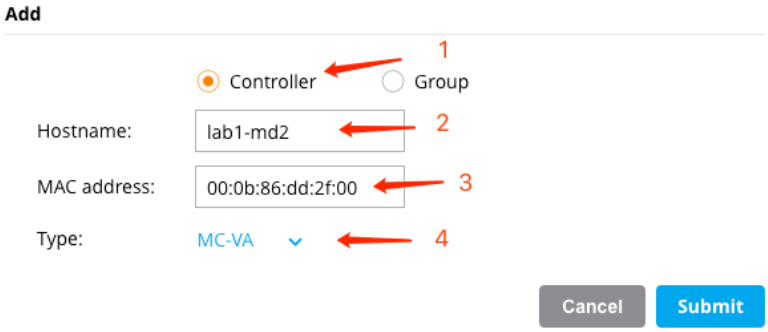


第4步：添加 MD 到用户节点/md/labX　<- X[1…6]

方法一：手动添加（mac 地址为第 2 步中看到的标记为 UNK 的控制器 mac 地址）

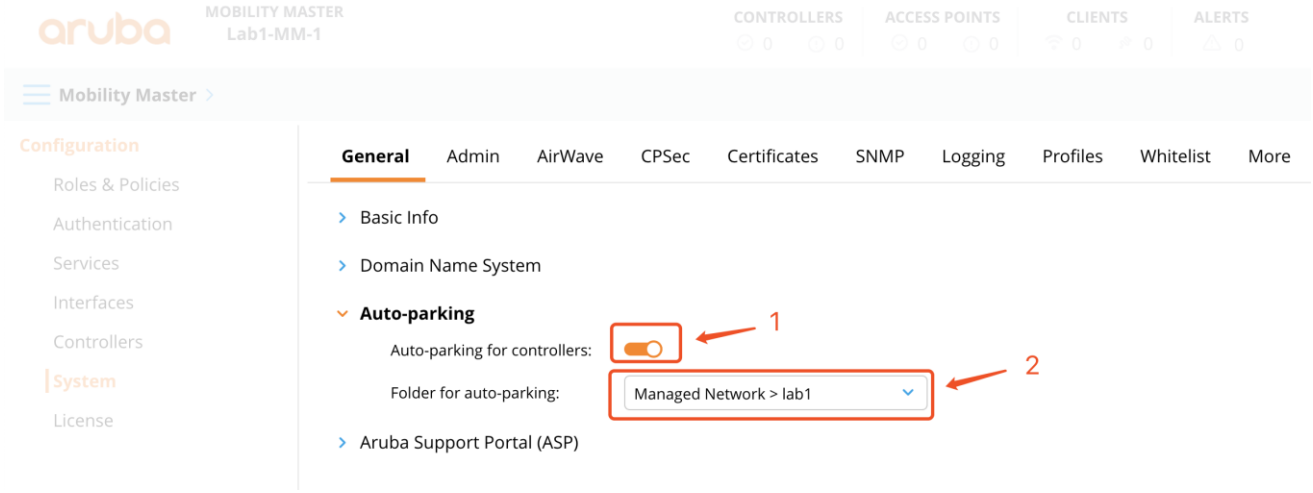
找到 Managed Network ,点击 labX 右边的“+”，弹出的选项卡中，选择“Controller”，添加两台控制器如下图：





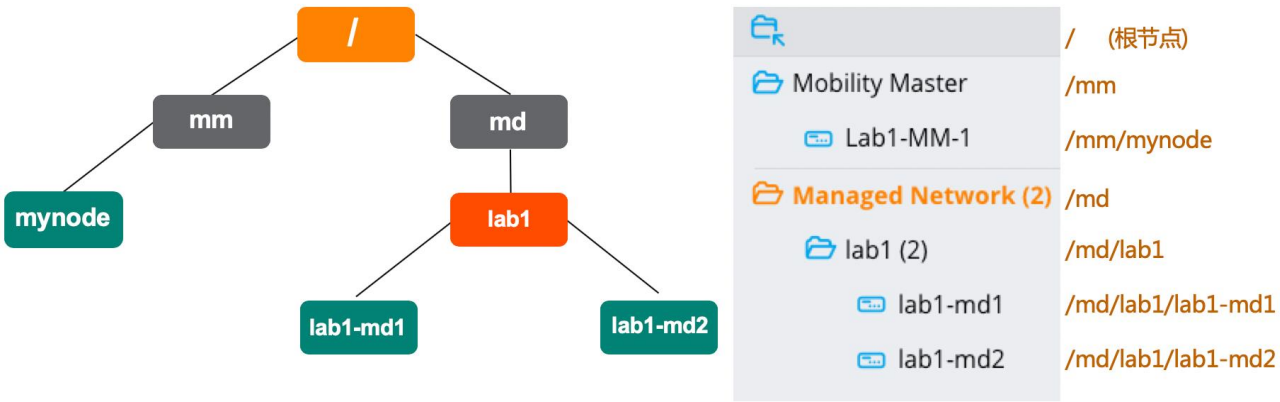
方法二：自动停靠

找到 Mobility Master - > Configuration -> System，在 General 选项卡中配置如下图所示



3.5 验证结果

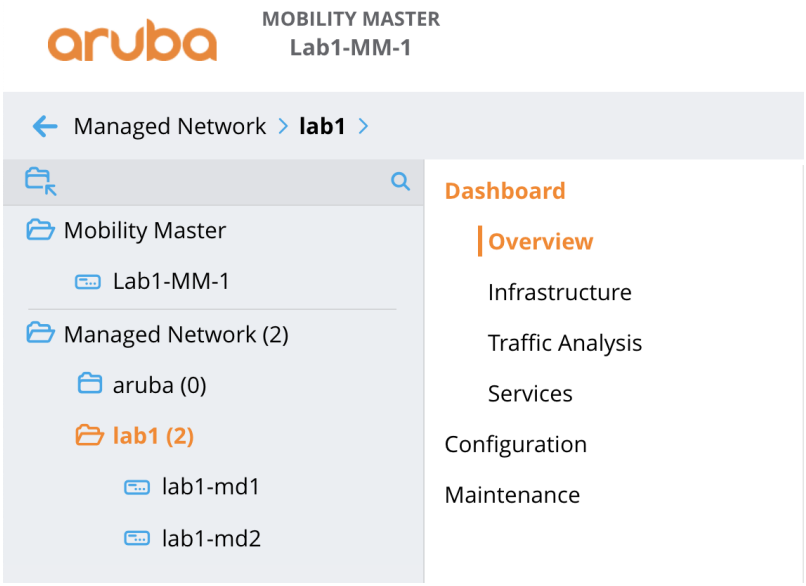
第1步：查看分层结构



✓ CLI:

```
(LabX-MM-1) [mm] (config) #show configuration node-hierarchy
Default-node is not configured. Autopark is disabled.
Configuration node hierarchy
---------------------------
Config Node              Type    Name
-----------              ----    ----
/                        System
/md                      System
/md/aruba                Group
/md/aruba/China          Group
/md/aruba/US             Group
/md/labX                 Group
/md/labX/00:0b:86:9a:af:37  Device  labX-md1
/md/labX/00:0b:86:dd:2f:00  Device  labX-md2
/mm                      System
/mm/mynode               System
```

✓ GUI:



第2步：查看配置同步状态

```
(LabX-MM-1) [mm] (config) #show switches

All Switches

------------

IP Address  IPv6 Address  Name      Location         Type  Model      Version      Status  Configuration State  Config Sync Time (sec)  Config ID

----------  ------------  ----      --------         ----  -----      -------      ------  -------------------  ----------------------  ---------

10.1.50.11  None          Lab1-MM-1 Building1.floor1 master ArubaMM-VA 8.4.0.0_68230 up      UPDATE SUCCESSFUL    0                       2

10.1.10.11  None          lab1-md1  Building1.floor1 MD     ArubaMC-VA 8.4.0.0_68230 up      UPDATE SUCCESSFUL    10                      2

10.1.10.12  None          lab1-md2  Building1.floor1 MD     ArubaMC-VA 8.4.0.0_68230 up      UPDATE SUCCESSFUL    10                      2


Total Switches:3
```

4 AOS8 LICENSE

4.1 用户需求

- ✓ 在MM添加相关License，并开启PEF和RFP feature。
- ✓ 开启license pool功能，将License分配到不同分层配置节点

4.2 实现思路

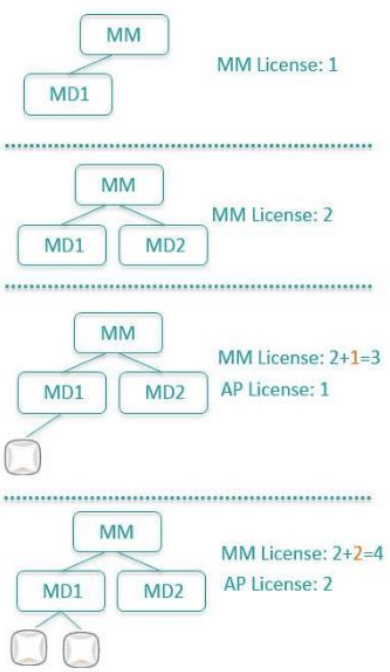
4.2.1 Centralized licensing 工作模式

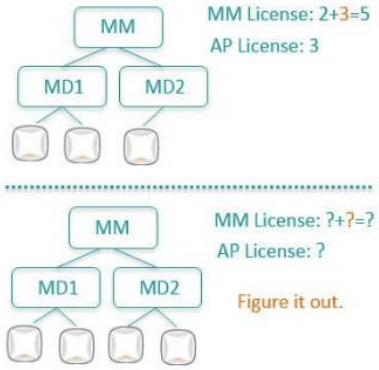
默认情况下，ArubaOS 8.0 中启用了集中许可（Centralized licensing）。 主 MM 维护许可证数据库。所有许可证都需要安装在 MM 上。

- ✓ 支持的模式：
  - ■ Mobility Master（MM）作为所有相关受管设备（MD）的许可服务器。
  - ■ 独立控制器（Standalone）充当另一个独立控制器（Standalone）的许可服务器。
- ✓ 不支持的模式：
  - ■ Mobility Master同时充当其关联的MD和Standalone控制器的许可服务器（8.2版本以前，8.3以后没有这个限制）

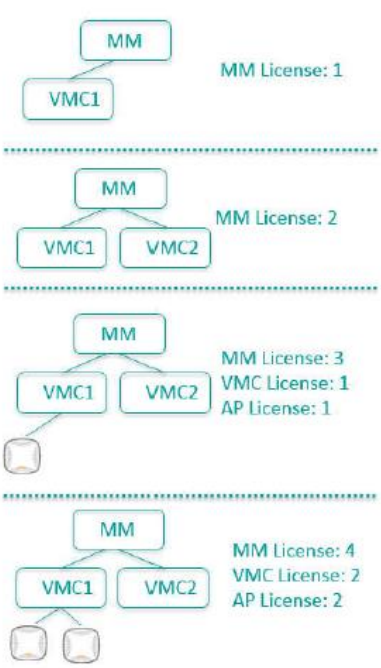
4.2.2 AOS 8 license 消耗计算

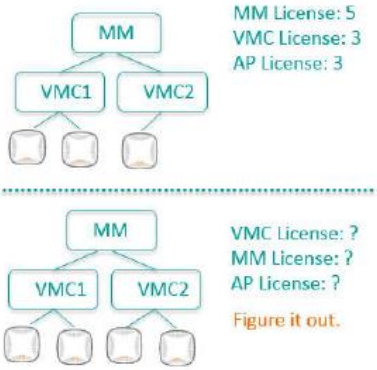
- ✓ MM License:
  - ■ 每个 MD 都会消耗 1 个 MM 许可。我们的两个 MD（MD1 和 MD2）消耗了两个 MM 许可。
  - ■ 每个 VMC 会消耗 1 个 MM 许可
  - ■ 在 MD 上启动的每个 AP 也将消耗 1 个 MM 许可。
- ✓ AP License:
  - ■ 在 MD 上启动的每个 AP 也将消耗 1 个 AP 许可证。
  - ■ 如果开启了 PEF 和 RFP 功能，同时会消耗一个 PEF 和一个 RFP 许可。
- ✓ VMC License:
  - ■ 在 VMC 上启动的每个 AP 将消耗 1 个 VMC 许可。
- ✓ License 计算练习 1:





✓ License 计算练习 2:





4.3 MM 配置（CLI）

4.3.1 在 mynode 节点添加 license

第1步: 添加 license

```
(LabX-MM-1) [mm] #cd /mm/mynode

(LabX-MM-1) [mynode] #license add <LICENSE KEY>
```

NOTE License 文件在桌面 Student Folder，如果 lic 已经添加，此步骤可以跳过

第2步: 查看添加到 license

```
(LabX-MM-1) [mm] #show license

License Table

-------------

Key                                                    Installed           Expires(Grace period expiry)  Flags  Service Type

---                                                    ---------           ----------------------------  -----  ------------

s37BbgwU-hdoW6e7H-ZxjM+c8q-qoQkJhVJ-SKBZELCq-k9SC5pZk-uNzhcgVf-u5wxFo+8-yxK7gNig-Ma4  2019-01-05 08:00:34  Never                       E     MM-VA: 50

UpbpPkNY-2mlbJIVG-Dkiyq6eE-rGLwKjcm-iJgyi0b+-Vyrz9RqJ-zAHZZyYH-HIc50+AM-t/ggIfBl-l9s  2019-01-05 08:00:51  Never                       E     MC-VA-RW: 10

Dlnsnify-83tqlWng-yHvFMmVZ-WpmjjSIE-xE2XWokV-ZxDoPCnT-a7d0EgbI-g2xsVovE-vy8ffM3t-Clo  2019-01-05 08:01:08  Never                       E     Access Points: 8

pwCuhbYz-rfG+CUZP-Uj0pQ06A-9PEd+pp0-RUyuK3h2-9Lbv8d0f-XT6NrHpb-AKjntsY5-DUopLp8I-32M  2019-01-05 08:01:25  Never                       E     Next Generation Policy Enforcement Firewall Module: 8

YdcR5o8K-xgod+Mr/-HfUWH4Az-3j/p3jT+-ogVVNyad-DKv/BQkp-pjRtHT3t-gBVRz3SX-4NAurYHm-26g  2019-01-05 08:01:44  Never                       E     RF Protect: 8


License Entries: 5

Flags: A - auto-generated; E - enabled; S - Subscription; R - reboot/activation key required to activate; D - Not enabled on license client

Note: Time under 'Installed' for Subscription licenses is the license generation time.
```

4.3.2 开启 PEF 和 RFP 功能

在本实验中，所有MM都已安装许可证。 在ArubaOS 8.0中，有一个名为feature bit的新东西。 添加完许可证

后，需要启用该功能。 默认启用VMC，MM和AP License功能。

第1步: 使用 SSH 方式登录到 Mobility Master (10.X.50.11) <- X[1…6]，进入 /mm 配置节点

```
(LabX-MM-1) [mynode] #cd /mm

(LabX-MM-1) [mm] #
```

第2步: 进入配置模式

```
(LabX-MM-1) [mm] #configure terminal

Enter Configuration commands, one per line. End with CNTL/Z

(LabX-MM-1) [mm] (config) #
```

第3步: 开启 PEF 功能和 RFP 功能

```
(LabX-MM-1) [mm] (config) #license-pool-profile-root

(LabX-MM-1) ^[mm] (License root(/) pool profile) #pefng-licenses-enable

Please ensure to add licenses before enabling feature bit.

(LabX-MM-1) ^[mm] (License root(/) pool profile) #rfp-license-enable

Please ensure to add licenses before enabling feature bit.

(LabX-MM-1) ^[mm] (License root(/) pool profile) #!

(LabX-MM-1) ^[mm] (config) #write memory

Saving Configuration...

Configuration Saved.
```

第4步: 验证结果

```
(LabX-MM-1) [mm] (config) #show license-pool-profile-root

License root(/) pool profile

----------------------------

Parameter            Value

---------            -----

enable PEFNG feature  Enabled

enable RFP feature    Enabled
```

```
enable ACR feature    Disabled
enable WebCC feature  Disabled
```

NOTE 在开启 PEF 功能和 RFP 功能之前，一定要确保 MM 上安装了这两种许可。如果没有添加 PEF 和 RPF 功能许可，切勿开启相关 feature。否则会导致 AP 无法正常上线。

4.3.3 license pool 功能

第1步: 为 /md/labX 配置节点（分组）启用 license pool 功能 <- 这里的 X 代表 lab 分组[1…6]

```
(LabX-MM-1) [mm] #configure terminal
(LabX-MM-1) [mm] (config) #license-pool-profile /md/labX    <- X[1…6]
(LabX-MM-1) ^[mm] (License pool profile "/md/lab1") #license-pool-path /md/labX    <- X[1…6]
(LabX-MM-1) ^[mm] (License pool profile "/md/lab1") #mm-licenses 5
(LabX-MM-1) ^[mm] (License pool profile "/md/lab1") #ap-licenses 5
(LabX-MM-1) ^[mm] (License pool profile "/md/lab1") #pefng-licenses 5
(LabX-MM-1) ^[mm] (License pool profile "/md/lab1") #!
```

第2步: 保存配置

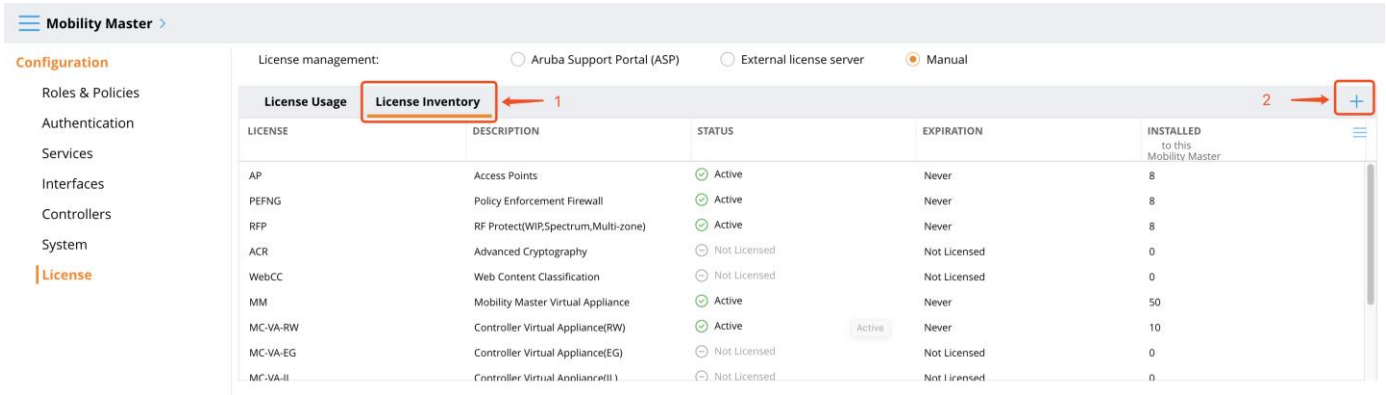
```
(LabX-MM-1) ^[mm] (config) #write memory
Saving Configuration...
Configuration Saved.
```

4.4 MM 配置（GUI）

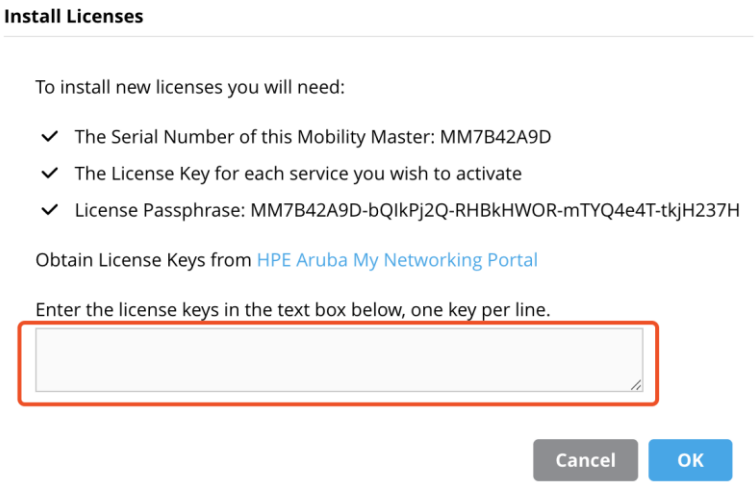
4.4.1 在 web 页面添加 license

第1步: 登录到 MM 的 Web UI: https://10.X.50.11 （这里的 X 代表 lab 分组[1…6]）

第2步: 找到 Mobility Master - > Configuration -> License，点击“License Inventory”，点击右侧的“+”添加 license，如下图所示



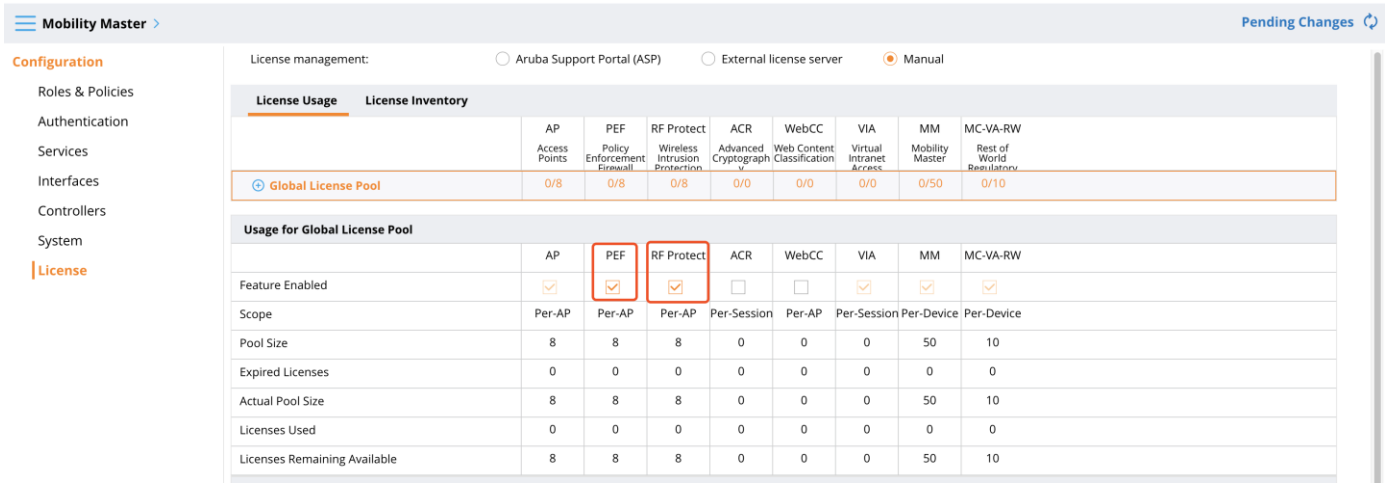
第3步：在弹出的提示框，输入对应的 license key



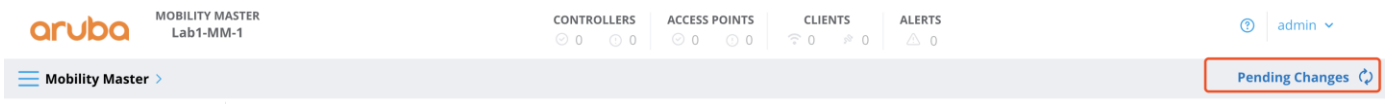
NOTE　本次 lab 所有 license 已经添加，此步骤可以跳过

4.4.2　开启 PEF 和 RFP 功能

第1步：找到 Mobility Master - > Configuration -> License，点击“License Useage”，选择启用“PEF”和“RFP”，如下图所示，并点击 “Submit”提交配置。

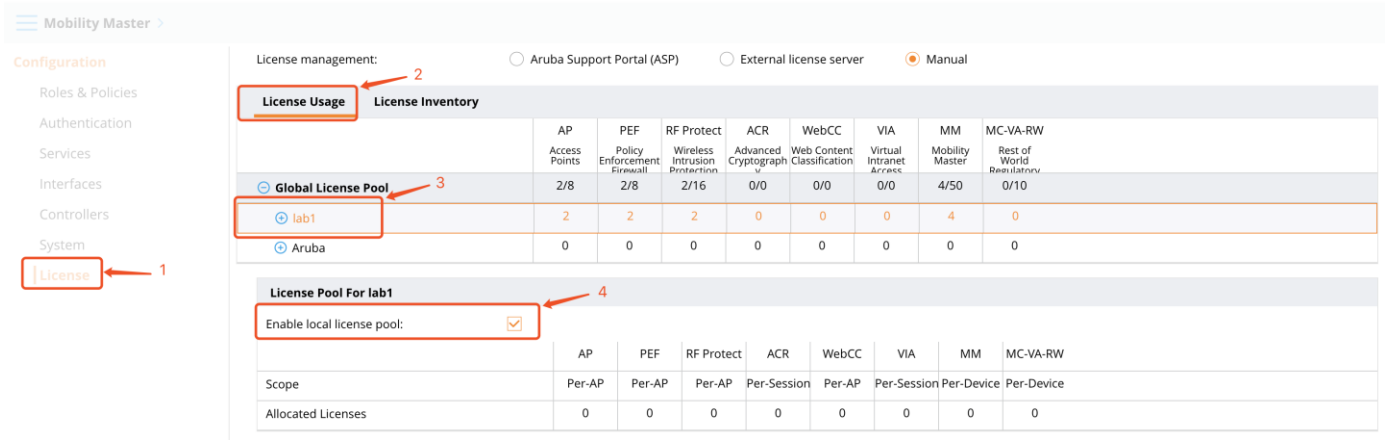


第2步：点击右上角的“Pending Changes”,保存配置

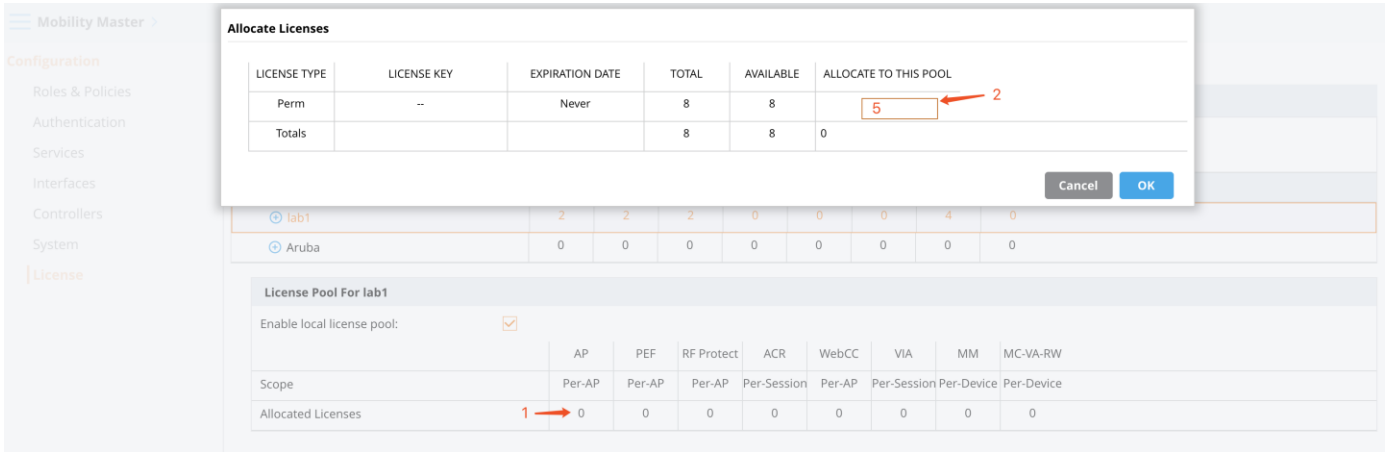


4.4.3 license pool 功能

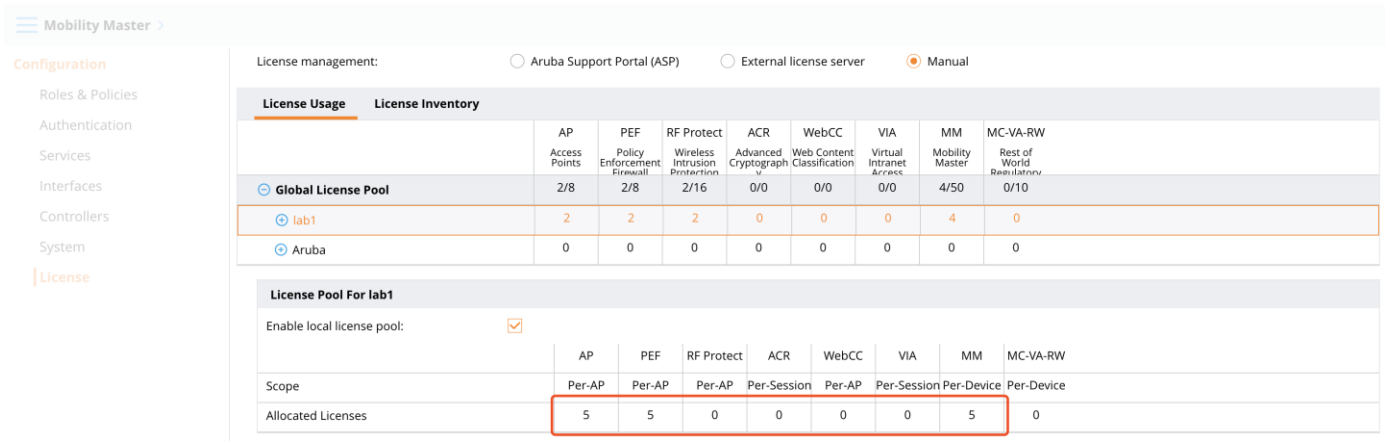
第1步：找到 Mobility Master - > Configuration -> License，点击“License Useage”，启用 labX 的 Enable local license pool 功能，如下图所示，（X[1…6]）



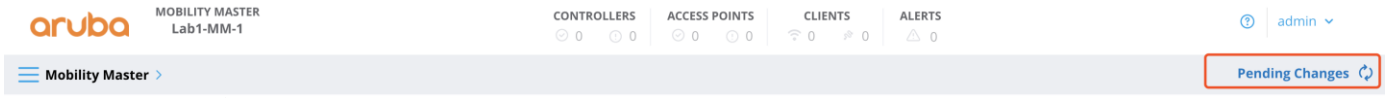
第2步：单击 AP 对应的 Allocated License 的数字“0”，在弹出的选项卡中，配置 ALLOCATE THIS POOL 为“5”，如下图所示，



第3步：依次分配 PEF，MM license 的数量为“5”，结果如下图所示：并点击 “Submit”提交配置。



第4步：点击右上角的“Pending Changes”,保存配置



4.5 验证结果

第1步：检查 license pool 开启。

```
(LabX-MM-1) [mm] # show license-pool-profile labX(具体可以用“？”查看profile name)


License pool profile "/md/lab1"

-------------------------------
```

Parameter	Value
License pool path	/md/labX
AP permanent licenses	5
AP expiry licenses	N/A
PEFNG permanent licenses	5
PEFNG expiry licenses	N/A
RFP permanent licenses	N/A
RFP expiry licenses	N/A
ACR permanent licenses	N/A
ACR expiry licenses	N/A
WebCC expiry licenses	N/A
WebCC subscription licenses	N/A
VIA permanent licenses	N/A
VIA expiry licenses	N/A
MM permanent licenses	5
MM expiry licenses	N/A
MC-VA Egypt permanent licenses	N/A
MC-VA Egypt expiry licenses	N/A
MC-VA Israel permanent licenses	N/A
MC-VA Israel expiry licenses	N/A
MC-VA Japan permanent licenses	N/A
MC-VA Japan expiry licenses	N/A
MC-VA USA permanent licenses	N/A
MC-VA USA expiry licenses	N/A
MC-VA Rest of the world permanent licenses	N/A
MC-VA Rest of the World expiry licenses	N/A

NOTE	这里我们只为/md/labX 配置节点分配了 MM、AP、PEF 许可，所以看到 RPF 许可的状态是 Disabled 的。

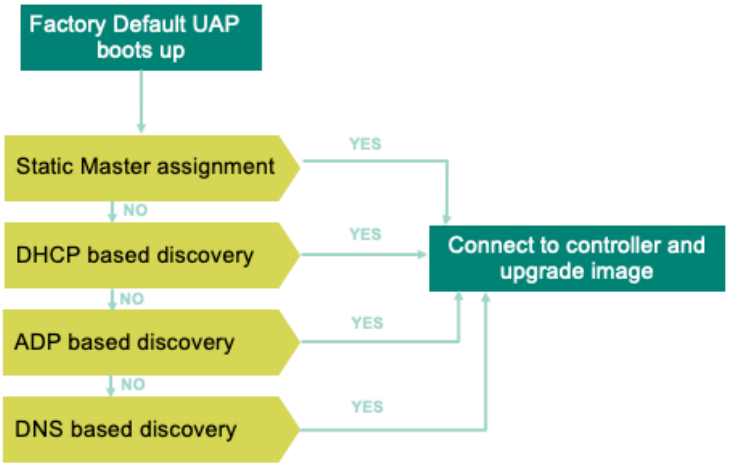
5 AP 上线操作

5.1 用户需求

用户希望AP实现零配置上线

5.2 实现思路

✓ Aruba AP如何找到指定的Aruba无线控制器



出厂配置的AP加电启动后发现控制器的顺序如下：

1. 在AP上静态配置了Master ip
   - Master IP为控制器IP地址或者控制器VRRP IP。
2. 通过DHCP发现控制器
   - DHCP下发了option 43 （控制器IP地址或者控制器VRRP IP）
   - option 60（ArubaAP）字段
3. 通过ADP协议发现控制器
   - AP和控制器在同一个网段
4. 通过DNS发现控制器
   - AP向aruba-master.<domain.com>域名发送DNS请求，
   - DNS服务器响应改请求为控制器IP地址或者控制器VRRP IP

在本lab中，我们采用的是第2种：DHCP方式

5.3 MM 配置（CLI）

5.3.1 关闭 CPSec 功能

第1步: 进入到/md/labX（这里的 X 代表 lab 分组[1…6]）配置节点

```
(LabX-MM-1) [mm] #cd /md/labX     <- X[1…6]

(LabX-MM-1) [labX] #
```

第2步: 关闭 CPSec 功能（第 2 步和第 3 步选择其中一步操作）

```
(LabX-MM-1) [labX] #configure terminal

(LabX-MM-1) [labX] (config) #control-plane-security

(LabX-MM-1) ^[labX] (Control Plane Security Profile) #no cpsec-enable
```

第3步: 保存配置

```
(LabX-MM-1) ^[labX] (Control Plane Security Profile) #write memory

Saving Configuration...

Configuration Saved.
```

5.3.2 启用 CPSec 功能 （注：5.3.1 和 5.3.2 配置二选一）

第4步: 开启 CPSec 功能

```
(LabX-MM-1) [labX] #configure terminal

(LabX-MM-1) [labX] (config) #control-plane-security

(LabX-MM-1) [labX] (Control Plane Security Profile) #cpsec-enable

(LabX-MM-1) ^[labX] (Control Plane Security Profile) #auto-cert-prov
```

第5步: 保存配置

```
(LabX-MM-1) ^[labX] (Control Plane Security Profile) #write memory

Saving Configuration...

Configuration Saved.
```

5.3.3 配置 VRRP

第1步: 进入到 labX-md1 设备配置节点，配置 VRRP，进程 ID:X0，VIP 为:10.X.10.10，优先级:120（这里的 X 代表 lab 分组[1…6]）

```
(LabX-MM-1) [mynode] #cd labX-md1     <- X[1…6]
(LabX-MM-1) [00:0b:86:9a:af:37] #configure terminal
```

第2步: 进入到 labX-md1 设备配置节点，配置 VRRP，进程 ID:X0，VIP:10.X.10.10，优先级:120（这里的 X 代表 lab 分组[1…6]）

```
(LabX-MM-1) [00:0b:86:9a:af:37] (config) #vrrp X0     <- X[1…6]
(LabX-MM-1) ^[00:0b:86:9a:af:37] (config-submode)#ip address 10.X.10.10     <- X[1…6]
(LabX-MM-1) ^[00:0b:86:9a:af:37] (config-submode)#authentication aruba123
(LabX-MM-1) ^[00:0b:86:9a:af:37] (config-submode)#priority 120
(LabX-MM-1) ^[00:0b:86:9a:af:37] (config-submode)#vlan X10     <- X[1…6]
(LabX-MM-1) ^[00:0b:86:9a:af:37] (config-submode)#no shutdown
(LabX-MM-1) ^[00:0b:86:9a:af:37] (config-submode)#!
(LabX-MM-1) ^[00:0b:86:9a:af:37] (config) #write memory
Saving Configuration...
Configuration Saved.
```

第3步: 进入到 labX-md2 设备配置节点，配置 VRRP，进程 ID:X0，VIP:10.X.10.10，优先级:110（这里的 X 代表 lab 分组[1…6]）

```
(LabX-MM-1) [00:0b:86:9a:af:37] (config) #cd labX-md2     <- X[1…6]
(LabX-MM-1) [00:0b:86:dd:2f:00] (config) #vrrp X0     <- X[1…6]
(LabX-MM-1) ^[00:0b:86:dd:2f:00] (config-submode)#ip address 10.X.10.10     <- X[1…6]
(LabX-MM-1) ^[00:0b:86:dd:2f:00] (config-submode)#authentication aruba123
(LabX-MM-1) ^[00:0b:86:dd:2f:00] (config-submode)#priority 110
(LabX-MM-1) ^[00:0b:86:dd:2f:00] (config-submode)#vlan X10     <- X[1…6]
(LabX-MM-1) ^[00:0b:86:dd:2f:00] (config-submode)#no shutdown
```

```
(LabX-MM-1) ^[00:0b:86:dd:2f:00] (config-submode)#!

(LabX-MM-1) ^[00:0b:86:dd:2f:00] (config) #write memory

Saving Configuration...

Configuration Saved.
```

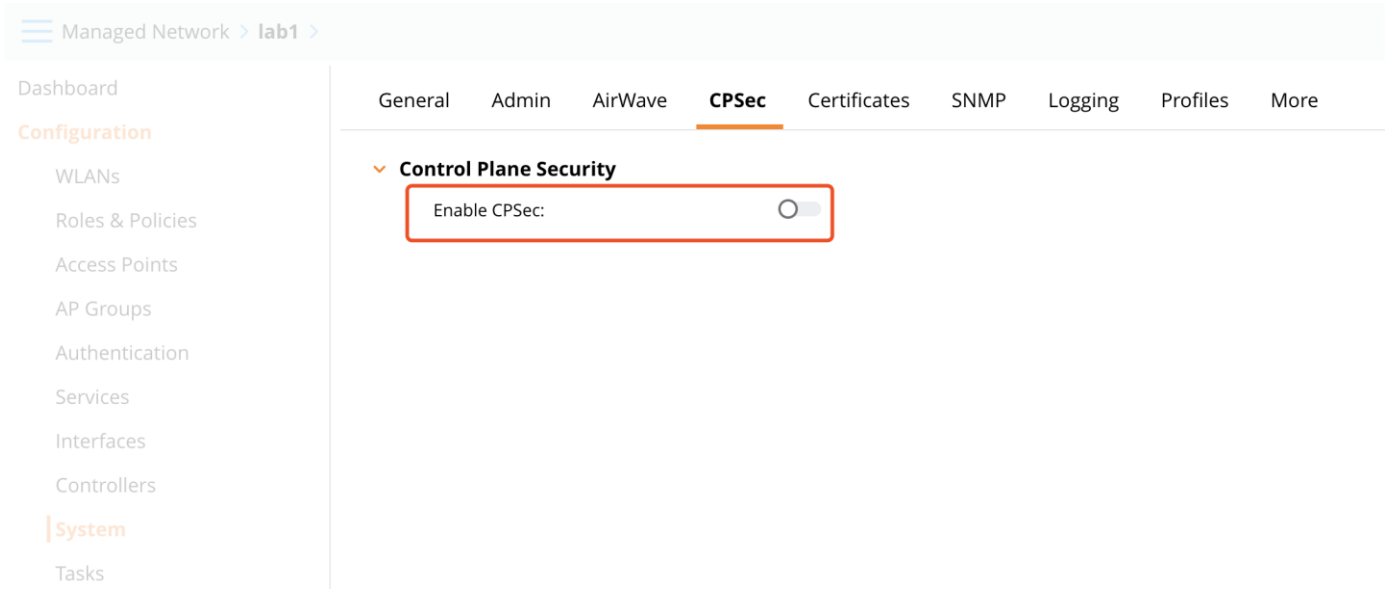
5.4 MM 配置（GUI）

5.4.1 关闭 CPSec 功能

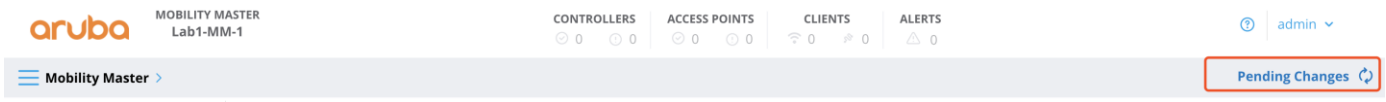
第1步: 找到 Managed Network - > labX -> Configuration -> System，点击“CPSec”，配置如下图所示

（这里的 X 代表 lab 分组[1…6]）（第 1 步和第 2 步选择其中一步操作）

✓ 关闭“Enable CPSec”，



第2步: 点击右上角的“Pending Changes”,保存配置



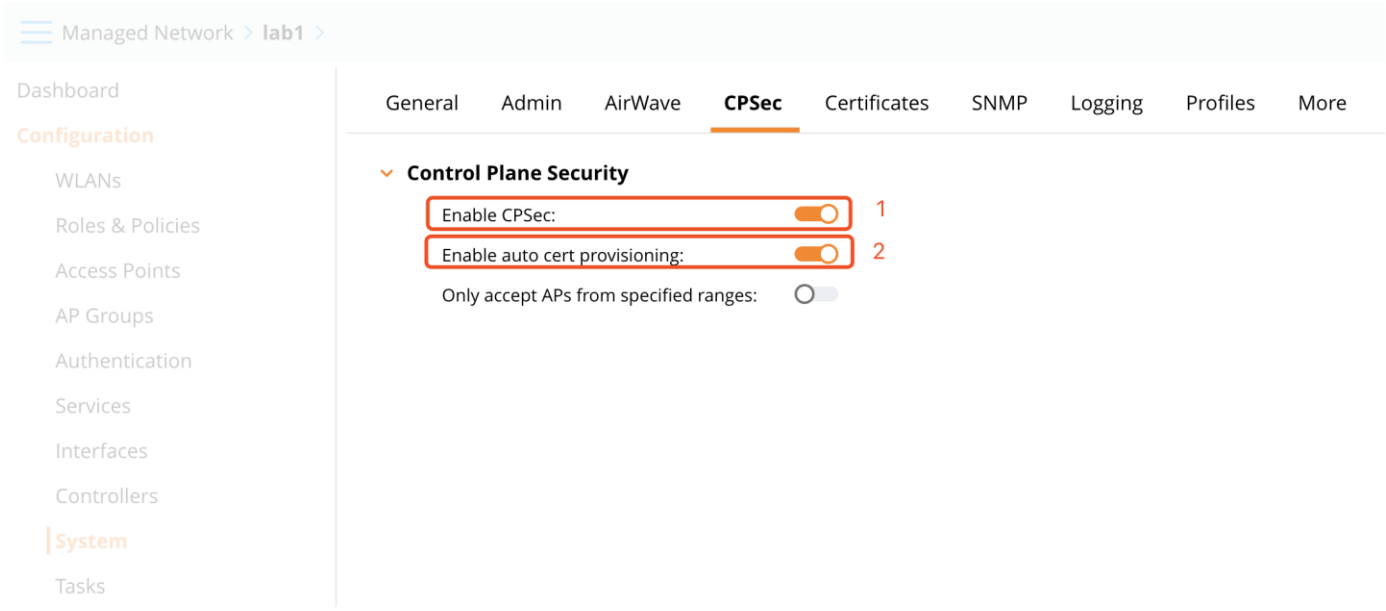
5.4.2 启用 CPSec 功能（注：5.4.1 和 5.4.2 配置二选一）

第1步: 找到 Managed Network - > labX -> Configuration -> System，点击“CPSec”，配置如下图所示

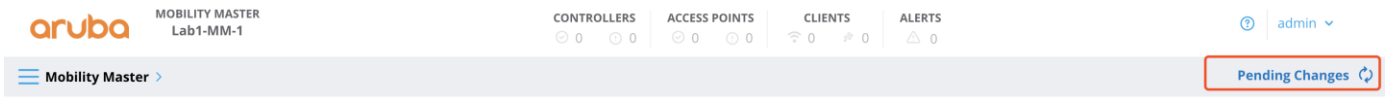
（这里的 X 代表 lab 分组[1…6]）（第 1 步和第 2 步选择其中一步操作）

✓ 启用 “Enable CPSec”，

✓ 启用 “Enable auto cert provisioning”

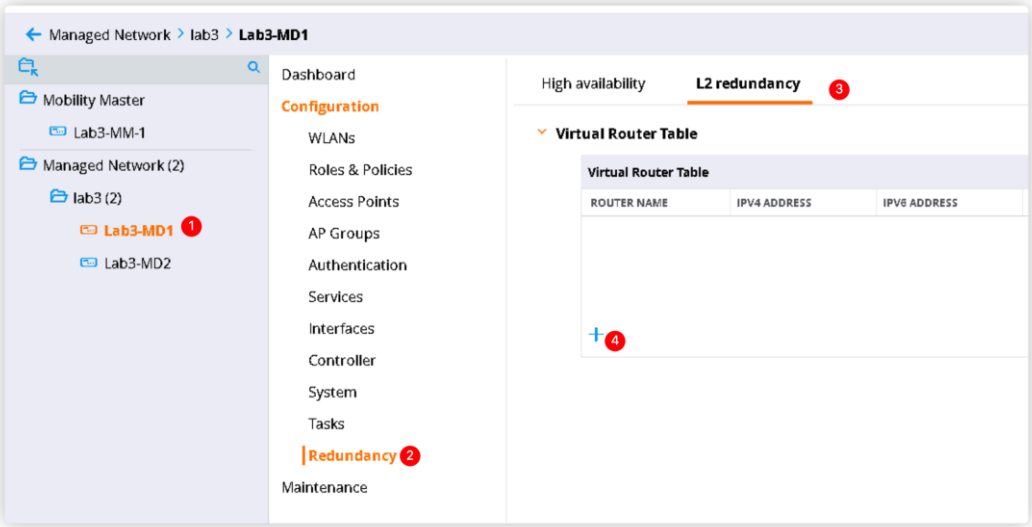


第2步: 点击右上角的“Pending Changes”,保存配置



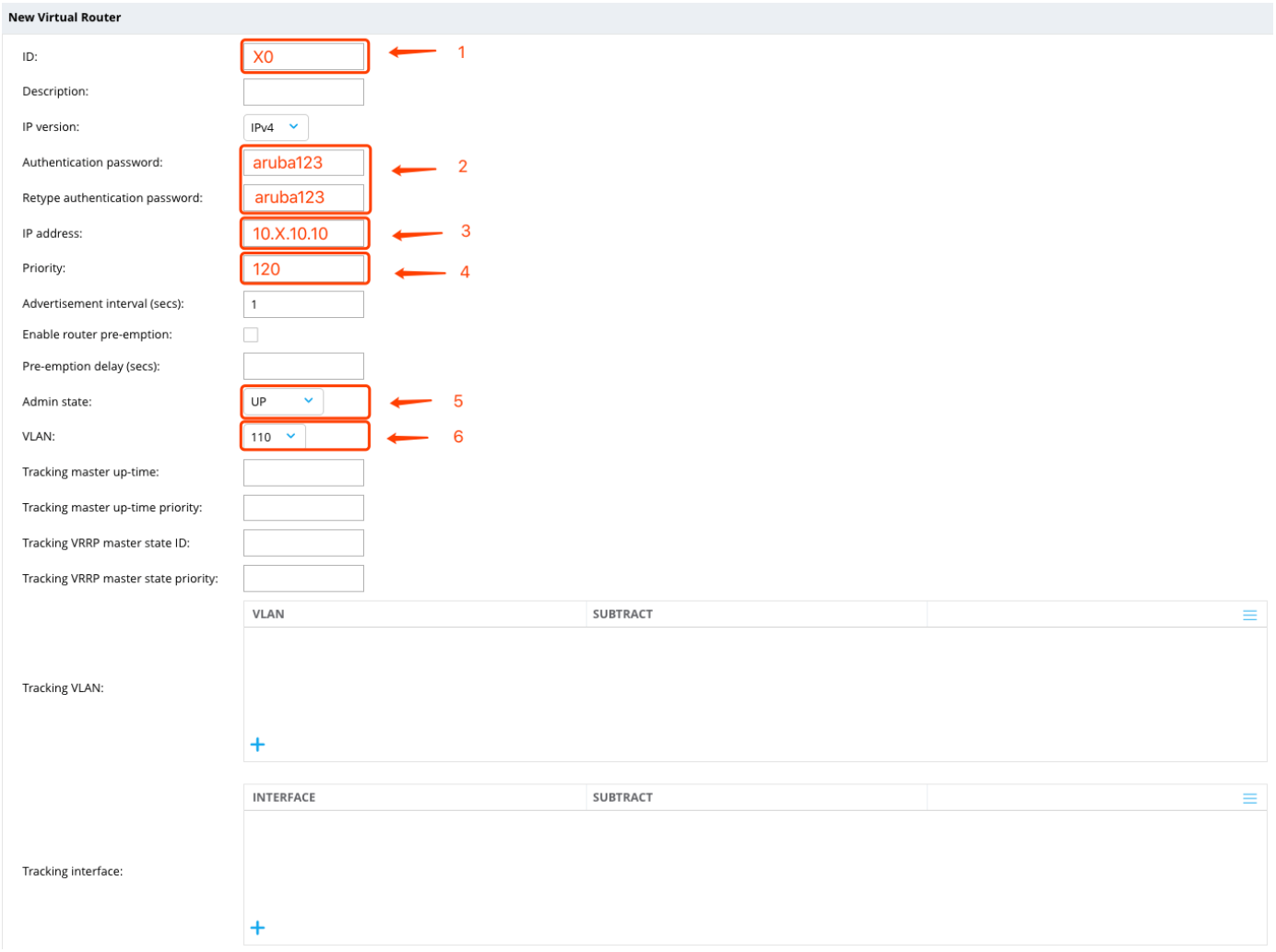
5.4.3 配置 VRRP

第1步: 找到 Managed Network - > labX ->labX-md1 -> Redundancy-> L2 redundancy，点击“Virtual Router Table”下方的“+”添加配置

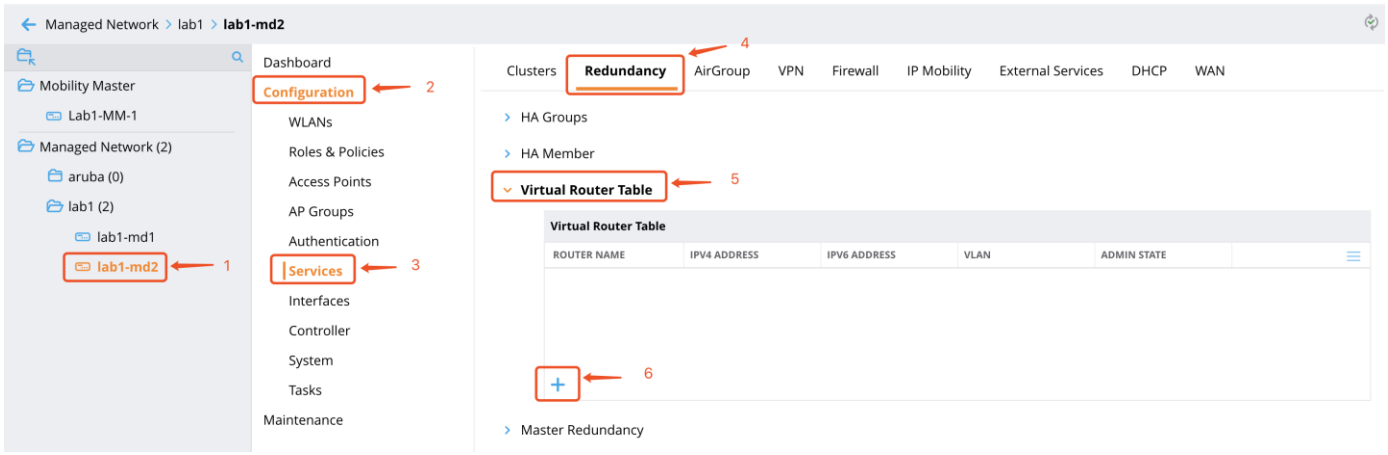


第2步：在弹出的选项卡中，输入以下参数配置 VRRP：

- ✓ ID：X0 <- X[1…6]
- ✓ Authentication password：aruba123
- ✓ Retype authentication password: aruba123
- ✓ IP address: 10.X.10.10 <- X[1…6]
- ✓ Priority: 120
- ✓ Admin state: UP
- ✓ VLAN: X10 <- X[1…6]

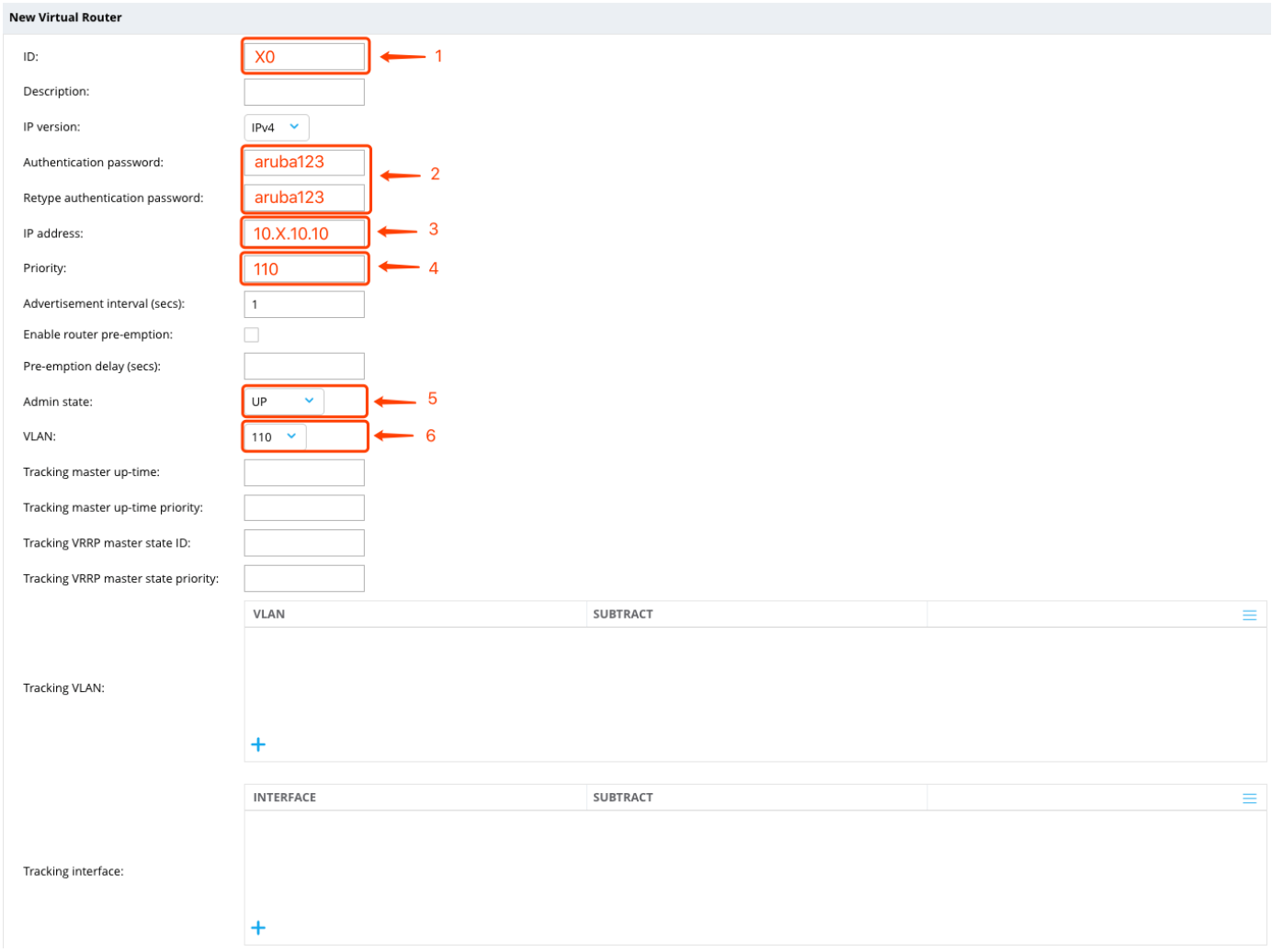


第3步：找到 Managed Network - > labX ->labX-md2 -> Configuration -> Services，点击“Virtual Router Table”下方的“+”添加配置

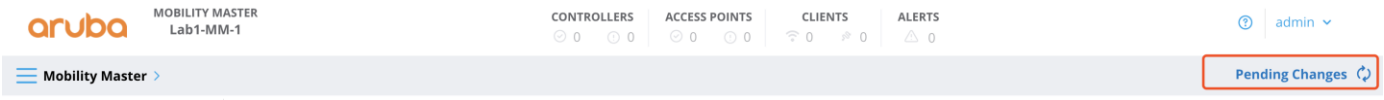


第4步：在弹出的选项卡中，输入以下参数配置 VRRP：

- ✓ ID：X0 <- X[1…6]
- ✓ Authentication password：aruba123
- ✓ Retype authentication password: aruba123
- ✓ IP address: 10.X.10.10 <- X[1…6]
- ✓ Priority: 120
- ✓ Admin state: UP
- ✓ VLAN: X10 <- X[1…6]



第5步：点击右上角的“Pending Changes”,保存配置



5.5 验证结果

第1步：登录到 MM，到/mm 目录，查看 AP 上线状态

✓ 未开启 cpsec 的情况如下：

```
(LabX-MM-1) [00:0b:86:9a:af:37] (config) #cd mm

(LabX-MM-1) [mm] (config) #show ap database

AP Database
```

```
-----------
Name            Group  AP Type  IP Address   Status     Flags  Switch IP   Standby IP
----            -----  -------  ----------   ------     -----  ---------   ----------
94:b4:0f:c1:3f:e0  labX   225     10.1.12.100  Up 17m:19s  UG     10.1.10.12  0.0.0.0
Total APs:1
```

✓ 开启 cpsec 的情况如下：

```
(LabX-MM-1) [mynode] #show ap database
AP Database
-----------
Name            Group  AP Type  IP Address   Status         Flags  Switch IP   Standby IP
----            -----  -------  ----------   ------         -----  ---------   ----------
94:b4:0f:c1:3f:e0  labX   225     10.1.12.100  Up 1d:3h:9m:56s  U2G    10.1.10.12  0.0.0.0
```

第2步：使用 logon 命令分别登录到 md1 和 md2，查看 vrrp 状态

➢ 登录到 md1 查看 vrrp 状态

```
(LabX-MM-1) [mm] (config) #logon 10.X.10.11    <- 这里的 X 代表 lab 分组[1…6]
(labX-md1) [MDC] #show vrrp X0    <- 这里的 X 代表 lab 分组[1…6]
Virtual Router 10:
  Description
  Admin State UP, VR State MASTER
  IP Address 10.1.10.10, MAC Address 00:00:5e:00:01:0a, vlan 110
  Priority 120, Advertisement 1 sec, Preemption Disable Delay 0
  Auth type PASSWORD, Auth data: ********
  tracking is not enabled
```

➢ 登录到 md2 查看 vrrp 状态

```
(LabX-MM-1) [mm] (config) #logon 10.X.10.12    <- 这里的 X 代表 lab 分组[1…6]
(labX-md2) [MDC] #show vrrp X0    <- 这里的 X 代表 lab 分组[1…6]
Virtual Router 10:
```

```
Description
Admin State UP, VR State BACKUP
IP Address 10.1.10.10, MAC Address 00:00:5e:00:01:0a, vlan 110
Priority 110, Advertisement 1 sec, Preemption Disable Delay 0
Auth type PASSWORD, Auth data: ********
tracking is not enabled
```

6 CLUSTER 集群配置

6.1 用户需求

实现AP的负载均衡功能，同时实现用户负载均衡功能，并且能够亚秒级故障切换

6.2 实现思路

在ArubaOS 8.0中，除了LMS，Backup-LMS，VRRP和HA的支持外，还引入了全新的冗余方法。被称为Cluster，将多个控制器聚集在一起，充当单个实体。 AP连接到控制器集群，客户端在控制器之间进行负载均衡。是一个完全负载均衡且完全冗余的系统，Cluster的突出优势是AP和客户端的亚秒级故障切换。

- ✓ ArubaOS 8.0最大支持12个节点集群。仅适用于由7200系列受管设备组成的集群。
- ✓ 如果集群是72xx和70xx控制器的混合，则集群大小限制为4个节点。
- ✓ 虚拟移动控制器（VMC）只能与其他VMC集群。 不支持混合使用VM和硬件平台。
- ✓ VMC的集群大小限制为最多4个节点
- ✓ 仅70xx控制器的集群大小也限制为最多4个节点。
- ✓ 禁用冗余时，每个控制器都会运行到其最大容量。
- ✓ 启用冗余后，每个集群成员的容量将达到其一半。

6.3 MM 配置（CLI）

第1步：登录到/md/labX 节点（<- 这里的 X 代表 lab 分组[1…6]）

```
(LabX-MM-1) [mynode] #cd /md/labX     <- X[1…6]
(LabX-MM-1) [labX] #configure terminal
```

第2步：配置 lc-cluster group-profile，并添加两台控制器。 （<- 这里的 X 代表 lab 分组[1…6]）

```
(LabX-MM-1) [labX] (config) #lc-cluster group-profile labX-cluster    <- X[1…6]

(LabX-MM-1) ^[labX] (Classic Controller Cluster Profile  "lab1-cluster") #controller 10.X.10.11 vrrp-ip 10.X.10.21 vrrp-vlan X10    <- X[1…6]

(LabX-MM-1) ^[labX] (Classic Controller Cluster Profile  "lab1-cluster") #controller 10.X.10.12 vrrp-ip 10.X.10.22 vrrp-vlan X10    <- X[1…6]

(LabX-MM-1) ^[labX] (Classic Controller Cluster Profile  "lab1-cluster") #!
```

第3步：切换到 labX-md1 配置节点，并将控制器关联到 labX-cluster（<- 这里的 X 代表 lab 分组[1…6]）

```
(LabX-MM-1) [labX] (config) #cd labX-md1    <- X[1…6]

(LabX-MM-1) [00:0b:86:9a:af:37] (config) #lc-cluster group-membership labX-cluster  <- X[1…6]

(LabX-MM-1) ^[00:0b:86:9a:af:37] (config) #write memory

Saving Configuration...

Configuration Saved.
```

第4步：切换到 labX-md2 配置节点，并将控制器关联到 labX-cluster（<- 这里的 X 代表 lab 分组[1…6]）

```
(LabX-MM-1) ^[00:0b:86:9a:af:37] (config) #cd labX-md2

(LabX-MM-1) ^[00:0b:86:dd:2f:00] (config) #lc-cluster group-membership labX-cluster <- X[1…6]
```

第5步：查看完成还未提交的配置内容

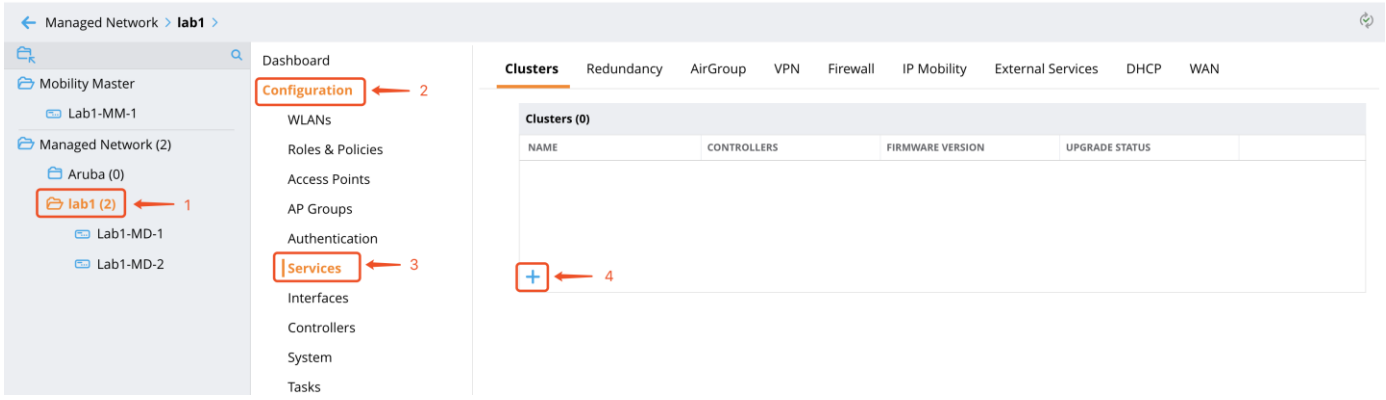
```
(LabX-MM-1) ^[labX] (config) #show configuration pending
```

第6步：保存配置

```
(LabX-MM-1) ^[labX] (config) #write memory

Saving Configuration...

Configuration Saved.
```

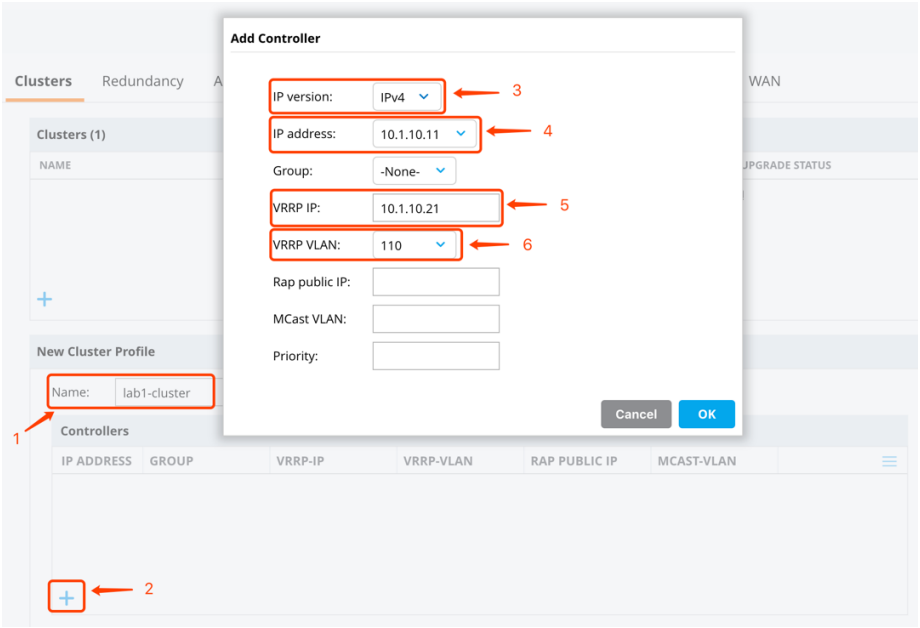
6.4 MM 配置（GUI）

第1步：找到 Managed Network - > labX -> Configuration -> Services，点击“Clusters” 下方的“+”，配置如下图所示（这里的 X 代表 lab 分组[1…6]）



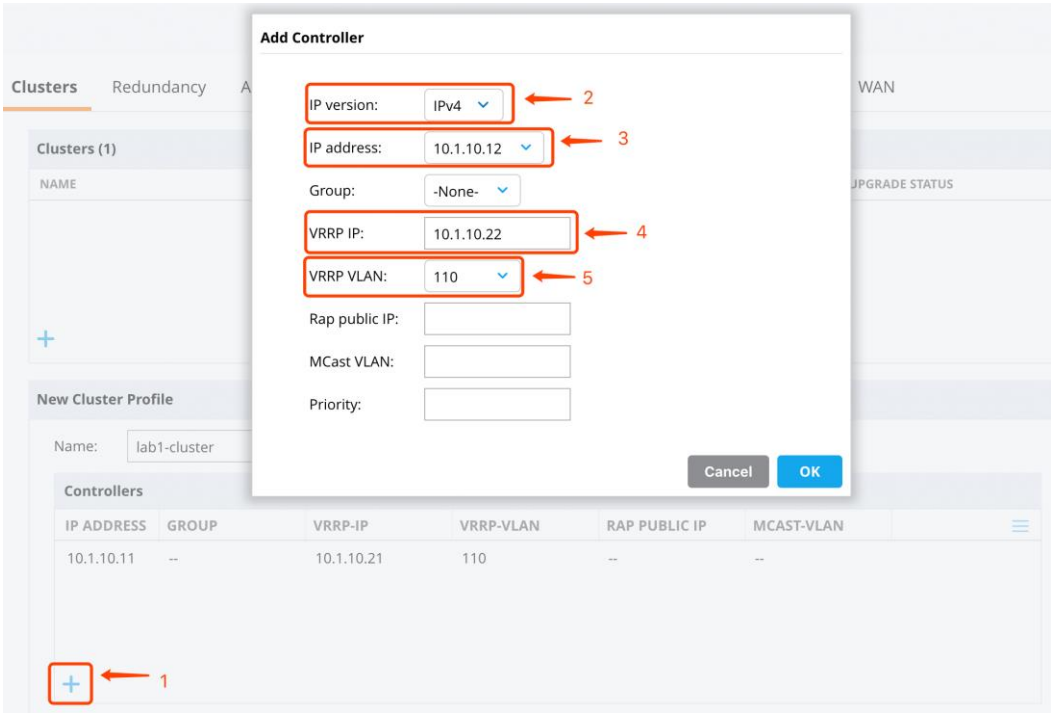
第2步：在弹出的选项卡中，添加 MD，配置参数如下（这里的 X 代表 lab 分组[1…6]），点击 OK。

- ✓ Name: labX-cluster
- ✓ IP version: IPV4
- ✓ IP address: 10.X.10.11
- ✓ VRRP IP: 10.X.10.21
- ✓ VRRP VLAN: X10

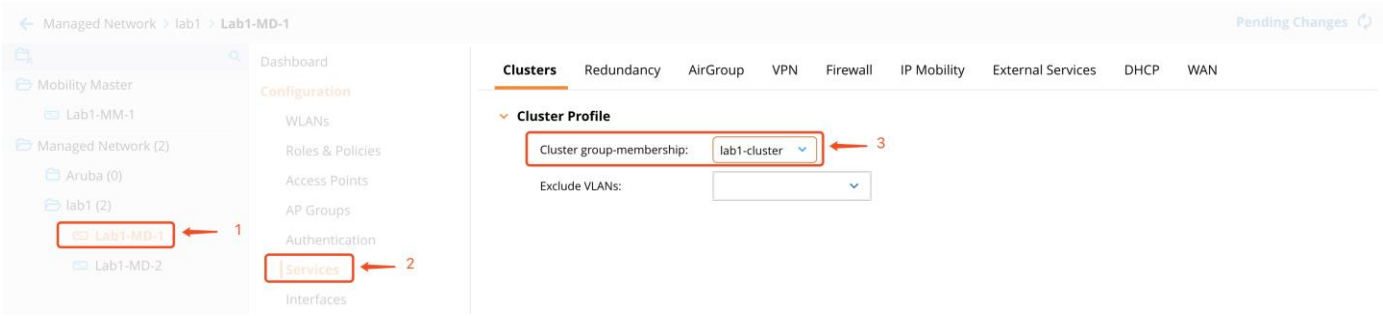


第3步：重复第 2 步，配置另外一台 MD，参数如下（这里的 X 代表 lab 分组[1…6]），点击 OK，并点击“Submit”

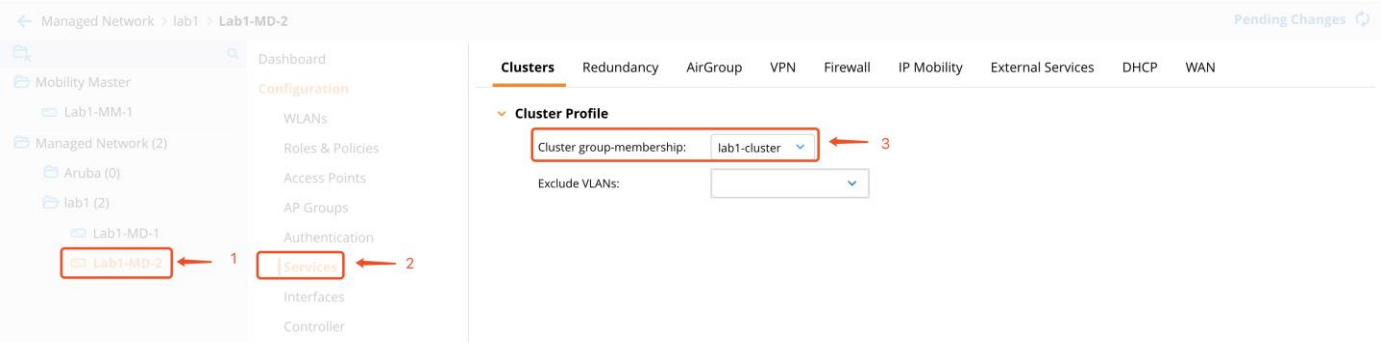
- ✓ IP version: IPV4
- ✓ IP address: 10.X.10.12
- ✓ VRRP IP: 10.X.10.22
- ✓ VRRP VLAN: X10



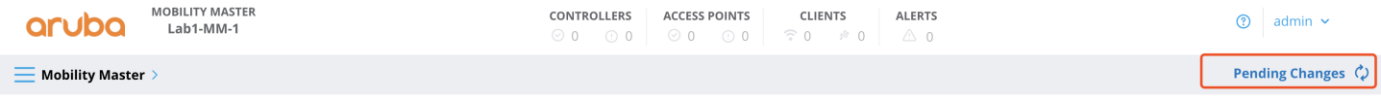
第4步：找到 Managed Network - > labX -> labX-MD1 ->Configuration -> Services，配置如下图所示,点击“Submit” （这里的 X 代表 lab 分组[1…6]）



第5步：找到 Managed Network - > labX -> labX-MD2 ->Configuration -> Services，配置如下图所示,点击“Submit” （这里的 X 代表 lab 分组[1…6]）



第6步：点击右上角的“Pending Changes”,保存配置



6.5 验证结果

第1步：登录到 /mm 节点，查看 AP 状态

✓ 可以看到 Switch IP 和 Standby IP 说明 AP 同时和两台控制器建立了隧道。

```
(LabX-MM-1) [mm] #show ap database

AP Database

-----------

Name            Group  AP Type  IP Address   Status       Flags  Switch IP   Standby IP

----            -----  -------  ----------   ------       -----  ---------   ----------

94:b4:0f:c1:3f:e0  labX   225      10.1.12.100  Up 3h:11m:34s  U2G    10.1.10.12  10.1.10.11
```

第2步：使用 logon 命令登录到 labX-md1。查看 cluster 状态（<- 这里的 X 代表 lab 分组[1…6]）

```
(LabX-MM-1) [mm] #logon 10.X.10.11

(labX-md1) [MDC] #show lc-cluster group-membership
```

```
Cluster Enabled, Profile Name =  “lab1-cluster"
Redundancy Mode On
Active Client Rebalance Threshold = 50%
Standby Client Rebalance Threshold = 75%
Unbalance Threshold = 5%
AP Load Balancing: Enabled
Active AP Rebalance Threshold = 50%
Active AP Unbalance Threshold = 5%
Active AP Rebalance AP Count = 30
Active AP Rebalance Timer = 1 minutes
Cluster Info Table
------------------
Type IPv4 Address    Priority Connection-Type STATUS
---- --------------- -------- --------------- ------
self     10.1.10.11      128          N/A CONNECTED (Member)
peer     10.1.10.12      128    L2-Connected CONNECTED (Leader, last HBT_RSP 70ms ago, RTD = 0.000 ms)
```

NOTE 请注意两个控制器 peer 状态是否为 L3-Connected？需要它们处于 L2 连接状态，以实现亚秒级故障转移。

```
(labX-md1) [MDC] #show lc-cluster vlan-probe status
Cluster VLAN Probe Status
-------------------------
Type IPv4 Address    REQ-SENT REQ-FAIL ACK-SENT ACK-FAIL REQ-RCVD ACK-RCVD VLAN_FAIL CONN-TYPE START/STOP
---- --------------- -------- -------- -------- -------- -------- -------- --------- --------- ----------
peer     10.1.10.12      13       0        6        0        6       13        0    L2 Conn     1/   1
```

第3步: 使用 logon 命令登录到 labX-md2。查看 cluster 状态（<- 这里的 X 代表 lab 分组[1…6]）

```
(LabX-MM-1) [mm] #logon 10.X.10.12

(labX-md2) [MDC] #show lc-cluster group-membership


Cluster Enabled, Profile Name =  “lab1-cluster"

Redundancy Mode On

Active Client Rebalance Threshold = 50%

Standby Client Rebalance Threshold = 75%

Unbalance Threshold = 5%

AP Load Balancing: Enabled

Active AP Rebalance Threshold = 50%

Active AP Unbalance Threshold = 5%

Active AP Rebalance AP Count = 30

Active AP Rebalance Timer = 1 minutes

Cluster Info Table

------------------

Type IPv4 Address    Priority Connection-Type STATUS

---- --------------- -------- --------------- ------

peer     10.1.10.11     128    L2-Connected CONNECTED (Member, last HBT_RSP 5ms ago, RTD = 1.060 ms)

self     10.1.10.12     128           N/A CONNECTED (Leader)
```

第4步: 切换到/md/labX 配置节点，创建一个新的 VLAN X20，并在两台 MD 的上行接口 Gi0/0/0 修剪 VLAN 只允许 vlan1,X10 通过。（<- 这里的 X 代表 lab 分组[1…6]）

```
(LabX-MM-1) [mynode] #cd /md/labX

(LabX-MM-1) [labX] #configure terminal

Enter Configuration commands, one per line. End with CNTL/Z
```

```
(LabX-MM-1) [labX] (config) #vlan X20
(LabX-MM-1) ^[labX] (config-submode)#!
(LabX-MM-1) ^[labX] (config) #write memory
Saving Configuration...
Configuration Saved.

(LabX-MM-1) [labX] (config) #cd labX-md1
(LabX-MM-1) [00:0b:86:9a:af:37] (config) #interface gigabitethernet 0/0/0
(LabX-MM-1) [00:0b:86:9a:af:37] (config-submode)#switchport trunk allowed vlan 1,X10
(LabX-MM-1) ^[00:0b:86:9a:af:37] (config-submode)#!
(LabX-MM-1) ^[00:0b:86:dd:2f:00] (config) #write memory
Saving Configuration...
Configuration Saved.

(LabX-MM-1) ^[00:0b:86:9a:af:37] (config) #cd labX-md2
(LabX-MM-1) ^[00:0b:86:dd:2f:00] (config) #interface gigabitethernet 0/0/0
(LabX-MM-1) ^[00:0b:86:dd:2f:00] (config-submode)#switchport trunk allowed vlan 1,X10
(LabX-MM-1) ^[00:0b:86:dd:2f:00] (config-submode)#!
(LabX-MM-1) ^[00:0b:86:dd:2f:00] (config) #write memory
Saving Configuration...
Configuration Saved.
```

第5步：登录到 labX-md1 和 labX-md2，再次查看 cluster 状态。（<- 这里的 X 代表 lab 分组[1…6]）
这时我们发现 cluster 状态由 L2 变成了 L3。是因为默认情况 MD 会向所有本地 vlan 发送 probe 探测数据包，我们刚刚到操作使得 vlan X20 的探测包无法通过上行接口导致。我们需要按照实际情况启动对应 vlan 的 probe 探测功能。

```
LabX-MM-1) [00:0b:86:9a:af:37] #mdc
 Redirecting to Managed Device Shell
```

```
(labX-md1) [MDC] #show lc-cluster group-membership

Cluster Enabled, Profile Name =  “lab1-cluster"

Redundancy Mode On

Active Client Rebalance Threshold = 50%

Standby Client Rebalance Threshold = 75%

Unbalance Threshold = 5%

AP Load Balancing: Enabled

Active AP Rebalance Threshold = 50%

Active AP Unbalance Threshold = 5%

Active AP Rebalance AP Count = 30

Active AP Rebalance Timer = 1 minutes

Cluster Info Table

------------------

Type IPv4 Address    Priority Connection-Type STATUS

---- --------------- -------- --------------- ------

self     10.1.10.11     128          N/A CONNECTED (Member)

peer     10.1.10.12     128    L3-Connected CONNECTED (Leader, last HBT_RSP 19ms ago, RTD = 0.000 ms)
```

第6步: 分别登录到 labX-md1 和 labX-md2。 (<- 这里的 X 代表 lab 分组[1…6])

✓ 登录到 labX-md1 查看 vlan probe 状态

```
(labX-md1) [MDC] #show lc-cluster vlan-probe status


Cluster VLAN Probe Status

-------------------------

Type IPv4 Address    REQ-SENT REQ-FAIL ACK-SENT ACK-FAIL REQ-RCVD ACK-RCVD VLAN_FAIL CONN-TYPE START/ST
OP

---- --------------- -------- -------- -------- -------- -------- -------- --------- --------- ----------

peer     10.1.10.12     43       0      11       0      11       26       120   L3 Conn     2/  2

(labX-md1) [MDC] #exit
```

```
Exiting Managed Device Shell
```

✓ 登录到 labX-md2 查看 vlan probe 状态

```
(LabX-MM-1) [00:0b:86:9a:af:37] #cd labX-md2
(LabX-MM-1) [00:0b:86:dd:2f:00] #mdc
 (labX-md2) [MDC] #show lc-cluster vlan-probe status
Cluster VLAN Probe Status
-------------------------
Type IPv4 Address    REQ-SENT REQ-FAIL ACK-SENT ACK-FAIL REQ-RCVD ACK-RCVD VLAN_FAIL CONN-TYPE START/STOP
---- --------------- -------- -------- -------- -------- -------- -------- --------- --------- ----------
peer     10.1.10.11      27       0       26       0       26       11       120    L3 Conn     2/   2
(labX-md2) [MDC] #
```

我们看到 vlan probe 探测数据包在 vlan X20 检测失败。因此需要以下操作

第7步：分别到 labX-md1 和 labX-md2 设备配置节点，完成以下配置。（<- 这里的 X 代表 lab 分组[1…6]）

```
(LabX-MM-1) [mynode] (config) #cd labX-md1
(LabX-MM-1) [00:0b:86:9a:af:37] (config) #lc-cluster exclude-vlan X20
(LabX-MM-1) ^[00:0b:86:9a:af:37] (config) #write memory
Saving Configuration...
Configuration Saved.
(LabX-MM-1) [00:0b:86:9a:af:37] (config) #cd labX-md2
(LabX-MM-1) [00:0b:86:dd:2f:00] (config) #lc-cluster exclude-vlan X20
(LabX-MM-1) ^[00:0b:86:9a:af:37] (config) #write memory
Saving Configuration...
Configuration Saved.
```

第8步: 分别登录到 labX-md1 和 labX-md2，查看状态。（<- 这里的 X 代表 lab 分组[1…6]）

```
(LabX-MM-1) [00:0b:86:dd:2f:00] #logon 10.1.10.11

(labX-md1) [MDC] #show lc-cluster vlan-probe status

Cluster VLAN Probe Status

-------------------------

Type IPv4 Address    REQ-SENT REQ-FAIL ACK-SENT ACK-FAIL REQ-RCVD ACK-RCVD VLAN_FAIL CONN-TYPE START/ST
OP

---- --------------- -------- -------- -------- -------- -------- -------- --------- --------- ----------

peer     10.1.10.12      46       0       12       0       12       29        0   L2 Conn     1/   1

(labX-md1) [MDC] #exit


(LabX-MM-1) [00:0b:86:dd:2f:00] #logon 10.1.10.12

(labX-md2) [MDC] #show lc-cluster vlan-probe status

Cluster VLAN Probe Status

-------------------------

Type IPv4 Address    REQ-SENT REQ-FAIL ACK-SENT ACK-FAIL REQ-RCVD ACK-RCVD VLAN_FAIL CONN-TYPE START/ST
OP

---- --------------- -------- -------- -------- -------- -------- -------- --------- --------- ----------

peer     10.1.10.11      32       0       29       0       29       12        0   L2 Conn     1/   1
```

7 USER ROLE

7.1 用户需求

为了实现基于角色的，高颗粒度的用户管理，客户希望采用User-role来进行管理。

7.2 实现思路

如果你要配置新的User-role，请确保你已安装LIC-PEF，LIC-PEF需要数量上和LIC-AP一致，否则将有AP无法正常启动工作，如果配置了License Pool，请确认MD所处的License Pool具有足够的LIC-AP及LIC-PEF，否则可能出现配置无法生效的情况。在User-role下，我们可以配置

- ✓ 一条或多条Policy，一个Policy可以由一条或多条Policy rule组成。
- ✓ 带宽限制，我们可以限制某个角色的整体带宽，或者单个用户的带宽，或者某个AP-GROUP的带宽，或者该角色下某个应用的带宽。
- ✓ 角色对应的认证Portal（详见Portal认证章节）。
- ✓ 角色对应的VLAN，重认证时间，最大的防火墙会话数。
- ✓ 是否对角色的数据进行DPI，WebCC， Openflow。

7.3 MM 配置（CLI）

第1步: 登录到/md/labX 节点，添加一个新的 Policy： labX-role1-acl（<- 这里的 X 代表 lab 分组[1…6]）

```
(LabX-MM-1) [mynode] #cd /md/labX     <- X[1…6]
(LabX-MM-1) [labX] #configure terminal
(LabX-MM-1) [labX] (config) #ip access-list session labX-role1-acl     <- X[1…6]
(LabX-MM-1) ^[labX] (config-submode)#user any any permit
(LabX-MM-1) ^[labX] (config-submode)#exit
```

第2步: 配置一个新 role：labX-role1，并将新创建的 policy 绑定到这个 role（<- 这里的 X 代表 lab 分组[1…6]）

```
(LabX-MM-1) ^[labX] (config) #user-role labX-role1     <- X[1…6]
(LabX-MM-1) ^[labX] (config-submode)#access-list session labX-role1-acl     <- X[1…6]
(LabX-MM-1) ^[labX] (config-submode)#write memory
```

```
(LabX-MM-1) [labX] (config-submode)#!
```

第3步：配置一个带宽策略并捆绑到刚才的 role 上（<- 这里的 X 代表 lab 分组[1…6]）

```
(LabX-MM-1) [labX] (config) #aaa bandwidth-contract 2M mbits 2
(LabX-MM-1) ^[labX] (config) #user-role labX-role1    <- X[1…6]
(LabX-MM-1) ^[labX] (config-submode)#bw-contract 2M per-user downstream
(LabX-MM-1) ^[labX] (config-submode)#bw-contract 2M per-user upstream
(LabX-MM-1) ^[labX] (config-submode)#write memory
(LabX-MM-1) [labX] (config-submode)#!
```

第4步：配置用户对应的防火墙会话数，关闭默认处于开启的 DPI，WEBCC，OPENFLOW 功能

```
(LabX-MM-1) [labX] (config) #user-role labX-role1    <- X[1…6]
(LabX-MM-1) ^[labX] (config-submode)#max-sessions 200
(LabX-MM-1) ^[labX] (config-submode)#dpi disable
(LabX-MM-1) ^[labX] (config-submode)#web-cc disable
(LabX-MM-1) ^[labX] (config-submode)#no openflow-enable
```

第5步：查看完成还未提交的配置内容

```
(LabX-MM-1) ^[labX] (config) #show configuration pending
```

第6步：保存配置

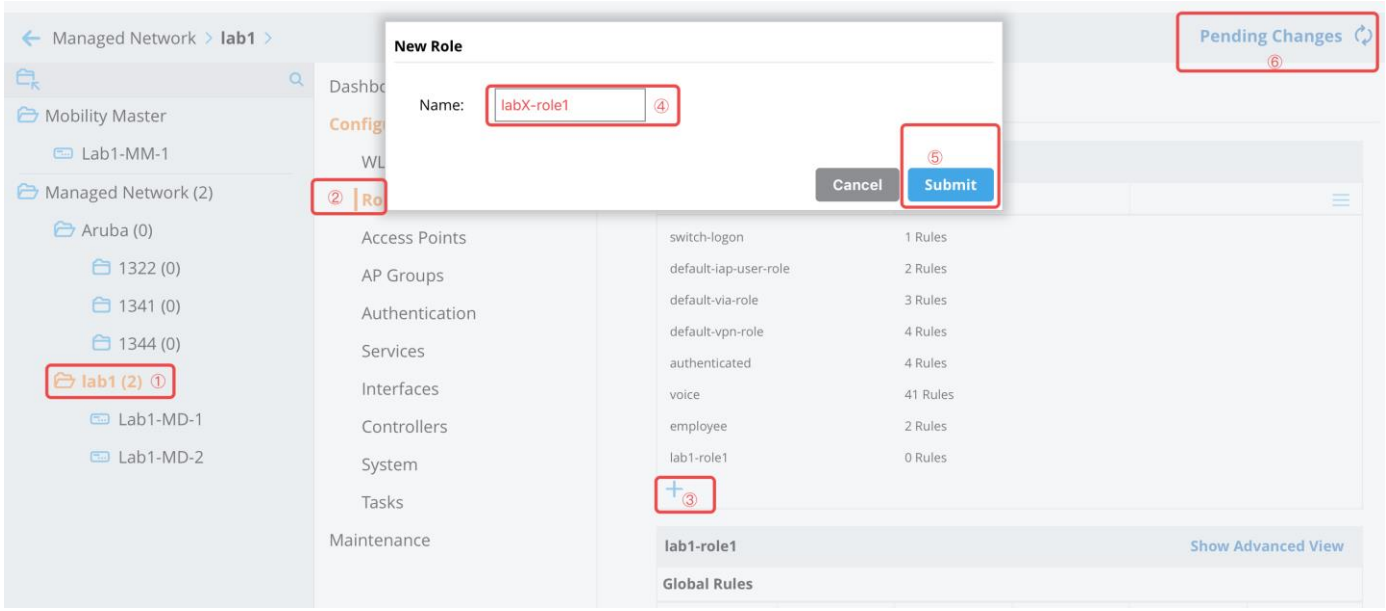
```
(LabX-MM-1) ^[labX] (config) #write memory
Saving Configuration...
Configuration Saved.
```

NOTE 在大多数情况下，我们不需要去配置角色下的 VLAN，我们推荐同一个 SSID 下的多个不同角色的用户都按 VAP 内配置的 VLAN 信息去获取地址。

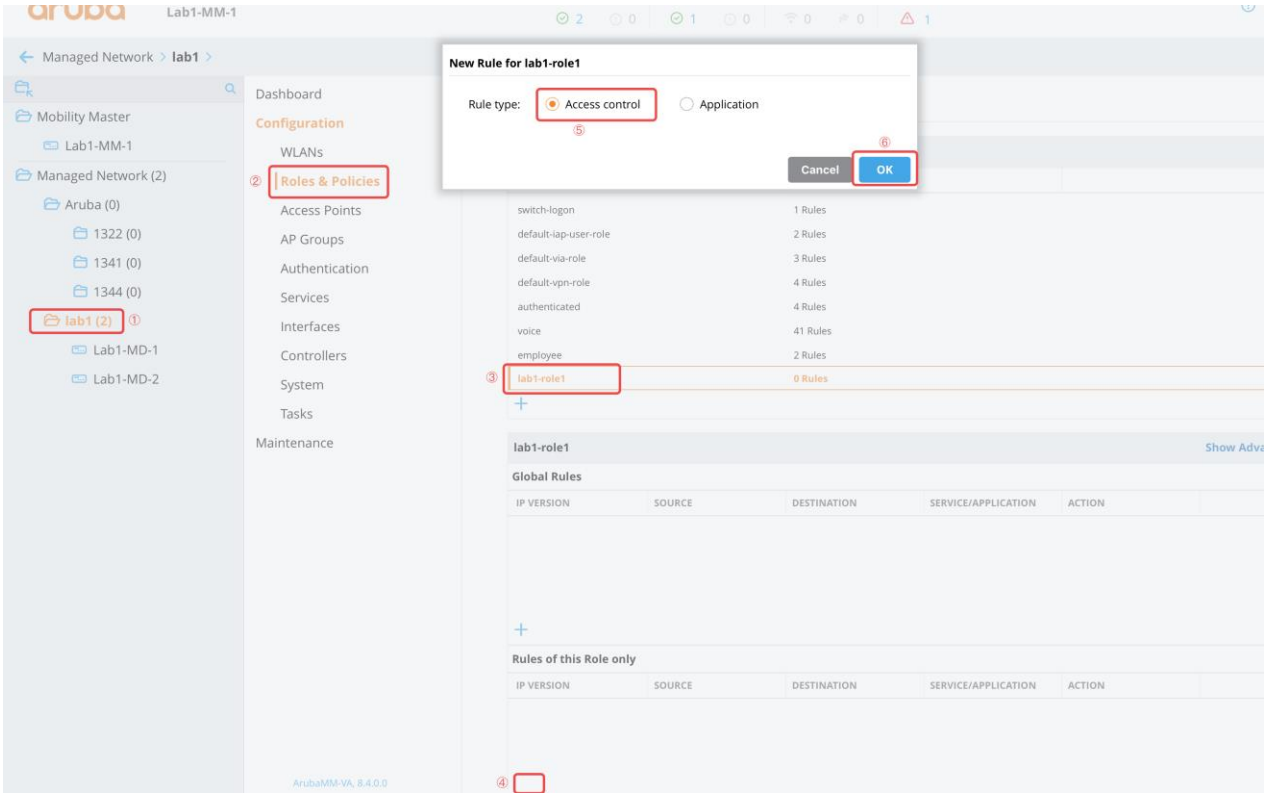
7.4 MM 配置（GUI）

第1步: 进入到 Managed Network - > labX -> Configuration，点击 “Role&Policies” 下方的 “+” <- 这里的 X 代表 lab 分组[1…6]

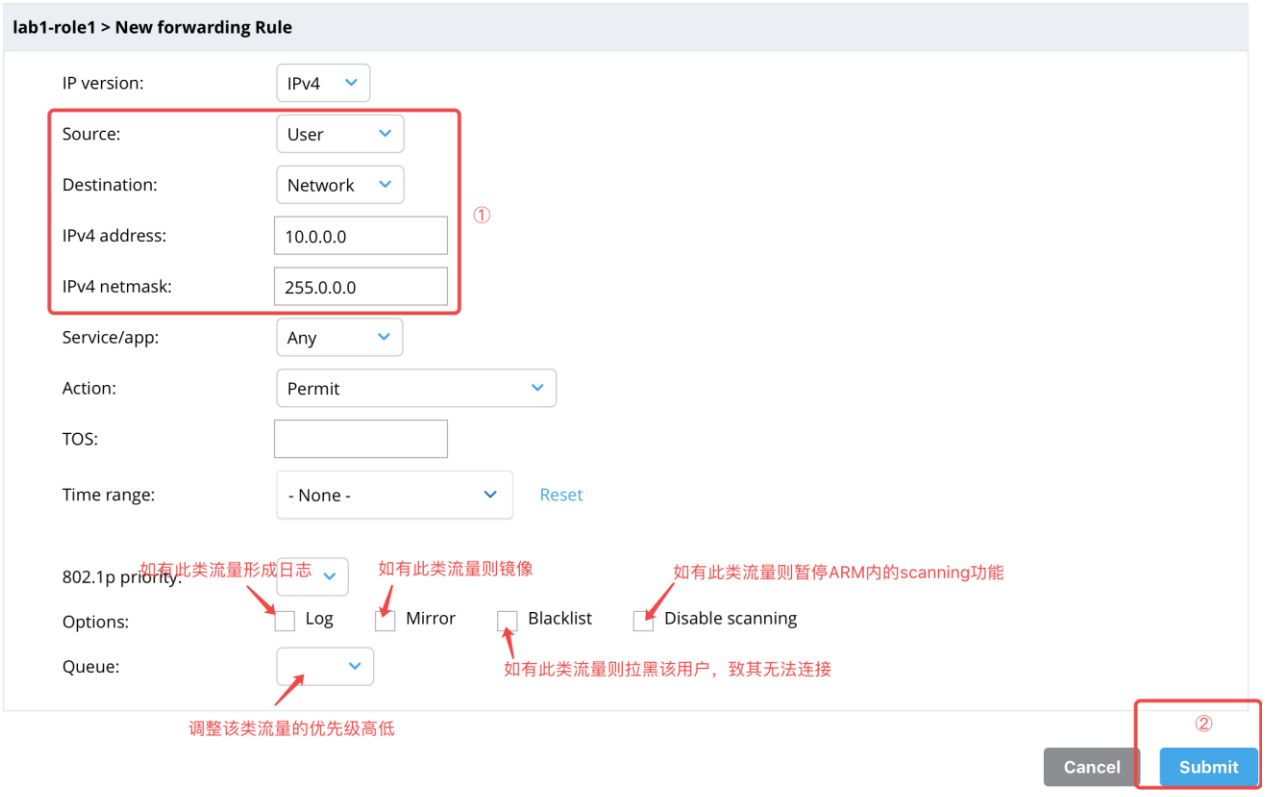
✓ 创建一个 LabX-role1 的 New Role，Submit 后，提交 Pending Changes 并确认。



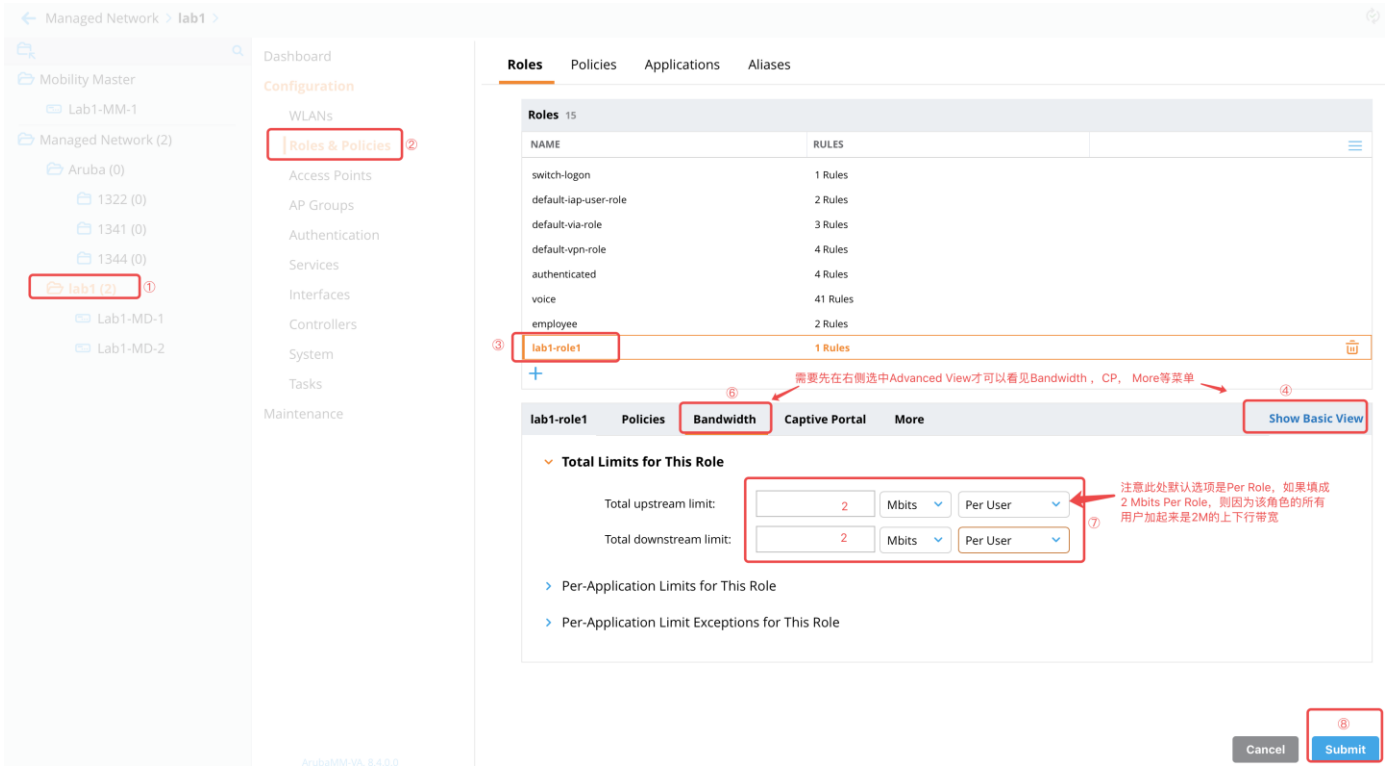
第2步: 进入到 Managed Network - > labX -> Configuration，点击 “Role&Policies” ，点击 LabX-role1 <- 这里的 X 代表 lab 分组[1…6]，在最下方 Rules of this Role Only 内点击＋，网页会弹出 Access Control 和 Application 的选择，此处我们选择 ACL（Application 感兴趣的话可以自行测试），并且 OK。



第3步：弹出的对话框如下，我们调整 Source 为 User，Destination 为 Network，并且输入 10.0.0.0/255.0.0.0，其余选项不动，Submit 后，回到主页面右上角，提交 Pending Changes 并确认。

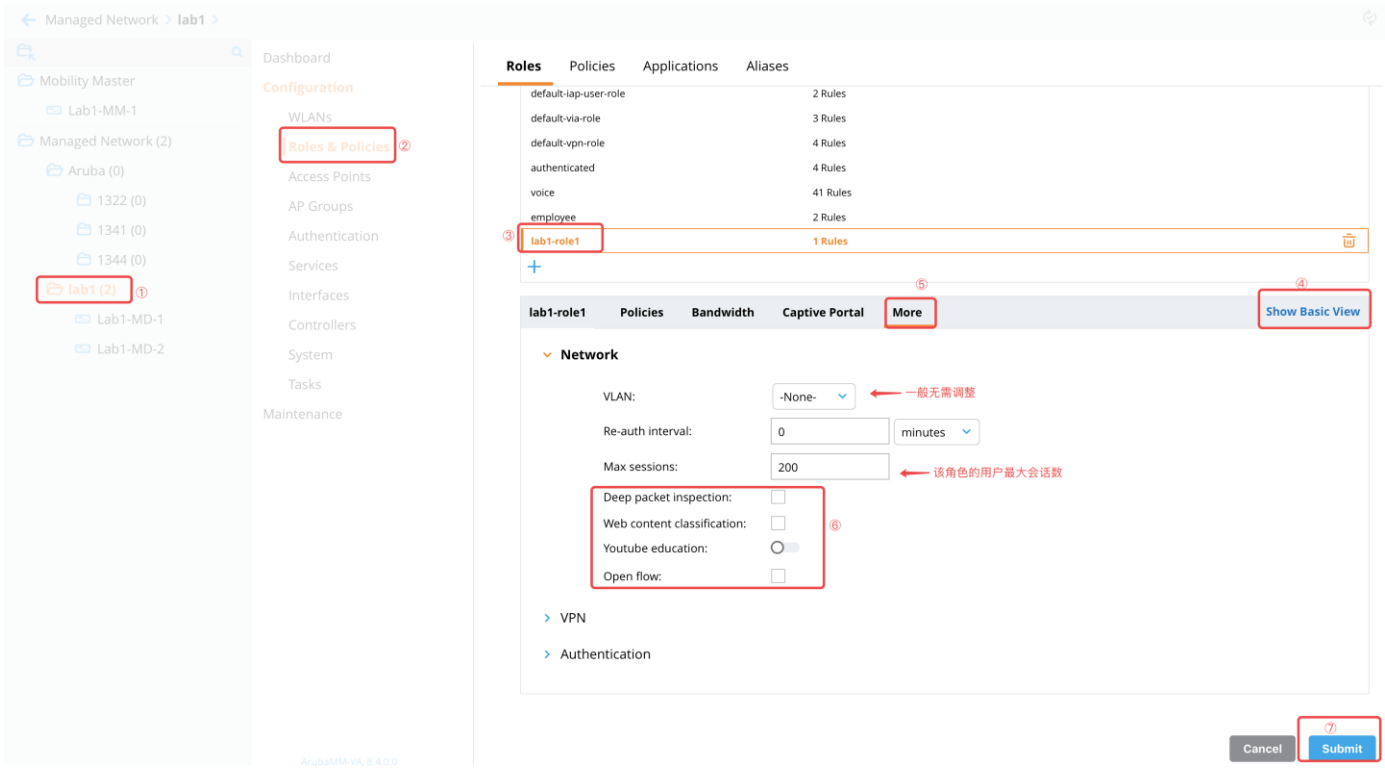


第4步：在前述 LabX-role1（<- 这里的 X 代表 lab 分组[1…6]）下，点击 Show Advanced View，方可看见下图中的 Bandwidth, Captive Portal, More 菜单，输入你想限速的值，例如 Upstream 2 Mbits Per-User, Downstream 2 Mbits Per-User，点击 Submit。回到主页面右上角，提交 Pending Changes 并确认。



NOTE 默认的带宽策略为 Per Role，如示例中未修改默认值，则意味着该 Role 下的多个用户共享 2M 的上下行带宽。

在前述 LabX-role1（<- 这里的 X 代表 lab 分组[1…6]）下，点击 Show Advanced View，方可看见下图中的 More 菜单，修改最大会话数为 200，消除 DPI, WebCC, Open flow 的选择框，点击 Submit。回到主页面右上角，提交 Pending Changes 并确认。



7.5 验证结果

(LabX-MD-1) #show rights labX-role1 <- X[1…6]

Valid = 'Yes'

CleanedUp = 'No'

Derived Role = 'labX-role1' <- X[1…6]

Up BW contract = 2m (2000000 bits/sec) (per-user) Down BW contract = 2m (2000000 bits/sec) (per-user)

L2TP Pool = default-l2tp-pool

PPTP Pool = default-pptp-pool

Number of users referencing it = 0

Periodic reauthentication: Disabled

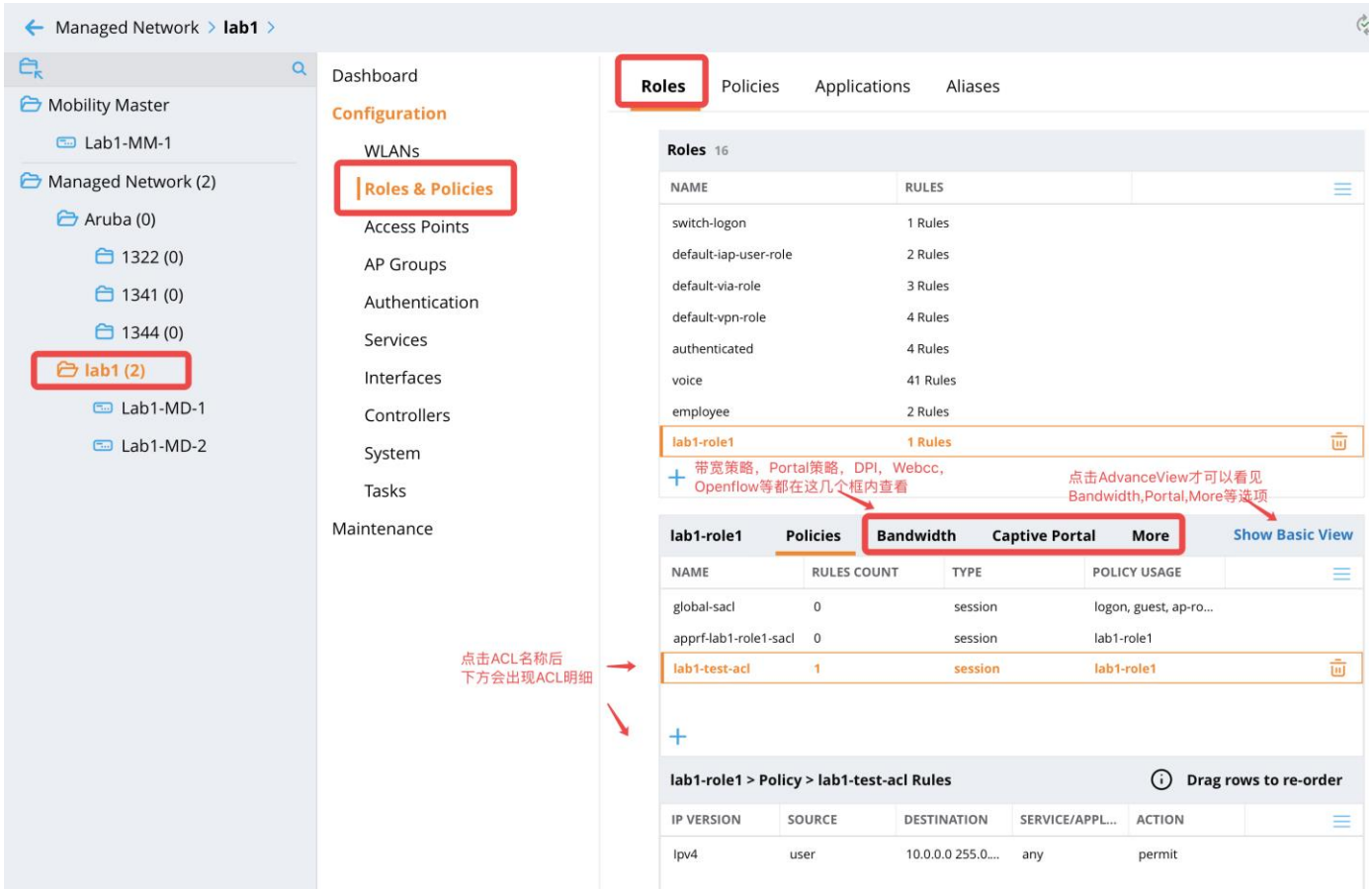
DPI Classification: Disabled

Youtube education: Disabled

Web Content Classification: Disabled

IP-Classification Enforcement: Enabled

```
 ACL Number = 88/0
 Openflow: Disabled
 Max Sessions = 200
 Check CP Profile for Accounting = TRUE
Application Exception List
--------------------------
Name  Type
----  ----
Application BW-Contract List
----------------------------
Name  Type  BW Contract  Id  Direction
----  ----  -----------  --  ---------
access-list List
----------------
Position  Name                Type     Location
--------  ----                ----     --------
1         global-sacl         session          <----系统生成
2         apprf-lab1-role1-sacl  session         <----系统生成
3         lab1-test-acl       session
```


Managed Network > lab1
Mobility Master
Lab1-MM-1
Managed Network (2)
Aruba (0)
1322 (0)
1341 (0)
1344 (0)
lab1 (2)
Lab1-MD-1
Lab1-MD-2
Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces
Controllers
System
Tasks
Maintenance
Roles
Policies
Applications
Aliases
Roles 16
NAME
RULES
switch-logon 1 Rules
default-iap-user-role 2 Rules
default-via-role 3 Rules
default-vpn-role 4 Rules
authenticated 4 Rules
voice 41 Rules
employee 2 Rules
lab1-role1 1 Rules
带宽策略，Portal策略，DPI，Webcc，
Openflow等都在这几个框内查看
点击AdvanceView才可以看见
Bandwidth,Portal,More等选项
lab1-role1
Policies
Bandwidth
Captive Portal
More
Show Basic View
NAME
RULES COUNT
TYPE
POLICY USAGE
global-sacl 0 session logon, guest, ap-ro...
apprf-lab1-role1-sacl 0 session lab1-role1
lab1-test-acl 1 session lab1-role1
点击ACL名称后
下方会出现ACL明细
lab1-role1 > Policy > lab1-test-acl Rules
Drag rows to re-order
IP VERSION
SOURCE
DESTINATION
SERVICE/APPL...
ACTION
Ipv4 user 10.0.0.0 255.0.... any permit

8 PSK

8.1 用户需求

客户希望实现类似家庭环境的预共享秘钥方式的连接，例如将无线密码设置为aruba123。

8.2 实现思路

先配置 aaa profile（规定认证规则及初始角色），wlan ssid-profile（规定 SSID 名称及秘钥）,然后将 aaa profile 和 wlan ssid-profile 组合形成一个 VAP（规定虚拟 AP 名称和默认用户 VLAN），然后将 VAP 和 AP-Group 进行捆绑，这样该 AP-Group 下的 AP 即可放出指定信号。由于 VAP 默认为集中转发模式，用户数据会交由控制器进行基于角色的策略管控，所以用户 VLAN 应该在控制器上存在。

8.3 MM 配置（CLI）

第1步: 使用 SSH 方式登录到 Mobility Master (10.X.50.11)

第2步: 在 Mobility Master（MM）上进入 /md/labX 配置节点，并进入配置模式

```
(LabX-MM-1) [mynode] #cd /md/labX    <- X[1…6]
(LabX-MM-1) [labX] #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(LabX-MM-1) [labX] (config) #
```

第3步: 将用户 VLAN X20 加到 MD1 上行接口的 trunk 允许 VLAN 列表

```
(LabX-MM-1) [mm] (config) #cd labX-md1    <- X[1…6]
(LabX-MM-1) [00:0b:86:9a:af:37] (config) #interface gigabitethernet 0/0/0
(LabX-MM-1) [00:0b:86:9a:af:37] (config-submode)#switchport trunk allowed vlan add X20 <-X[1~6]
(LabX-MM-1) ^[00:0b:86:9a:af:37] (config-submode)#write m
Saving Configuration...
Configuration Saved.
```

第4步: 将用户 VLAN X20 加到 MD2 上行接口的 trunk 允许 VLAN 列表

```
(LabX-MM-1) [00:0b:86:9a:af:37] (config-submode)#cd labX-md2    <- X[1…6]
(LabX-MM-1) [00:0b:86:dd:2f:00] (config) #interface gigabitethernet 0/0/0
(LabX-MM-1) [00:0b:86:dd:2f:00] (config-submode)#switchport trunk allowed vlan add X20 <-X[1~6]
(LabX-MM-1) ^[00:0b:86:dd:2f:00] (config-submode)#write memory
Saving Configuration...
Configuration Saved.
```

第5步：增加一个新的 aaa profile “labX-psk-aaa”

```
(LabX-MM-1) [labX] (config) #aaa profile labX-psk-aaa    <- X[1…6]
(LabX-MM-1) ^[labX] (AAA Profile "lab1-psk-aaa") #initial-role authenticated
(LabX-MM-1) ^[labX] (AAA Profile "lab1-psk-aaa") #authentication-dot1x default-psk
(LabX-MM-1) ^[labX] (AAA Profile "lab1-psk-aaa") #!
```

第6步：增加一个新的 ssid profile “labX-psk-ssid”

```
(LabX-MM-1) ^[labX] (config) #wlan ssid-profile labX-psk-ssid    <- X[1…6]
(LabX-MM-1) ^[labX] (SSID Profile "lab1-psk-ssid") #essid labX-psk    <- X[1…6]
(LabX-MM-1) ^[labX] (SSID Profile "lab1-psk-ssid") #wpa-passphrase aruba123
(LabX-MM-1) ^[labX] (SSID Profile "lab1-psk-ssid") #opmode wpa2-psk-aes
(LabX-MM-1) ^[labX] (SSID Profile "lab1-psk-ssid") #!
```

第7步：增加一个新的 virtual-ap profile “labX-psk-vap”

```
(LabX-MM-1) ^[labX] (config) #wlan virtual-ap labX-psk-vap    <- X[1…6]
(LabX-MM-1) ^[labX] (Virtual AP profile "lab1-psk-vap") #aaa-profile labX-psk-aaa    <-X[1…6]
(LabX-MM-1) ^[labX] (Virtual AP profile "lab1-psk-vap") #ssid-profile labX-psk-ssid <-X[1…6]
(LabX-MM-1) ^[labX] (Virtual AP profile "lab1-psk-vap") #vlan X20    <- X[1…6]
(LabX-MM-1) ^[labX] (Virtual AP profile "lab1-psk-vap") #!
```

第8步: 增加一个新的 ap-group “labX-group”，并将 labX-psk-vap 关联到这个 ap-group。

```
(LabX-MM-1) ^[labX] (config) #ap-group labX-group     <- X[1…6]
(LabX-MM-1) ^[labX] (AP group "lab1-group") #virtual-ap labX-psk-vap     <- X[1…6]
(LabX-MM-1) ^[labX] (AP group "lab1-group") #!
```

第9步: 保存配置

```
(LabX-MM-1) ^[labX] (config) #write memory
Saving Configuration...
Configuration Saved.
```

第10步:将 AP 分配到 “labX-group”

```
(LabX-MM-1) [labX] (config) #ap-regroup ap-name 94:b4:0f:c1:3f:e0 labX-group      <- X[1…6]
NOTE: For cert RAP/CAP ap-group specified in RAP/CAP whitelist will take precedence.
```

第11步:查看完成还未提交的配置内容

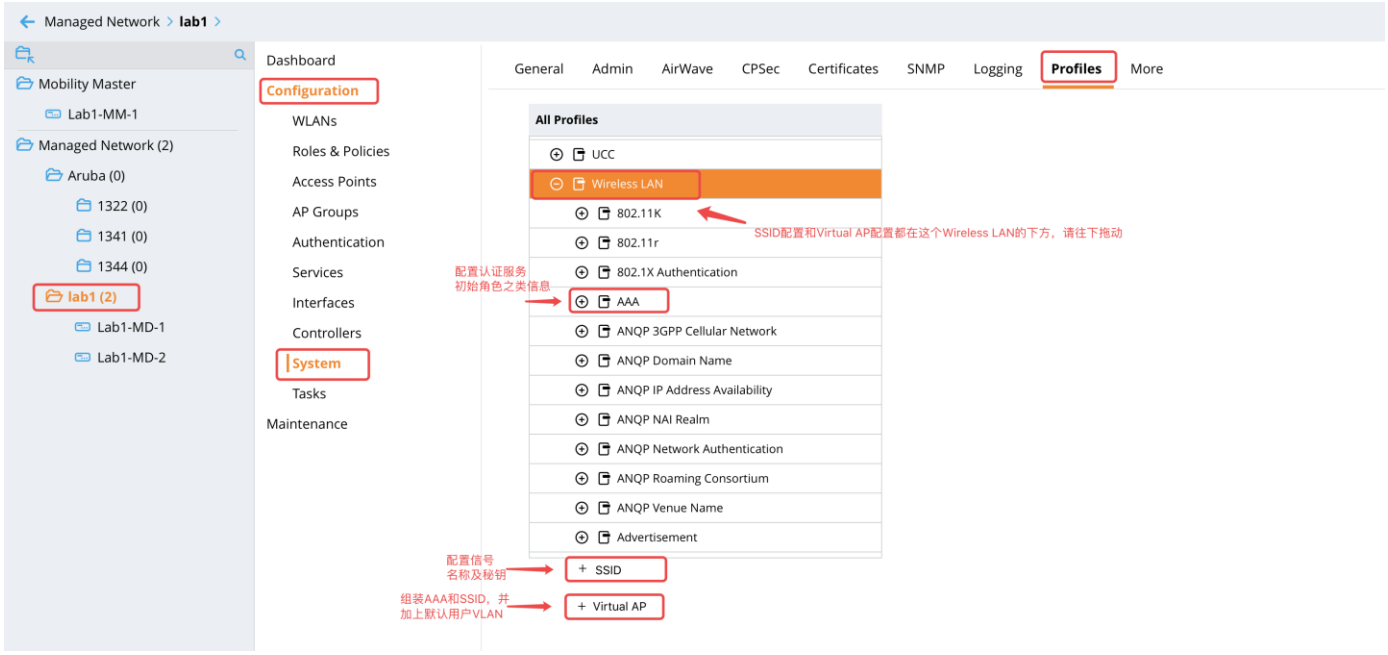
```
(LabX-MM-1) ^[labX] (config) #show configuration pending
```

第12步:保存配置

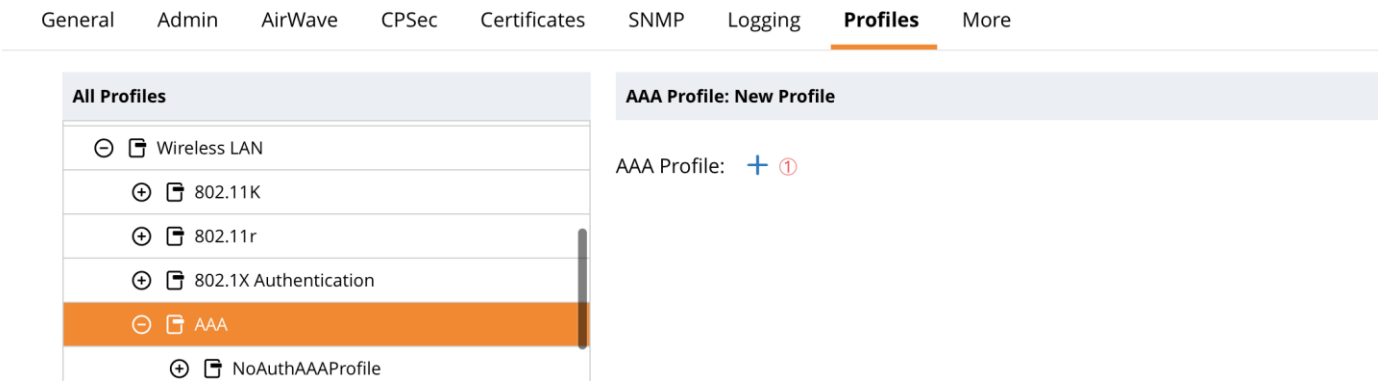
```
(LabX-MM-1) ^[labX] (config) #write memory
Saving Configuration...
Configuration Saved.
```

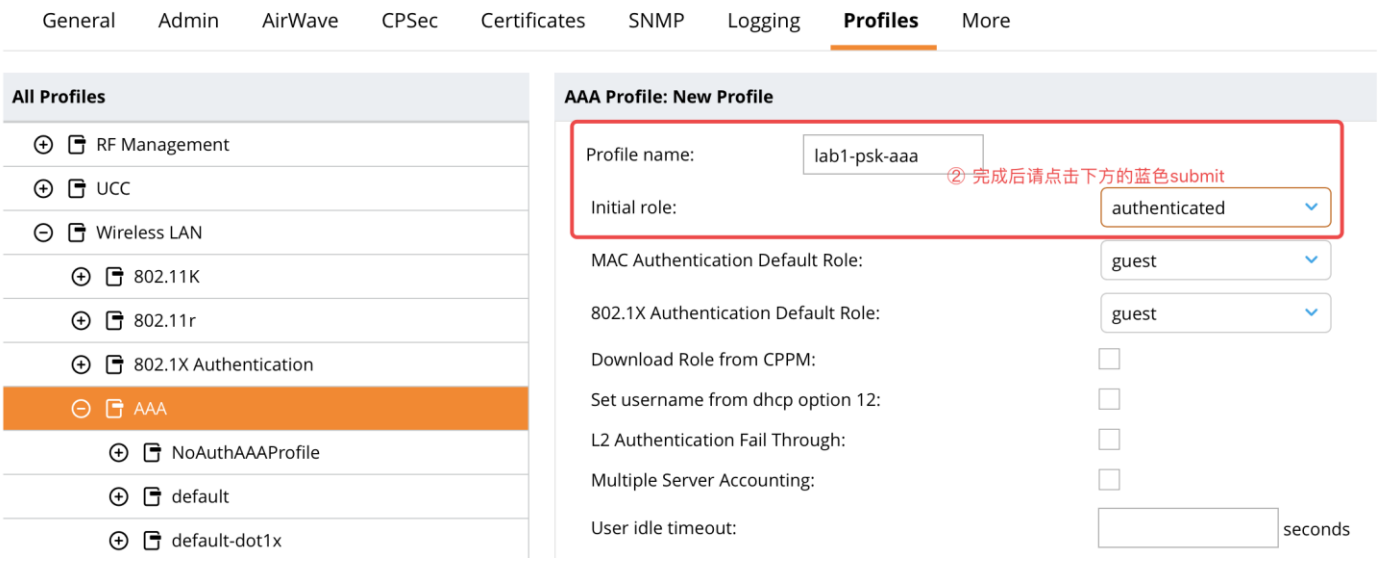
8.4 MM 配置（GUI）

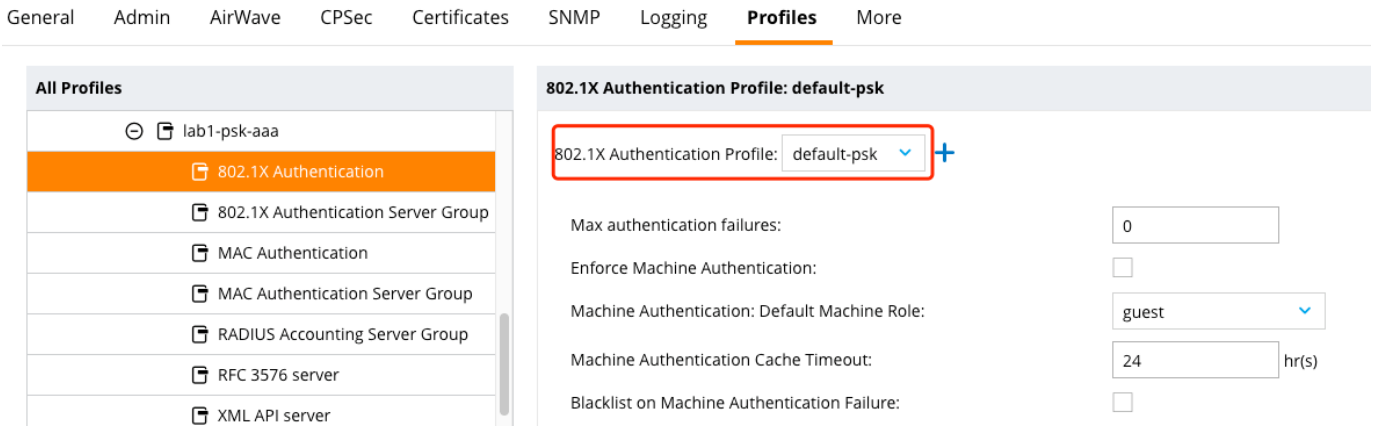
第1步: 进入到 Managed Network -> labX -> Configuration -> System，点击“Profiles”
在“Wireless LAN”中找到配置 AAA, SSID, Virtual AP 的路径，



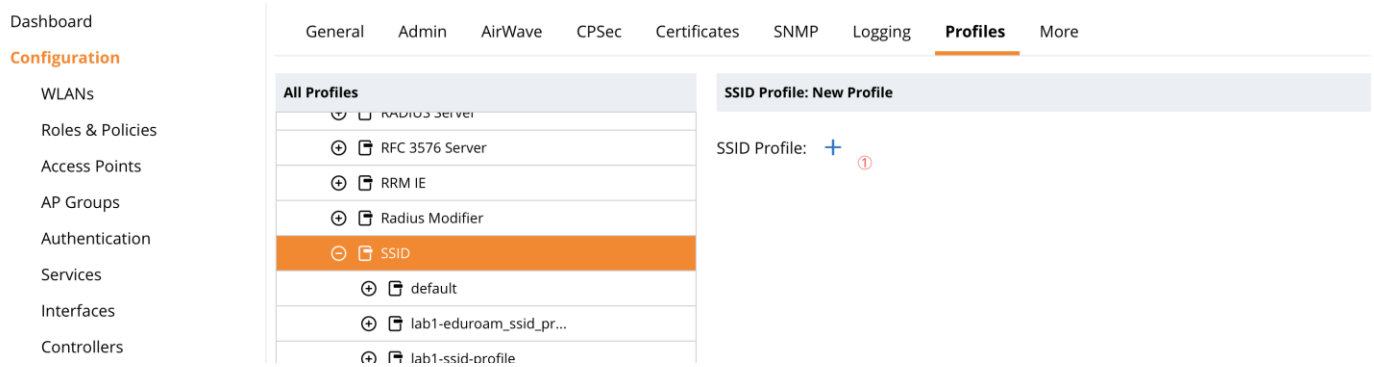
第2步: 配置 AAA, 点击＋，新建 AAA profile name 为： “labX-psk-aaa”，修改初始角色为：” authenticated”，配置 802.1X Authentication Profile 为： “default-psk”，点击右下角 submit
<- 这里的 X 代表 lab 分组[1…6]

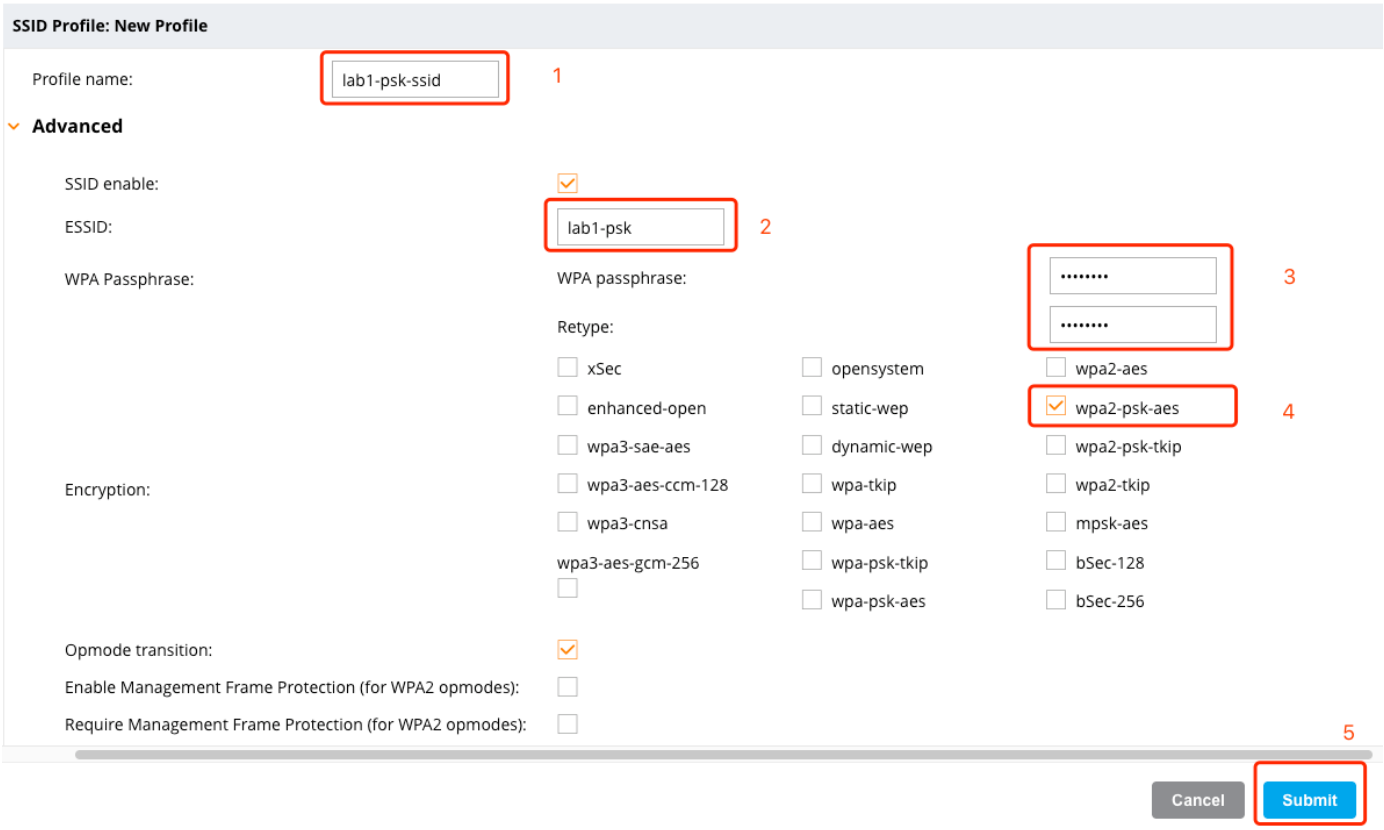




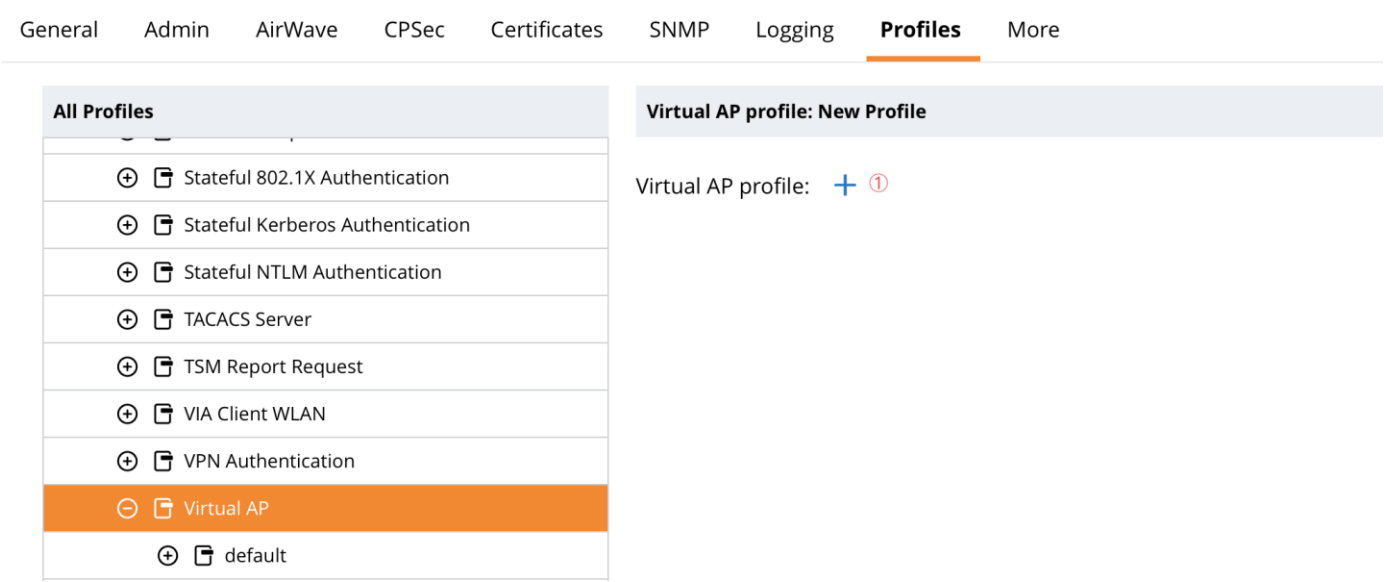


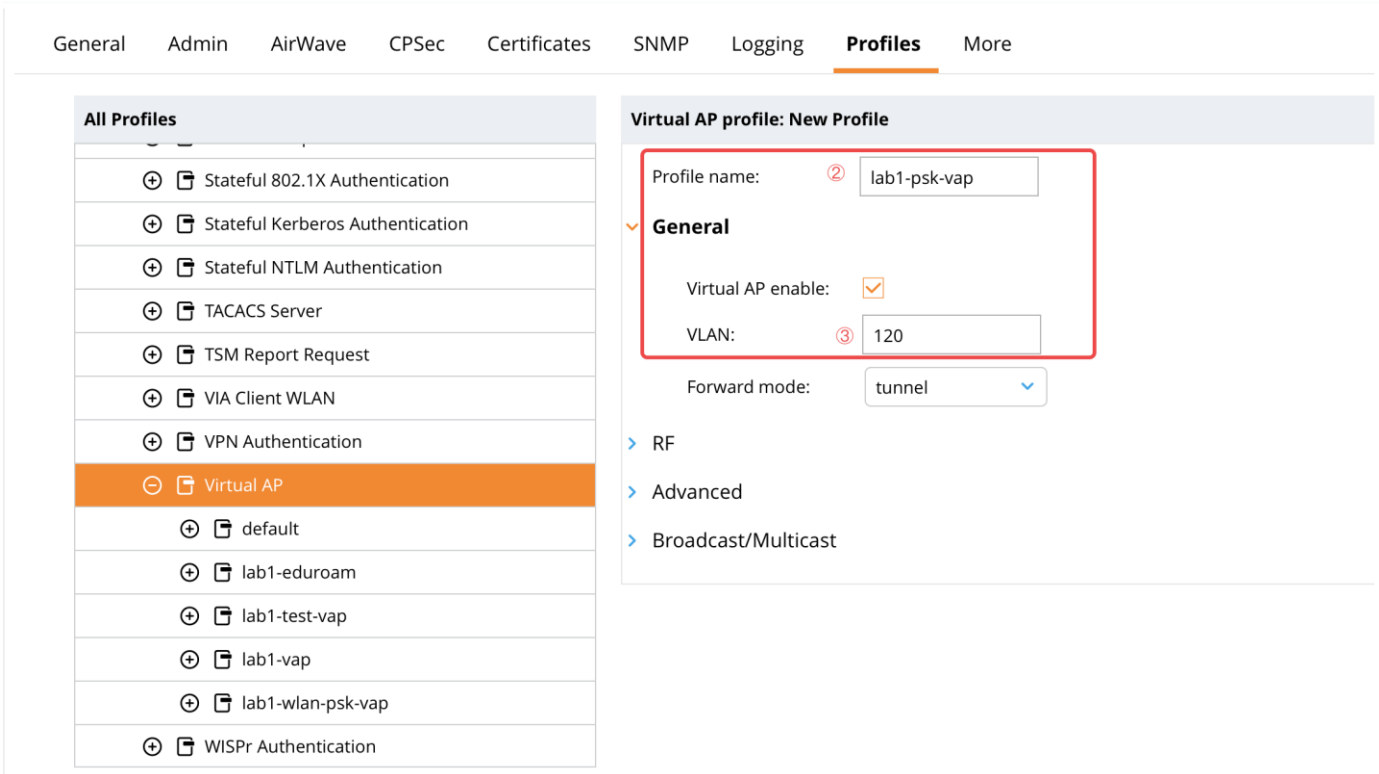
第3步：配置 SSID Profile，点击＋，新建 SSID profile name 为“labX-psk-ssid”,输入 ESSID 为 labX-psk，输入密码 aruba123 并确认密码，勾选认证方法“wpa2-psk-aes”最后点击右下角 Submit <- 这里的 X 代表 lab 分组[1…6]

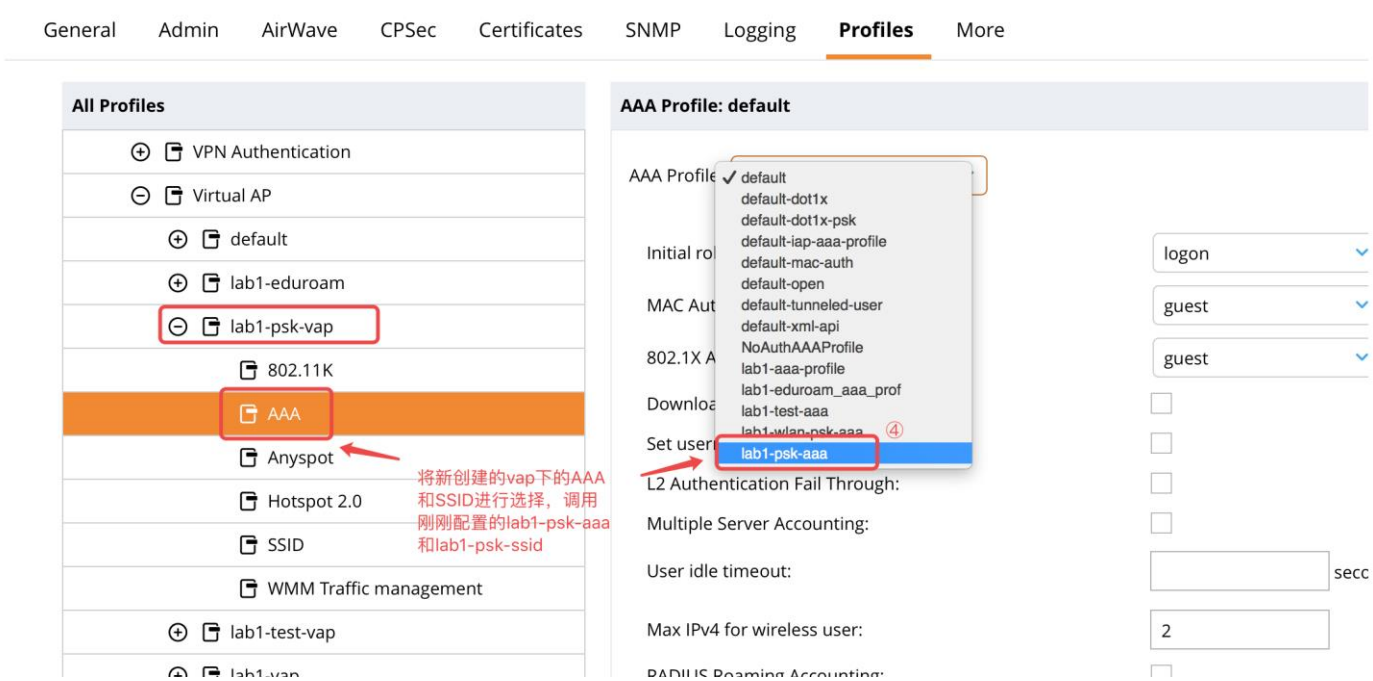


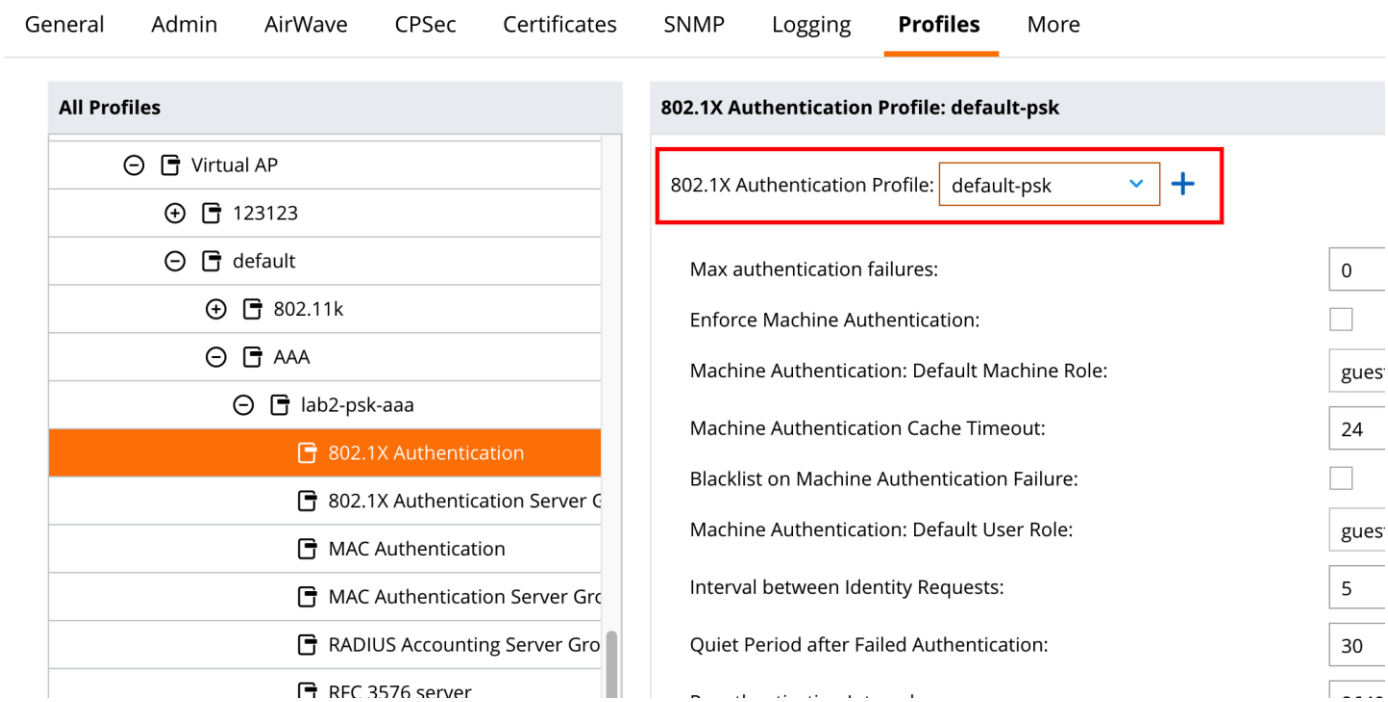


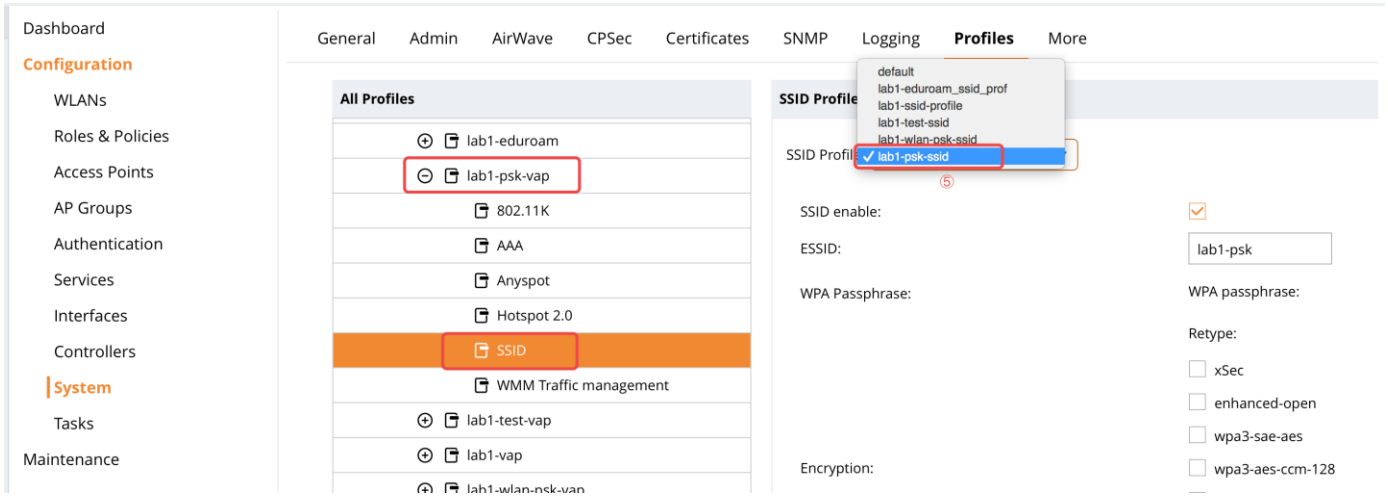
第4步：配置 VAP Profile，点击＋，新建 VAP profile name 为 “labX-psk-vap”,输入 VLAN 为 X20，点击右下角 Submit，然后将 labX-psk-vap 下的 AAA 和 SSID 分别选择 labX-psk-aaa 和 labX-psk-ssid 并且保存 <- 这里的 X 代表 lab 分组[1…6]



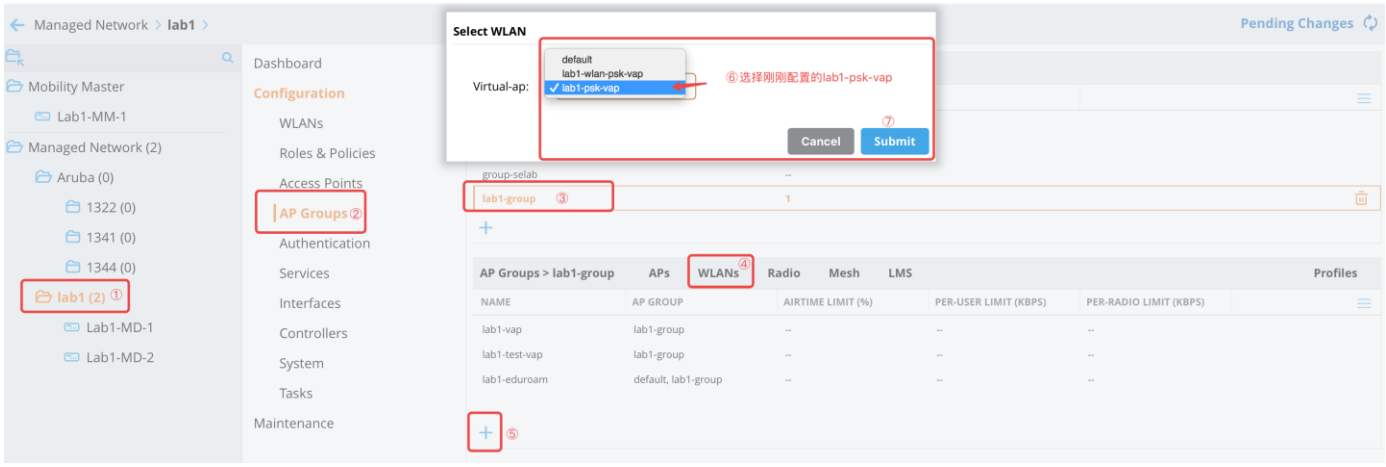

General
Admin
AirWave
CPSec
Certificates
SNMP
Logging
Profiles
More
All Profiles
Stateful 802.1X Authentication
Stateful Kerberos Authentication
Stateful NTLM Authentication
TACACS Server
TSM Report Request
VIA Client WLAN
VPN Authentication
Virtual AP
default
lab1-eduroam
lab1-test-vap
lab1-vap
lab1-wlan-psk-vap
WISPr Authentication
Virtual AP profile: New Profile
Profile name:
②
lab1-psk-vap
General
Virtual AP enable:
VLAN:
③
120
Forward mode:
tunnel
RF
Advanced
Broadcast/Multicast


General
Admin
AirWave
CPSec
Certificates
SNMP
Logging
Profiles
More
All Profiles
VPN Authentication
Virtual AP
default
lab1-eduroam
lab1-psk-vap
802.11K
AAA
Anyspot
Hotspot 2.0
SSID
WMM Traffic management
lab1-test-vap
AAA Profile: default
AAA Profile
default
default-dot1x
default-dot1x-psk
default-iap-aaa-profile
default-mac-auth
default-open
default-tunneled-user
default-xml-api
NoAuthAAAProfile
lab1-aaa-profile
lab1-eduroam_aaa_prof
lab1-test-aaa
④
lab1-psk-aaa
Initial ro
logon
MAC Aut
guest
802.1X A
guest
Downloa
Set user
L2 Authentication Fail Through:
Multiple Server Accounting:
User idle timeout:
secc
Max IPv4 for wireless user:
2
将新创建的vap下的AAA和SSID进行选择，调用刚刚配置的lab1-psk-aaa和lab1-psk-ssid

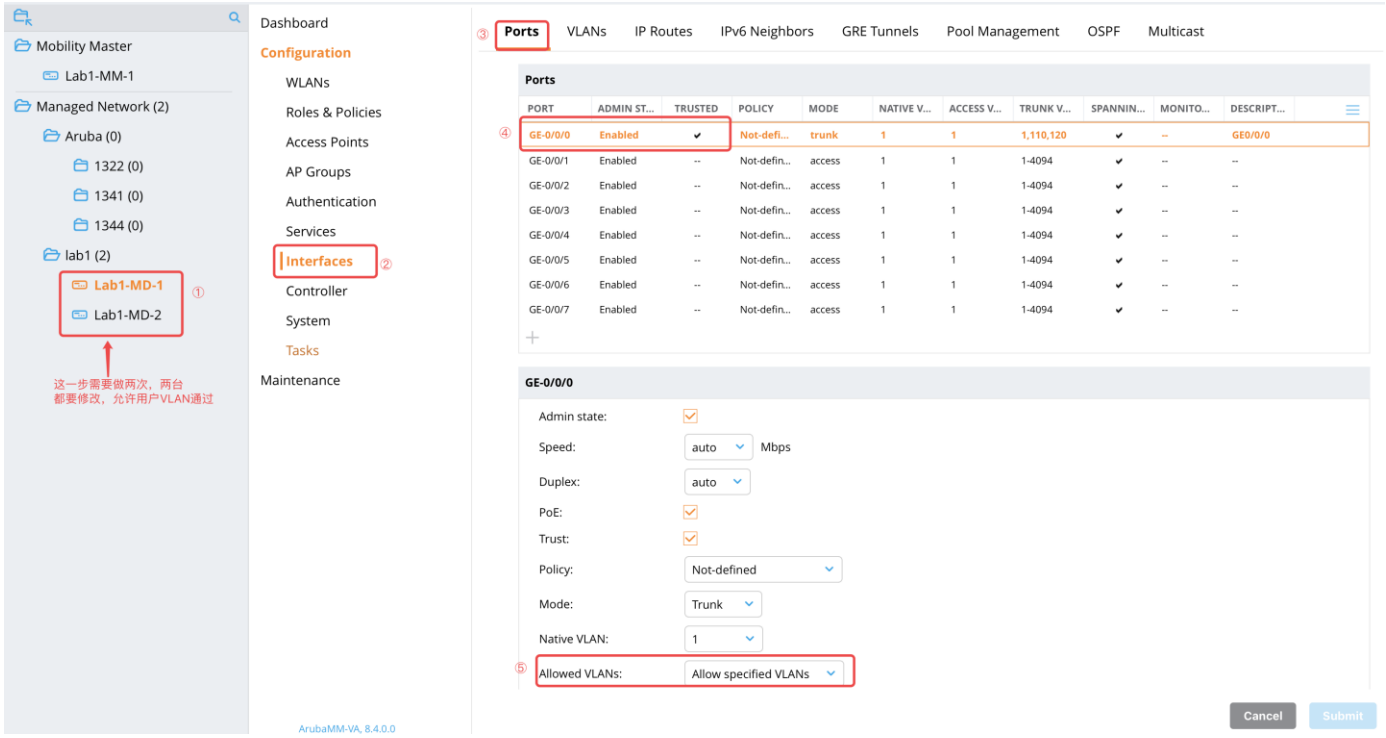


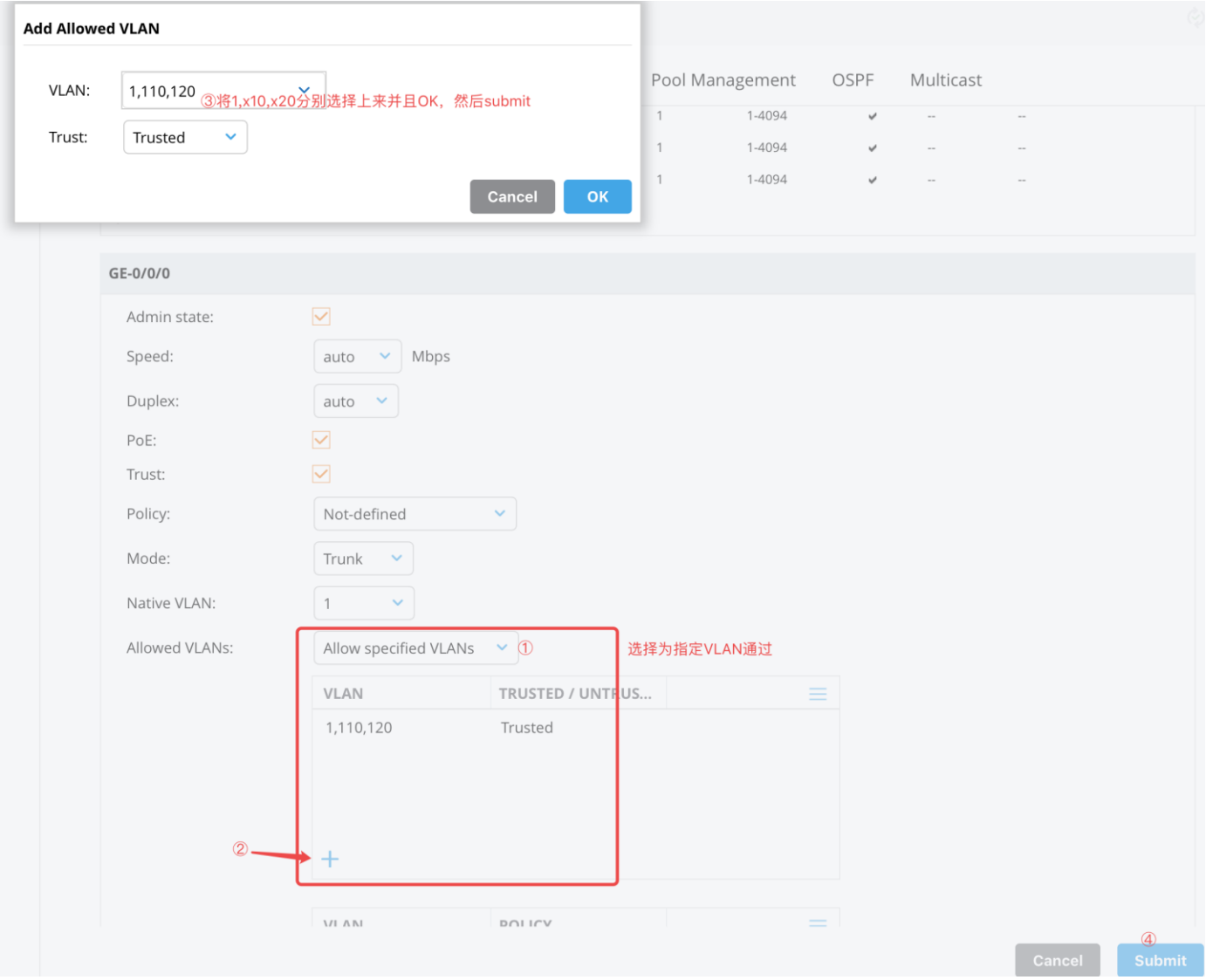


第5步：配置 AP-GROUP，在 Managed Network 中，选择 Lab1，选择 AP-Group，点击＋，新建一个 AP-Group，名称为 labX-Group，选中这个配置的 labX-Group，选择其 WLAN 配置，在图示的＋点击添加 VAP，选择“labX-psk-vap”,点击 Submit，然后点击右上角 Pending Changes 确认配置。 <- 这里的 X 代表 lab 分组[1…6]

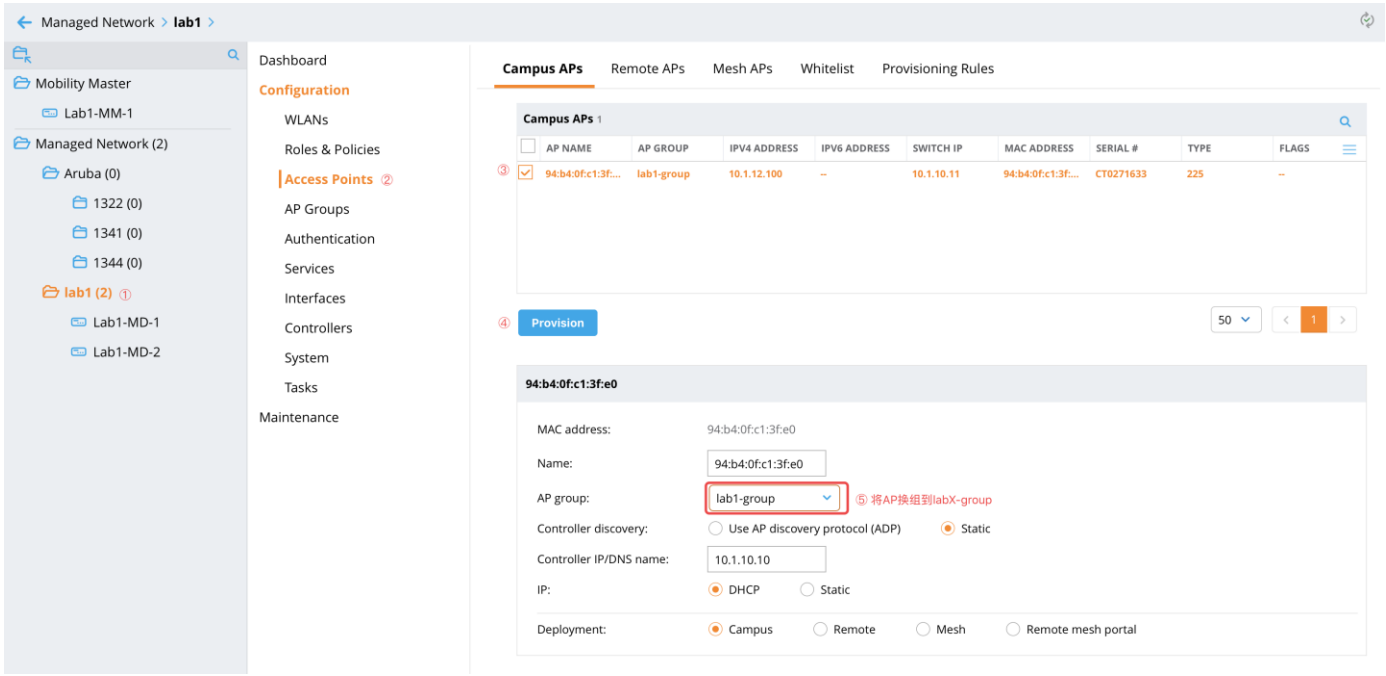


第6步：分别将 LabX-MD1 和 LabX-MD2 的上联接口 GE-0/0/0 的 allowed VLANS 修改为 1,X10,X20 可通过。 Submit 并且点击右上角 Pending Changes 确认配置。 <- 这里的 X 代表 lab 分组[1…6]





第7步：默认 AP 连接到控制器后，AP-Group 会是 default，我们需要将 AP 移动到上述配置的 labX-Group。按下图示例，从 LabX---Configuration---Access Point---Campus AP---勾选需要移动组的 AP---点击 provision 菜单，在新出来的对话框中，选择 labX-Group，然后保存。AP 会重启并完成换组动作。在 AP 换到 labX-Group 组后，会吐出 labX-psk 的信号，你可以在 Wireless Client 的远程桌面里，去完成连接动作并验证状态。 <- 这里的 X 代表 lab 分组[1…6]



NOTE

我们在新增配置时，需要先配置 AAA Profile 和 SSID Profile，才能组装成 VAP，并且引用到 AP-Group 中去，我们可以理解为逐级嵌套关系。反过来，如果要删除某些低层级配置，例如删除 AAA Profile，得先确认其是否被某个高层级的 VAP 引用，我们得解除 VAP 的引用关系才能删除 AAA Profile。查看引用关系的命令格式为 show references, 例如 show references wlan ssid-profile xxx 或者 show references wlan virtual-ap xxx

8.5 验证结果

第1步：使用 SSH 方式登录到 Mobility Master (10.X.50.11) 查看 AP 终结的 MD

```
(LabX-MM-1) [labX] (config) #cd mm

(LabX-MM-1) [mm] (config) #show ap database


AP Database

-----------

Name              Group      AP Type  IP Address   Status    Flags  Switch IP   Standby IP

----              -----      -------  ----------   ------    -----  ---------   ----------

94:b4:0f:c1:3f:e0  labX-group  225     10.1.12.100  Up 3m:8s  2     10.1.10.11  10.1.10.11
```

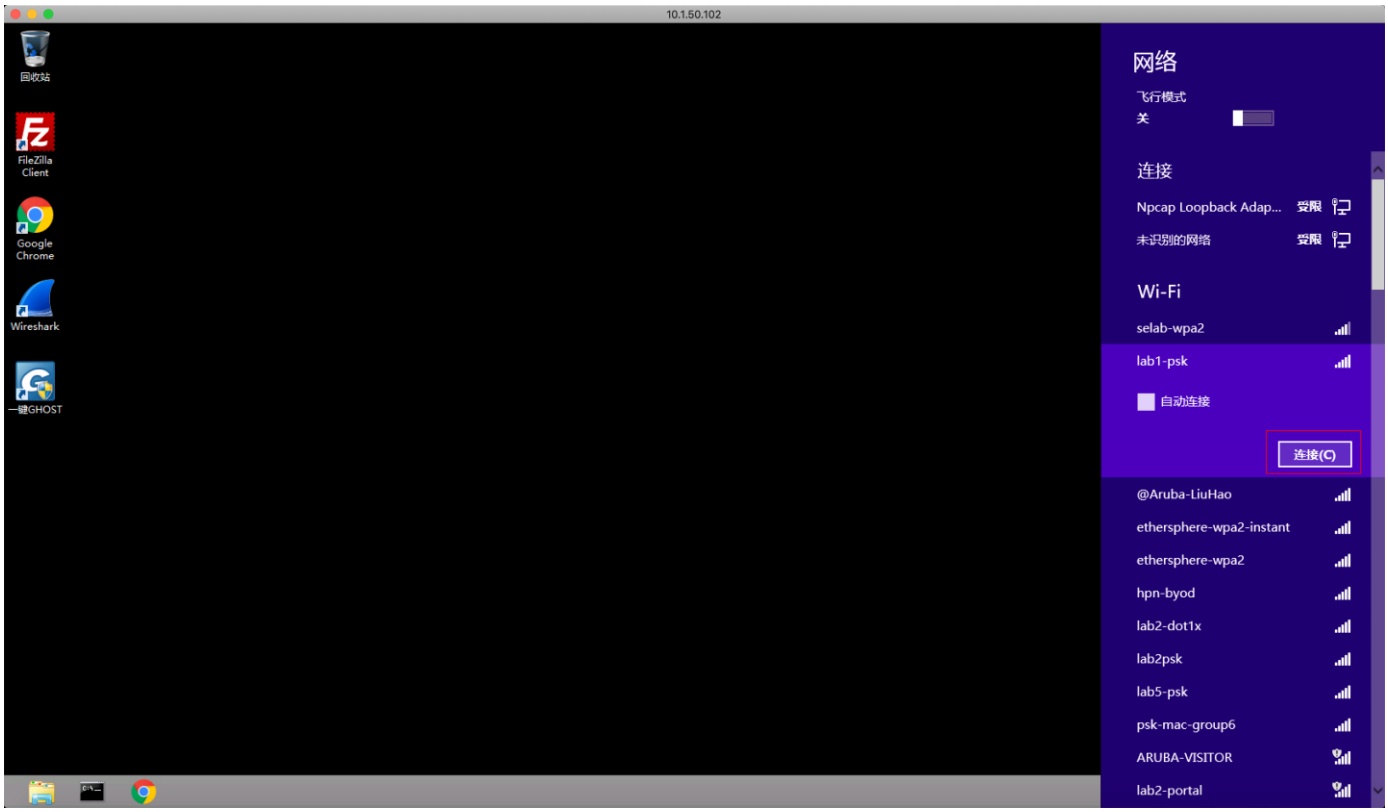
第2步：使用 logon 命令登录到 AP 终结的控制器 (示例中 AP 终结在 10.X.10.12) 查看释放的 SSID

```
(LabX-MM-1) [mm] (config) #logon 10.1.10.11

(labX-md1) [MDC] #show ap essid

ESSID Summary

-------------

ESSID     APs  Clients  VLAN(s)  Encryption

-----     ---  -------  -------  ----------

labX-psk  1    0        110      WPA2 PSK AES

Num ESSID:1
```

NOTE

由于配置完成后。默认从命令行 show wlan ssid-profile labx-psk-ssid-profile 查看时，WPA Passphrase 会显示为 ********，如果希望查看被隐藏的密码，可以先输入(Labx-MD-1) #encrypt disable，然后再 show wlan ssid-profile labx-psk-ssid-profile，即可看见密码，记住密码后，请再输入一次(Labx-MD-1) #encrypt enable 即可恢复默认状态

第3步：RDP 远程登录到无线测试终端（10.X.50.102），连接到无线 SSID：1abX-psk



第4步：登录到 MM 的/mm 节点，查看用户在线情况

```
(LabX-MM-1) [mm] (config) #show global-user-table list


Global Users

------------

   IP          MAC           Name   Current switch  Role        Auth  AP name         Roaming   Essid    Bssid           Phy
Profile      Type  User Type

----------  ------------      ------  --------------  ----        ----  -------         -------   -----    -----           ---   -------
 ----  ---------

10.1.20.100  7c:7a:91:46:52:b7        10.1.10.11      authenticated       94:b4:0f:c1:3f:e0  Wireless  lab1-psk  94:b4:0f:93:fe:
10  a-VHT  lab1-psk-aaa  N/A   WIRELESS
```

9 MAC 认证

9.1 用户需求

客户希望只有指定哪些MAC的终端才能连接无线网，如MAC不对则无法关联。

9.2 实现思路

先配置 aaa profile（规定认证规则，认证服务器及初始角色），wlan ssid-profile（规定 SSID 名称）,然后将 aaa profile 和 wlan ssid-profile 组合形成一个 VAP（规定虚拟 AP 名称和默认用户 VLAN），然后将 VAP 和 AP-Group 进行捆绑，这样该 AP-Group 下的 AP 即可放出指定信号。在认证服务器上（示例为 clearpass），我们也需要对应的配置 MAC 账号，以及 MAC 认证策略。

9.3 MM 配置（CLI）

第1步: 使用 SSH 方式登录到 Mobility Master: 10.X.50.11 （<- 这里的 X 代表 lab 分组[1…6]）

第2步: 在 Mobility Master（MM）上进入 /md/labX 配置节点，并进入配置模式

```
(LabX-MM-1) [mynode] #cd /md/labX    <- X[1…6]
(LabX-MM-1) [labX] #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(LabX-MM-1) [labX] (config) #
```

第3步: 增加一个新的 radius 认证服务器 “labX-cppm “

```
(LabX-MM-1) [labX] (config) #aaa authentication-server radius labX-cppm    <- X[1…6]
(LabX-MM-1) ^[labX] (RADIUS Server "cppm") #host 10.0.50.41    <- [1-6 组采用同一个 CPPM]
(LabX-MM-1) ^[labX] (RADIUS Server "cppm") #key aruba123
(LabX-MM-1) ^[labX] (RADIUS Server "cppm") #!
```

第4步: 增加一个新的 radius 服务器组 “labX-sg”

```
(LabX-MM-1) ^[labX] (config) #aaa server-group labX-sg    <- X[1…6]
(LabX-MM-1) ^[labX] (Server Group “lab1-sg") #auth-server labX-cppm    <- X[1…6]
(LabX-MM-1) ^[labX] (Server Group “lab1-sg") #!
```

第5步：增加一个新的角色叫 mac-failed，其默认策略为 any any any deny，用于 mac 认证失败的用户：

```
(LabX-MM-1) ^ [labX] (config) #ip access-list session mac-failed
(LabX-MM-1) ^[labX] (config-submode)# any any any deny
(LabX-MM-1) ^[labX] (config-submode)#!
(LabX-MM-1) ^[labX] (config) #user-role mac-failed
(LabX-MM-1) ^[labX] (config-submode)#access-list session mac-failed
(LabX-MM-1) ^[labX] (config-submode)#write memory
(LabX-MM-1) [labX] (config-submode)#!
```

第6步：增加一个新的 mac 认证配置 labX-mac（定义 mac 认证用户名和密码的格式，默认小写不带分隔符）

```
(LabX-MM-1) [labX] (config) #aaa authentication mac labX-mac    <- X[1…6]
(LabX-MM-1) ^[labX] (MAC Authentication Profile  “lab1-mac") #case lower
(LabX-MM-1) ^[labX] (MAC Authentication Profile  “lab1-mac") #delimiter none
(LabX-MM-1) ^[labX] (MAC Authentication Profile  “lab1-mac") #!
```

第7步：增加一个新的 aaa profile “labX-mac-aaa”，使用 labX-sg 作为认证和计费服务器，mac 认证成功获得 authenticated 角色，失败获得 mac-failed 角色

```
(LabX-MM-1) ^[labX] (config) #aaa profile labX-mac-aaa    <- X[1…6]
(LabX-MM-1) ^[labX] (AAA Profile  “lab1-mac-aaa") #initial-role mac-failed
(LabX-MM-1) ^[labX] (AAA Profile  “lab1-mac-aaa") #mac-default-role authenticated
(LabX-MM-1) ^[labX] (AAA Profile  “lab1-mac-aaa") #authentication-mac labX-mac    <- X[1…6]
(LabX-MM-1) ^[labX] (AAA Profile  “lab1-mac-aaa") #mac-server-group labX-sg    <- X[1…6]
(LabX-MM-1) ^[labX] (AAA Profile  “lab1-mac-aaa") #radius-accounting labX-sg    <- X[1…6]
(LabX-MM-1) ^[labX] (AAA Profile  “lab1-mac-aaa") #!
```

第8步：增加一个新的 ssid profile “labX-mac-ssid”

```
(LabX-MM-1) ^[labX] (config) #wlan ssid-profile labX-mac-ssid    <- X[1…6]
(LabX-MM-1) ^[labX] (SSID Profile  “lab1-mac-ssid") #essid labX-mac    <- X[1…6]
(LabX-MM-1) ^[labX] (SSID Profile  “lab1-mac-ssid") #!
```

第9步: 增加一个新的 virtual-ap profile “labX-mac-vap”

```
(LabX-MM-1) ^[labX] (config) #wlan virtual-ap labX-mac-vap    <- X[1…6]
(LabX-MM-1) ^[labX] (Virtual AP profile “lab1-mac-vap") #aaa-profile labX-mac-aaa  <-X[1…6]
(LabX-MM-1) ^[labX] (Virtual AP profile “lab1-mac-vap") #ssid-profile labX-mac-ssid  <-X[1…6]
(LabX-MM-1) ^[labX] (Virtual AP profile “lab1-mac-vap") #vlan X20    <- X[1…6]
(LabX-MM-1) ^[labX] (Virtual AP profile “lab1-mac-vap") #!
```

第10步:将 virtual-ap “labX-mac-vap” 添加到 ap-group “labX-group” 中。

```
(LabX-MM-1) ^[labX] (config) #ap-group labX-group    <- X[1…6]
(LabX-MM-1) ^[labX] (AP group "lab1-group") #virtual-ap labX-mac-vap    <- X[1…6]
(LabX-MM-1) ^[labX] (AP group "lab1-group") #!
```

第11步:查看完成还未提交的配置内容

```
(LabX-MM-1) ^[labX] (config) #show configuration pending
```

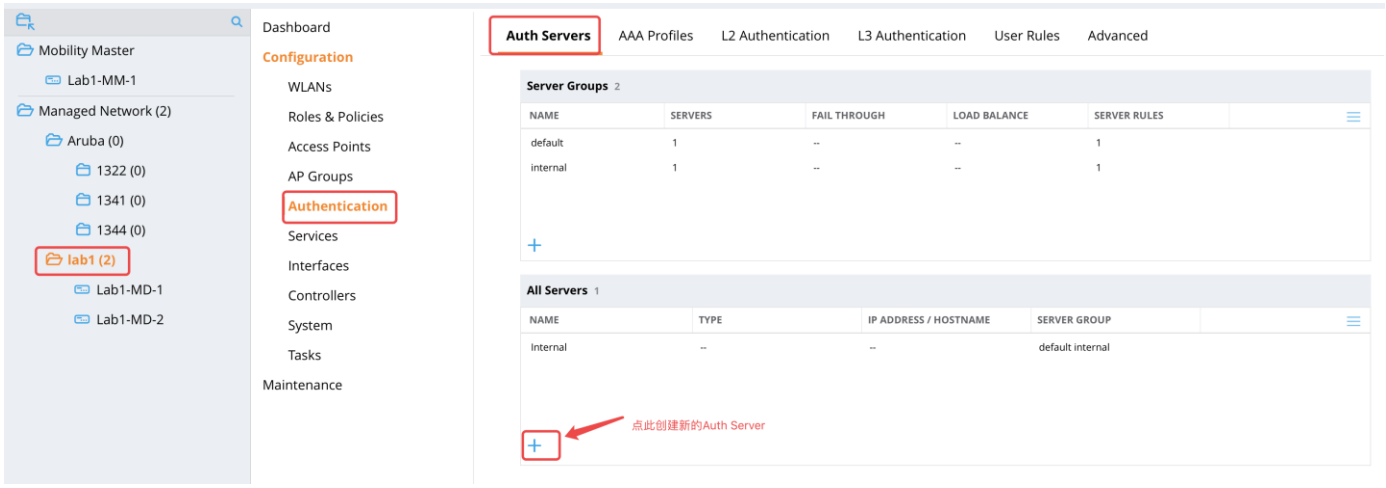
第12步:保存配置

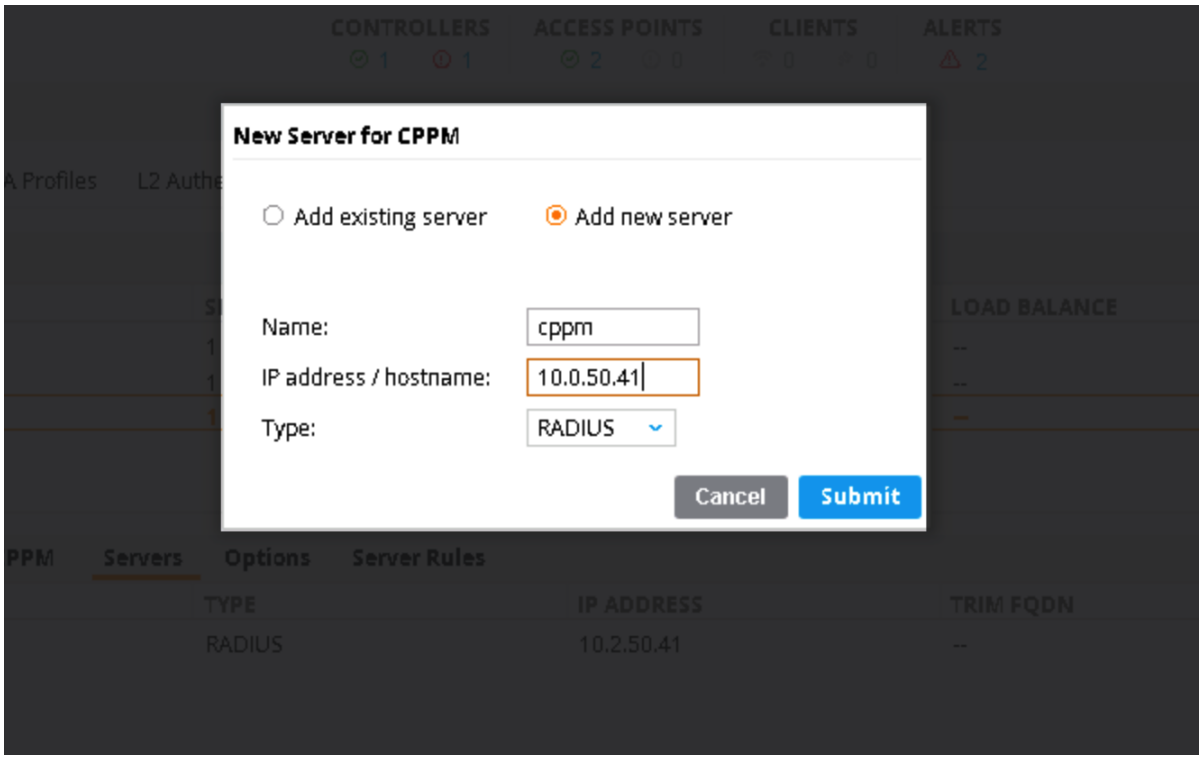
```
(LabX-MM-1) ^[labX] (config) #write memory
Saving Configuration...
Configuration Saved.
```

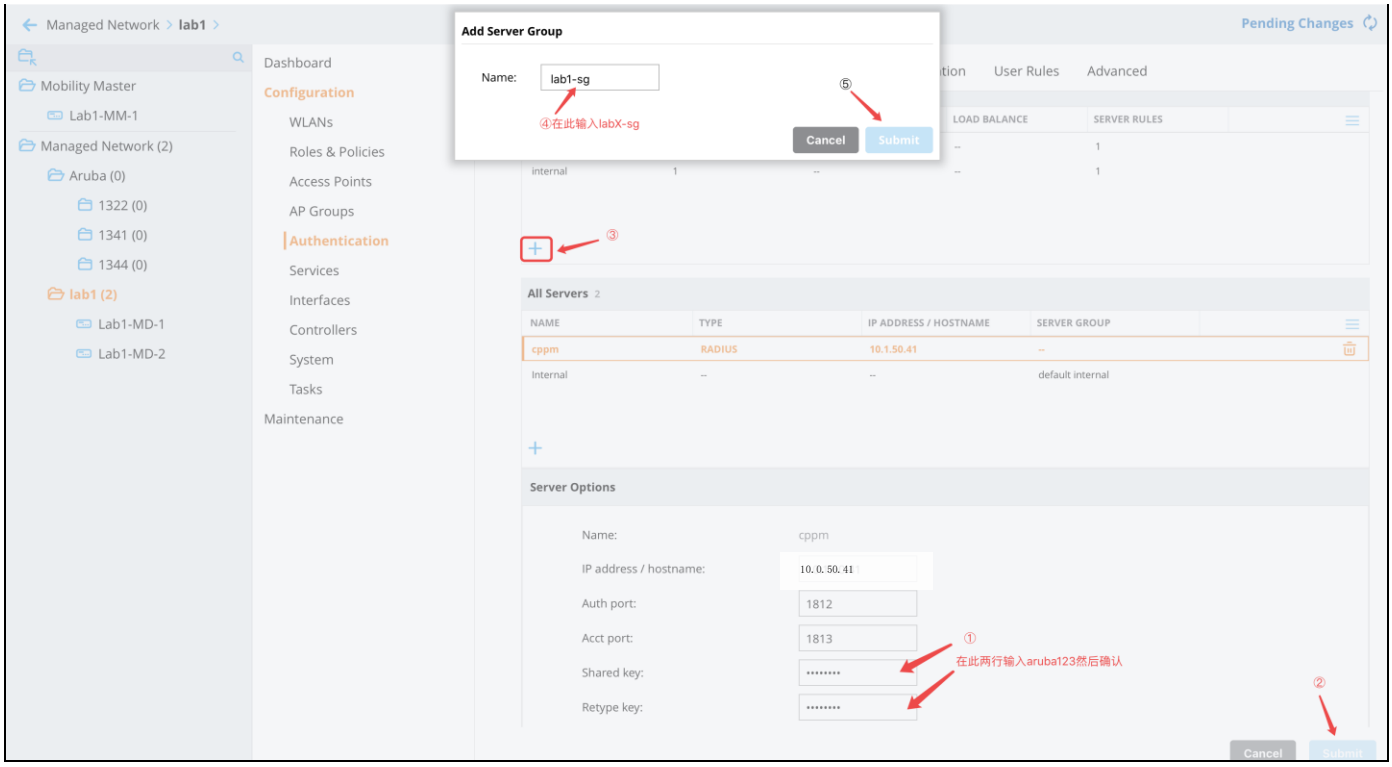
9.4 MM 配置（GUI）

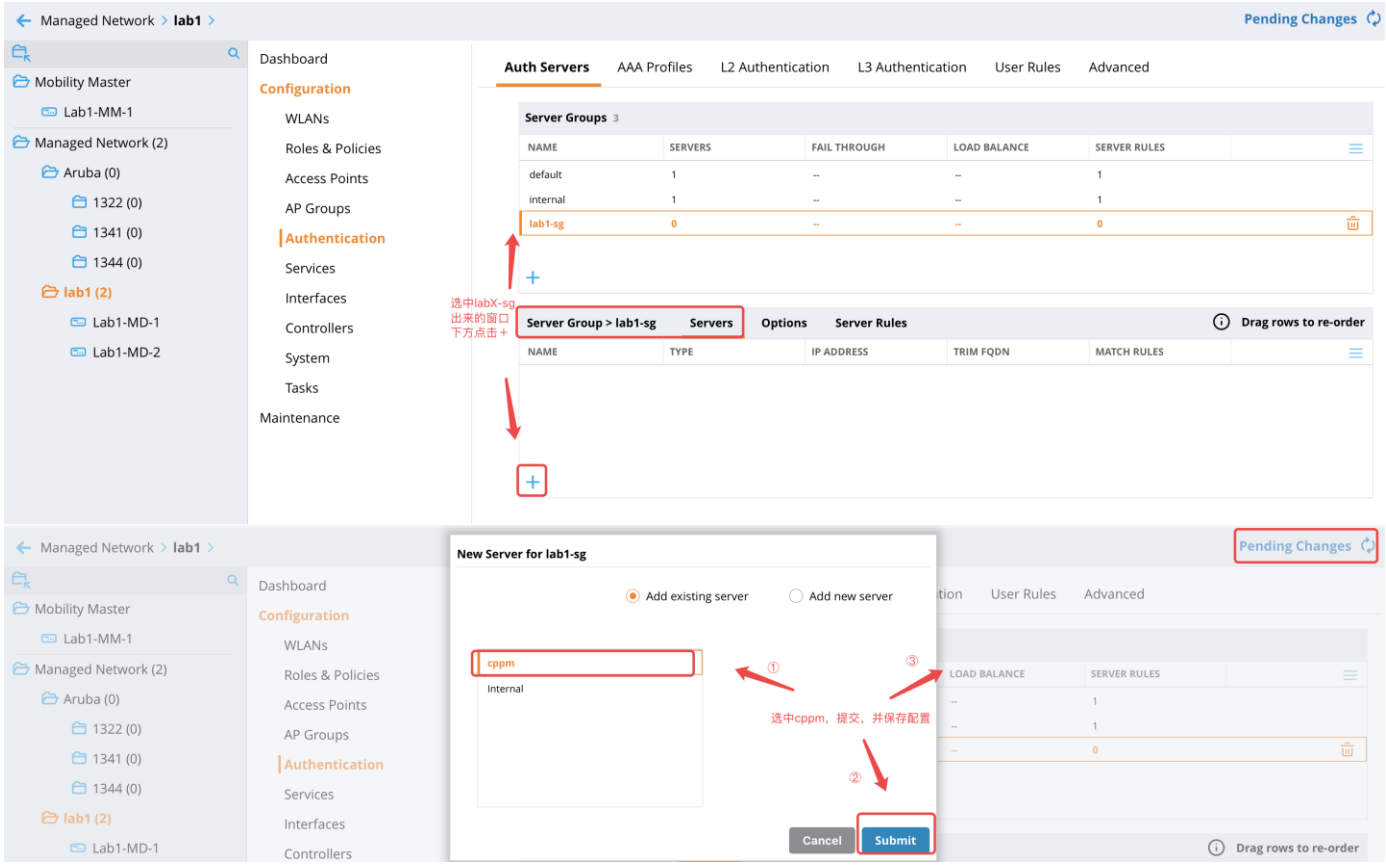
由于本节的认证引入了 Clearpass 作为认证源，需要在配置 AAA 前，提前预备好认证相关配置，以便调用。

第1步：先创建 auth servers, 在 LabX 的 Configuration --- Authentication --- Auth Servers ---All Servers 下添加新的认证服务器，name 为 cppm，IP 为 10.0.50.41，确认，然后再在新窗口内，将 Radius 共享秘钥设置为 aruba123。然后再在 Auth Servers 下的 Server Group 中点击＋，创建一个新的 ServerGroup 名为 LabX-sg，并将 cppm 添加在组内。

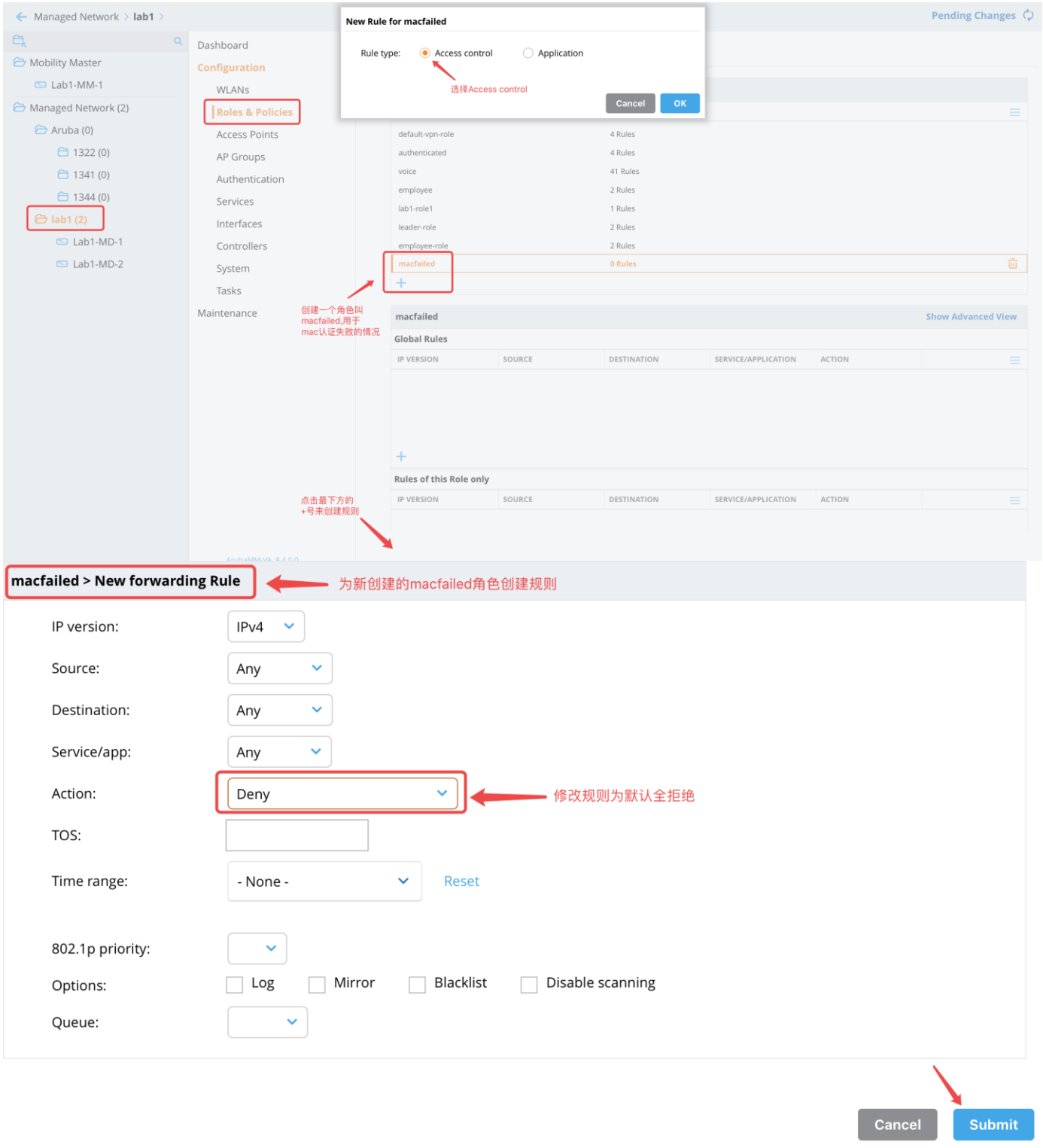




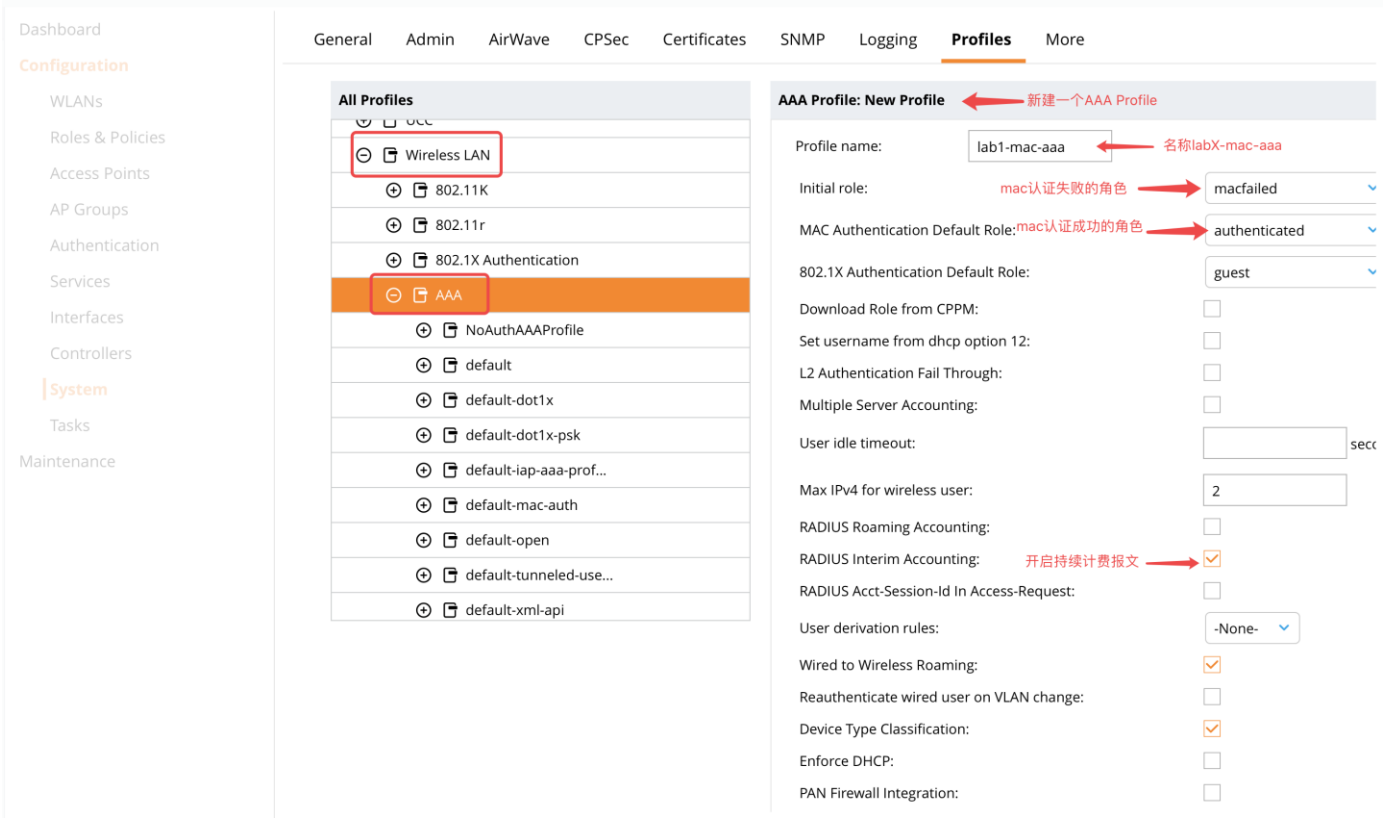

Managed Network > lab1 >
Pending Changes
Add Server Group
Name:
lab1-sg
④在此输入labX-sg
⑤
Cancel
Submit
Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces
Controllers
System
Tasks
Maintenance
Mobility Master
Lab1-MM-1
Managed Network (2)
Aruba (0)
1322 (0)
1341 (0)
1344 (0)
lab1 (2)
Lab1-MD-1
Lab1-MD-2
User Rules
Advanced
LOAD BALANCE
SERVER RULES
③
All Servers 2
NAME
TYPE
IP ADDRESS / HOSTNAME
SERVER GROUP
cppm
RADIUS
10.1.50.41
Internal
default internal
Server Options
Name:
cppm
IP address / hostname:
10.0.50.41
Auth port:
1812
Acct port:
1813
Shared key:
Retype key:
①
在此两行输入aruba123然后确认
②
Cancel
Submit

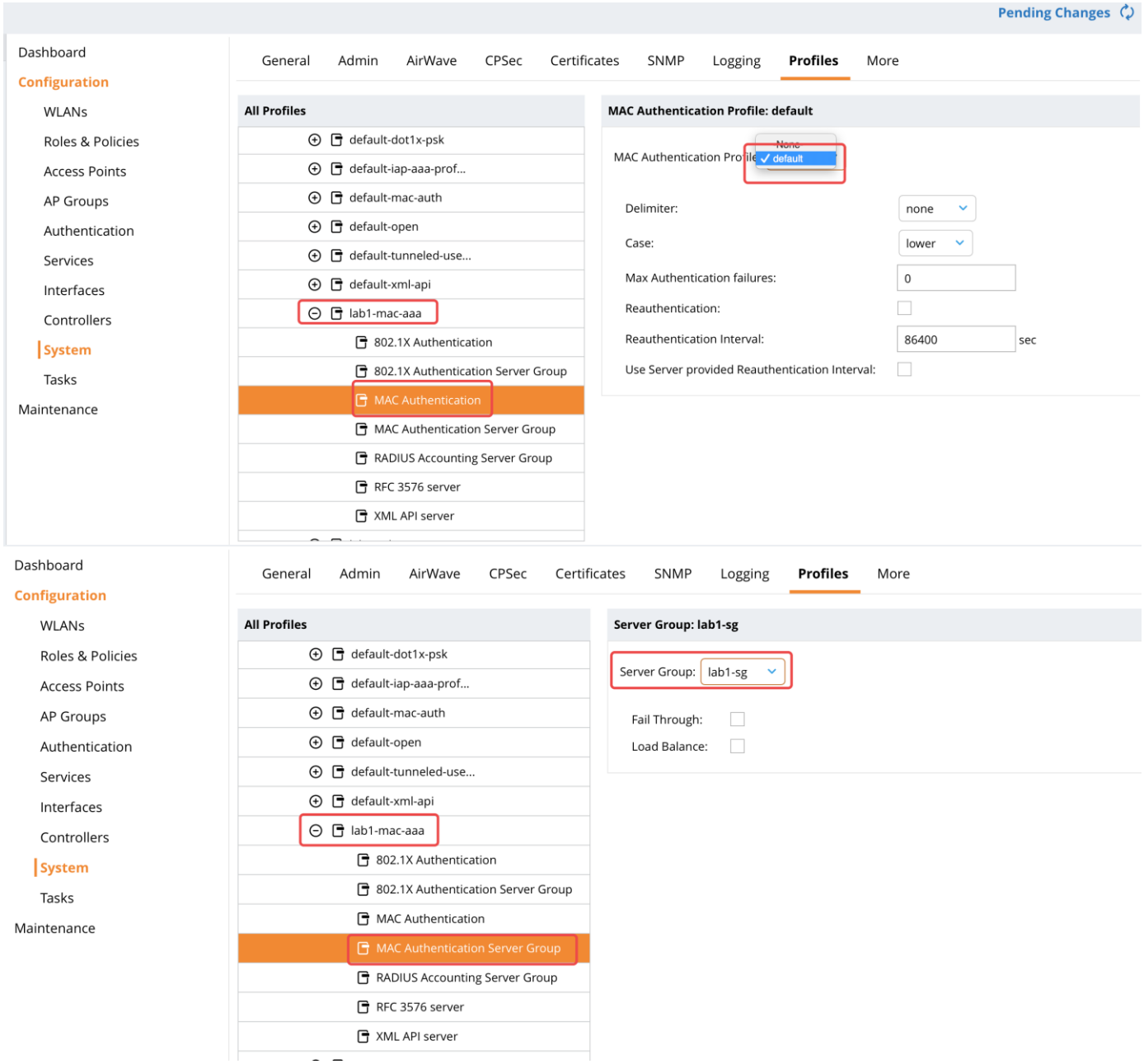

Managed Network > lab1 >
Pending Changes
Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces
Controllers
System
Tasks
Maintenance
Mobility Master
Lab1-MM-1
Managed Network (2)
Aruba (0)
1322 (0)
1341 (0)
1344 (0)
lab1 (2)
Lab1-MD-1
Lab1-MD-2
Auth Servers
AAA Profiles
L2 Authentication
L3 Authentication
User Rules
Advanced
Server Groups 3
NAME
SERVERS
FAIL THROUGH
LOAD BALANCE
SERVER RULES
default
internal
lab1-sg
选中labX-sg
出来的窗口
下方点击＋
Server Group > lab1-sg
Servers
Options
Server Rules
Drag rows to re-order
NAME
TYPE
IP ADDRESS
TRIM FQDN
MATCH RULES
New Server for lab1-sg
Add existing server
Add new server
cppm
Internal
①
③
选中cppm，提交，并保存配置
②
Cancel
Submit
Drag rows to re-order

第2步：再按前述文档中的步骤创建一个角色叫 macfailed(请不要取名为 denyall，系统隐藏了该角色，如果你在 MM 配置后会发现 MD 上实际无法调用该角色)，用于 mac 认证失败的场景。选择其规则为 any any any deny，并保存配置。

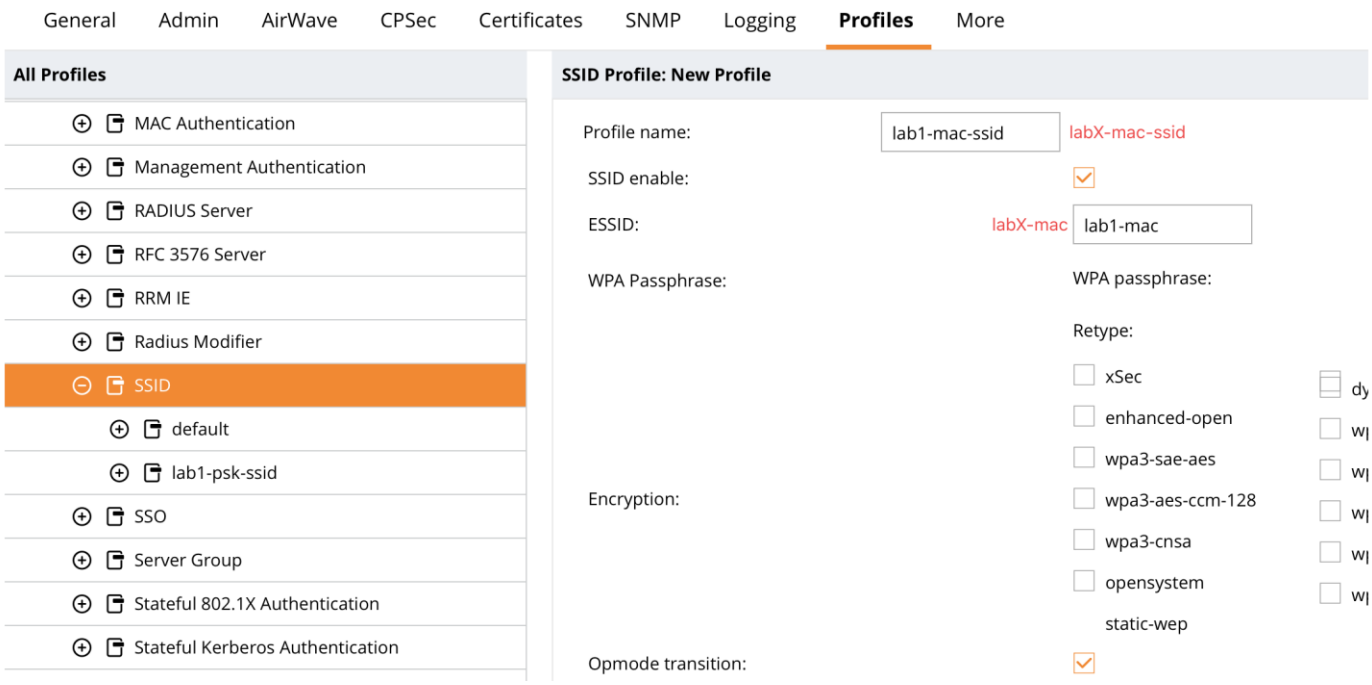


第3步：先完成 aaa profile，我们进入 All profiles 下的 Wireless LAN 下的 AAA，新加一个 AAA profile，取名为 labX-mac-aaa，修改其认证失败的角色为 macfailed，成功的角色为 authenticated，并开启计费报文，然后点 submit。在新出来的 labX-mac-aaa 下方，我们依次修改 mac authentication profile 为 default; mac authentication server group 为 labX-sg; radius accounting server-group 为 labX-sg，并依次保存。

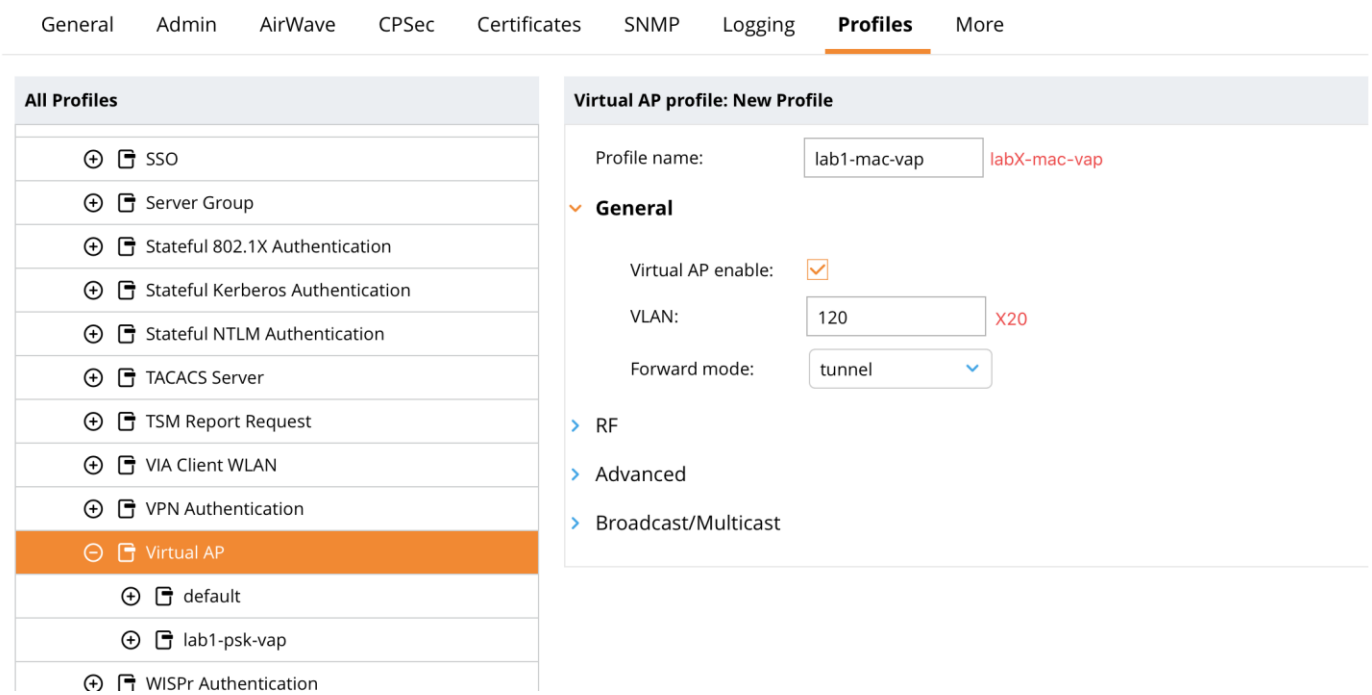


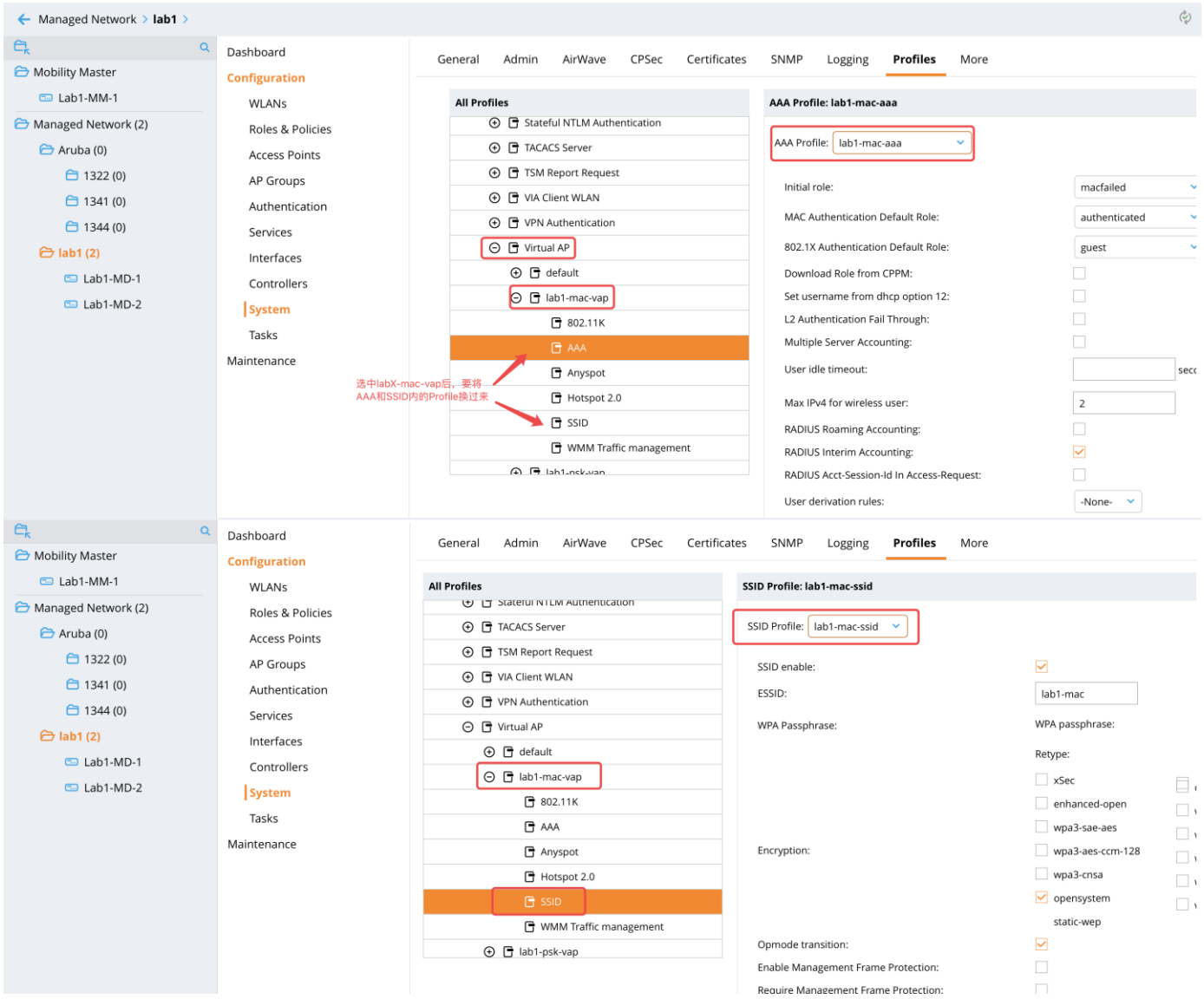


第4步：创建 SSID profile，如下图新建 labX-mac-ssid

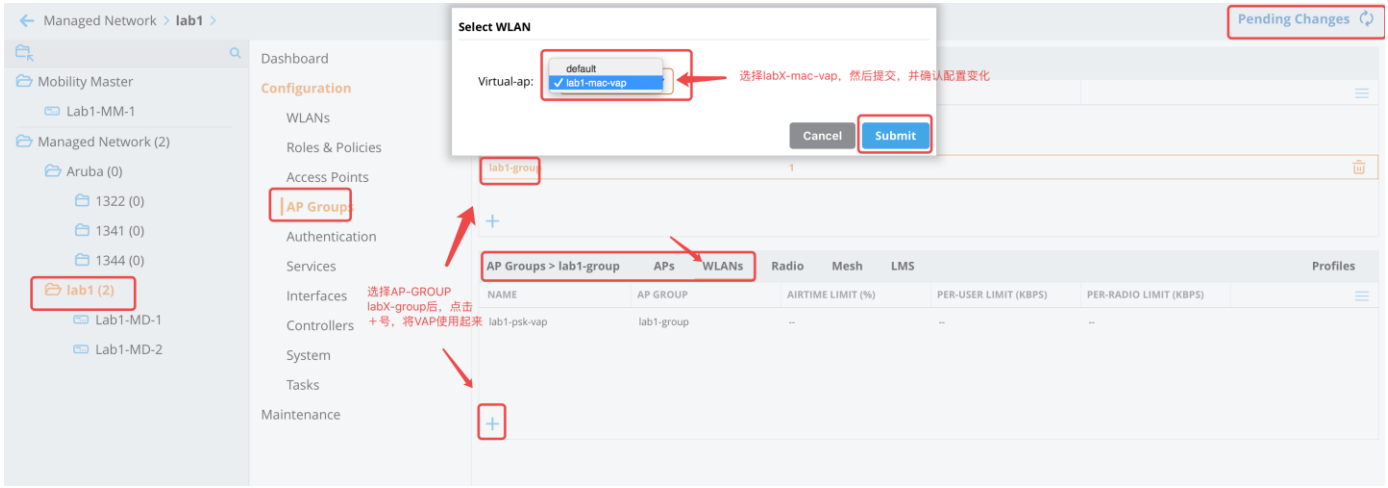


第5步：新建 Virtual AP, VAP 名字为 labX-mac-vap, VLAN 为 X20，保存后，修改 VAP 内的 AAA profile 为 labX-mac-aaa，SSID profile 修改为 labX-mac-ssid.



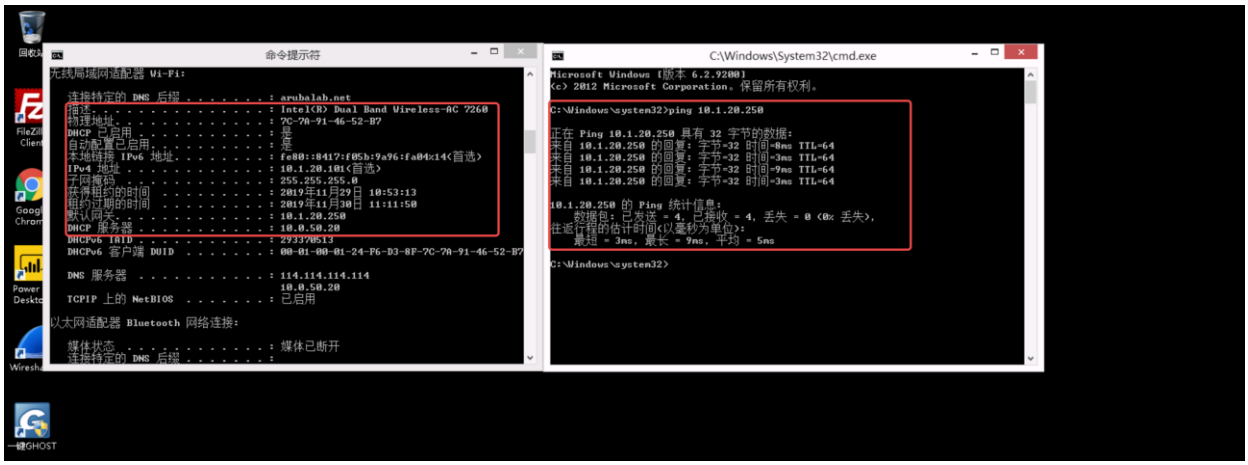


第6步：在 AP-GROUP labX-group 下，选择 WLANS，添加刚做好的 VAP，然后 submit 并点击右上角的 pending changes 确认配置，AP 即放出 labX-mac 信号可供测试



9.5 验证结果

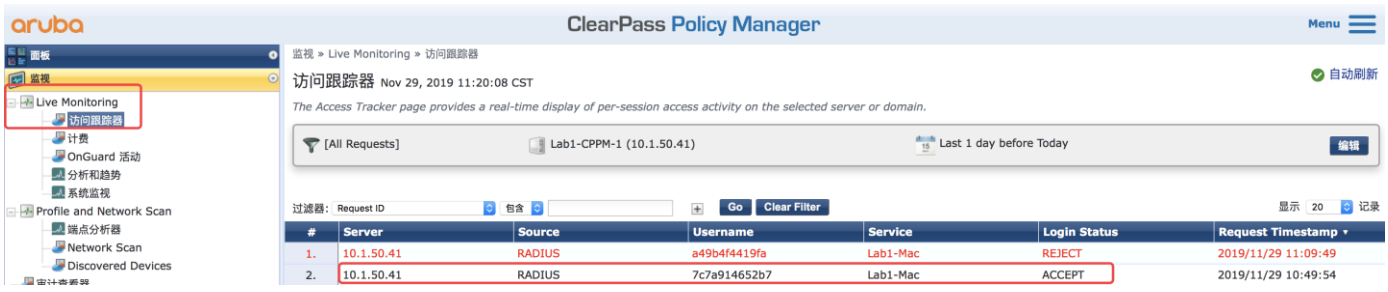
第1步：我们先将 LabX 的无线终端连接到 labX-mac，然后分别 Window 桌面，控制器，以及 clearpass 来确定是否正常。



第2步: 在 MM 上确认用户是否正常在线。

```
(LabX-MM-1) [mm] #show global-user-table list

Global Users

------------

  IP          MAC              Name          Current switch  Role          Auth  AP name          Roaming  Essid         Bssid
Phy  Profile       Type  User Type

----------  -------------  ------  --------------  ----  ----  --------  --------  -----  -----  ---  ----
---  ----  ---------

10.1.20.101  7c:7a:91:46:52:b7  7c7a914652b7  10.1.10.11  authenticated  MAC  94:b4:0f:c1:3f:e0  Wireless  lab1-
mac  94:b4:0f:93:fe:00  a-VHT  lab1-mac-aaa  Win 8  WIRELESS
```

第3步: 在 Clearpass (https://10.0.50.41)的访问追踪器里查看是否有用户送上来的 MAC 地址，是否击中了正确的策略名称，是否被 Accept 了。



NOTE 可在过滤器(username)中过滤自己的 MAC 地址，便于查询结果。

10 802.1X 认证

10.1 用户需求

客户希望采用更安全的认证和加密方式来连接无线网，指定802.1x的认证服务在Clearpass上完成。

10.2 实现思路

先配置 aaa profile（规定认证规则，认证服务器及初始角色），wlan ssid-profile（规定 SSID 名称）,然后将 aaa profile 和 wlan ssid-profile 组合形成一个 VAP（规定虚拟 AP 名称和默认用户 VLAN），然后将 VAP 和 AP-Group 进行捆绑，这样该 AP-Group 下的 AP 即可放出指定信号。在认证服务器上（示例为 clearpass），我们也需要对应的配置可供 1x 认证的账号，以及 1x 的认证策略。

10.3 MM 配置（CLI）

第1步: 使用 SSH 方式登录到 Mobility Master (10.X.50.11)，在 Mobility Master（MM）上进入 /md/labX 配置节点，并进入配置模式 <- 这里的 X 代表 lab 分组[1…6]

```
(LabX-MM-1) [mynode] #cd /md/labX    <- X[1…6]
(LabX-MM-1) [labX] #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(LabX-MM-1) [labX] (config) #
```

第2步: 在第 9.3 章节中的第 3，第 4 步骤中，我们已经添加了一个 radius 服务器组 “labX-sg”，本章节将调用这个认证服务器。

第3步: 增加一个新的 aaa profile “labX-1x-aaa”

```
(LabX-MM-1) ^[labX] (config) #aaa profile labX-1x-aaa    <- X[1…6]
(LabX-MM-1) ^[labX] (AAA Profile "lab1-1x-aaa") #dot1x-default-role authenticated
(LabX-MM-1) ^[labX] (AAA Profile "lab1-1x-aaa") #authentication-dot1x default
(LabX-MM-1) ^[labX] (AAA Profile "lab1-1x-aaa") #dot1x-server-group labX-sg    <- X[1…6]
(LabX-MM-1) ^[labX] (AAA Profile "lab1-1x-aaa") #radius-accounting labX-sg    <- X[1…6]
(LabX-MM-1) ^[labX] (AAA Profile "lab1-1x-aaa") #!
```

第4步：增加一个新的 ssid profile “labX-1x-ssid”

```
(LabX-MM-1) ^[labX] (config) #wlan ssid-profile labX-1x-ssid    <- X[1…6]
(LabX-MM-1) ^[labX] (SSID Profile "lab1-1x-ssid") #essid labX-1x    <- X[1…6]
(LabX-MM-1) ^[labX] (SSID Profile "lab1-1x-ssid") #opmode wpa2-aes
(LabX-MM-1) ^[labX] (SSID Profile "lab1-1x-ssid") #!
```

第5步：组合一个 VAP “labX-1x-vap”

```
(LabX-MM-1) ^[labX] (config) #wlan virtual-ap labX-1x-vap    <- X[1…6]
(LabX-MM-1) ^[labX] (Virtual AP profile "lab1-1x-vap") #aaa-profile labX-1x-aaa    <-X[1…6]
(LabX-MM-1) ^[labX] (Virtual AP profile "lab1-1x-vap") #ssid-profile labX-1x-ssid    <-X[1…6]
(LabX-MM-1) ^[labX] (Virtual AP profile "lab1-1x-vap") #vlan X20    <- X[1…6]
(LabX-MM-1) ^[labX] (Virtual AP profile "lab1-1x-vap") #!
```

第6步：将 VAP 在 AP-GROUP 中调用，保存，放出信号来

```
(LabX-MM-1) [labX] (config) #ap-group labX-group    <- X[1…6]
(LabX-MM-1) [labX] (AP group "lab1-group") #virtual-ap labX -1x-vap    <- X[1…6]
(LabX-MM-1) ^[labX] (AP group "lab1-group") #write m
```

第7步：查看完成还未提交的配置内容

```
(LabX-MM-1) ^[labX] (config) #show configuration pending
```

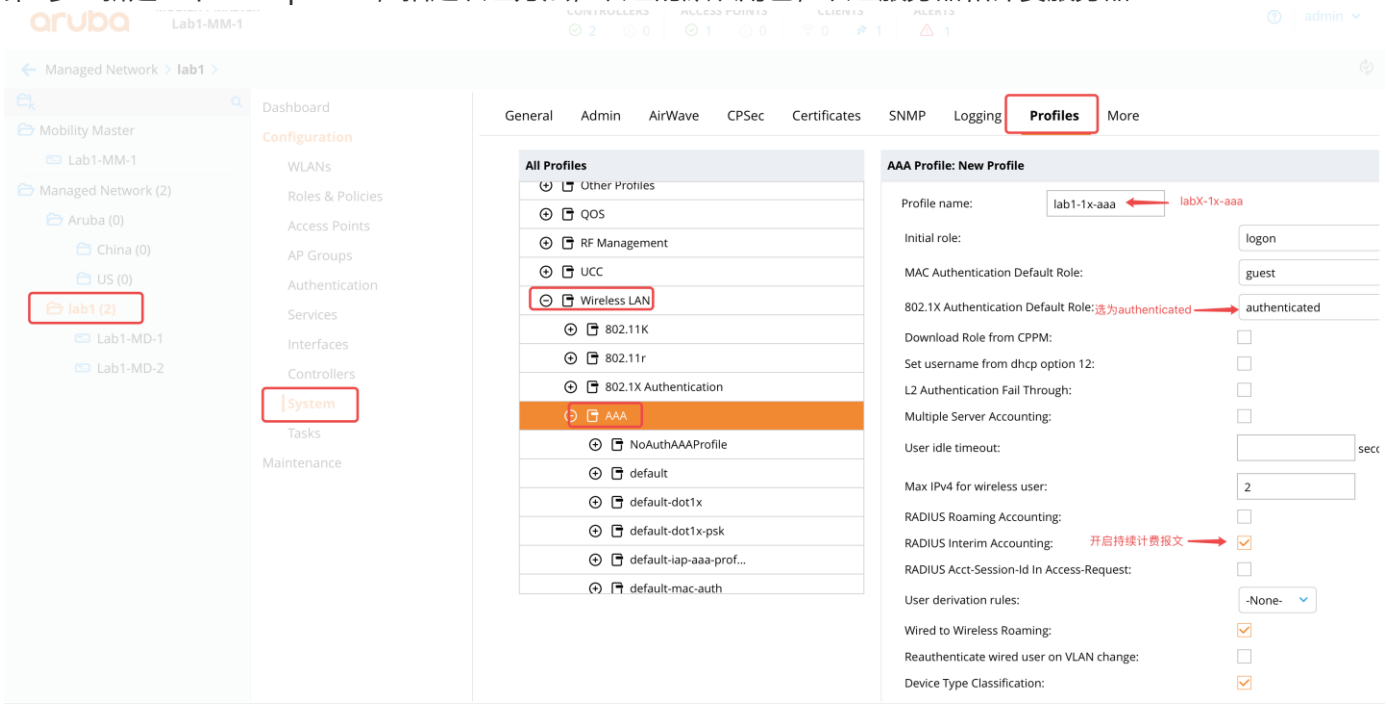
第8步：保存配置

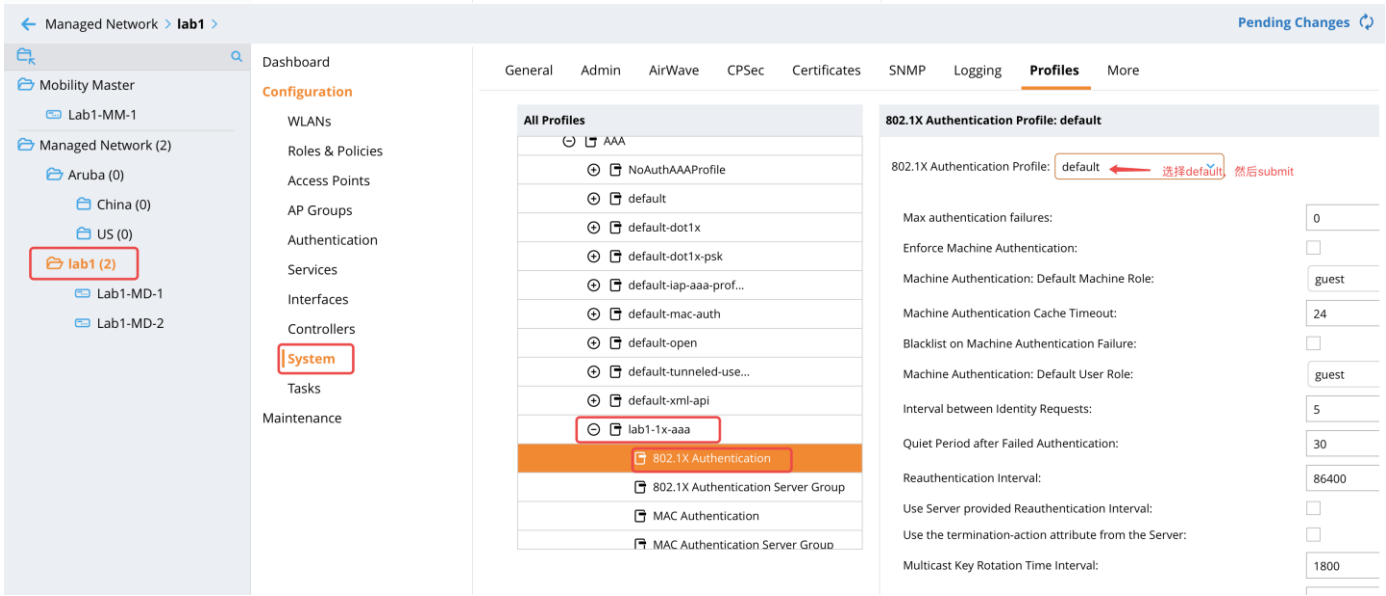
```
(LabX-MM-1) ^[labX] (config) #write memory
Saving Configuration...
Configuration Saved.
```

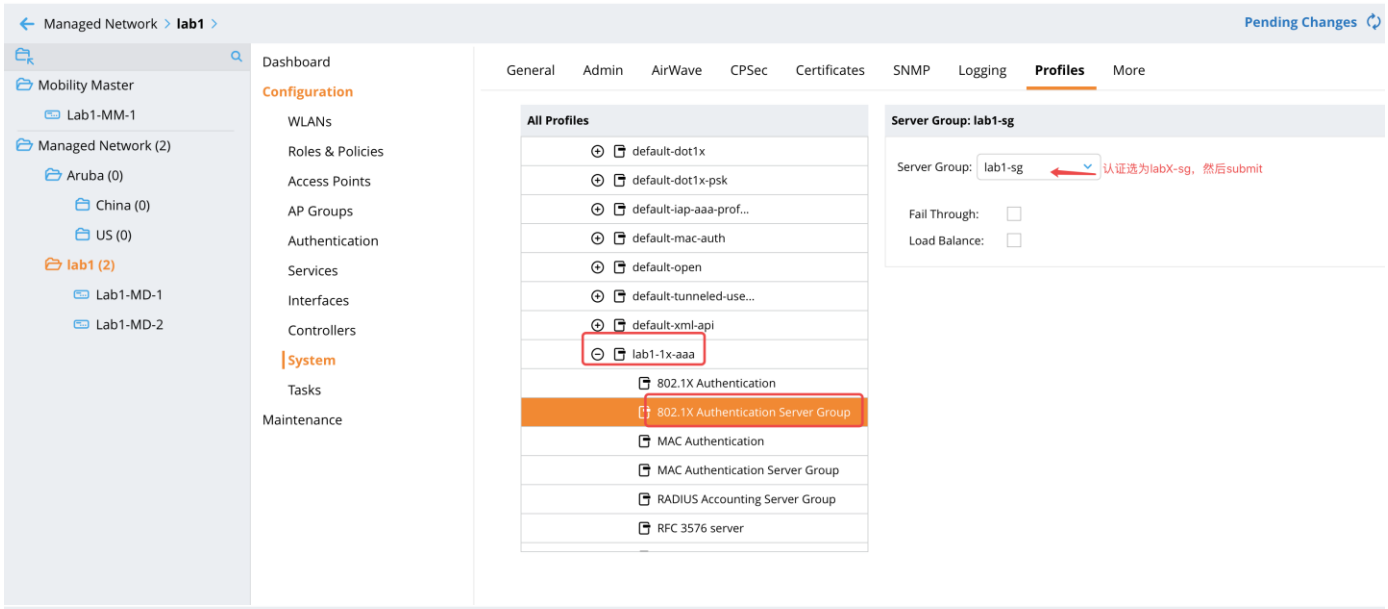
10.4 MM 配置（GUI）

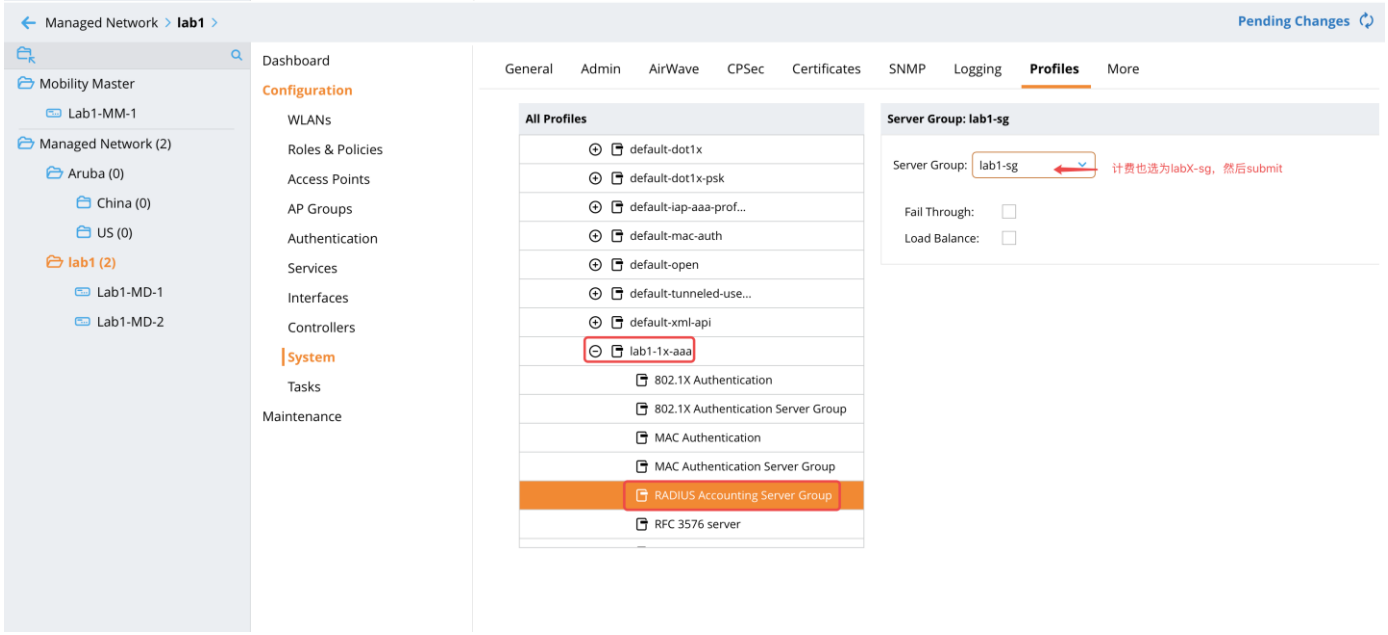
第1步：本章节相应的 ClearPass 配置在前两页文件中已经完成描述，如果您想使用 GUI 配置 1x 认证，也请先按前述 Clearpass 配置完成对应配置，再进入 MM 上的配置。另外本节不赘述 server group 配置，请参考前一章节 MAC 认证内配置的 radius 服务器组 “labX-sg”配置，

第2步：新建一个 AAA profile，指定认证方法，认证的默认角色，认证服务器和计费服务器

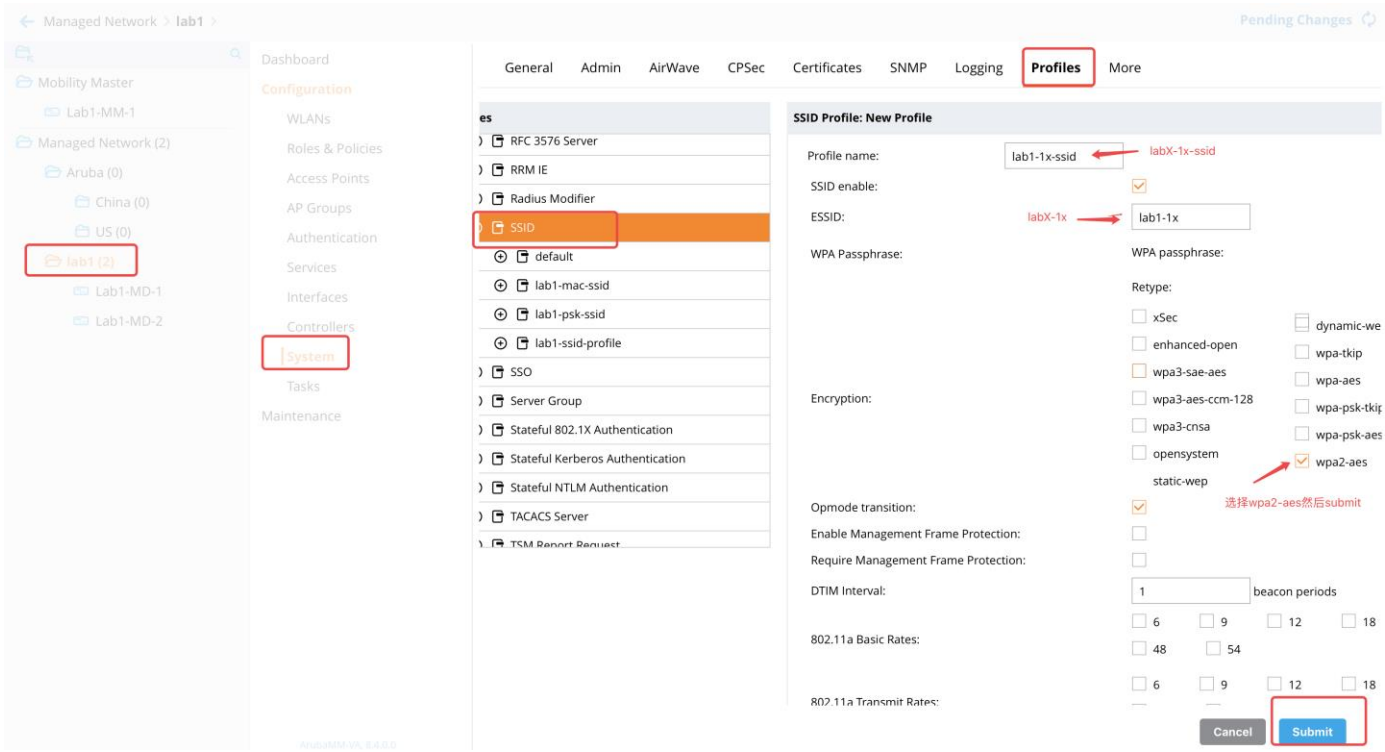




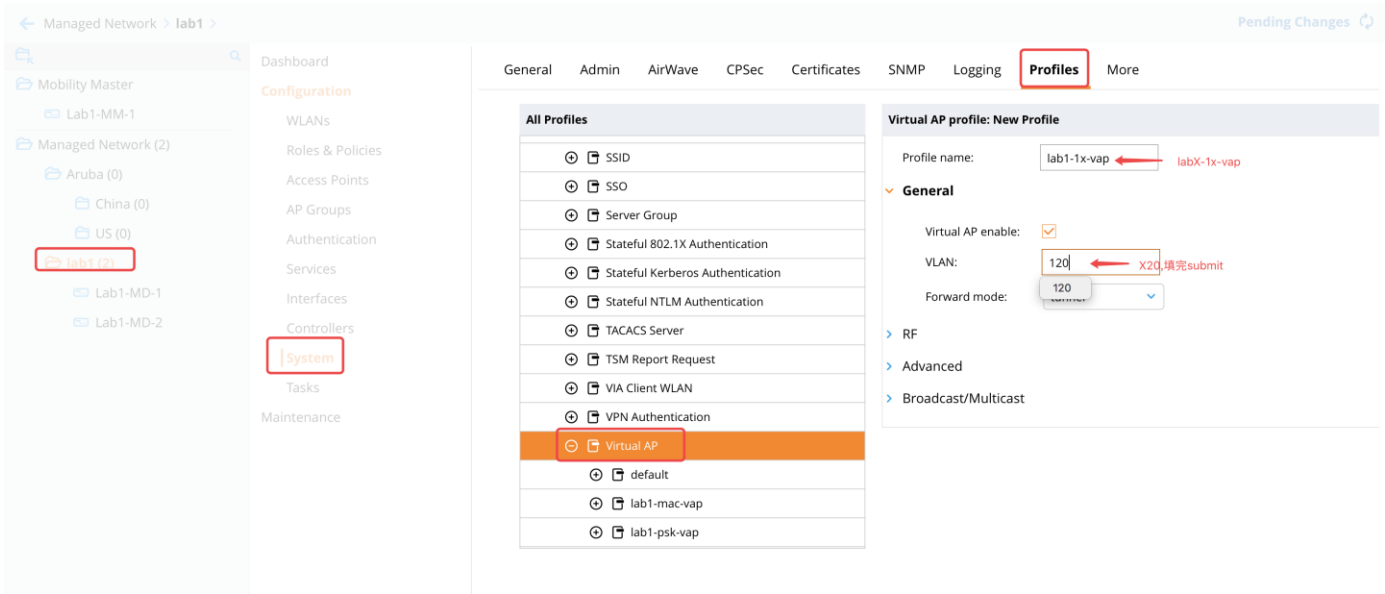


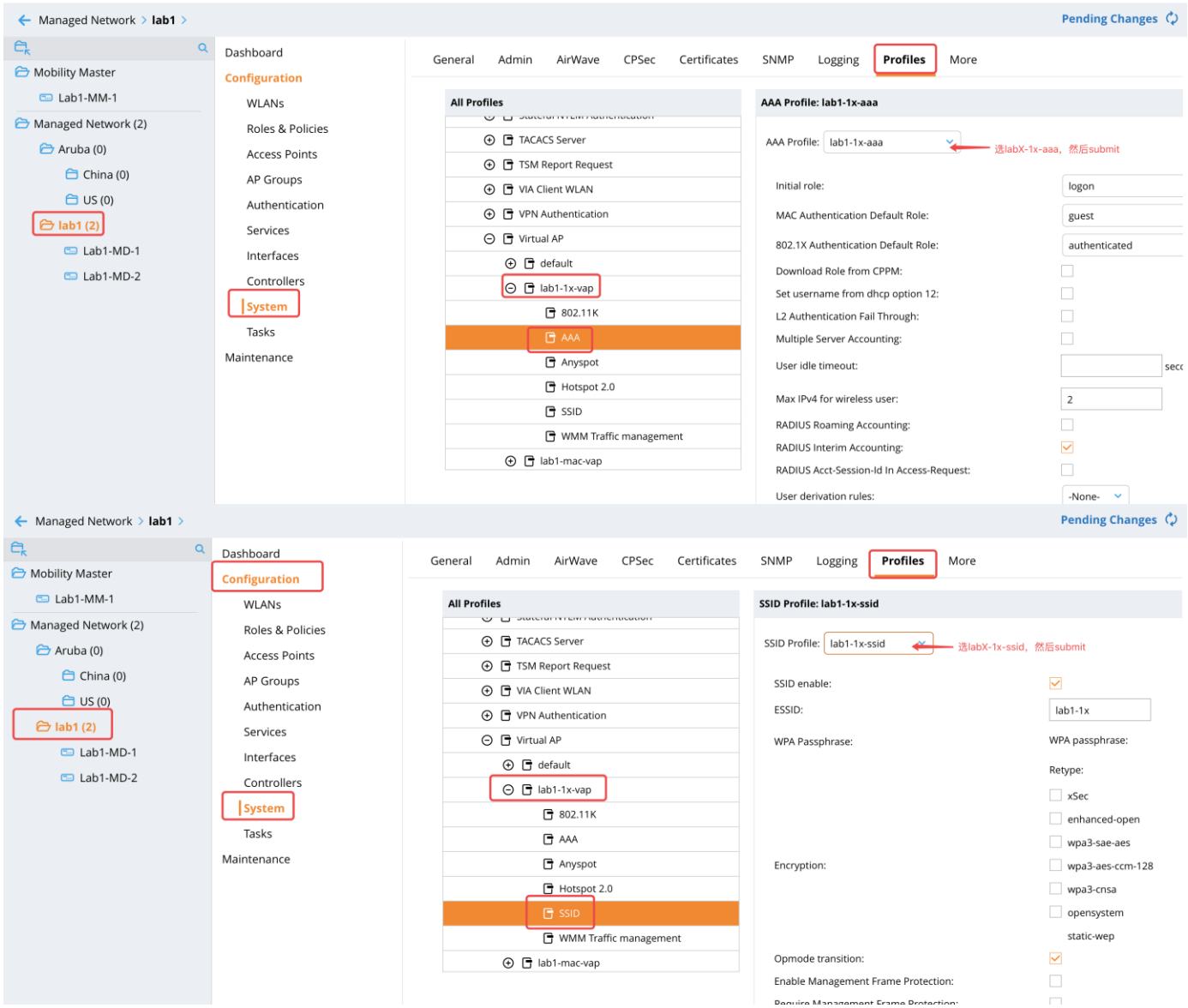


第3步：新建一个 SSID profile，指定 SSID 名称和认证加密方式

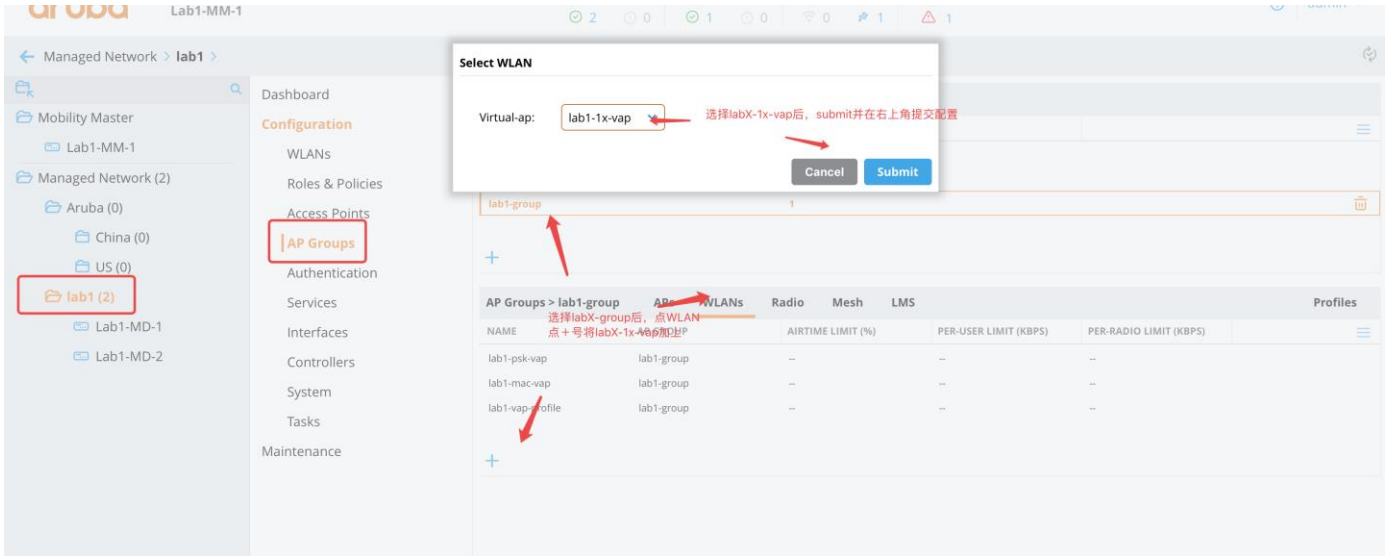


第4步：组合出一个 VAP，添加刚刚的 AAA profile 和 SSID profile，选择 VLAN



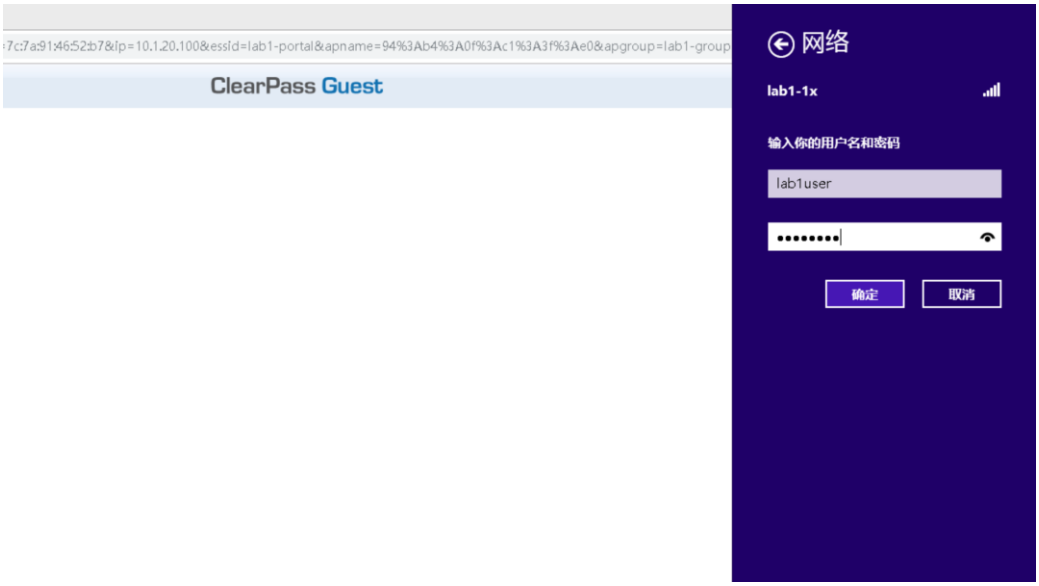


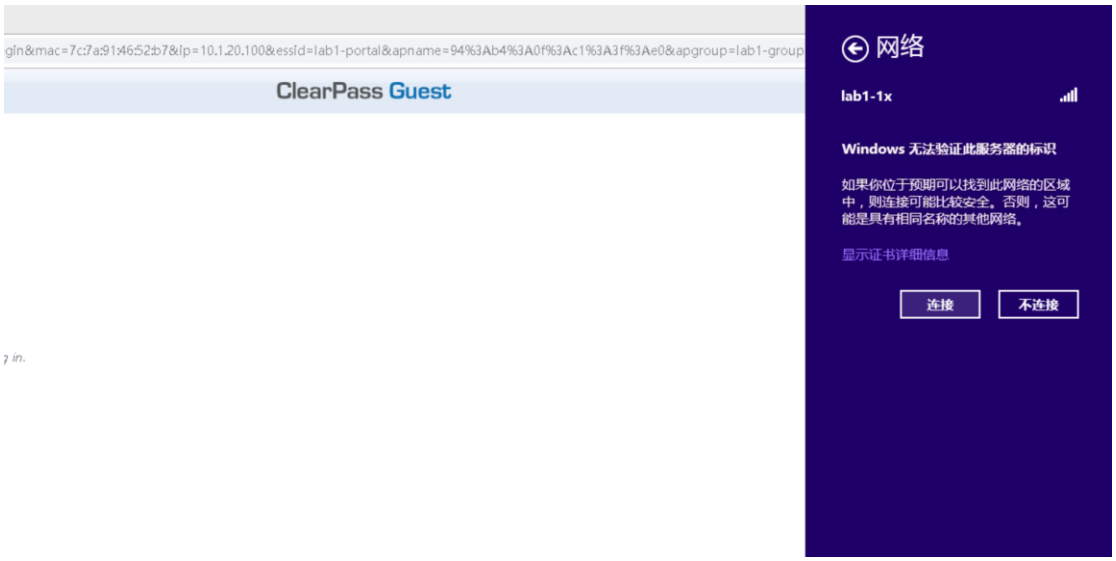
第5步：在现有的 AP-GROUP labX-group 下，调用上述 VAP，放出信号后，可以开始测试。

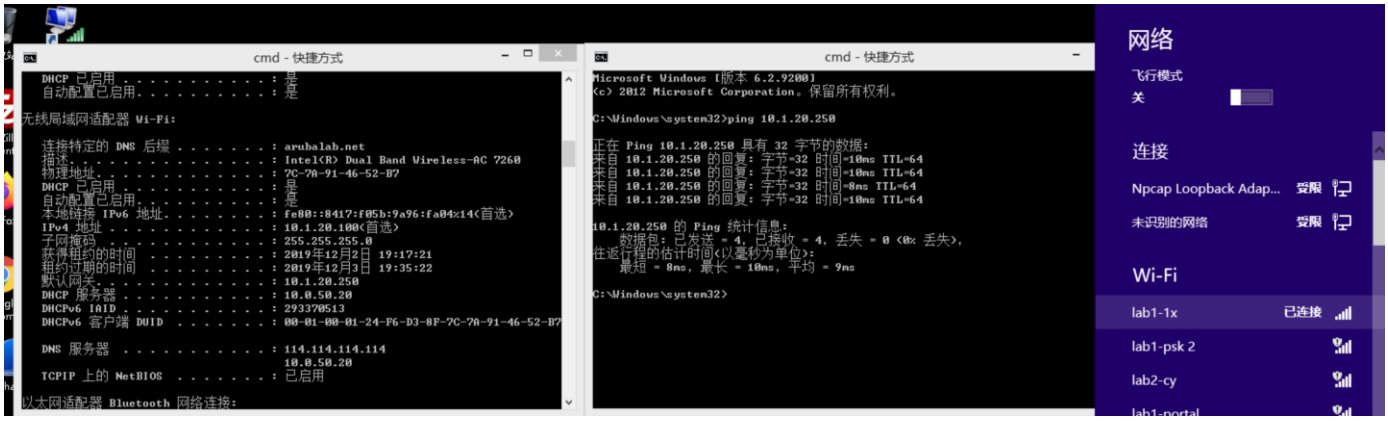


10.5 验证结果

第1步：我们先将 LabX 的无线终端连接到 labX-1x，然后分别 Window 桌面，控制器，以及 clearpass 来确定是否正常。在 windows 中连接 labX-1x，弹出对话框输入 labXuser,密码也是 labXuser，确定后，弹出证书的对话框，选择连接。



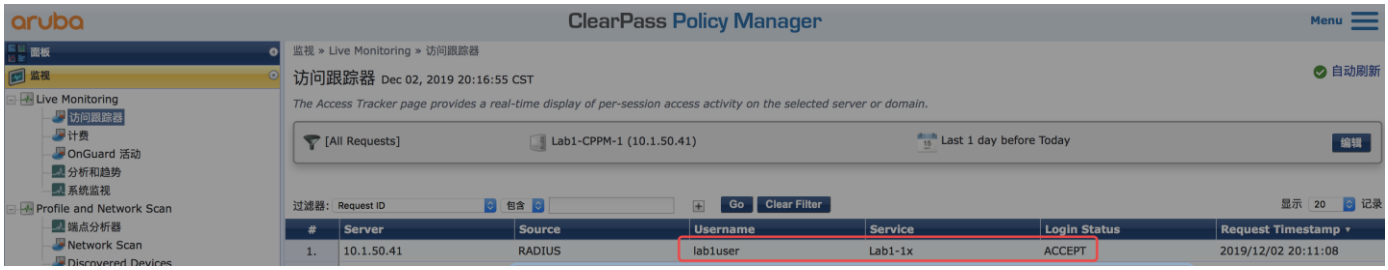

gln&mac=7c:7a:91:46:52:b7&ip=10.1.20.100&essid=lab1-portal&apname=94%3Ab4%3A0f%3Ac1%3A3f%3Ae0&apgroup=lab1-group
ClearPass Guest
网络
lab1-1x
Windows 无法验证此服务器的标识
如果你位于预期可以找到此网络的区域中，则连接可能比较安全。否则，这可能是具有相同名称的其他网络。
显示证书详细信息
连接
不连接


cmd - 快捷方式
DHCP 已启用 . . . . . : 是
自动配置已启用. . . . . : 是
无线局域网适配器 Wi-Fi:
连接特定的 DNS 后缀 . . . . . : arubalab.net
描述. . . . . : Intel(R) Dual Band Wireless-AC 7260
物理地址. . . . . : 7C-7A-91-46-52-B7
DHCP 已启用 . . . . . : 是
自动配置已启用. . . . . : 是
本地链接 IPv6 地址. . . . . : fe80::8417:f05b:9a96:fa04x14(首选)
IPv4 地址 . . . . . : 10.1.20.100(首选)
子网掩码 . . . . . : 255.255.255.0
获得租约的时间 . . . . . : 2019年12月2日 19:17:21
租约过期的时间 . . . . . : 2019年12月3日 19:35:22
默认网关. . . . . : 10.1.20.250
DHCP 服务器 . . . . . : 10.0.50.20
DHCPv6 IAID . . . . . : 293370513
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-24-F6-D3-8F-7C-7A-91-46-52-B7
DNS 服务器 . . . . . : 114.114.114.114
10.0.50.20
TCPIP 上的 NetBIOS . . . . . : 已启用
以太网适配器 Bluetooth 网络连接:
cmd - 快捷方式
Microsoft Windows [版本 6.2.9200]
(c) 2012 Microsoft Corporation。保留所有权利。
C:\Windows\system32>ping 10.1.20.250
正在 Ping 10.1.20.250 具有 32 字节的数据:
来自 10.1.20.250 的回复: 字节=32 时间=10ms TTL=64
来自 10.1.20.250 的回复: 字节=32 时间=10ms TTL=64
来自 10.1.20.250 的回复: 字节=32 时间=8ms TTL=64
来自 10.1.20.250 的回复: 字节=32 时间=10ms TTL=64
10.1.20.250 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 8ms, 最长 = 10ms, 平均 = 9ms
C:\Windows\system32>
网络
飞行模式
关
连接
Npcap Loopback Adap...
受限
未识别的网络
受限
Wi-Fi
lab1-1x
已连接
lab1-psk 2
lab2-cy

第2步: 在 MM 上确认用户是否正常在线。

```
(LabX-MM-1) [mm] #show global-user-table list


Global Users

------------

   IP          MAC           Name     Current switch  Role         Auth    AP name          Roaming   Essid        Bssid
Phy    Profile      Type   User Type

----------  ------------      ------   --------------  ----         ----    --------         --------  -----        -----           ---    ------
-      ----   ---------

10.1.20.100  7c:7a:91:46:52:b7  lab1user   10.1.10.11     authenticated  802.1x  94:b4:0f:c1:3f:e0  Wireless  lab1-1x
    94:b4:0f:93:fe:13  a-VHT  lab1-1x-aaa  Win 8  WIRELESS
```

第3步: 在 Clearpass(https://10.0.50.41)的访问追踪器里查看是否有用户送上来的 1x 认证，是否击中了正确的策略名称，是否被 Accept 了。



NOTE 可在过滤器 username 中过滤查询，便于查看结果。

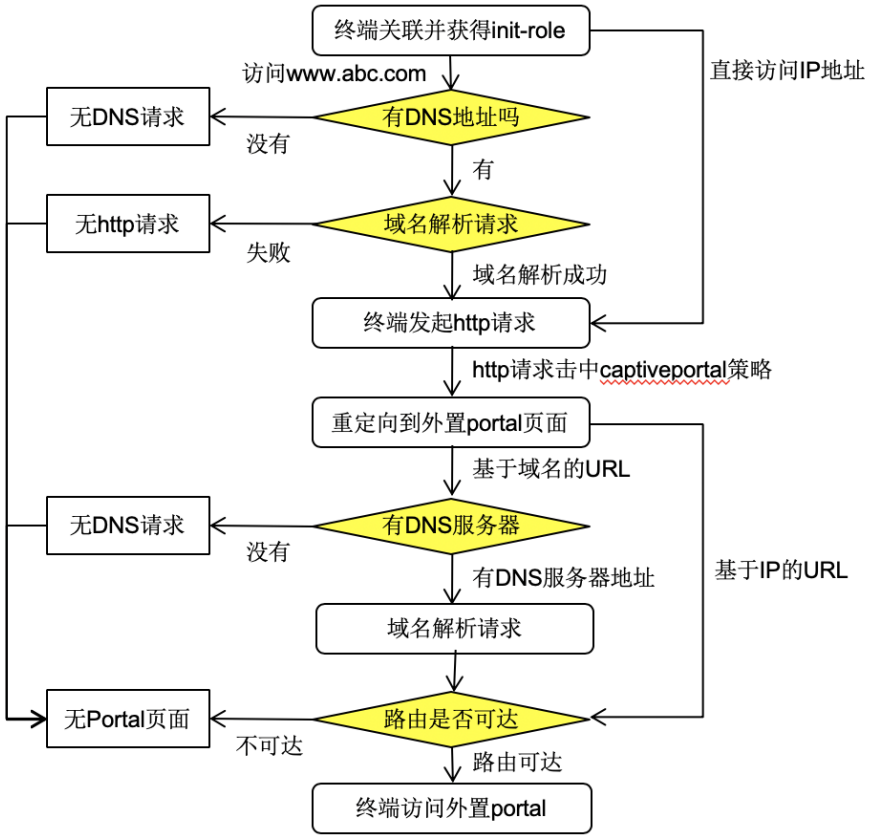
11 外置 PORTAL 认证

11.1 用户需求

通过AC实现重定向到外置Portal Server做Open SSID下的Portal认证。

11.2 实现思路

✓ Aruba Portal认证流程



11.3 MM 配置（CLI）

第1步: 登录到/md/labX 节点（<- 这里的 X 代表 lab 分组[1…6]）

```
(LabX-MM-1) [mynode] #cd /md/labX     <- X[1…6]
(LabX-MM-1) [labX] #configure terminal
(LabX-MM-1) [labX] (config) #  确保在 MD 或者 LabX 层级下进行以下配置！！！
```

第2步：开启控制器防火墙 DNAT 功能

```
(LabX-MM-1) [labX] (config) #firewall
(LabX-MM-1) [labX] (config-submode) #allow-tri-session
(LabX-MM-1) [labX] (config-submode)#write memory
(LabX-MM-1) [labX] (config-submode)#!
```

第3步：在第 9.3 章节中的第 3，第 4 步骤中，我们已经添加了一个 radius 服务器组 “labX-sg”，本章节将调用这个认证服务器。

第4步：配置 L3 Authentication 并关联认证组

```
(LabX-MM-1) [labX] (config) #aaa authentication captive-portal labX-cap    <- X[1…6]
(LabX-MM-1) ^[labX] (Captive Portal Authentication Profile "lab1-cap") #login-page http://10.0.50.41/guest/login.php        <- [1-6 组一样]//定义外置 Portal URL
(LabX-MM-1) ^[labX] (Captive Portal Authentication Profile "lab1-cap") #default-role authenticated
(LabX-MM-1) ^[labX] (Captive Portal Authentication Profile "lab1-cap") #logon-wait minimum-delay 1
(LabX-MM-1) ^[labX] (Captive Portal Authentication Profile "lab1-cap") #logon-wait maximum-delay 1
(LabX-MM-1) ^[labX] (Captive Portal Authentication Profile "lab1-cap") #no welcome-page   //关闭认证成功后的欢迎页面
(LabX-MM-1) ^[labX] (Captive Portal Authentication Profile  “lab1-cap") #server-group labX-sg   <-X[1…6] //关联认证组
(LabX-MM-1) ^[labX] (Captive Portal Authentication Profile  “lab1-cap") #write memory
(LabX-MM-1) [labX] (Captive Portal Authentication Profile  “lab1-cap") #!
```

第5步：定义外置服务器别名

```
(LabX-MM-1) [labX] (config) #netdestination portal-srv
(LabX-MM-1) ^[labX] (config-submode)#host 10.0.50.41
(LabX-MM-1) ^[labX] (config-submode)#!
```

第6步：定义外置 Portal 服务器访问策略

```
(LabX-MM-1) ^[labX] (config) #ip access-list session labX-portal-acl    <- X[1…6]
(LabX-MM-1) ^[labX] (config-submode)#user alias portal-srv svc-http permit   //放行 http
(LabX-MM-1) ^[labX] (config-submode)#user alias portal-srv svc-https permit  //放行 https
(LabX-MM-1) ^[labX] (config-submode)#!
```

第7步: 定义初始 initial role，需要允许访问 Portal 服务器

```
(LabX-MM-1) ^[labX] (config) #user-role labX-portal-logon    <- X[1…6]
(LabX-MM-1) ^[labX] (config-submode)#captive-portal labX-cap <- X[1…6]//关联 Portal 认证文件
(LabX-MM-1) ^[labX] (config-submode)#access-list session logon-control   //调用默认 logon-control
(LabX-MM-1) ^[labX] (config-submode)#access-list session labX-portal-acl <- X[1…6]//放行 Portal 服务器
(LabX-MM-1) ^[labX] (config-submode)#access-list session captiveportal   //调用默认弹 Portal 策略
(LabX-MM-1) ^[labX] (config-submode)#!
```

第8步: 配置 AAA 认证

```
(LabX-MM-1) [labX] (config) #aaa profile labX-portal-aaa    <- X[1…6]
(LabX-MM-1) ^[labX] (AAA Profile   “lab1-portal-aaa") #initial-role labX-portal-logon <-X[1~6]
(LabX-MM-1) ^[labX] (AAA Profile   “lab1-portal-aaa") #!
```

第9步: 配置 SSID

```
(LabX-MM-1) [labX] (config) #wlan ssid-profile labX-portal-ssid    <- X[1…6]
(LabX-MM-1) ^[labX] (SSID Profile   “lab1-portal-ssid") #essid labX-portal    <- X[1…6]
(LabX-MM-1) [labX] (SSID Profile   “lab1-portal-ssid") #!
```

第10步:配置 Virtual AP

```
(LabX-MM-1) [labX] (config) #wlan  virtual-ap labX-portal-vap    <- X[1…6]
(LabX-MM-1) ^[labX] (Virtual AP profile   “lab1-portal-vap") #aaa-profile labX-portal-aaa <-X[1~6]
(LabX-MM-1) ^[labX] (Virtual AP profile   “lab1-portal-vap") #ssid-profile labX-portal-ssid
(LabX-MM-1) ^[labX] (Virtual AP profile   “lab1-portal-vap ") #vlan X20    <- X[1…6]
(LabX-MM-1) ^[labX] (Virtual AP profile   “lab1-portal-vap ") #!
```

第11步:将 VAP 在 AP-GROUP 中调用。

```
(LabX-MM-1) [labX] (config) #ap-group labX-group    <- X[1…6]
(LabX-MM-1) [labX] (AP group   “lab1-group") #virtual-ap labX-portal-vap    <- X[1…6]
```

第12步:查看完成还未提交的配置内容

```
(LabX-MM-1) ^[labX] (config) #show configuration pending
```

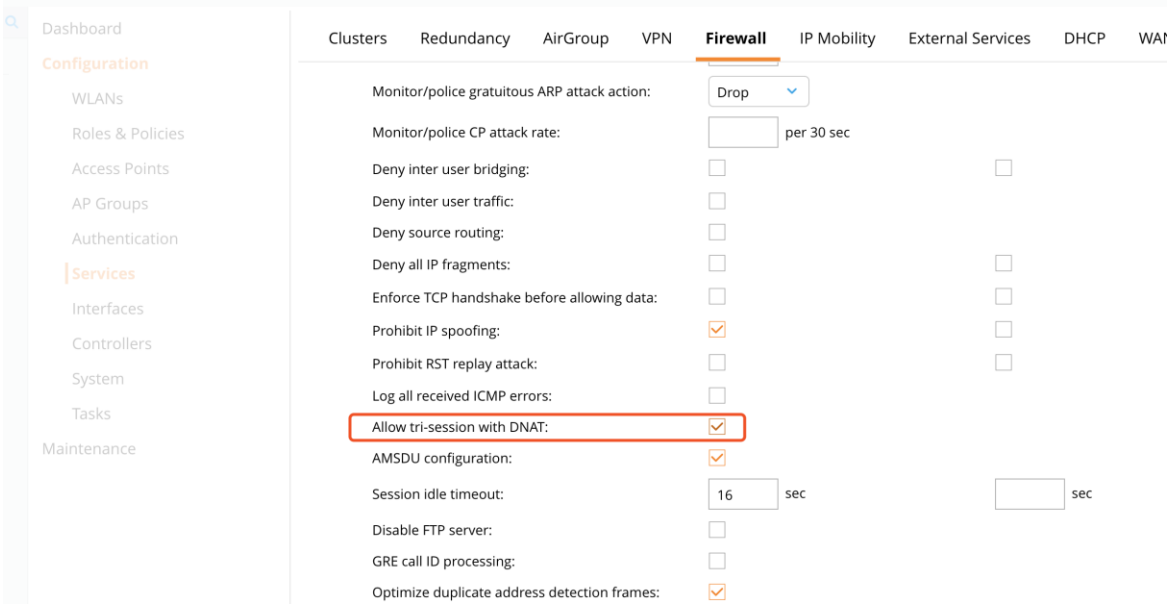
第13步:保存配置

```
(LabX-MM-1) ^[labX] (config) #write memory

Saving Configuration...

Configuration Saved.
```

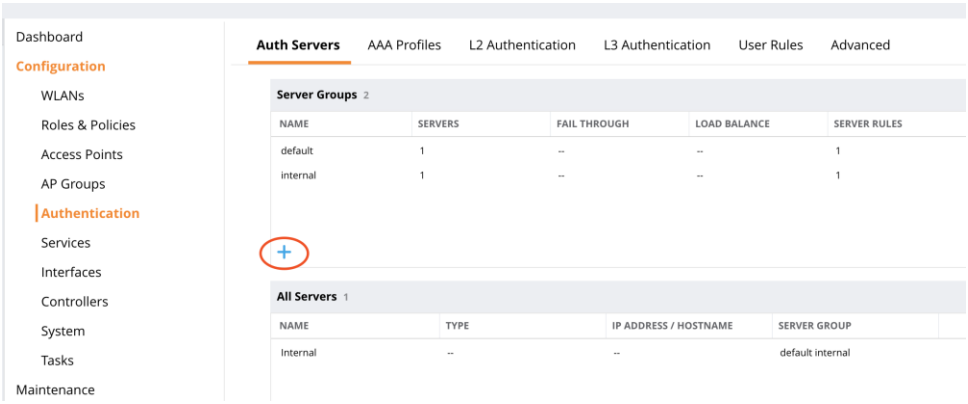
11.4 MM 配置（GUI）

第1步: 登录到 MM 的 Web UI: https://10.X.50.11 （X[1…6]）

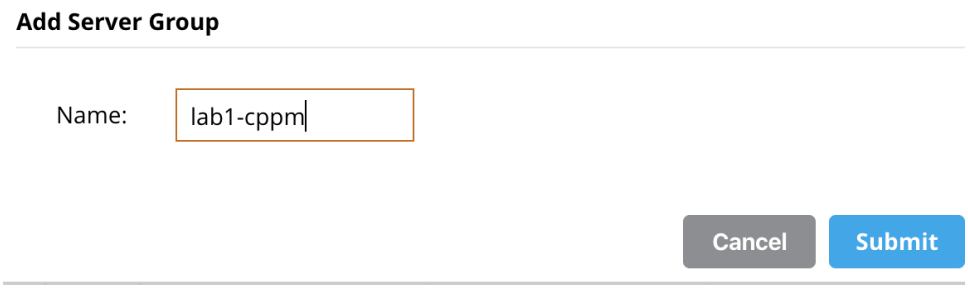
第2步: 开启控制器防火墙 DNAT 功能。Mobility Network- >LabX- >Services- >Firewall- >Allow tri-session with DNAT



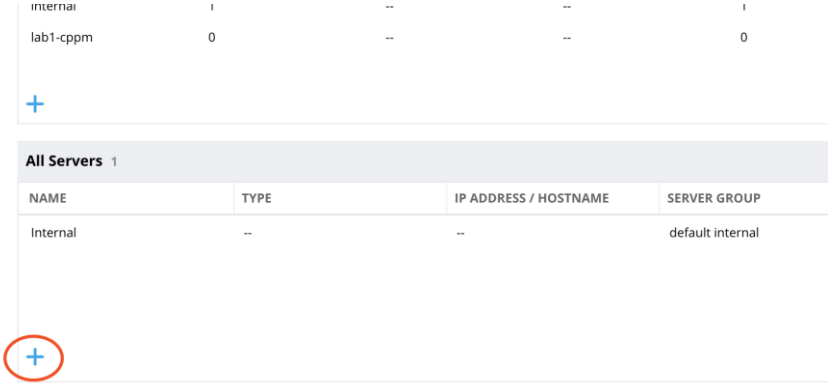
第3步: 创建认证服务器。Mobility Network- >LabX- > Configuration -> Authentication -> Auth Servers

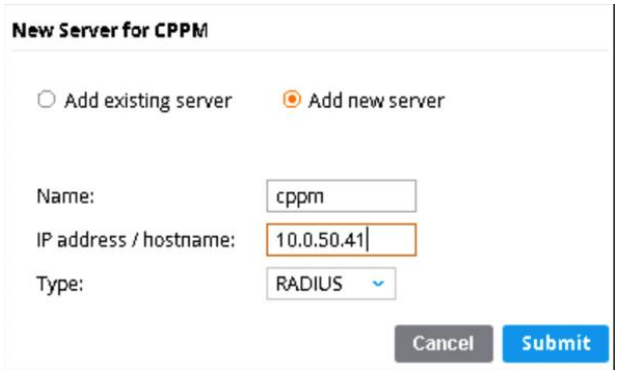


第4步：添加 Server Group

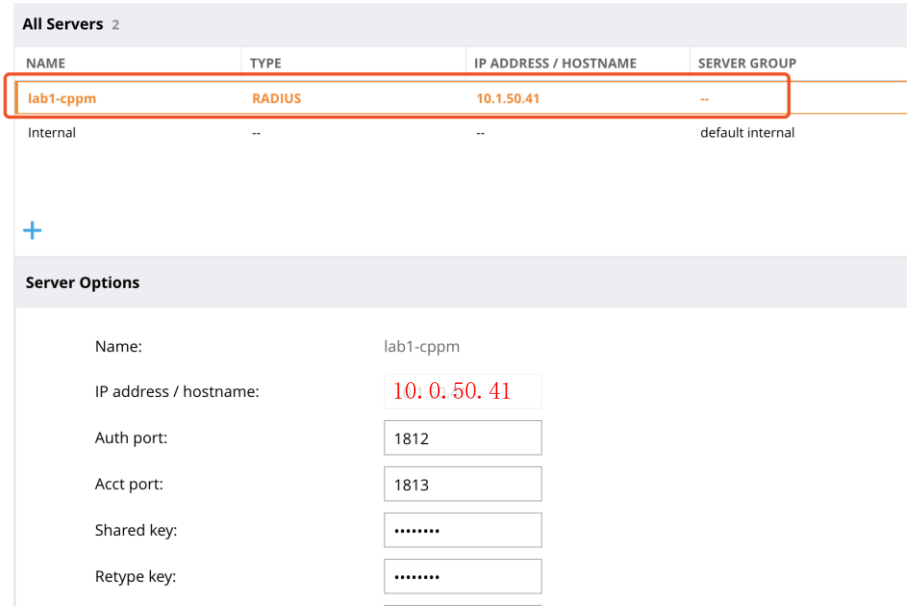


第5步：添加 Server



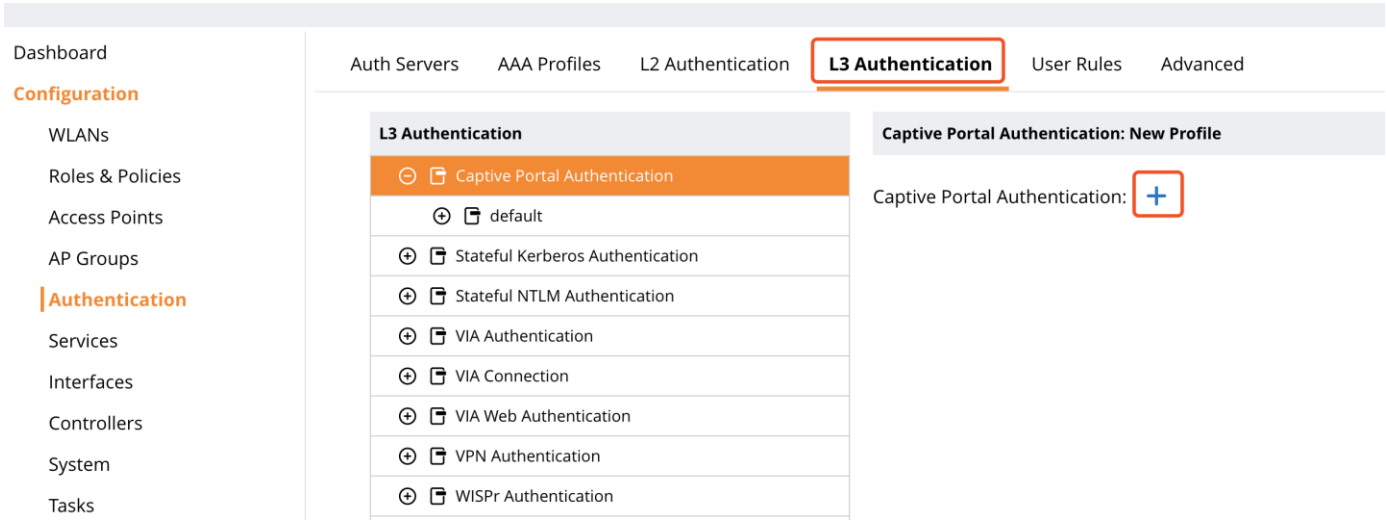


第6步：点击 server 名称，配置详细信息。Key 必须与认证服务器一致，本 lab 所有 key 采用 aruba123

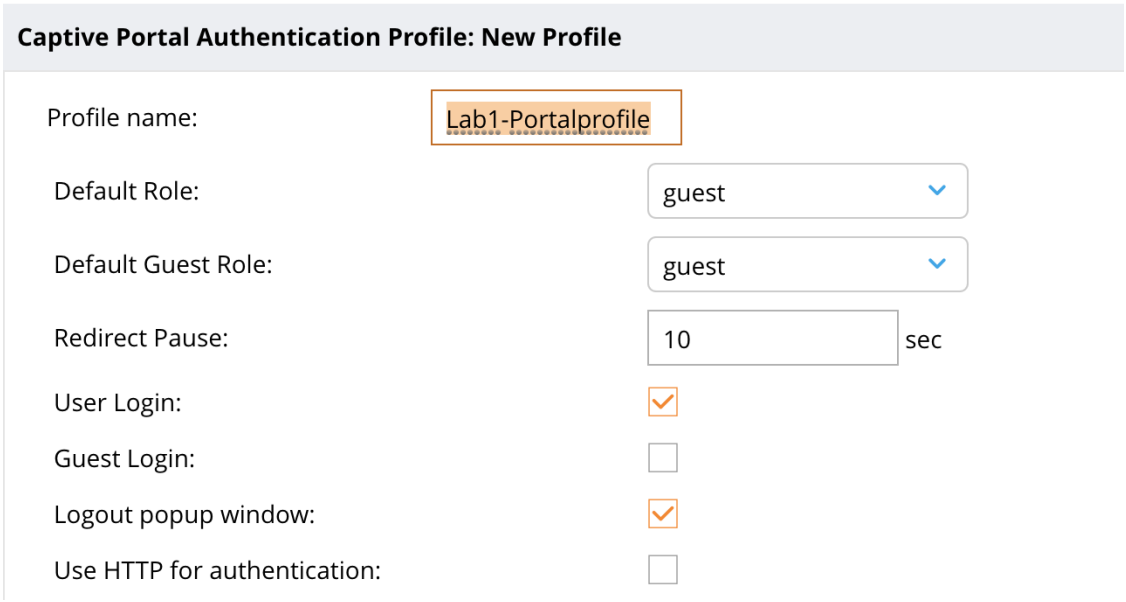


第7步：配置 L3 Authentication：添加 Captive Portal Authentication Profile 。Mobility Network- >LabX- > Configuration -> Authentication ->L3 Authentication，点击“Captive Portal Authentication”，

1) 点击”+”新增 Profile，如下图所示



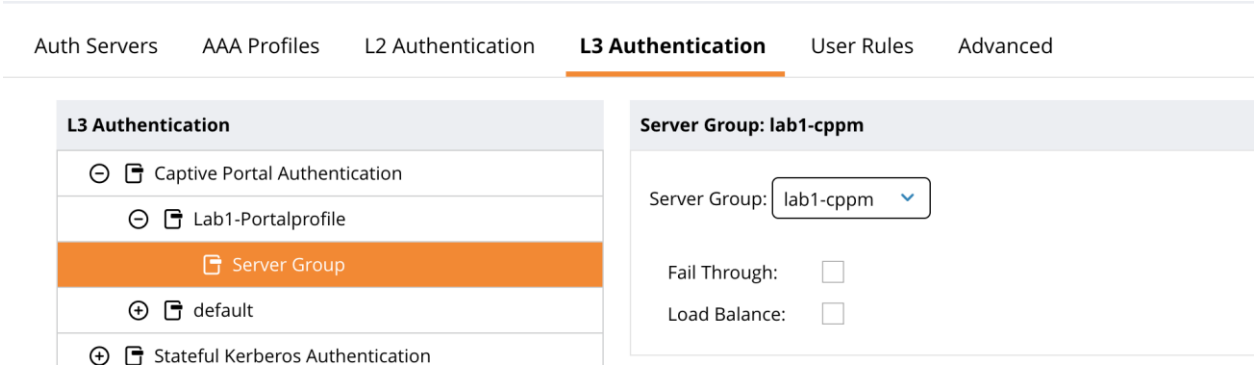
2) 填写 Captive Portal Authentication Profile 名称



3) 填写 Login page 地址，也就是用户终端弹出的 Portal 页面地址。请填写各自外置 Portal 的页面地址。本手册采用 Lab 环境中 Clearpass 访客页面。（默认是控制器内置 Portal 页面地址）点击 “Submit”提交配置。

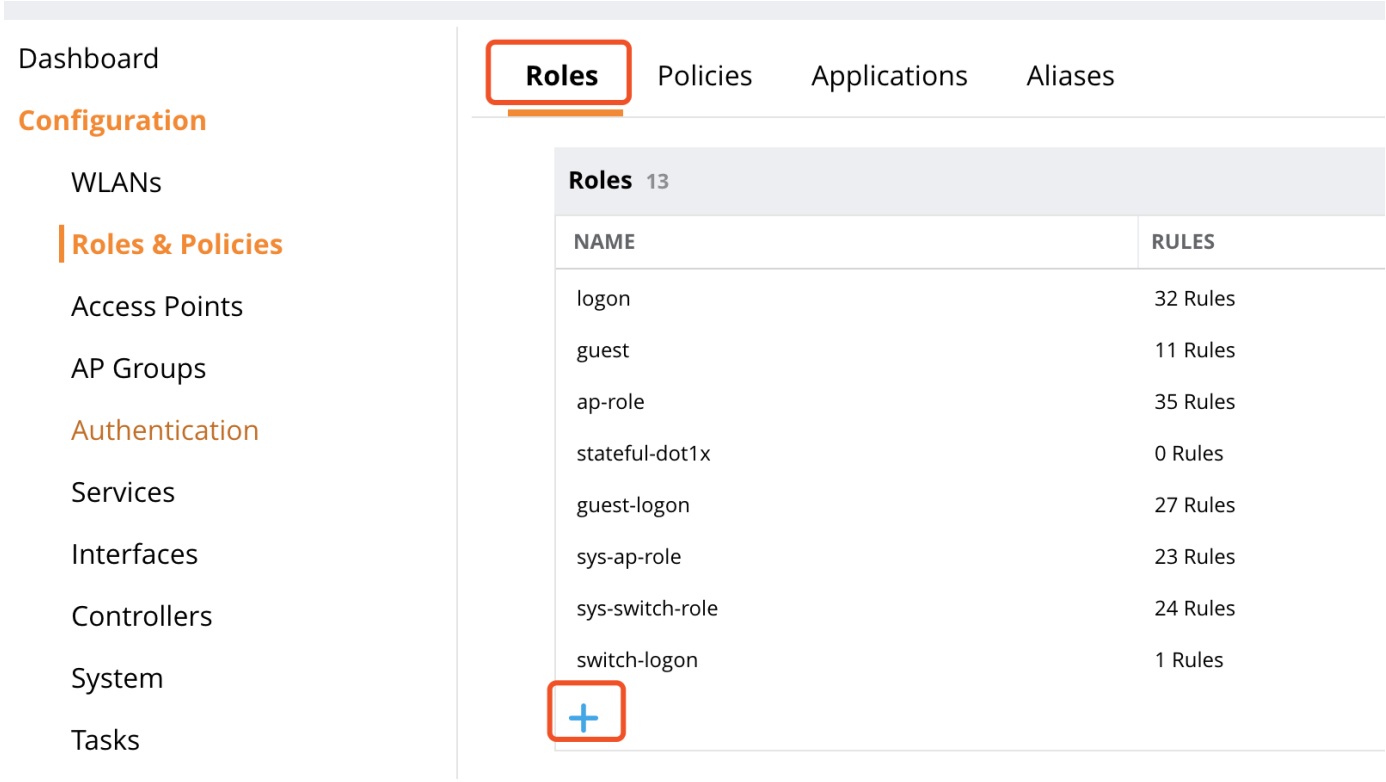
Tips：Welcome Page 页面是认证成功后的欢迎页面，根据实际需求填写，本例关闭 welcome page

4) 关联认证服务器

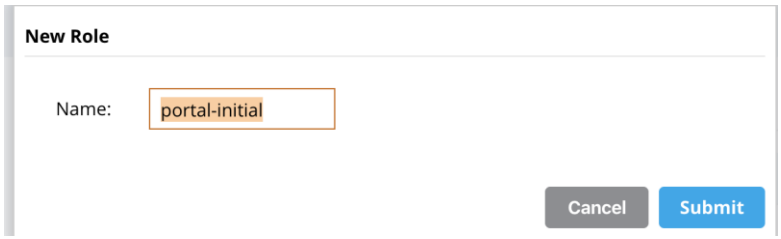


第8步：配置 Role：创建用于弹 portal 的初始角色(initial-role)及相关权限。Mobility Network- >LabX- > Configuration -> Roles & Policies，点击“Roles”，

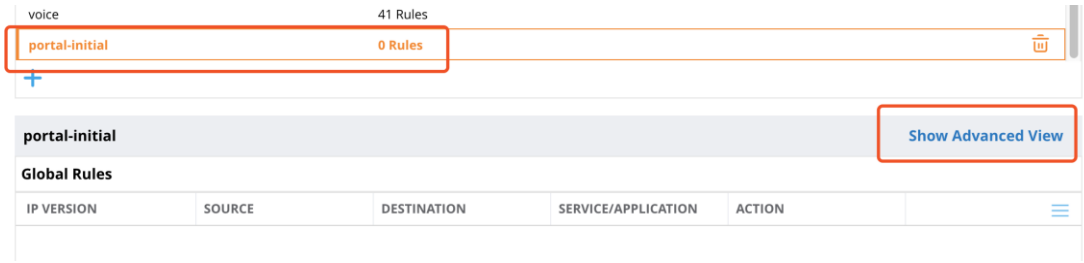
1) 点击”+”新增 role，如下图所示



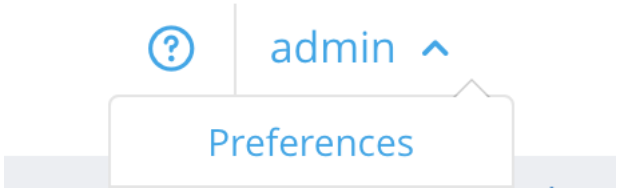
2) 新建 initial role 名称

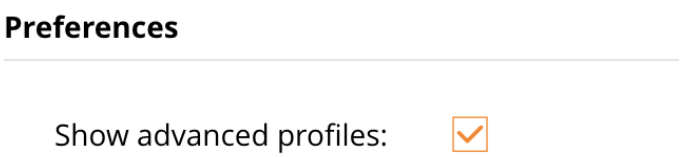


3) 点击新建的 Portal initial role（labX-portal-guest-logon），选择高级视图 Show Advanced View

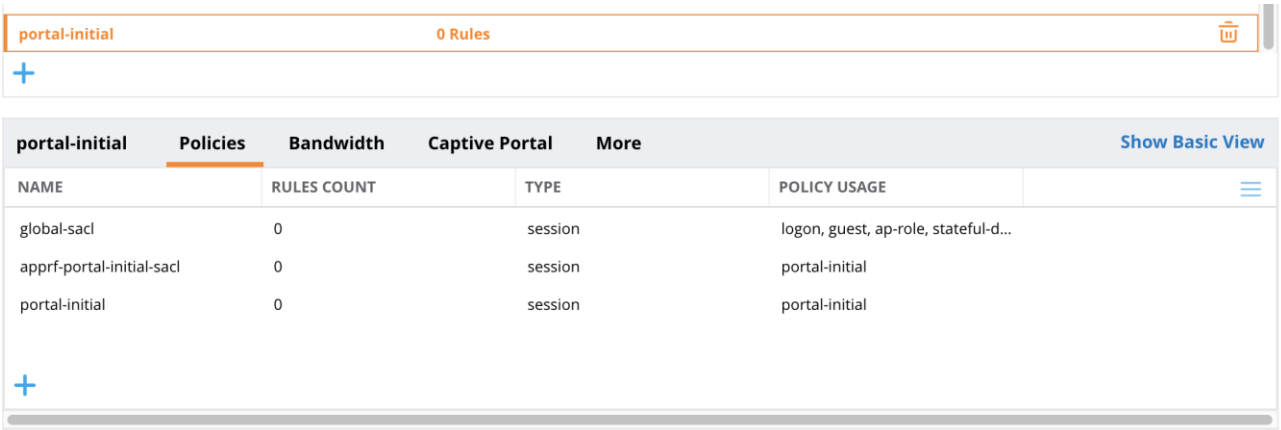


Tips：如果没有 Show Advanced View，请点击右上角 admin>Preferences 打开高级 profile

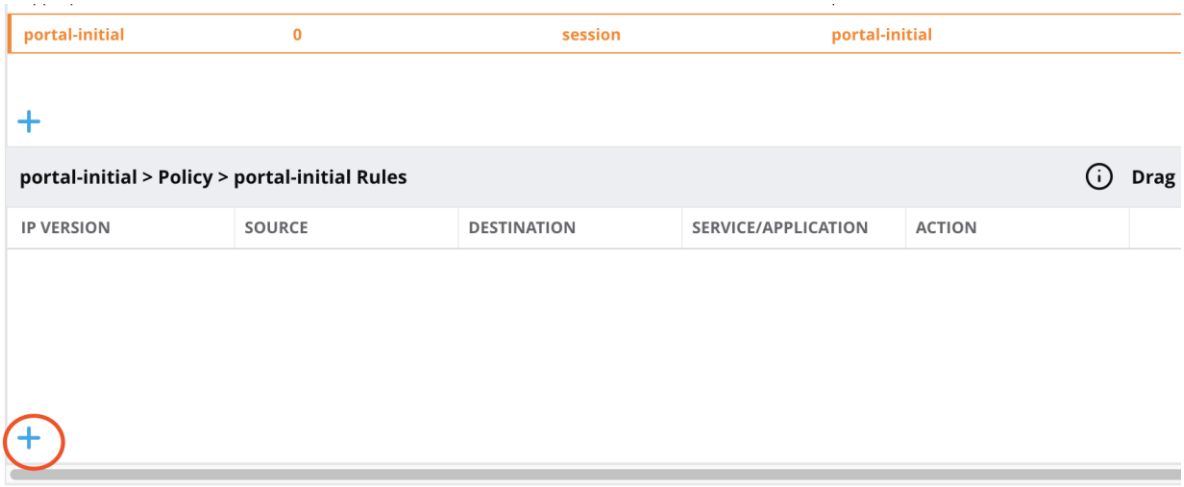




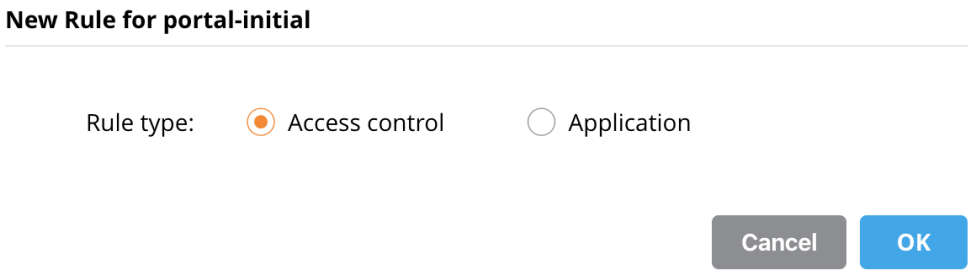
4) 新建 role 默认策略如下：



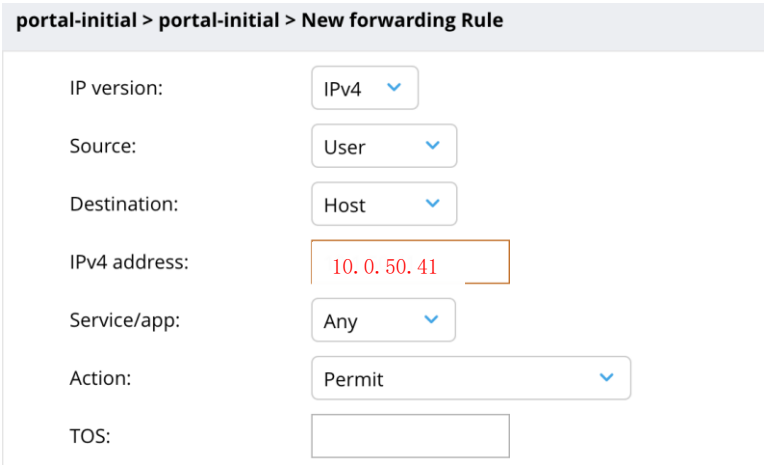
5) 设置外置 Portal 服务器访问策略，点击自动生成的 police 名称”portal-initial（labX-portal-guest-logon）“ 然后添加相关 rule



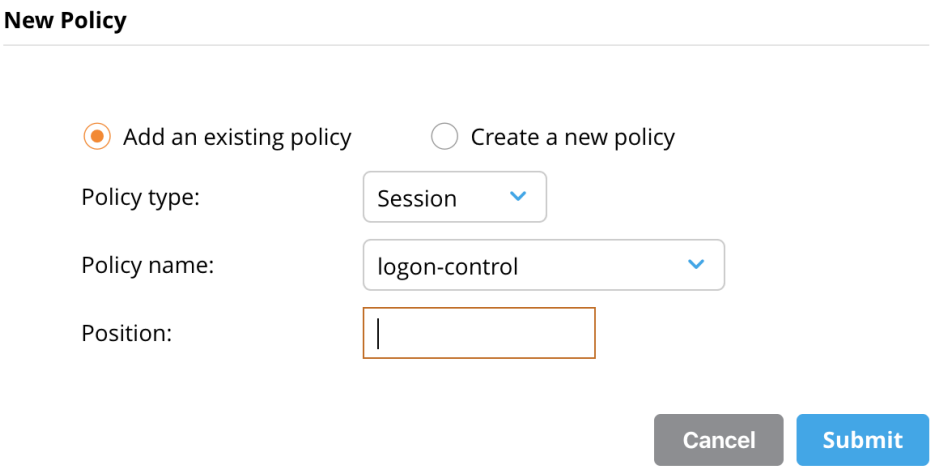
6) 选择 rule 类型”Access control”



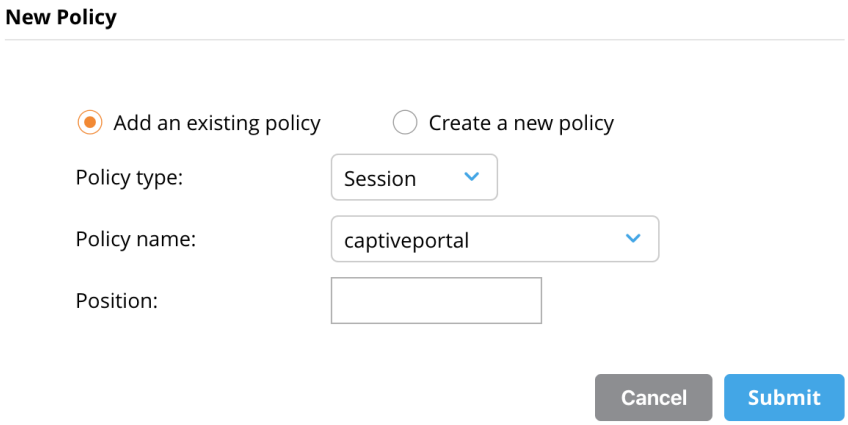
7) 添加外置 Portal 服务器地址，选择 permit 并提交



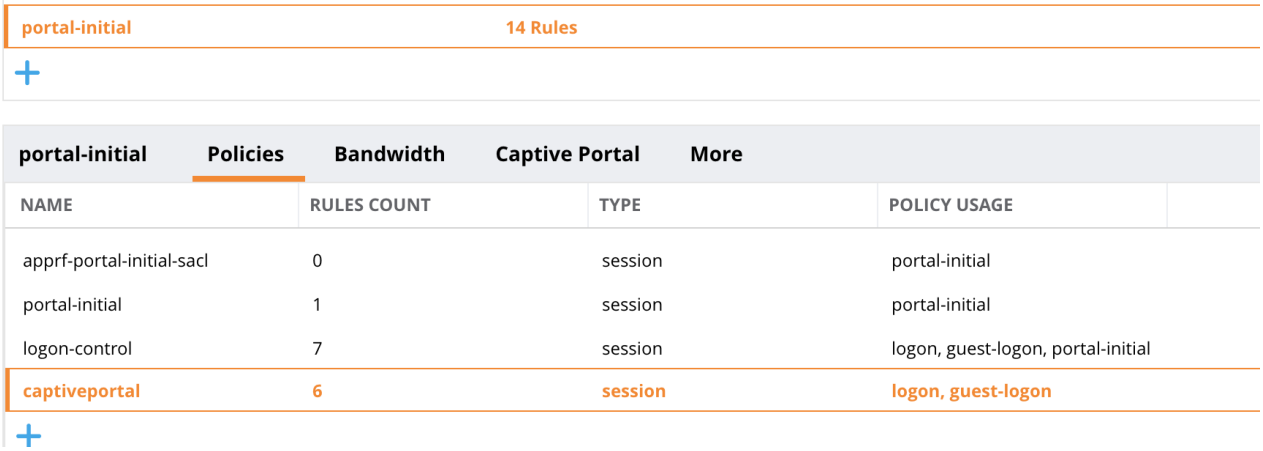
8) 添加用于用户基本权限的策略，调用系统自带”logon-control”即可。



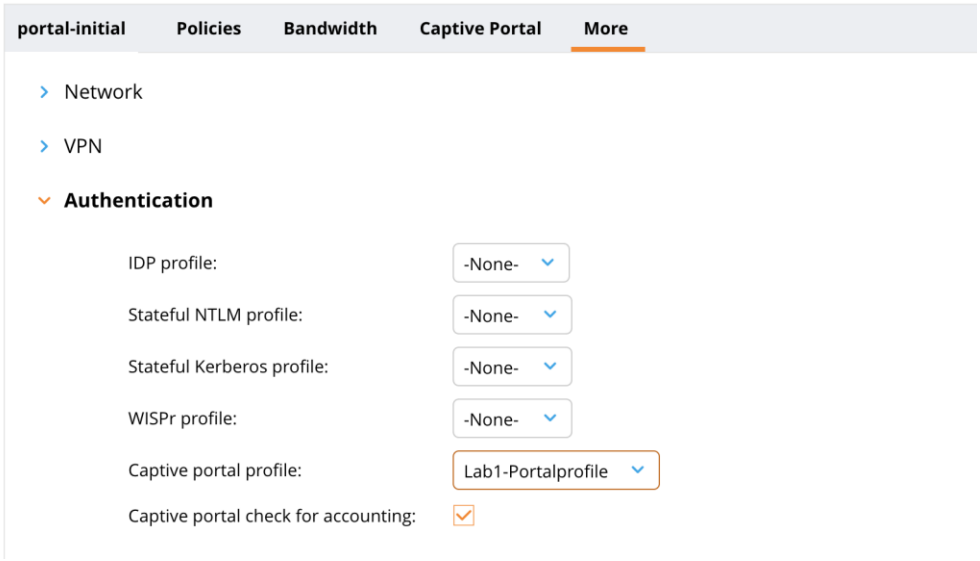
9) 添加用于终端弹 Portal 的策略，调用系统自带”captiveportal”即可



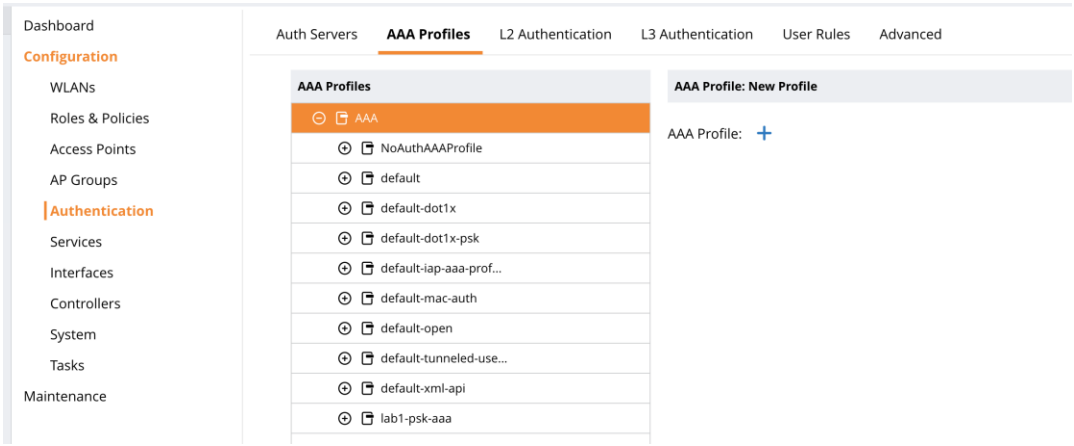
10) 完成 portal initial role 策略如下，点击提交。



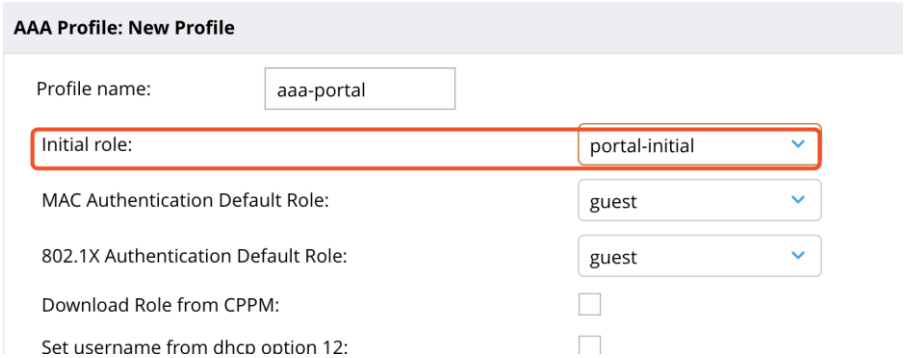
11) 关联 Captive Portal profile，点击”More”,下拉选择 11.4.3 建立的 Portal profile。确认并提交。



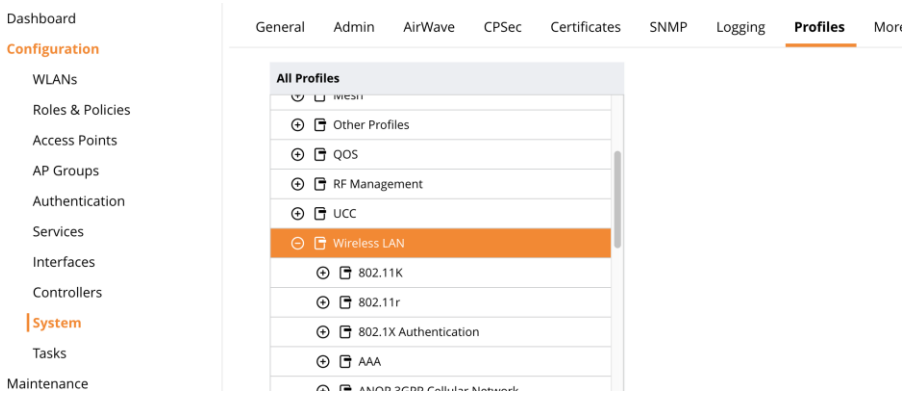
第9步：配置 AAA 认证创建 Portal 认证 AAA profile。Mobility Network- >LabX- > Configuration -> Authentication -> AAA Profiles

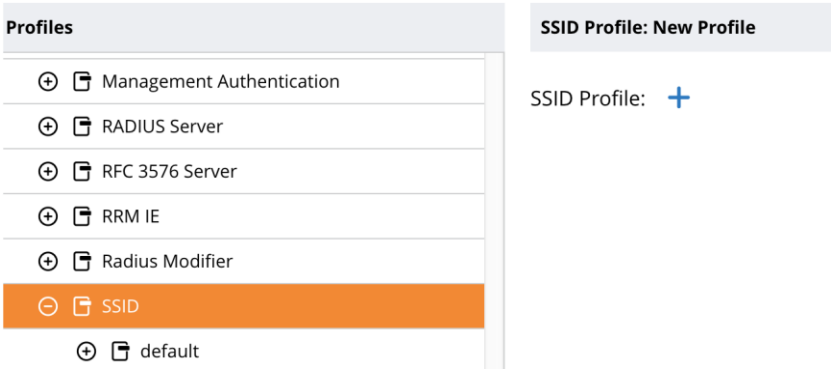


1) 填写 profile 名称，勾选 initial role

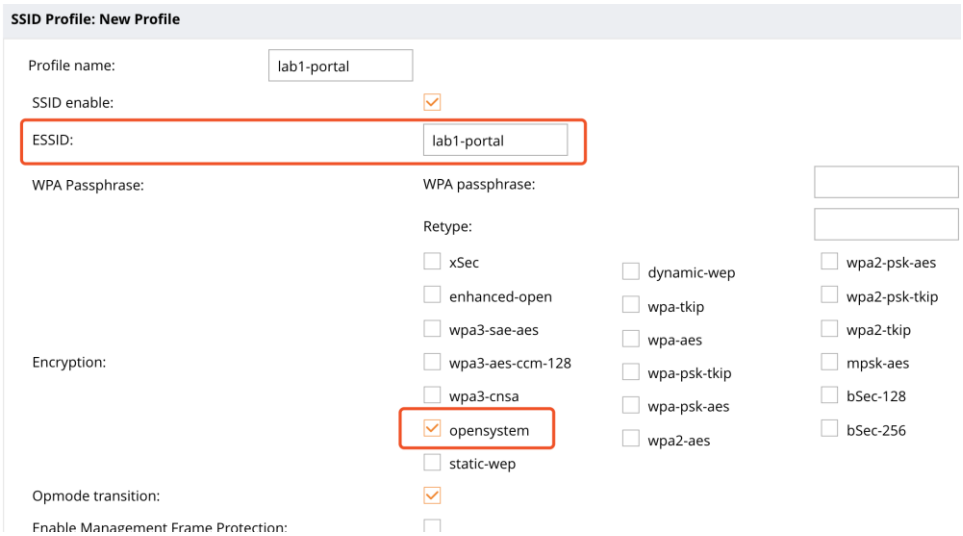


第10步:配置 SSID，创建用于 Portal 认证的 SSID profile。Mobility Network- >LabX- > Configuration -> System-> Wireless LAN-> SSID

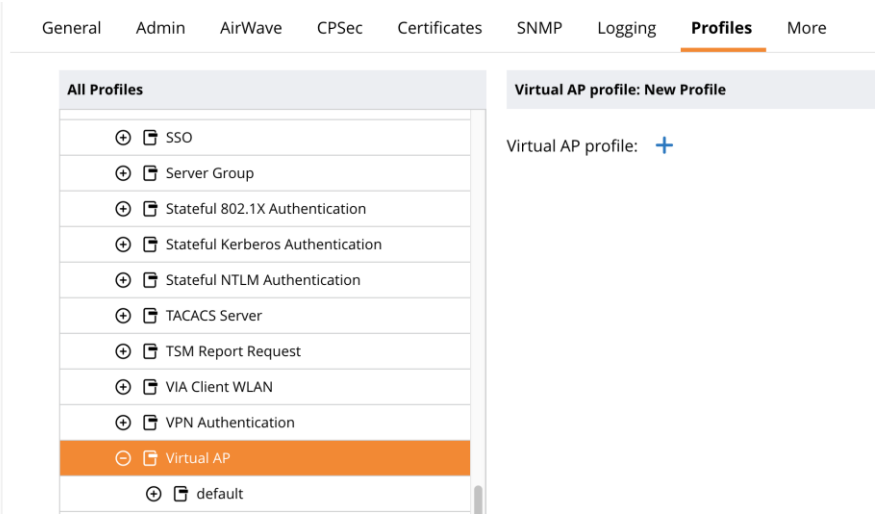




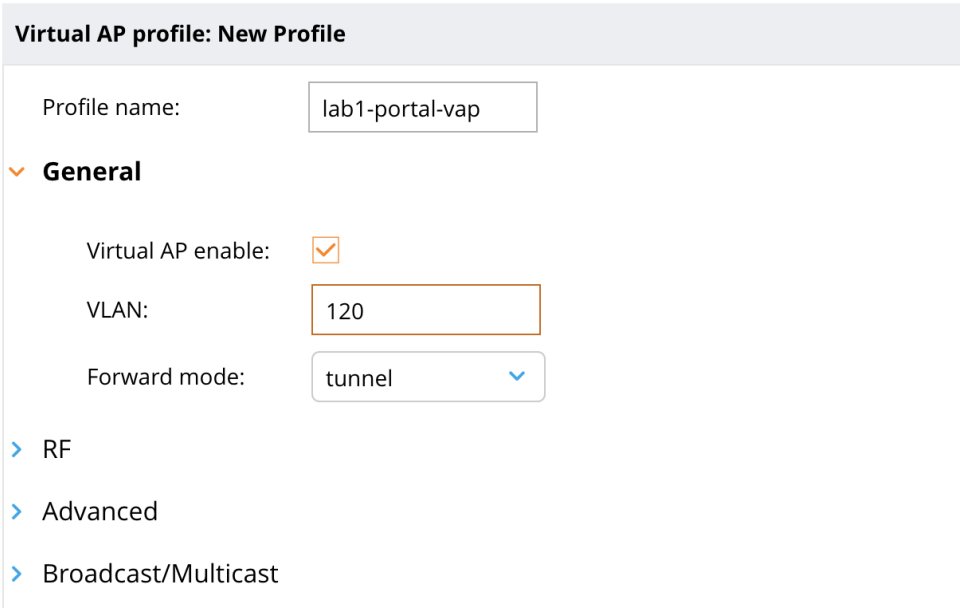
1) 新建 SSID，名称 labX-portal。采用 open 不加密方式。确认并提交。



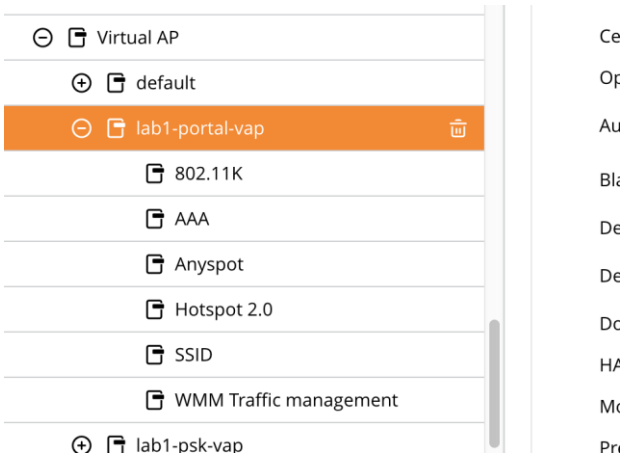
第11步:配置 Virtual AP，创建用于 Portal 认证的 Virtual AP profile。Mobility Network- >LabX- > Configuration -> System-> Wireless LAN-> Virtual AP

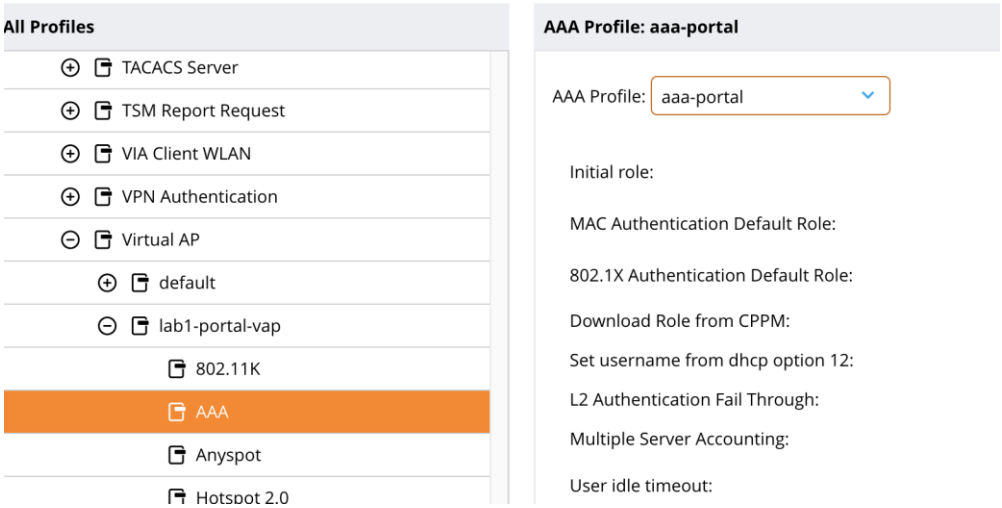


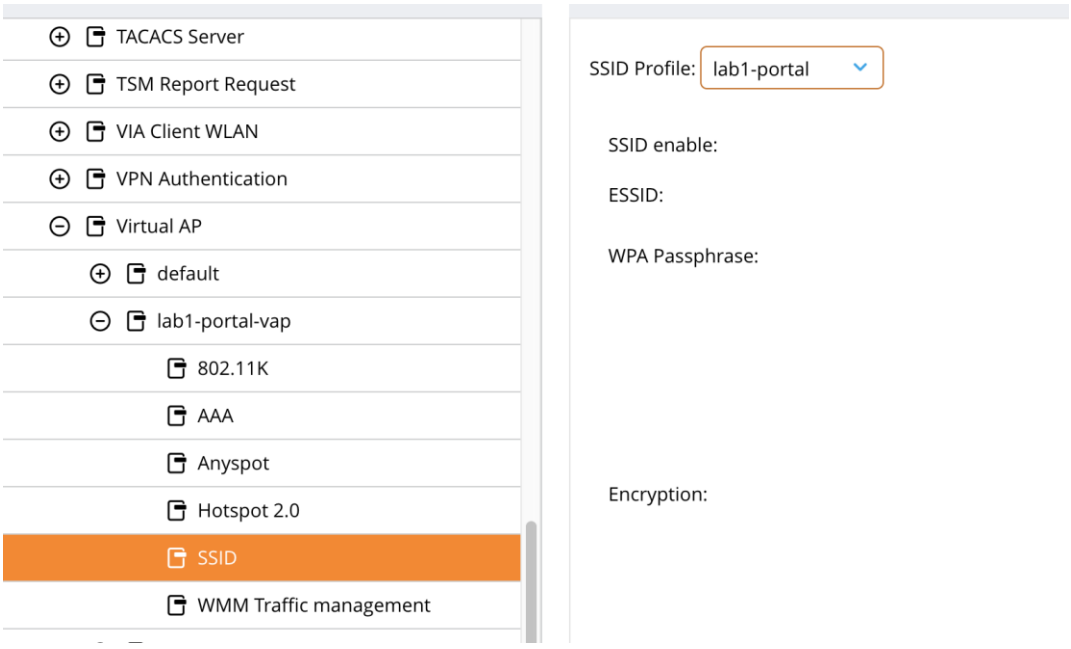
1) 填写 profile 名称，填写用户 vlan X20 （X 代表 Lab 1-6）



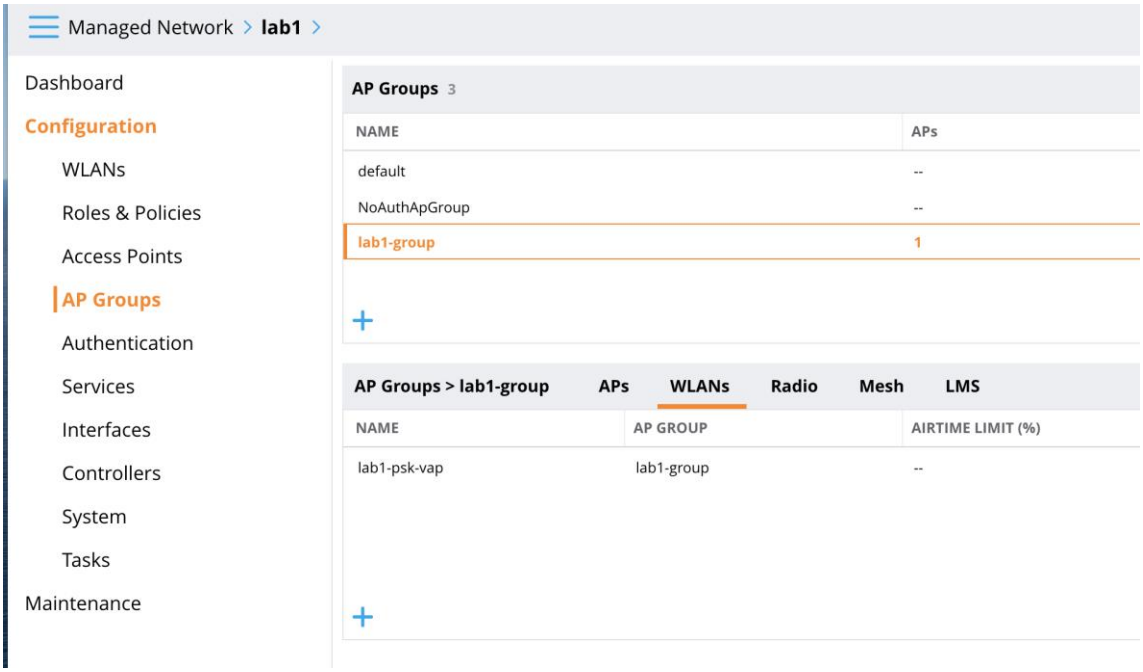
2) Virtual AP 关联 AAA profile 和 SSID profile，确认并提交，过程如下图：


Virtual AP
default
lab1-portal-vap
802.11K
AAA
Anyspot
Hotspot 2.0
SSID
WMM Traffic management
lab1-psk-vap

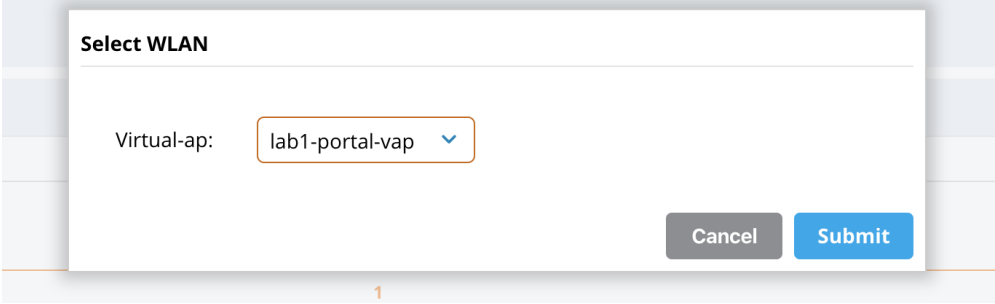

All Profiles
TACACS Server
TSM Report Request
VIA Client WLAN
VPN Authentication
Virtual AP
default
lab1-portal-vap
802.11K
AAA
Anyspot
Hotspot 2.0
AAA Profile: aaa-portal
AAA Profile: aaa-portal
Initial role:
MAC Authentication Default Role:
802.1X Authentication Default Role:
Download Role from CPPM:
Set username from dhcp option 12:
L2 Authentication Fail Through:
Multiple Server Accounting:
User idle timeout:


TACACS Server
TSM Report Request
VIA Client WLAN
VPN Authentication
Virtual AP
default
lab1-portal-vap
802.11K
AAA
Anyspot
Hotspot 2.0
SSID
WMM Traffic management
SSID Profile: lab1-portal
SSID enable:
ESSID:
WPA Passphrase:
Encryption:

第12步:配置 AP Group：创建 AP Group 或者在现有 AP Group 添加 portal Virtual AP profile。Mobility Network- >LabX- > Configuration -> AP Groups



1) 点击 WLAN 添加 Virtual AP



11.5 验证结果

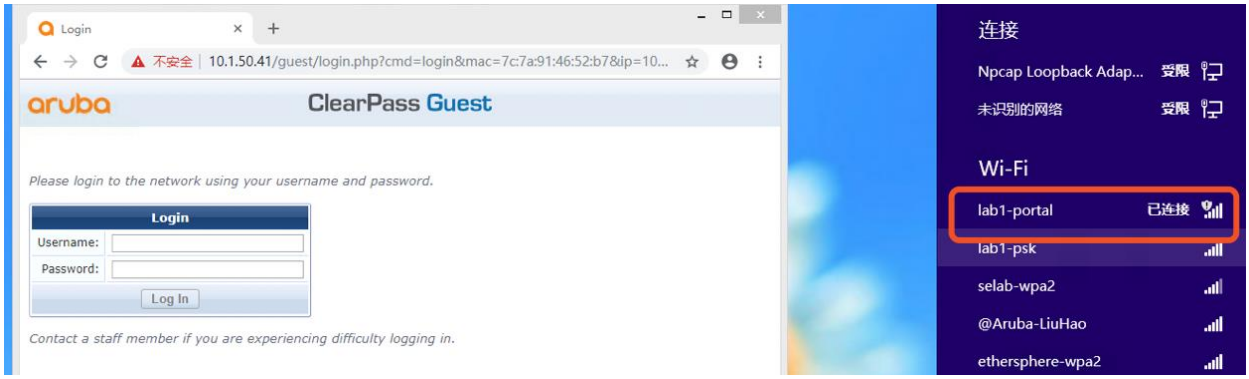
第1步: 确保没有配置错误

```
(labX-md1) [MDC] #show profile-errors

Invalid Profiles

----------------

Profile  Error

-------  -----
```

第2步：查看 SSID 是否释放

```
(labX-md1) [MDC] #show ap essid

ESSID Summary

-------------

ESSID       APs  Clients  VLAN(s)  Encryption

-----       ---  -------  -------  ----------

labX-portal  1    0        120      Open
```

第3步：远程桌面登录 10.X.50.102 测试（测试账号密码 labXuser/labXuser）



第4步：查看认证前用户 role

```
(lab1-md1) [MDC] #show user

This operation can take a while depending on number of users. Please be patient ....

Users

-----

   IP          MAC          Name     Role          Age(d:h:m)  Auth  VPN link  AP name          Roaming   Essid/Bssid/Phy
               Profile      Forward mode  Type    Host Name   User Type

----------  ------------     ------   ----          ----------  ----  --------  -------          -------   ---------------
-------       ------------ ----   ---------  ---------

10.1.20.100  7c:7a:91:46:52:b7          labX-portal-logon  00:00:00                  94:b4:0f:c1:3f:e0  Wireless  lab1-portal/94:
b4:0f:93:fe:12/a-VHT  lab1-portal-aaa  tunnel       Win 8          WIRELESS


User Entries: 1/1

 Curr/Cum Alloc:1/15 Free:0/14 Dyn:1 AllocErr:0 FreeErr:0
```

第5步: 查看认证后用户 role 及认证方式

```
(lab1-md1) [MDC] #show user

This operation can take a while depending on number of users. Please be patient ....


Users

-----

   IP          MAC           Name     Role          Age(d:h:m)  Auth  VPN link  AP name          Roaming   Essid/Bssid/Phy
            Profile        Forward mode  Type   Host Name  User Type

----------  ------------     ------   ----        ----------  ----  --------  -------         -------  ---------------                ---
----        ------------  ----   ---------  ---------

10.1.20.100  7c:7a:91:46:52:b7  labXcauser  authenticated  00:00:00    Web           94:b4:0f:c1:3f:e0  Wireless  lab1-portal
/94:b4:0f:93:fe:12/a-VHT  lab1-portal-aaa  tunnel       Win 8          WIRELESS


User Entries: 1/1

Curr/Cum Alloc:1/14 Free:0/13 Dyn:1 AllocErr:0 FreeErr:0
```

12 MAC+PORTAL 无感知认证

12.1 用户需求

通过mac认证实现无感知认证，用户再次联网无需输入用户密码。

12.2 实现思路

创建一个新的 SSID：labX-mac-caching。创建一个新的 aaa profile，同时启用 mac 认证和 portal 认证，这里调用 11 章中创建的 portal 配置，initial role 配置。

12.3 MM 配置（CLI）

第9步：增加一个新的 aaa profile “labX-mac-caching-aaa”，使用 labX-sg 作为认证和计费服务器，mac 认证成功获得 authenticated 角色，失败获得 lab1-portal-logon 角色

```
(LabX-MM-1) [labX] (config) #aaa profile labX-mac-caching-aaa    <- X[1…6]
(LabX-MM-1) ^[labX] (AAA Profile "lab1-mac-caching-aaa") #initial-role labX-portal-logon
(LabX-MM-1) ^[labX] (AAA Profile "lab1-mac-caching-aaa") #authentication-mac labX-mac
(LabX-MM-1) ^[labX] (AAA Profile "lab1-mac-caching-aaa") #mac-server-group labX-sg
(LabX-MM-1) ^[labX] (AAA Profile "lab1-mac-caching-aaa") #radius-accounting labX-sg
(LabX-MM-1) ^[labX] (AAA Profile "lab1-mac-aaa") #mac-default-role authenticated
(LabX-MM-1) ^[labX] (AAA Profile "lab1-mac-caching-aaa") #!
```

第10步:增加一个新的 ssid profile “labX-mac-caching-ssid”

```
(LabX-MM-1) ^[labX] (config) #wlan ssid-profile labX-mac-caching-ssid    <- X[1…6]
(LabX-MM-1) ^[labX] (SSID Profile "lab1-mac-caching-ssid") #essid labX-mac-caching
(LabX-MM-1) ^[labX] (SSID Profile "lab1-mac-caching-ssid") #!
```

第11步:增加一个新的 virtual ap profile “labX-mac-caching-vap”

```
(LabX-MM-1) ^[labX] (config) #wlan virtual-ap labX-mac-caching-vap
(LabX-MM-1) ^[labX] (Virtual AP profile "lab1-mac-caching-vap") #aaa-profile labX-mac-caching-aaa    <- X[1…6]
(LabX-MM-1) ^[labX] (Virtual AP profile "lab1-mac-caching-vap") #ssid-profile labX-mac-caching-ssid    <- X[1…6]
(LabX-MM-1) ^[labX] (Virtual AP profile "lab1-mac-caching-vap") #vlan X20    <- X[1…6]
```

```
(LabX-MM-1) ^[labX] (Virtual AP profile "lab1-mac-caching-vap") #!
```

第12步:将 virtual-ap 关联到 AP Group

```
(LabX-MM-1) [labX] (config) #ap-group labX-group    <- X[1…6]
(LabX-MM-1) [labX] (AP group   “lab1-group") #virtual-ap labX-mac-caching-vap    <- X[1…6]
```

第13步:查看完成还未提交的配置内容

```
(LabX-MM-1) ^[labX] (config) #show configuration pending
```

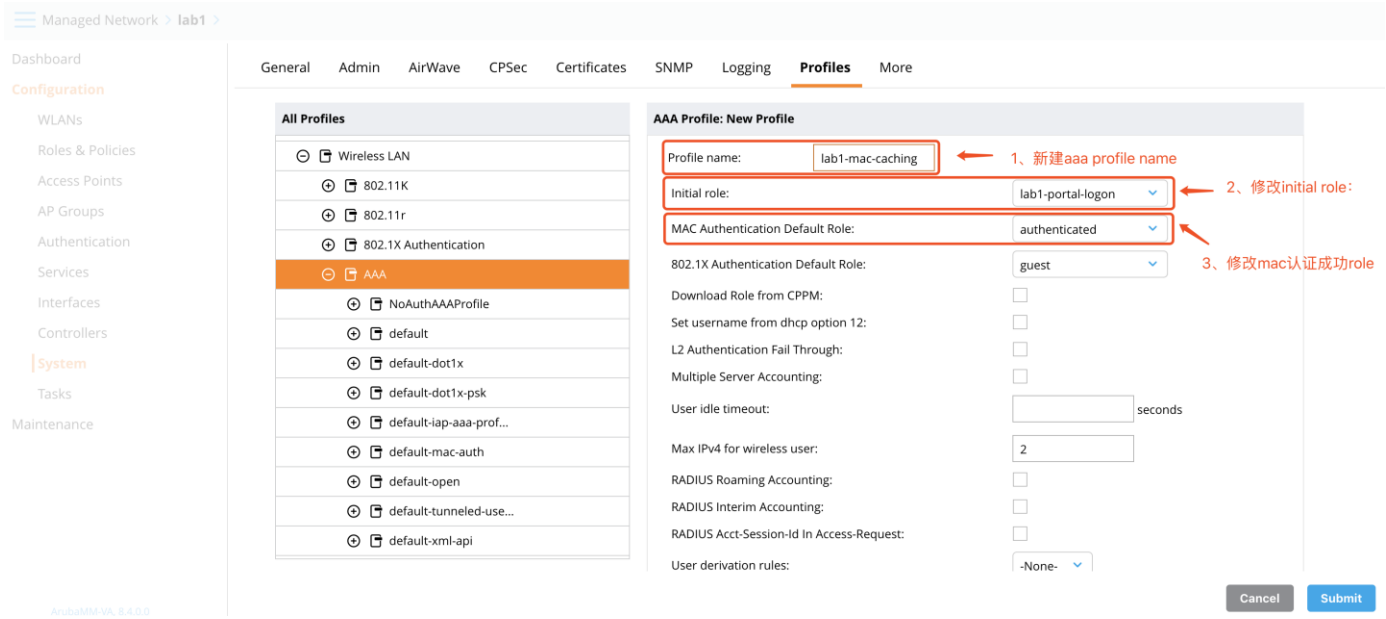
第14步:保存配置

```
(LabX-MM-1) ^[labX] (config) #write memory
Saving Configuration...
Configuration Saved.
```

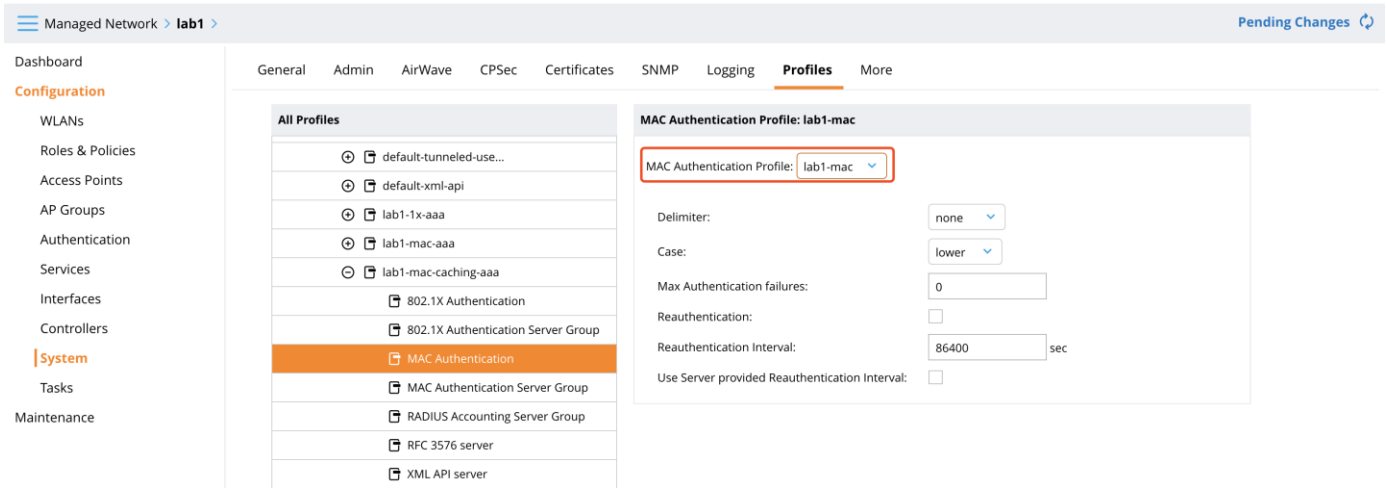
12.4 MM 配置（GUI）

第1步：进入到 Managed Network -> labX -> Configuration -> System，点击“Profiles”

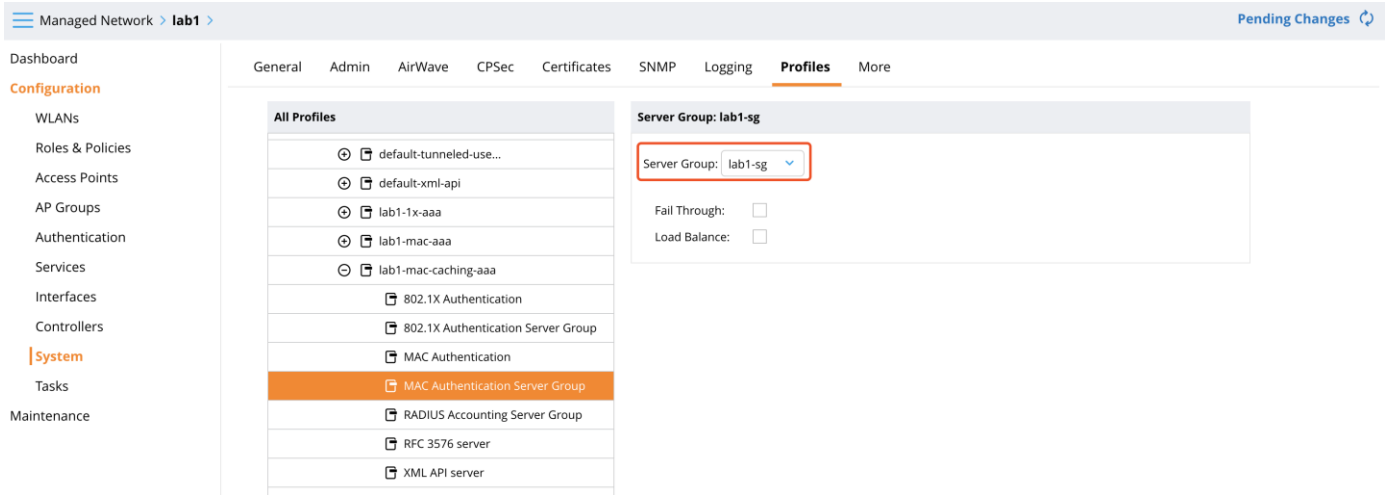
第2步：配置 AAA, 点击＋，新建 AAA profile name 为“labX-mac-caching-aaa”，修改初始角色为 labX-portal-logon，修改 MAC Authentication Default Role：authenticated。点击右下角 submit <- 这里的 X 代表 lab 分组[1…6]



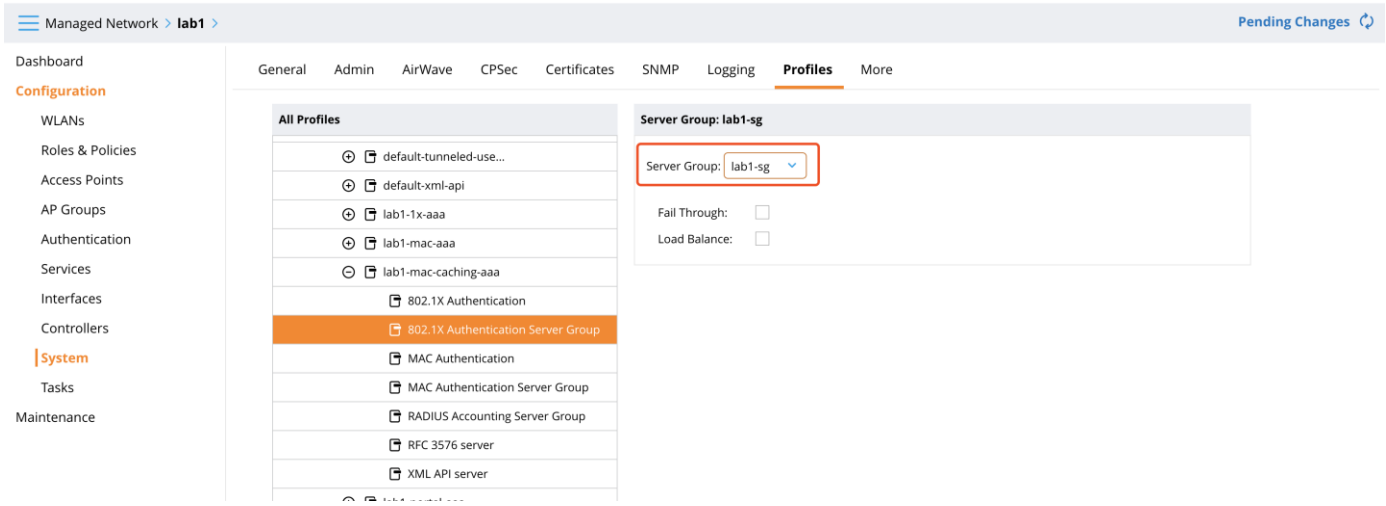
第3步：开启 mac 认证，选中刚创建的 aaa profile：labX-mac-caching-aaa。点击 MAC Authentication，配置如下，点击下方“Submit”



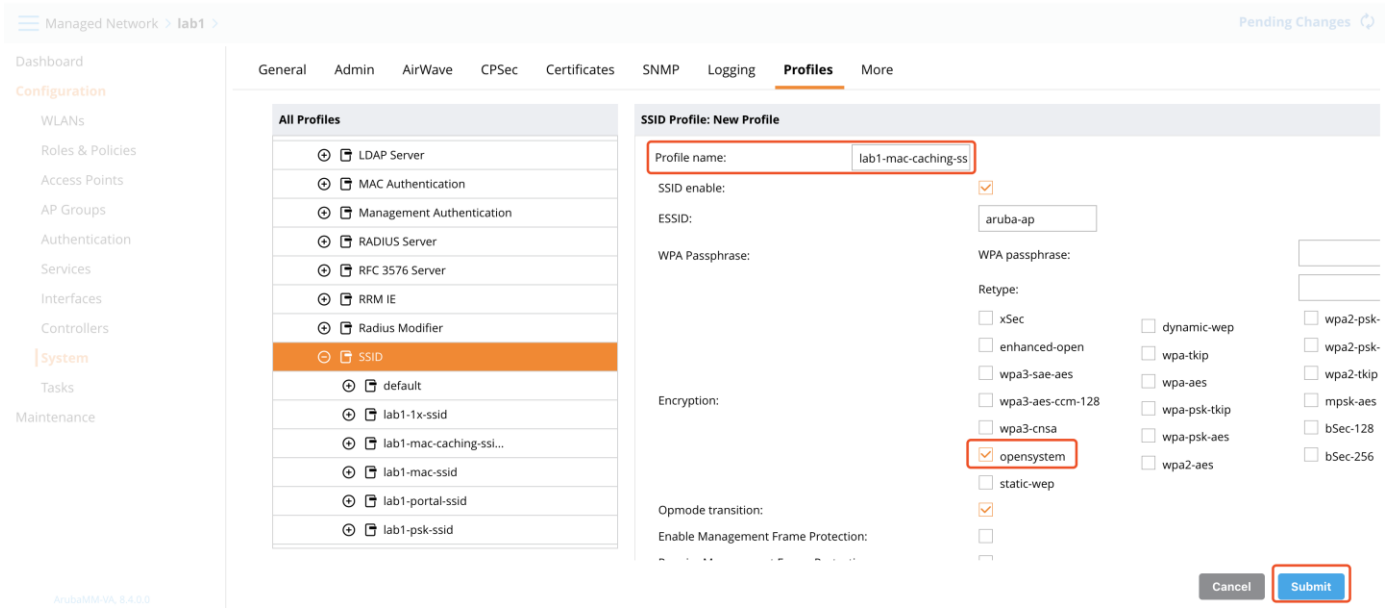
第4步：调用 mac 认证服务器组。点击下方的“Submit”



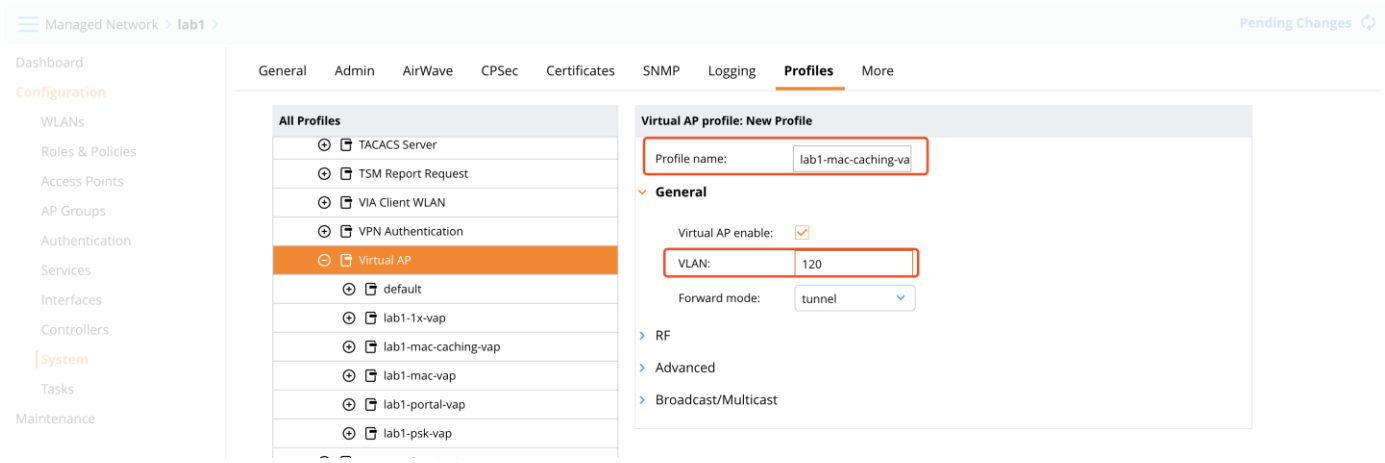
第5步：调用 aaa 计费服务器组。点击下方的“Submit”



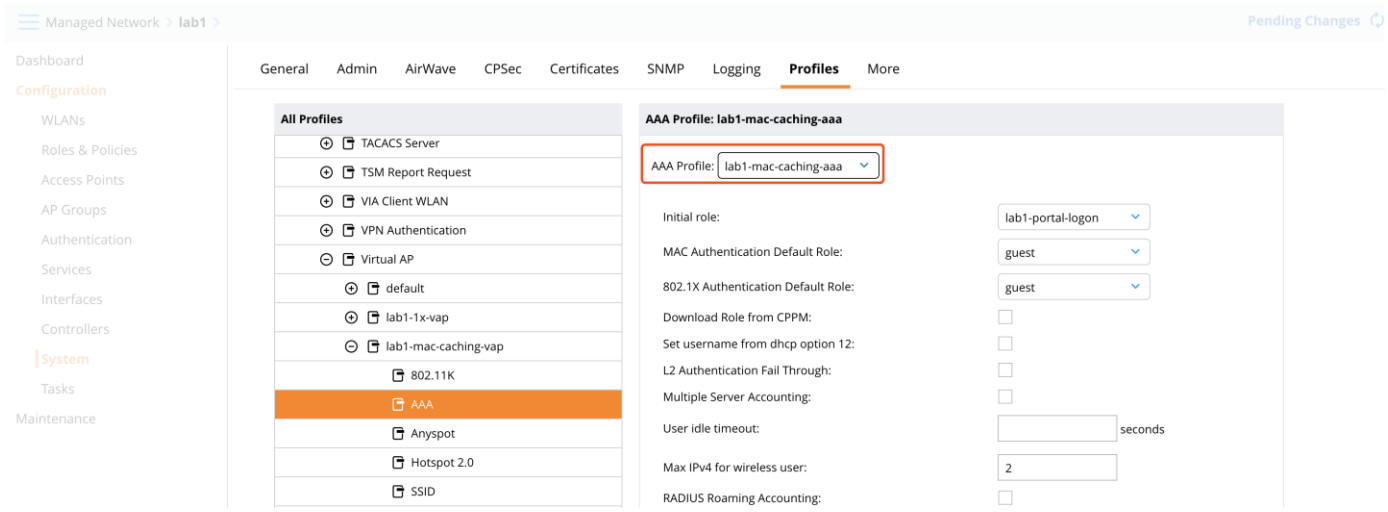
第6步：配置 SSID, 点击＋，新建 SSID profile name 为“labX-mac-caching-ssid”,点击下方“Submit”



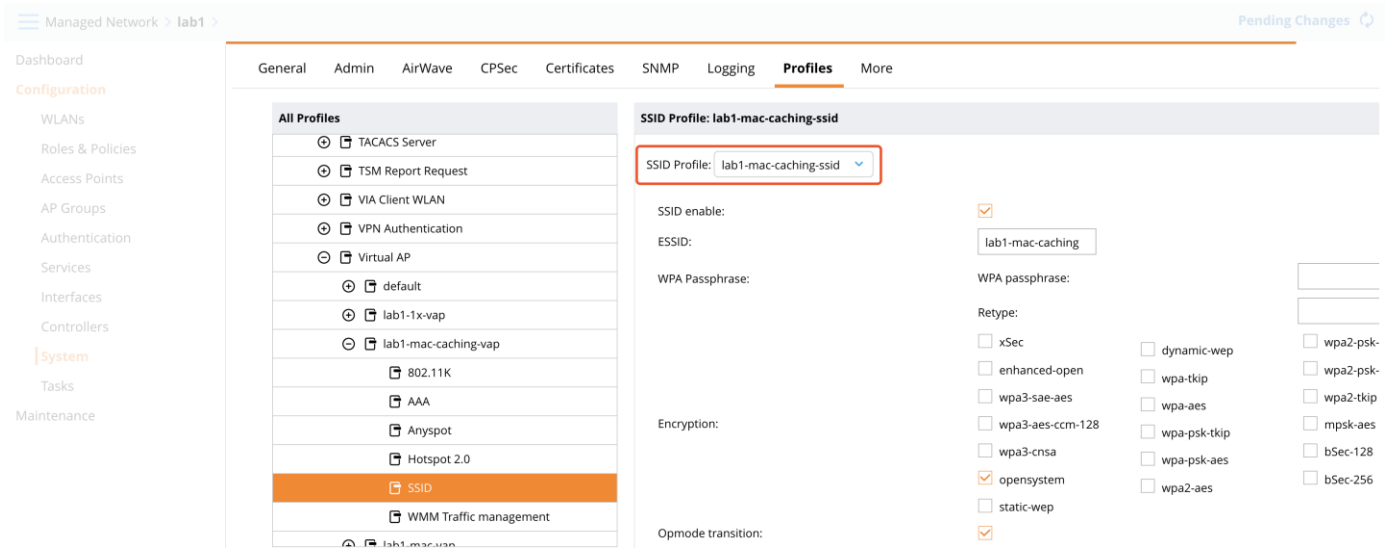
第7步：配置 Virtual，点击＋，新建 Virtual ap profile name 为“labX-mac-caching-vap”，vlan：X20，点击下方“Submit”



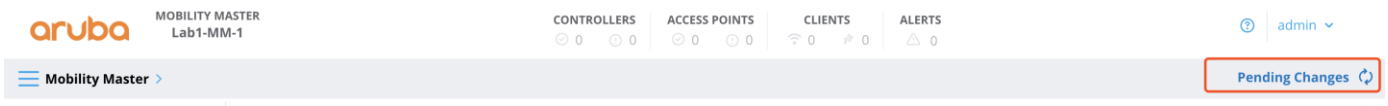
第8步：点击新建的 Virtual ap profile，关联 aaa profile：labX-mac-caching-aaa，点击下方“Submit”



第9步：点击新建的 Virtual ap profile，关联 ssid profile：labX-mac-caching-ssid，点击下方“Submit”



第10步:点击右上角的“Pending Changes”,保存配置



12.5 验证结果

第1步：查看第一次登录初始角色

```
(lab1-md1) [MDC] #show user

This operation can take a while depending on number of users. Please be patient ....

Users

-----

   IP          MAC           Name     Role            Age(d:h:m)  Auth  VPN link  AP name          Roaming   Essid/Bssid/Phy
                    Profile            Forward mode  Type   Host Name  User Type

----------  ------------      ------   ----           ----------  ----  --------  -------         -------   ---------------
   -------           ------------  ----   ---------  ---------

10.1.20.100  7c:7a:91:46:52:b7          labX-portal-logon  00:00:00                  94:b4:0f:c1:3f:e0  Wireless  lab1-mac-cachi
ng/94:b4:0f:93:fe:14/a-VHT  lab1-mac-caching-aaa  tunnel       Win 8          WIRELESS


User Entries: 1/1

 Curr/Cum Alloc:1/3 Free:0/2 Dyn:1 AllocErr:0 FreeErr:0
```

第2步：访客测试账号：guestX@arubalab.net （X=1...6） 密码 aruba123

第3步：查看通过认证后的角色

```
(lab1-md1) [MDC] #show user

This operation can take a while depending on number of users. Please be patient ....
```

```
Users

-----

   IP          MAC          Name                Role          Age(d:h:m)  Auth  VPN link  AP name          Roaming    Essid/Bssid
/Phy                    Profile           Forward mode  Type   Host Name  User Type

----------  ------------      ------              ----        ----------  ----  --------  -------          -------    ---------------
           -------           ------------  ----   ---------  ---------

10.1.20.100  7c:7a:91:46:52:b7  guest1@arubalab.net  authenticated  00:00:01    Web           94:b4:0f:c1:3f:e0  Wireless  l
ab1-mac-caching/94:b4:0f:93:fe:14/a-VHT  lab1-mac-caching-aaa  tunnel       Win 8          WIRELESS


User Entries: 1/1

 Curr/Cum Alloc:1/1 Free:0/0 Dyn:1 AllocErr:0 FreeErr:0
```

第4步：将用户踢下线，

```
(lab1-md1) [MDC] #aaa user delete all

1 users deleted
```

第5步：然后查看用户认证情况。

```
(lab1-md1) [MDC] #show user

This operation can take a while depending on number of users. Please be patient ....

Users

-----

   IP          MAC          Name                Role          Age(d:h:m)  Auth  VPN link  AP name          Roaming    Essid/Bssid
/Phy                    Profile           Forward mode  Type   Host Name  User Type

----------  ------------      ------              ----        ----------  ----  --------  -------          -------    ---------------
           -------           ------------  ----   ---------  ---------

10.1.20.100  7c:7a:91:46:52:b7  guest1@arubalab.net  authenticated  00:00:00    MAC           94:b4:0f:c1:3f:e0  Wireless  l
ab1-mac-caching/94:b4:0f:93:fe:14/a-VHT  lab1-mac-caching-aaa  tunnel       Win 8          WIRELESS


User Entries: 1/1

 Curr/Cum Alloc:1/2 Free:0/1 Dyn:1 AllocErr:0 FreeErr:0
```

----------全文完----------