



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..... **6**

1 LAB 拓扑环境和设备登录信息 **7**

1.1 LAB 内容简介	7
1.2 LAB 设备及拓扑	7
1.3 LAB 设备 VLAN 和 IP 信息	8
1.4 LAB 设备登录账号和密码	8
1.5 设备 CONSOLE 连接方式	9
1.6 AP 重启操作	9

2 AOS8 分层配置(NODE HIERARCHY)..... **10**

2.1 用户需求	10
2.2 实现思路	10
2.3 熟悉 AOS8 常用的 CLI 命令	11
2.3.1 查看 MM 所有配置节点 (配置路径)	11
2.3.2 更改配置节点	12
2.3.3 进入设备 (控制器/MD) 配置节点	12
2.3.4 远程登录 MD (控制器) 的方法	13
2.3.5 查看配置的方法	14
2.3.6 配置提示符	15
2.4 MM 配置 (CLI)	15
2.5 MM 配置 (GUI)	15
2.6 验证结果	17

3 MM 接收管理 MD **19**

3.1 用户需求	19
3.2 控制器配置	19
3.2.1 通过 CONSOLE 初始化 7010-1 (MD1)	19

3.2.2 通过 CONSOLE 初始化 7010-2 (MD2)	22
3.3 MM 配置 (CLI)	25
3.4 MM 配置 (GUI)	27
3.5 验证结果.....	29
4 AOS8 LICENSE	32
4.1 用户需求.....	32
4.2 实现思路.....	32
4.2.1 CENTRALIZED LICENSING 工作模式.....	32
4.2.2 AOS 8 LICENSE 消耗计算.....	32
4.3 MM 配置 (CLI)	33
4.3.1 在 MYNODE 节点添加 LICENSE.....	33
4.3.2 开启 PEF 和 RFP 功能.....	34
4.3.3 LICENSE POOL 功能.....	36
4.4 MM 配置 (GUI)	36
4.4.1 在 WEB 页面添加 LICENSE.....	36
4.4.2 开启 PEF 和 RFP 功能.....	37
4.4.3 LICENSE POOL 功能.....	38
4.5 验证结果.....	39
5 AP 上线操作.....	42
5.1 用户需求.....	42
5.2 实现思路.....	42
5.3 MM 配置 (CLI)	43
5.3.1 关闭 CPSEC 功能	43
5.3.2 启用 CPSEC 功能 (注：5.3.1 和 5.3.2 配置二选一)	43
5.3.3 配置 VRRP	43
5.4 MM 配置 (GUI)	45
5.4.1 关闭 CPSEC 功能	45
5.4.2 启用 CPSEC 功能 (注：5.4.1 和 5.4.2 配置二选一)	45
5.4.3 配置 VRRP	46
5.5 验证结果.....	49

6 CLUSTER 集群配置.....	51
6.1 用户需求	51
6.2 实现思路	51
6.3 MM 配置 (CLI)	51
6.4 MM 配置 (GUI)	53
6.5 验证结果	55
7 USER ROLE.....	62
7.1 用户需求	62
7.2 实现思路	62
7.3 MM 配置 (CLI)	62
7.4 MM 配置 (GUI)	64
7.5 验证结果	67
8 PSK.....	70
8.1 用户需求	70
8.2 实现思路	70
8.3 MM 配置 (CLI)	70
8.4 MM 配置 (GUI)	73
8.5 验证结果	81
9 MAC 认证.....	83
9.1 用户需求	83
9.2 实现思路	83
9.3 MM 配置 (CLI)	83
9.4 MM 配置 (GUI)	86
9.5 验证结果	93
10 802.1X 认证.....	95

10.1 用户需求	95
10.2 实现思路	95
10.3 MM 配置 (CLI)	95
10.4 MM 配置 (GUI)	97
10.5 验证结果	101
<u>11 外置 PORTAL 认证</u>	<u>104</u>
11.1 用户需求	104
11.2 实现思路	104
11.3 MM 配置 (CLI)	104
11.4 MM 配置 (GUI)	107
11.5 验证结果	119
<u>12 MAC+PORTAL 无感知认证</u>	<u>122</u>
12.1 用户需求	122
12.2 实现思路	122
12.3 MM 配置 (CLI)	122
12.4 MM 配置 (GUI)	124
12.5 验证结果	128

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

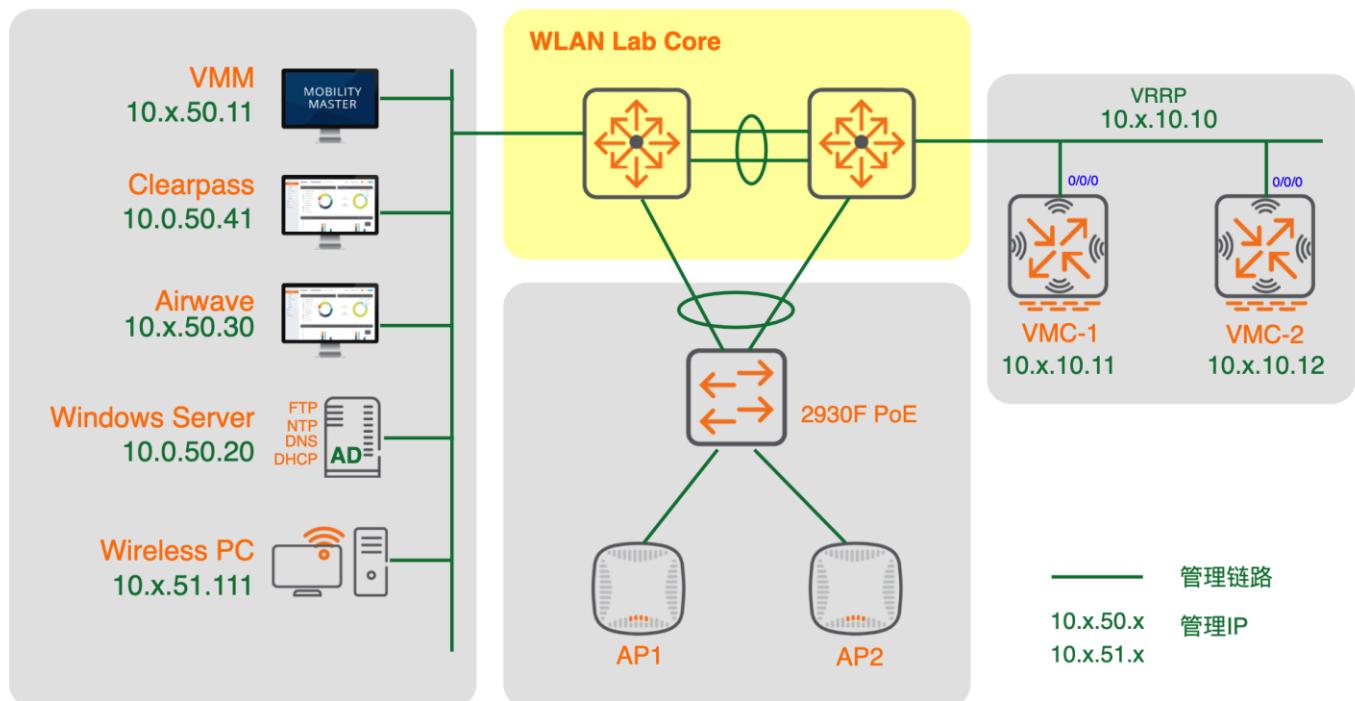
1 LAB 拓扑环境和设备登录信息

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

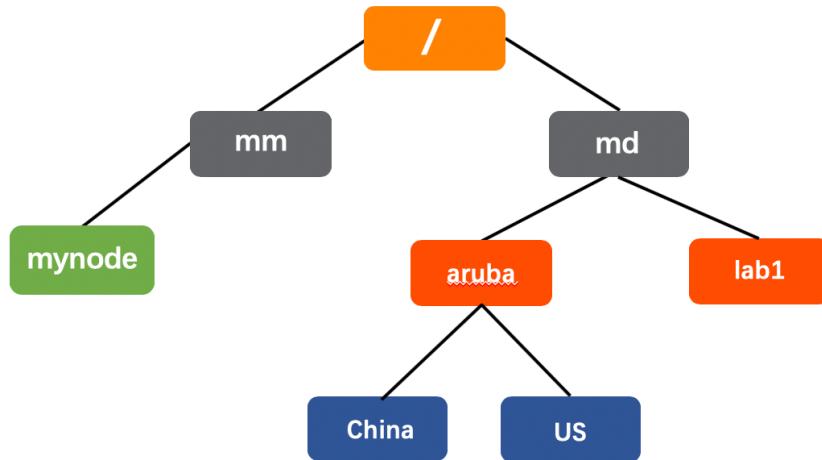
直接右键点击AP操作重启。

2 AOS8 分层配置(NODE HIERARCHY)

2.1 用户需求

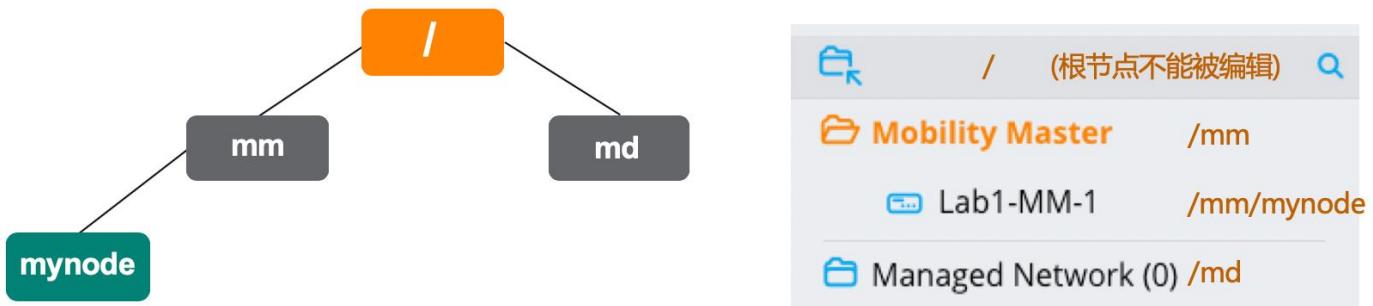
在这个lab中我们需要按照以下需求创建节点层次结构

- ✓ 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。

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

NOTE

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/cyCAhazTs7cxl.
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
```

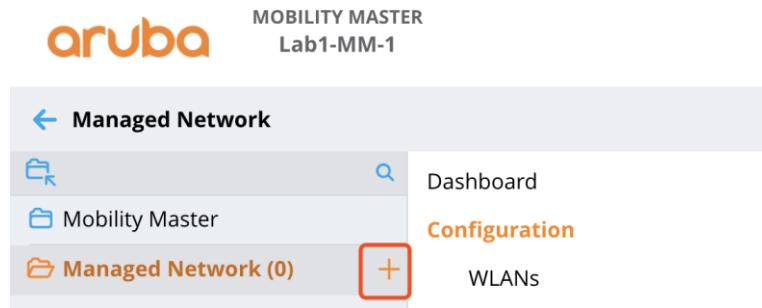
第2步：创建用户节点 (Node Hierarchy)，如下：

```
(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
```

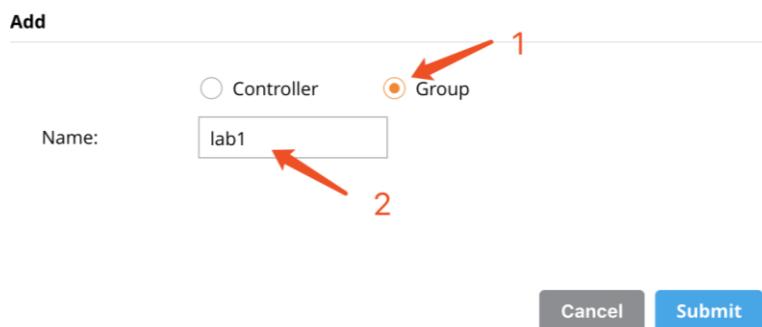
2.5 MM 配置 (GUI)

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]）

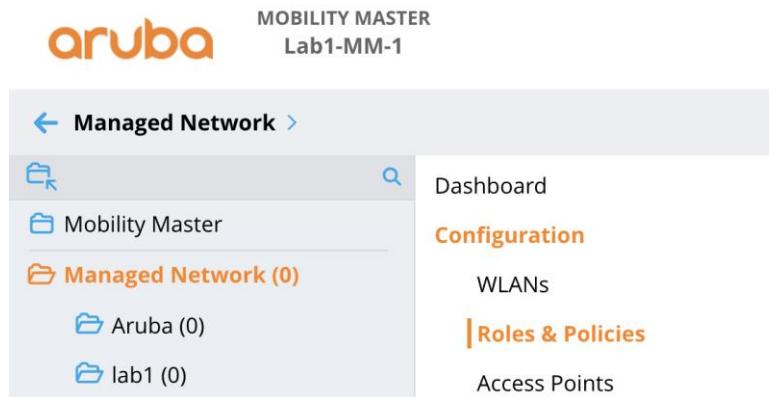
第2步：点击 Managed Network 右边的 “+”



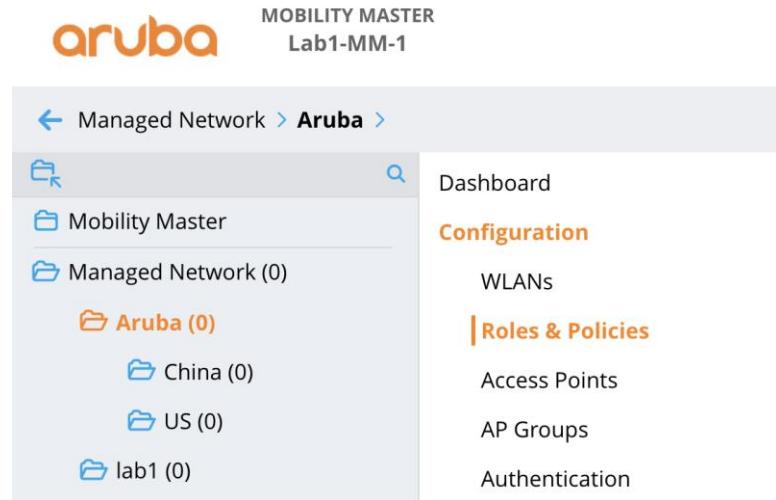
第3步：在弹出到选项卡中，选中 Group（对应cli里的node），在 Name 中输入“labX”，然后点击“Submit”（<- 这里的 X 代表 lab 分组[1…6]）



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	

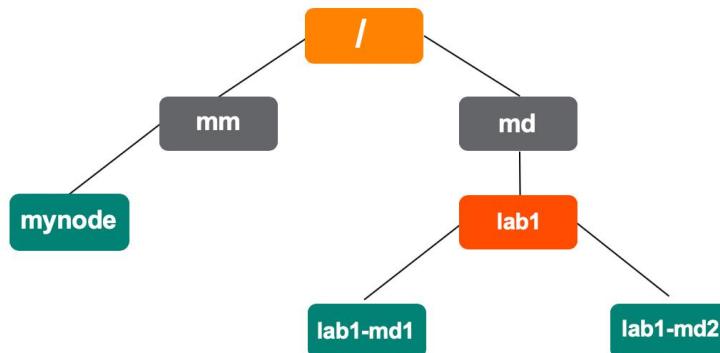
第2步：WEB 页面查看分层结构，验证创建的用户节点（Node Hierarchy）

The screenshot shows the Aruba Mobility Master interface. At the top, it displays "MOBILITY MASTER" and "Lab1-MM-1". The left sidebar shows a navigation tree under "Aruba (0)": "China (0)", "US (0)", and "lab1 (0)". To the right, there are several configuration sections: "Dashboard", "Configuration" (which is currently selected), "WLANS", "Roles & Policies" (which is highlighted with a border), "Access Points", "AP Groups", and "Authentication".

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. Press '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: lab**X**-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. Press 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-l> 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 Sync 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

The screenshot shows the Aruba Mobility Master configuration interface. On the left, there is a sidebar with the following navigation options: Roles & Policies, Authentication, Services, Interfaces, **Controllers** (which is selected), System, and License. The main content area has two tabs: "Local Controller IPSec Keys" and "Add New IPSec Controller".

Local Controller IPSec Keys tab (Table View):

IPV4 ADDRESS OF THE LOCAL	IPV6 ADDRESS OF THE LOCAL	KEY	MAC ADDRESS OF THE LOCAL	CERT TYPE

Add New IPSec Controller tab (Form View):

1. A red arrow points to the "+" button in the top-left corner of the form.

2. A red arrow points to the "Local controller IPV4:" field containing "10.X.10.11".

3. A red arrow points to the "IPSec key:" field containing "aruba123".

4. A red arrow points to the "Retype IPSec key:" field containing "aruba123".

✓ 添加 MD2

The screenshot shows the 'Local Controller IPSec Keys' section. A red arrow labeled '1' points to the '+' button in the 'Add New IPSec Controller' dialog. Red arrows labeled '2', '3', and '4' point to the 'Local controller IPv4' field containing '10.X.10.12', the 'IPSec key' field containing 'aruba123', and the 'Retype IPSec key' field also containing 'aruba123' respectively.

第3步：点击右上角 Pending Changes，完成配置提交

The screenshot shows the 'Local Controller IPSec Keys' table with two entries: '10.1.10.11' and '10.1.10.12'. A red box highlights the 'Pending Changes' button in the top right corner of the interface.

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：

The dialog has the following fields and settings:

- Controller** radio button selected (labeled 1)
- Hostname:** lab1-md1 (labeled 2)
- MAC address:** 00:0b:86:9a:af:37 (labeled 3)
- Type:** MC-VA (labeled 4)
- Buttons:** Cancel and Submit

Add

<input checked="" type="radio"/> Controller	<input type="radio"/> Group
Hostname:	lab1-md2
MAC address:	00:0b:86:dd:2f:00
Type:	MC-VA

Cancel **Submit**

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

Mobility Master >

Configuration

- Roles & Policies
- Authentication
- Services
- Interfaces
- Controllers
- System**
- License

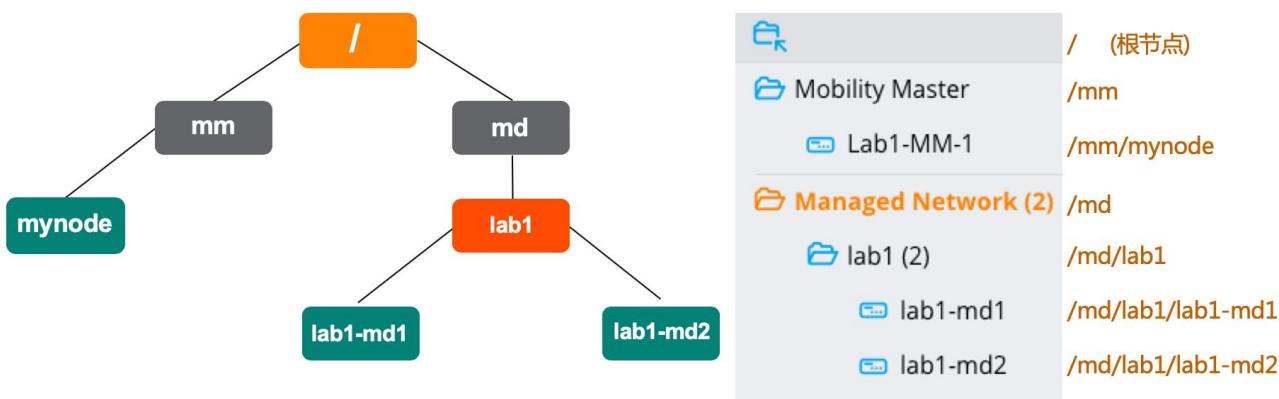
General Admin AirWave CPSec Certificates SNMP Logging Profiles Whitelist More

> Basic Info
 > Domain Name System
> Auto-parking
 Auto-parking for controllers: 1
 Folder for auto-parking: 2 Managed Network > lab1

> Aruba Support Portal (ASP)

3.5 验证结果

第1步：查看分层结构



✓ CLI:

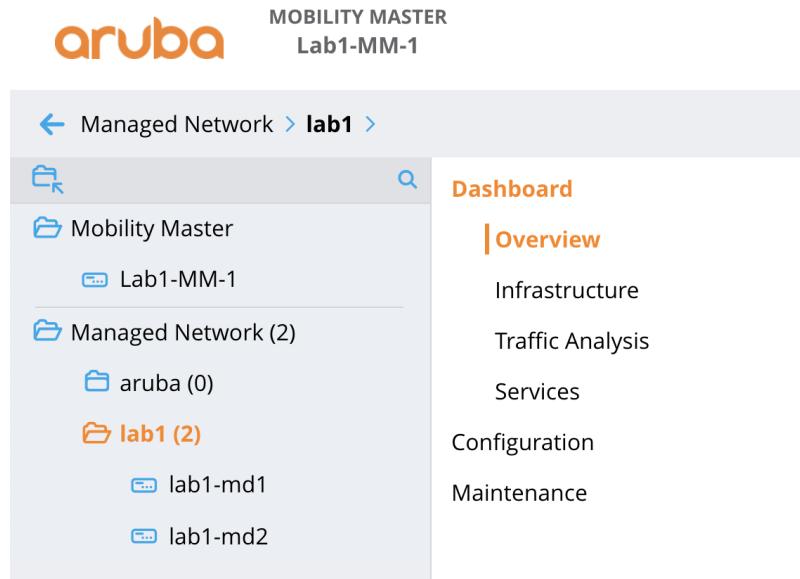
```
(LabX-MM-1) [mm] (config) #show configuration node-hierarchy
```

```
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

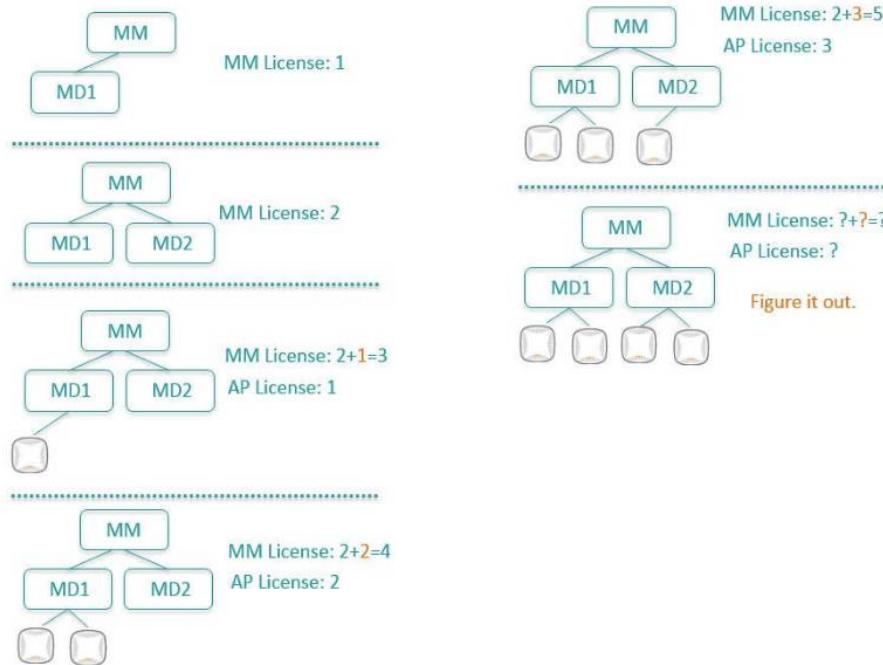
4.2.1 Centralized licensing 工作模式

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。

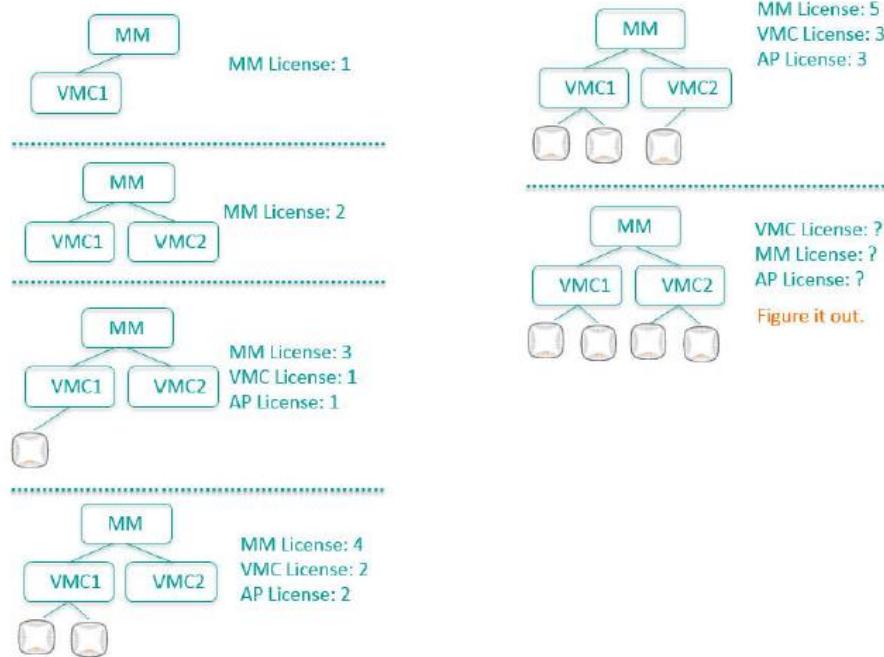
- ✓ 支持的模式：
 - Mobility Master (MM) 作为所有相关受管设备 (MD) 的许可服务器。
 - 独立控制器 (Standalone) 充当另一个独立控制器 (Standalone) 的许可服务器。
- ✓ 不支持的模式：
 - Mobility Master 同时充当其关联的 MD 和 Standalone 控制器的许可服务器 (8.2 版本以前，8.3 以后没有这个限制)

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 8:00:34 Never	E MM-VA: 50	2019-01-05 0		
UpbpPkNY-2mlbJIVG-Dkiyq6eE-rGLwKjcm-iJgyi0b+-Vyrz9RqJ-zAHZZyYH-HIc50+AM-t/gglfBl-l9s Never	E MC-VA-RW: 10	2019-01-05 08:00:51		
Dlnsnify-83tqlWng-yHvFMmVZ-WpmjjSIE-xE2XWokV-ZxDoPCnT-a7d0EgbI-g2xsVovE-vy8ffM3t-Clo 08 Never	E Access Points: 8	2019-01-05 08:01:		
pwCuhbYz-rfG+CUZP-Uj0pQ06A-9PEd+pp0-RUyuK3h2-9Lbv8d0f-XT6NrHpb-AKjntsY5-DUopLp8I-32M 01:25 Never	E Next Generation Policy Enforcement Firewall Module: 8	2019-01-05 08:		
YdcR5o8K-xgod+Mr/-HfUWH4Az-3j/p3jT+-ogVVNyad-DKv/BQkp-pjRtHT3t-gBVRz3SX-4NAurYHm-26g 8:01:44 Never	E RF Protect: 8	2019-01-05 0		

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

LICENSE	DESCRIPTION	STATUS	EXPIRATION	INSTALLED to this Mobility Master
AP	Access Points	<input checked="" type="radio"/> Active	Never	8
PEFNG	Policy Enforcement Firewall	<input checked="" type="radio"/> Active	Never	8
RFP	RF Protect(WiP,Spectrum,Multi-zone)	<input checked="" type="radio"/> Active	Never	8
ACR	Advanced Cryptography	<input type="radio"/> Not Licensed	Not Licensed	0
WebCC	Web Content Classification	<input type="radio"/> Not Licensed	Not Licensed	0
MM	Mobility Master Virtual Appliance	<input checked="" type="radio"/> Active	Never	50
MC-VA-RW	Controller Virtual Appliance(RW)	<input checked="" type="radio"/> Active	Never	10
MC-VA-EG	Controller Virtual Appliance(EG)	<input type="radio"/> Not Licensed	Not Licensed	0
MC-VA-IL	Controller Virtual Appliance(IL)	<input type="radio"/> Not Licensed	Not Licensed	0

第3步：在弹出的提示框，输入对应的 license key

Install Licenses

To install new licenses you will need:

- ✓ The Serial Number of this Mobility Master: MM7B42A9D
- ✓ The License Key for each service you wish to activate
- ✓ License Passphrase: MM7B42A9D-bQIkPj2Q-RHBkHWOR-mTYQ4e4T-tkjH237H

Obtain License Keys from [HPE Aruba My Networking Portal](#)

Enter the license keys in the text box below, one key per line.

Cancel

OK

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 Usage”，选择启用“PEF”和“RFP”，如下图所示，并点击“Submit”提交配置。

The screenshot shows the 'License Usage' tab of the Global License Pool. It displays the following data:

	AP	PEF	RF Protect	ACR	WebCC	VIA	MM	MC-VA-RW
Access Points	0/8	0/8	0/8	0/0	0/0	0/0	0/50	0/10

Below this, the 'Usage for Global License Pool' section provides a detailed breakdown of license usage across various features and scopes.

第2步：点击右上角的“Pending Changes”，保存配置

The screenshot shows the top navigation bar with the 'Pending Changes' button highlighted in red.

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])

The screenshot shows the 'License Usage' tab of the Global License Pool. It highlights the following steps:

1. Click on the 'License' link in the left sidebar.
2. Click on the 'License Usage' tab.
3. Select the 'lab1' license pool from the list.
4. Check the 'Enable local license pool' checkbox.

Below the table, a 'License Pool For lab1' section shows the configuration for the selected pool.

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，

LICENSE TYPE	LICENSE KEY	EXPIRATION DATE	TOTAL	AVAILABLE	ALLOCATE TO THIS POOL
Perm	--	Never	8	8	5
Totals			8	8	0

License Pool For lab1

Enable local license pool:	AP	PEF	RF Protect	ACR	WebCC	VIA	MM	MC-VA-RW
<input checked="" type="checkbox"/>	Per-AP	Per-AP	Per-AP	Per-Session	Per-AP	Per-Session	Per-Device	Per-Device
Allocated Licenses	1 → 0	0	0	0	0	0	0	0

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。

AP Access Points	PEF Policy Enforcement Firewall	RF Protect Wireless Intrusion Protection	ACR Advanced Cryptograph	WebCC Web Content Classification	VIA Virtual Intranet Access	MM Mobility Master	MC-VA-RW Rest of World Resiliency
2/8	2/8	2/16	0/0	0/0	0/0	4/50	0/10
lab1	2	2	0	0	0	4	0
Aruba	0	0	0	0	0	0	0

License Pool For lab1

Enable local license pool:	AP	PEF	RF Protect	ACR	WebCC	VIA	MM	MC-VA-RW
<input checked="" type="checkbox"/>	Per-AP	Per-AP	Per-AP	Per-Session	Per-AP	Per-Session	Per-Device	Per-Device
Allocated Licenses	5	5	0	0	0	0	5	0

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。

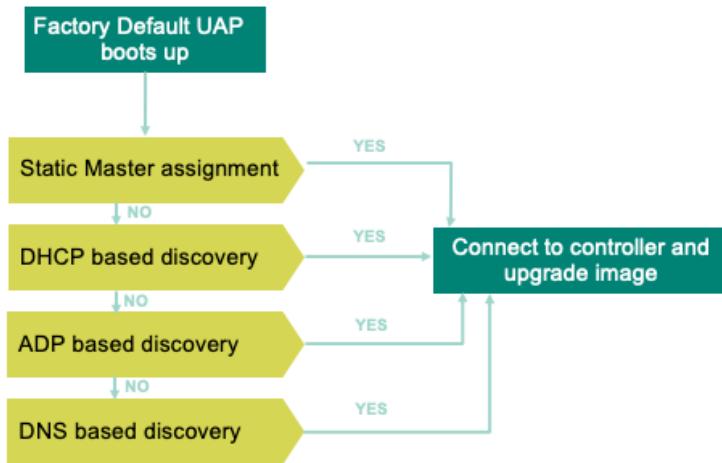
5 AP 上线操作

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” ,

The screenshot shows the Aruba Mobility Master interface. On the left, there's a sidebar with 'Managed Network > lab1 >' followed by a list of configuration options: Dashboard, Configuration (selected), WLANs, Roles & Policies, Access Points, AP Groups, Authentication, Services, Interfaces, Controllers, System (selected), and Tasks. At the top, a navigation bar has tabs for General, Admin, AirWave, CPSC (which is highlighted in orange), Certificates, SNMP, Logging, Profiles, and More. Below the tabs, under the 'System' section, is a 'Control Plane Security' section with a heading 'Control Plane Security' and a toggle switch labeled 'Enable CPSC' which is currently off (gray).

第2步: 点击右上角的 “Pending Changes” ,保存配置

The screenshot shows the Aruba Mobility Master dashboard. It includes the Aruba logo, network information (MOBILITY MASTER Lab1-MM-1), and various statistics like Controller, AP, Client, and Alert counts. In the bottom right corner, there is a 'Pending Changes' button with a circular arrow icon, which is highlighted with a red box.

5.4.2 启用 CPSC 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 “CPSC” , 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 CPSC” ,

- ✓ 启用 “Enable auto cert provisioning”

Managed Network > lab1 >

General Admin AirWave **CPsec** Certificates SNMP Logging Profiles More

Control Plane Security

Enable CPsec: 1

Enable auto cert provisioning: 2

Only accept APs from specified ranges:

第2步：点击右上角的“Pending Changes”，保存配置

aruba MOBILITY MASTER Lab1-MM-1

CONTROLLERS ACCESS POINTS CLIENTS ALERTS

Mobility Master > Pending Changes

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

Managed Network > lab3 > Lab3-MD1

Dashboard Configuration

WLANs Roles & Policies

Access Points AP Groups

Authentication Services

Interfaces Controller

System Tasks

Redundancy 2

High availability **L2 redundancy** 3

Virtual Router Table

ROUTER NAME IPV4 ADDRESS IPV6 ADDRESS

+ 4

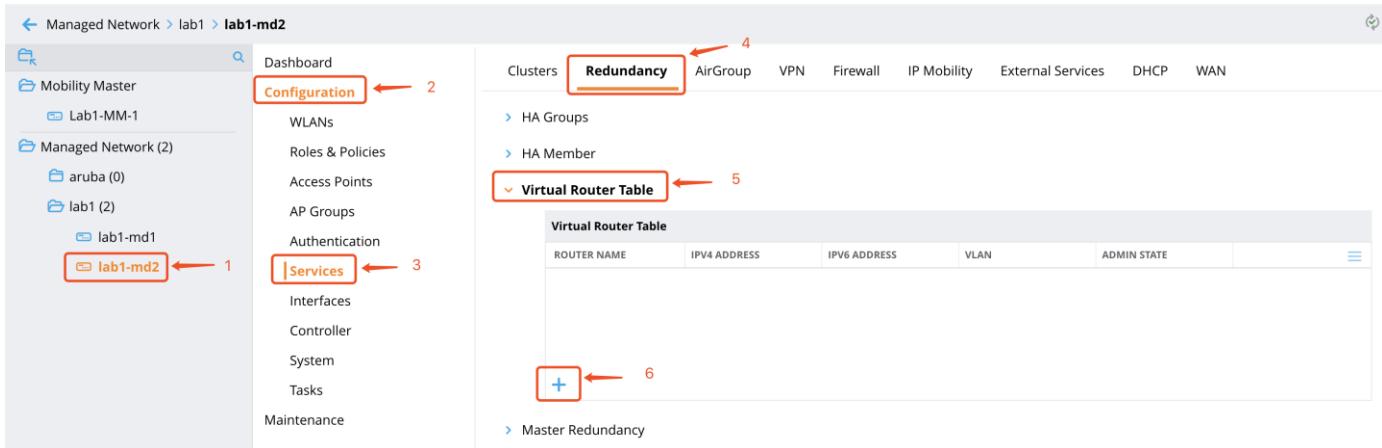
第2步：在弹出的选项卡中，输入以下参数配置 VRRP：

- ✓ 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]

New Virtual Router

ID:	X0	1
Description:		
IP version:	IPv4	
Authentication password:	aruba123	2
Retype authentication password:	aruba123	
IP address:	10.X.10.10	3
Priority:	120	4
Advertisement interval (secs):	1	
Enable router pre-emption:	<input type="checkbox"/>	
Pre-emption delay (secs):		
Admin state:	UP	5
VLAN:	110	6
Tracking master up-time:		
Tracking master up-time priority:		
Tracking VRRP master state ID:		
Tracking VRRP master state priority:		
VLAN		SUBTRACT
Tracking VLAN: +		
INTERFACE		SUBTRACT
Tracking interface: +		

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]

New Virtual Router

ID:	X0	1		
Description:				
IP version:	IPv4			
Authentication password:	aruba123	2		
Retype authentication password:	aruba123	3		
IP address:	10.X.10.10	3		
Priority:	110	4		
Advertisement interval (secs):	1			
Enable router pre-emption:	<input type="checkbox"/>			
Pre-emption delay (secs):				
Admin state:	UP	5		
VLAN:	110	6		
Tracking master up-time:				
Tracking master up-time priority:				
Tracking VRRP master state ID:				
Tracking VRRP master state priority:				
<table border="1"> <thead> <tr> <th>VLAN</th> <th>SUBTRACT</th> </tr> </thead> </table>			VLAN	SUBTRACT
VLAN	SUBTRACT			
Tracking VLAN:				
<table border="1"> <thead> <tr> <th>INTERFACE</th> <th>SUBTRACT</th> </tr> </thead> </table>			INTERFACE	SUBTRACT
INTERFACE	SUBTRACT			
Tracking interface:				

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

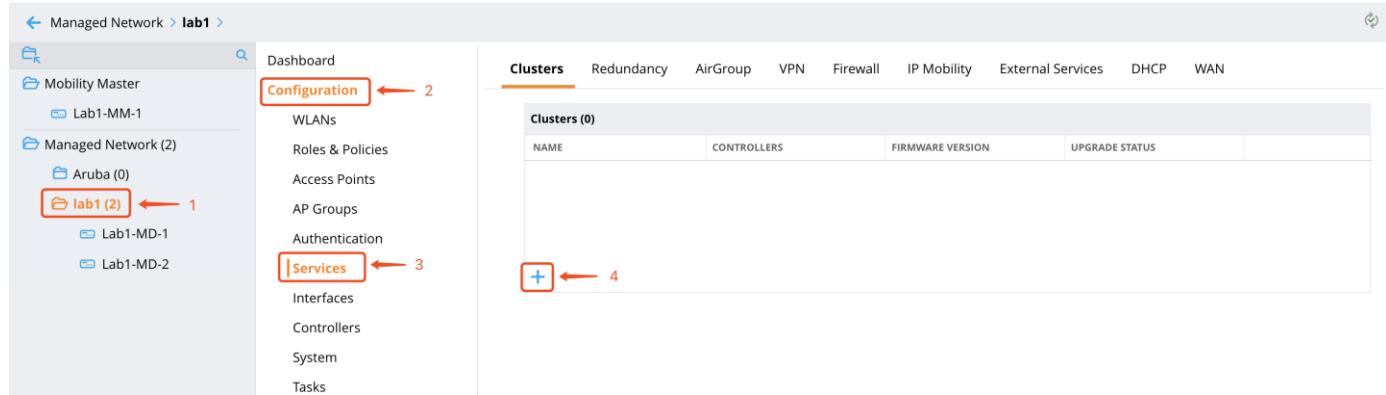
```
(LabX-MM-1) ^[labX] (config) #show configuration pending
```

第6步：保存配置

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

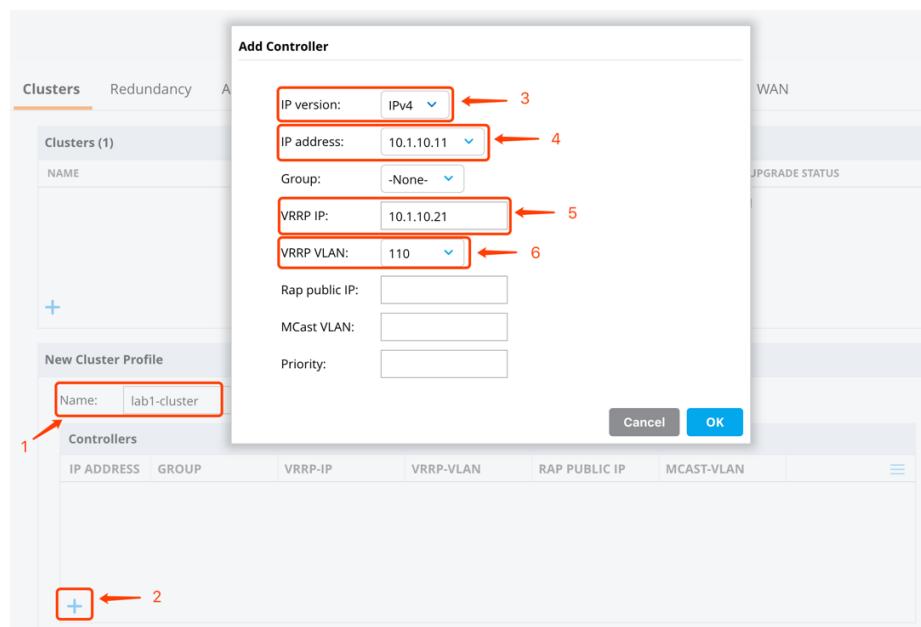
6.4 MM 配置 (GUI)

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])



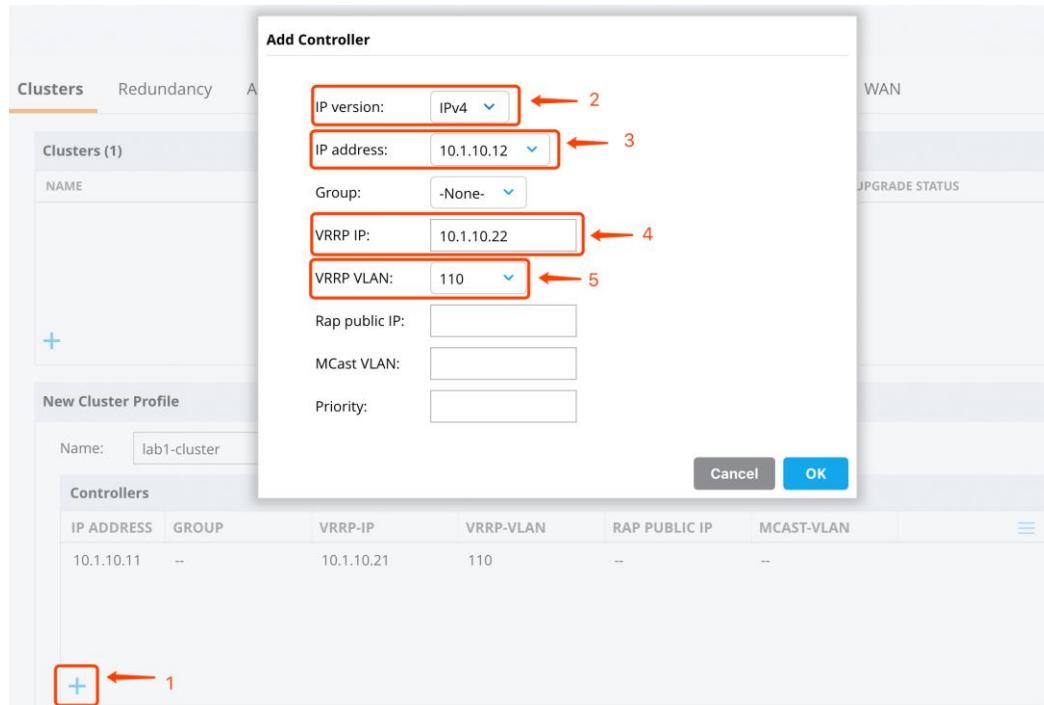
第2步: 在弹出的选项卡中, 添加 MD, 配置参数如下 (这里的 X 代表 lab 分组[1…6]) , 点击 OK。

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



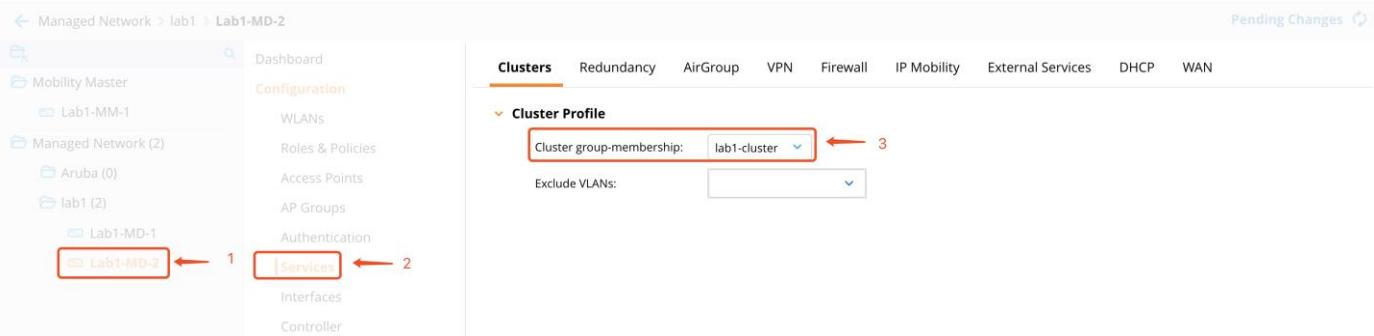
第3步：重复第2步，配置另外一台MD，参数如下（这里的X代表lab分组[1…6]），点击OK，并点击“Submit”

- ✓ 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，
我们刚刚的操作使得 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/STOP
peer	10.1.10.12	43	0	11	0	11	26	120	L3 Conn	2/ 2

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/ST
OP
-----
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

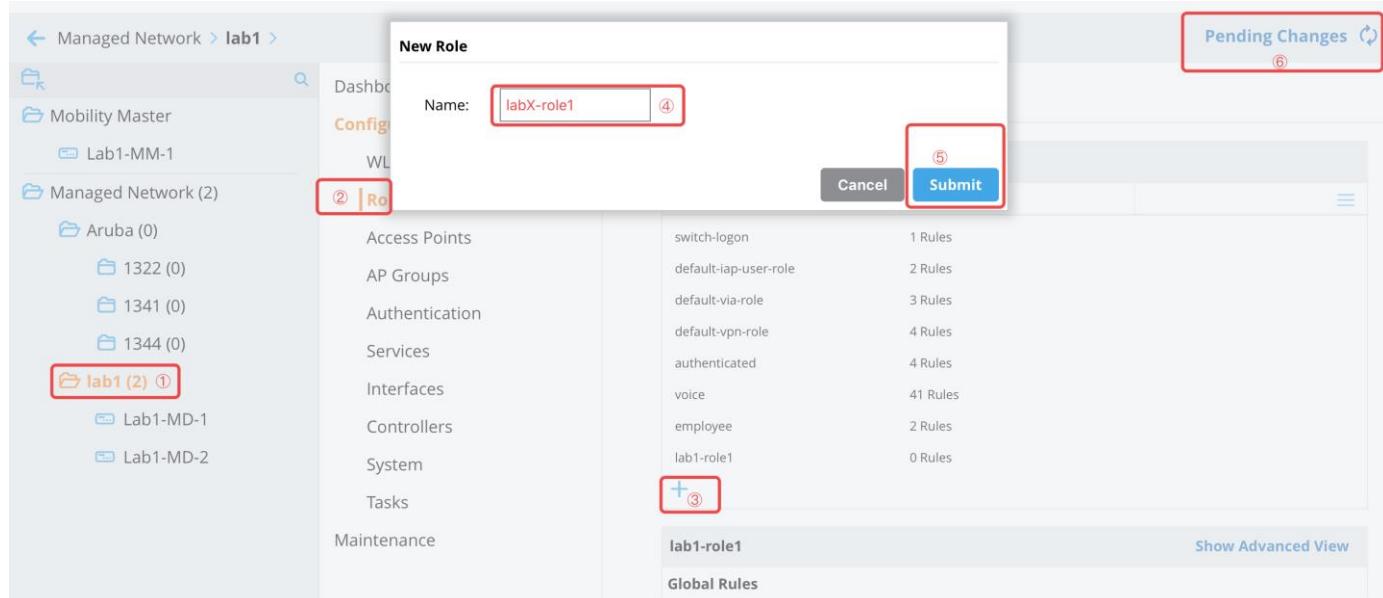
```
(LabX-MM-1) ^[labX] (config) #write memory
Saving Configuration...
Configuration Saved.
```

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。

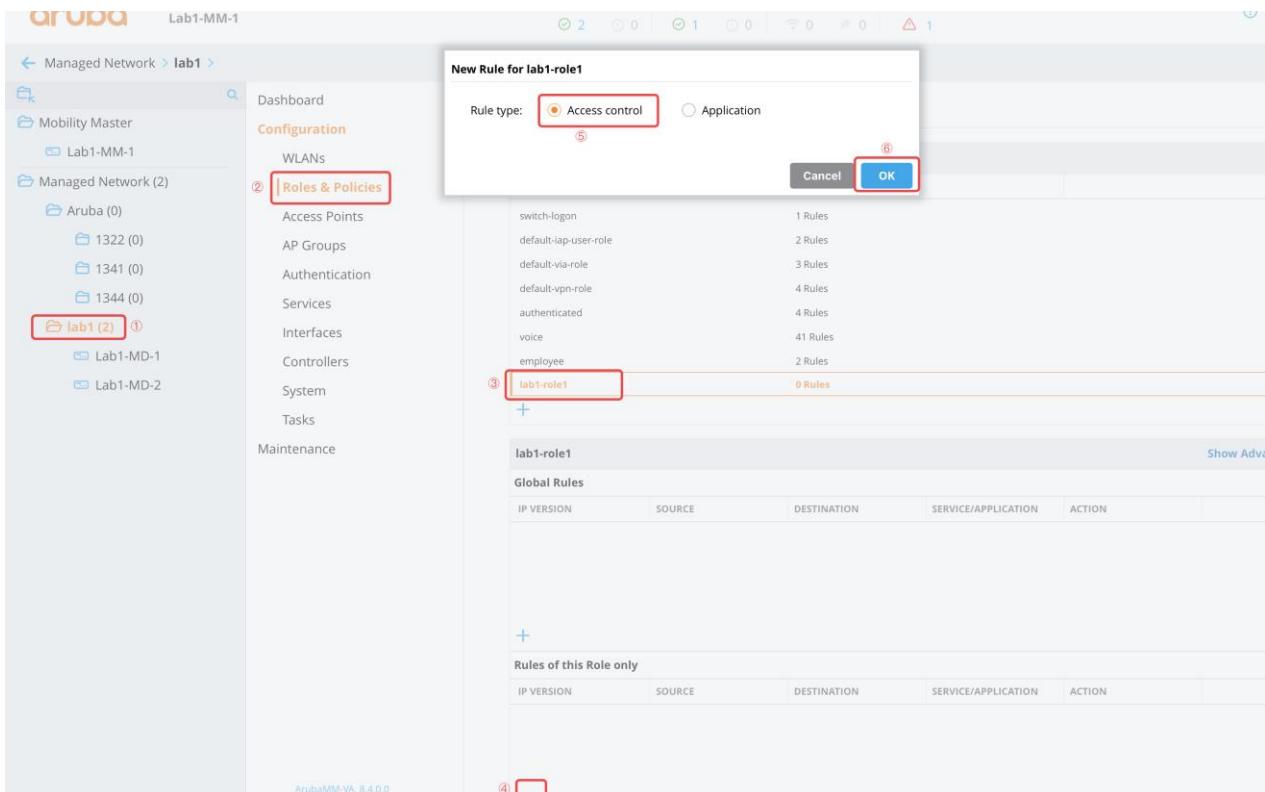
7.4 MM 配置 (GUI)

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。

lab1-role1 > New forwarding Rule

IP version:	IPv4
Source:	User
Destination:	Network
IPv4 address:	10.0.0.0
IPv4 netmask:	255.0.0.0
Service/app:	Any
Action:	Permit
TOS:	
Time range:	- None -
802.1p priority:	如有此类流量形成日志
Options:	<input type="checkbox"/> Log <input type="checkbox"/> Mirror <input type="checkbox"/> Blacklist <input type="checkbox"/> Disable scanning
Queue:	调整此类流量的优先级高低
<input type="button" value="Cancel"/> <input type="button" value="Submit"/>	

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。

The screenshot shows the ArubaOS8 interface for managing roles. On the left, the navigation tree shows 'Managed Network > lab1'. Under 'Configuration', 'WLANs' is expanded, showing 'Roles & Policies' (highlighted with a red box) and other options like 'Access Points', 'AP Groups', etc. In the 'Roles & Policies' section, 'lab1-role1' is selected (highlighted with a red box). At the top of the main panel, tabs for 'Roles', 'Policies', 'Applications', and 'Aliases' are visible, with 'Roles' being the active tab. Below the tabs, a table lists roles with their rule counts: switch-logon (1 Rules), default-lap-user-role (2 Rules), default-via-role (3 Rules), default-vpn-role (4 Rules), authenticated (4 Rules), voice (41 Rules), and employee (2 Rules). The 'lab1-role1' row is highlighted with a red box. Below the table, there are four tabs: 'lab1-role1', 'Policies', 'Bandwidth' (highlighted with a red box), and 'Captive Portal / More'. A note with a red arrow points to the 'More' tab, stating: '需要先在右侧选中Advanced View才可以看见Bandwidth, CP, More等菜单' (You need to select 'Advanced View' on the right side to see the Bandwidth, CP, More menus). To the right of the tabs, a button labeled 'Show Basic View' is shown. In the 'Bandwidth' section, there are two input fields: 'Total upstream limit' and 'Total downstream limit', each with a value of '2' and dropdown menus for 'Mbits' and 'Per User'. A note next to these fields says: '注意此处默认选项是Per Role, 如果填成2 Mbits Per Role, 则因为该角色的所有用户加起来是2M的上下行带宽' (Note: the default option here is 'Per Role'. If you enter '2 Mbits Per Role', because all users under this role add up to 2M, it will result in 2M of total bandwidth for both uplink and downlink). At the bottom right, there are 'Cancel' and 'Submit' buttons.

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。

The screenshot shows the Aruba Mobility Master interface under the 'Configuration' section. The left sidebar lists network components like Mobility Master, Managed Network, and AP Groups. The 'Roles & Policies' section is selected and highlighted with a red box. A new role, 'lab1-role1', is being created, also highlighted with a red box. The main pane displays the 'Roles' tab with a list of existing roles and their rule counts. The 'Network' tab is active, showing configuration options for the new role. A red box highlights the 'More' tab at the top right of the configuration pane.

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 >

Configuration

WLANs

Roles & Policies (highlighted)

Access Points

AP Groups

Authentication

Services

Interfaces

Controllers

System

Tasks

Maintenance

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

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

点 ACL 名称后下方会出现 ACL 明细

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]

General Admin AirWave CPSEC Certificates SNMP Logging **Profiles** More

All Profiles

- + RF Management
- + UCC
- Wireless LAN
 - + 802.11K
 - + 802.11r
 - + 802.1X Authentication
- AAA**
 - + NoAuthAAAProfile
 - + default
 - + default-dot1x

AAA Profile: New Profile

Profile name: lab1-psk-aaa
② 完成后请点击下方的蓝色submit

Initial role: **authenticated**

MAC Authentication Default Role: guest

802.1X Authentication Default Role: guest

Download Role from CPPM:

Set username from dhcp option 12:

L2 Authentication Fail Through:

Multiple Server Accounting:

User idle timeout: seconds

General Admin AirWave CPSEC Certificates SNMP Logging **Profiles** More

All Profiles

- lab1-psk-aaa
 - 802.1X Authentication**
 - + 802.1X Authentication Server Group
 - + MAC Authentication
 - + MAC Authentication Server Group
 - + RADIUS Accounting Server Group
 - + RFC 3576 server
 - + XML API server

802.1X Authentication Profile: default-psk

802.1X Authentication Profile: **default-psk** +

Max authentication failures: 0

Enforce Machine Authentication:

Machine Authentication: Default Machine Role: guest

Machine Authentication Cache Timeout: 24 hr(s)

Blacklist on Machine Authentication Failure:

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]

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controllers

General Admin AirWave CPSEC Certificates SNMP Logging **Profiles** More

All Profiles

- RADIUS Server
- + RFC 3576 Server
- + RRM IE
- + Radius Modifier
- SSID**
 - + default
 - + lab1-eduroam_ssid_pr...
 - + lab1-ssid-profile

SSID Profile: New Profile

SSID Profile: + ①

SSID Profile: New Profile

Profile name:	<input type="text" value="lab1-psk-ssid"/> 1	
Advanced		
SSID enable:	<input checked="" type="checkbox"/>	
ESSID:	<input type="text" value="lab1-psk"/> 2	
WPA Passphrase:		
Retype:		
Encryption:	<input type="checkbox"/> xSec <input type="checkbox"/> enhanced-open <input type="checkbox"/> wpa3-sae-aes <input type="checkbox"/> wpa3-aes-ccm-128 <input type="checkbox"/> wpa3-cnsa <input type="checkbox"/> wpa3-aes-gcm-256 <input type="checkbox"/>	<input type="checkbox"/> opensystem <input type="checkbox"/> static-wep <input type="checkbox"/> dynamic-wep <input type="checkbox"/> wpa-tkip <input type="checkbox"/> wpa-aes <input type="checkbox"/> wpa-psk-tkip <input type="checkbox"/> wpa-psk-aes <input type="checkbox"/>
Opemode transition:	<input checked="" type="checkbox"/>	
Enable Management Frame Protection (for WPA2 opmodes):	<input type="checkbox"/>	
Require Management Frame Protection (for WPA2 opmodes):	<input type="checkbox"/>	

5

Cancel **Submit**

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 <ul style="list-style-type: none"> + <input type="checkbox"/> Stateful 802.1X Authentication + <input type="checkbox"/> Stateful Kerberos Authentication + <input type="checkbox"/> Stateful NTLM Authentication + <input type="checkbox"/> TACACS Server + <input type="checkbox"/> TSM Report Request + <input type="checkbox"/> VIA Client WLAN + <input type="checkbox"/> VPN Authentication - <input type="checkbox"/> Virtual AP + <input type="checkbox"/> default 	Virtual AP profile: New Profile <p>Virtual AP profile: + ①</p>
---	---

Virtual AP profile: New Profile

Profile name: lab1-psk-vap
Virtual AP enable:
VLAN: 120
Forward mode: tunnel

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

AAA Profile: default

AAA Profile: default
Initial role: logon
MAC Auto-Provisioning: guest
802.1X Authentication: guest
Downloaded profile: guest
Set user profile: lab1-psk-aaa
L2 Authentication Fail Through:
Multiple Server Accounting:
User idle timeout:
Max IPv4 for wireless user: 2
RADIUS Roaming Accounting:

All Profiles

- + VPN Authentication
- Virtual AP
- + default
- + lab1-eduroam
- + lab1-psk-vap**
- + AAA**
- + Anyspot
- + 802.11K
- + SSID**
- + Hotspot 2.0
- + WMM Traffic management
- + lab1-test-vap
- + lab1-wlan

All Profiles

- ⊖ Virtual AP
- ⊕ 123123
- ⊖ default
- ⊕ 802.11k
- ⊖ AAA
- ⊖ lab2-psk-aaa
- ⊕ 802.1X Authentication**
- ⊕ 802.1X Authentication Server Group
- ⊕ MAC Authentication
- ⊕ MAC Authentication Server Group
- ⊕ RADIUS Accounting Server Group
- ⊕ RFC 3576 server

802.1X Authentication Profile: default-psk

802.1X Authentication Profile: **default-psk** +

Max authentication failures: 0

Enforce Machine Authentication:

Machine Authentication: Default Machine Role: guest

Machine Authentication Cache Timeout: 24

Blacklist on Machine Authentication Failure:

Machine Authentication: Default User Role: guest

Interval between Identity Requests: 5

Quiet Period after Failed Authentication: 30

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces
- Controllers
- System**
- Tasks
- Maintenance

General Admin AirWave CPSec Certificates SNMP Logging **Profiles** More

All Profiles

- ⊖ lab1-eduroam
- ⊖ lab1-psk-vap**
- ⊕ 802.11k
- ⊕ AAA
- ⊕ Anyspot
- ⊕ Hotspot 2.0
- ⊕ SSID**
- ⊕ WMM Traffic management
- ⊕ lab1-test-vap
- ⊕ lab1-vap
- ⊖ lab1-wlan-psk-van

SSID Profile

SSID Profile: **lab1-psk-ssid**

SSID enable:

ESSID: lab1-psk

WPA Passphrase:

Retype:

x5Sec

enhanced-open

wpa3-sae-aes

wpa3-aes-ccm-128

Encryption:

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]

The screenshot shows two overlapping windows. The top window is titled "Add Allowed VLAN" with fields for "VLAN" (set to 1,110,120) and "Trust" (set to Trusted). A note in red says: "③将1,x10,x20分别选择上来并且OK, 然后submit" (Select 1, x10, x20 and click OK, then submit). The bottom window is titled "GE-0/0/0" and shows network settings like Admin state, Speed, Duplex, PoE, Trust, Policy, Mode, Native VLAN (set to 1), and Allowed VLANs. The "Allowed VLANs" section has a dropdown set to "Allow specified VLANs" (marked with ①) and a note in red: "选择为指定VLAN通过" (Select for specified VLAN passage). It lists one entry: VLAN 1,110,120 with Trust status Trusted. A red box highlights this list, and a red arrow points to the "+" button at the bottom left of the list (marked with ②). The bottom right of the window has "Cancel" and "Submit" buttons, with "Submit" marked with ④.

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]

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

NOTE 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
```

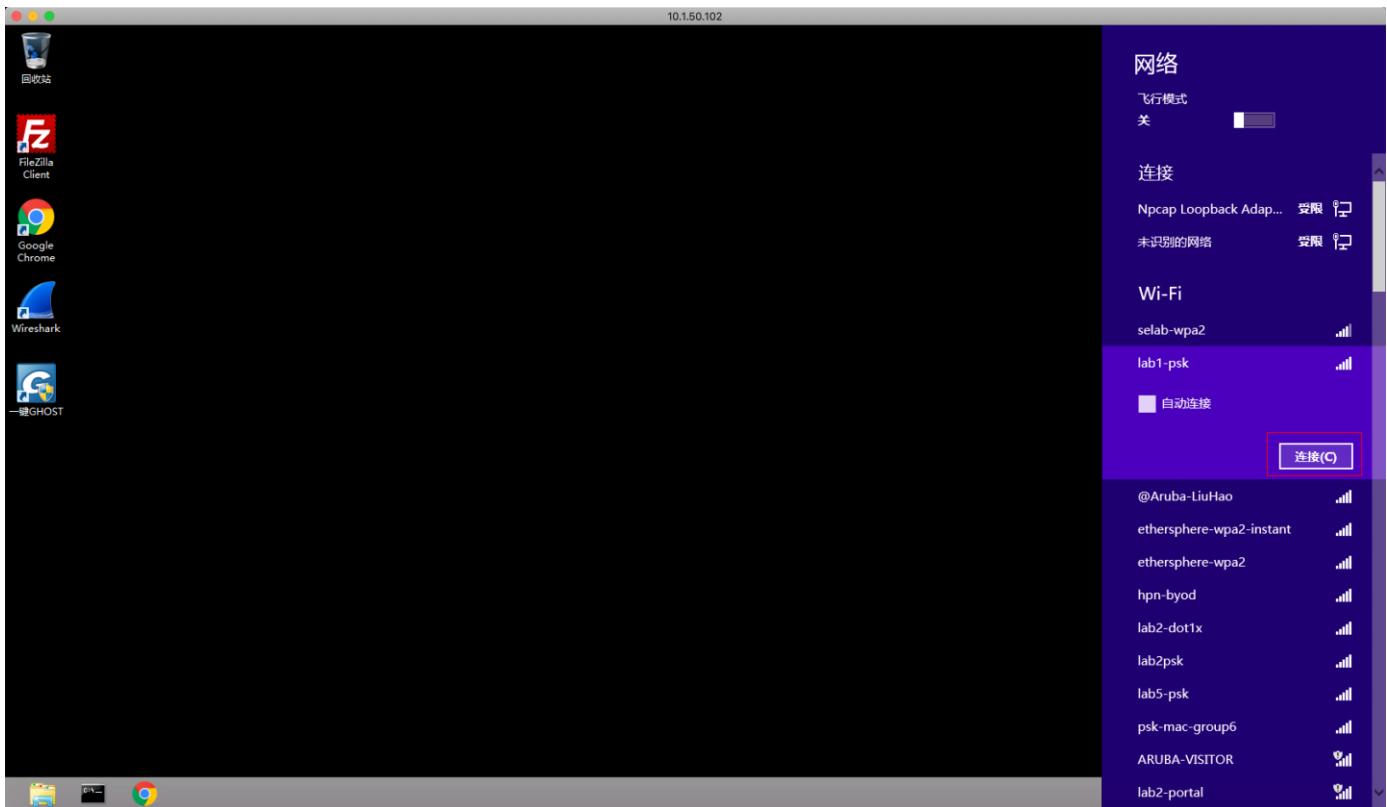
ESSID Summary

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 Profile	MAC Type	Name User	Current switch Type	Role Type	Auth	AP name	Roaming	Essid	Bssid	Phy
10.1.20.100 10 a-VHT	7c:7a:91:46:52:b7 lab1-psk-aaa		10.1.10.11 N/A	authenticated WIRELESS		94:b4:0f:c1:3f:e0	Wireless	lab1-psk	94:b4:0f:93:fe:	

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 ppm，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 ppm 添加在组内。

NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SERVER RULES
default	1	--	--	1
internal	1	--	--	1

NAME	TYPE	IP ADDRESS / HOSTNAME	SERVER GROUP
Internal	--	--	default internal

New Server for CPPM

Add existing server Add new server

Name:

IP address / hostname:

Type:

Add Server Group

Name: lab1-sg
④在此输入labX-sg

Cancel Submit
⑤

All Servers 2

NAME	TYPE	IP ADDRESS / HOSTNAME	SERVER GROUP
cppm	RADIUS	10.1.50.41	-

Internal

Server Options

Name: cppm
IP address / hostname: 10.0.50.41
Auth port: 1812
Acct port: 1813
Shared key: ① 在此两行输入aruba123然后确认.
Retype key: ②

Cancel

Auth Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

Server Groups 3

NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SERVER RULES
default	1	--	--	1
internal	1	--	--	1
lab1-sg	0	--	--	0

选中lab1-sg出来的窗口下方点击+

Server Group > lab1-sg Servers Options Server Rules

Drag rows to re-order

+ +

New Server for lab1-sg

① Add existing server ② Add new server

③ 选中cppm, 提交, 并保存配置

cppm Internal

Cancel Submit

Pending Changes

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。

The screenshot shows the ArubaOS8 web interface. On the left, the navigation tree is visible with 'lab1' selected. In the center, a modal window titled 'New Rule for macfailed' is open. The 'Rule type:' section has 'Access control' selected. A red arrow points to the 'Access control' radio button with the text '选择 Access control'. Below the modal, a table lists existing roles: default-vpn-role, authenticated, voice, employee, lab1-role1, leader-role, employee-role, and macfailed. A red box highlights the 'macfailed' row. Another red arrow points to the '+ Create New Role' button below the table with the text '创建一个角色叫 macfailed, 用于 mac 认证失败的情况'.

At the bottom of the main interface, a red box highlights the 'macfailed > New forwarding Rule' link. A red arrow points to it with the text '为新创建的macfailed角色创建规则'.

In the 'macfailed > New forwarding Rule' configuration window, several fields are set: IP version: IPv4, Source: Any, Destination: Any, Service/app: Any, Action: Deny (highlighted with a red box), TOS: - None -, Time range: - None -. A red arrow points to the 'Action: Deny' dropdown with the text '修改规则为默认全拒绝'.

At the bottom right of the configuration window, there are 'Cancel' and 'Submit' buttons. A red arrow points to the 'Submit' button.

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。

The screenshot shows the ArubaOS8 configuration interface. On the left, the navigation menu is visible with sections like Dashboard, Configuration, WLANs, Roles & Policies, Access Points, AP Groups, Authentication, Services, Interfaces, Controllers, System (which is selected), Tasks, and Maintenance. The main panel has tabs for General, Admin, AirWave, CPSec, Certificates, SNMP, Logging, Profiles (which is selected), and More. The 'Profiles' tab is active, and the 'All Profiles' section is displayed. Under 'All Profiles', there is a list of profiles: Wireless LAN, 802.11K, 802.11r, 802.1X Authentication, AAA (highlighted with an orange box), NoAuthAAAProfile, default, default-dot1x, default-dot1x-psk, default-iap-aaa-profile..., default-mac-auth, default-open, default-tunneled-use..., and default-xml-api. The 'AAA Profile: New Profile' dialog is open on the right, titled '新建一个AAA Profile'. It contains the following fields:

- Profile name:** lab1-mac-aaa (highlighted with a red arrow)
- Initial role:** mac认证失败的角色 (highlighted with a red arrow) → macfailed
- MAC Authentication Default Role:** mac认证成功的角色 (highlighted with a red arrow) → authenticated
- 802.1X Authentication Default Role:** guest
- Download Role from CPPM:**
- Set username from dhcp option 12:**
- L2 Authentication Fail Through:**
- Multiple Server Accounting:**
- User idle timeout:** seconds
- Max IPv4 for wireless user:** 2
- RADIUS Roaming Accounting:**
- RADIUS Interim Accounting:** 开启持续计费报文 (highlighted with a red arrow) →
- RADIUS Acct-Session-Id In Access-Request:**
- User derivation rules:** -None-
- Wired to Wireless Roaming:**
- Reauthenticate wired user on VLAN change:**
- Device Type Classification:**
- Enforce DHCP:**
- PAN Firewall Integration:**

The screenshot shows two separate configuration pages from the ArubaOS8 interface, both titled "Profiles".

Top Configuration:

- Left Sidebar:** Includes links for Dashboard, Configuration (WLANs, Roles & Policies, Access Points, AP Groups, Authentication, Services, Interfaces, Controllers), System (Tasks, Maintenance), and a Pending Changes button.
- Right Content:** Shows the "All Profiles" list with items like default-dot1x-psk, default-iap-aaa-prof..., default-mac-auth, default-open, default-tunneled-use..., default-xml-api, and lab1-mac-aaa. The "MAC Authentication" item is highlighted with a red box.
- Details View:** A modal for "MAC Authentication Profile: default" shows settings for Delimiter (none), Case (lower), Max Authentication failures (0), Reauthentication (unchecked), Reauthentication Interval (86400 sec), and Use Server provided Reauthentication Interval (unchecked). The "default" profile is selected in the dropdown.

Bottom Configuration:

- Left Sidebar:** Same as the top one.
- Right Content:** Shows the "All Profiles" list with the same items as the top page. The "MAC Authentication Server Group" item is highlighted with a red box.
- Details View:** A modal for "Server Group: lab1-sg" shows the "Server Group: lab1-sg" dropdown selected. It also includes options for Fail Through and Load Balance.

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

General Admin AirWave CPSec Certificates SNMP Logging **Profiles** More

All Profiles	
<input type="button" value="⊕"/>	<input type="checkbox"/> MAC Authentication
<input type="button" value="⊕"/>	<input type="checkbox"/> Management Authentication
<input type="button" value="⊕"/>	<input type="checkbox"/> RADIUS Server
<input type="button" value="⊕"/>	<input type="checkbox"/> RFC 3576 Server
<input type="button" value="⊕"/>	<input type="checkbox"/> RRM IE
<input type="button" value="⊕"/>	<input type="checkbox"/> Radius Modifier
<input type="button" value="⊖"/>	<input type="checkbox"/> SSID
<input type="button" value="⊕"/>	<input type="checkbox"/> default
<input type="button" value="⊕"/>	<input type="checkbox"/> lab1-psk-ssid
<input type="button" value="⊕"/>	<input type="checkbox"/> SSO
<input type="button" value="⊕"/>	<input type="checkbox"/> Server Group
<input type="button" value="⊕"/>	<input type="checkbox"/> Stateful 802.1X Authentication
<input type="button" value="⊕"/>	<input type="checkbox"/> Stateful Kerberos Authentication

SSID Profile: New Profile

Profile name:	<input type="text" value="lab1-mac-ssid"/> labX-mac-ssid	
SSID enable:	<input checked="" type="checkbox"/>	
ESSID:	<input type="text" value="labX-mac"/> lab1-mac	
WPA Passphrase:	WPA passphrase:	
	<input type="text"/>	
	Retype:	
	<input type="checkbox"/> xSec	<input type="checkbox"/> dy
	<input type="checkbox"/> enhanced-open	<input type="checkbox"/> w
	<input type="checkbox"/> wpa3-sae-aes	<input type="checkbox"/> w
	<input type="checkbox"/> wpa3-aes-ccm-128	<input type="checkbox"/> w
	<input type="checkbox"/> wpa3-cnsa	<input type="checkbox"/> w
	<input type="checkbox"/> opensystem	<input type="checkbox"/> w
	static-wep	<input type="checkbox"/> w
Encryption:	<input checked="" type="checkbox"/>	
Opmode transition:	<input checked="" type="checkbox"/>	

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.

General Admin AirWave CPSec Certificates SNMP Logging **Profiles** More

All Profiles	
<input type="button" value="⊕"/>	<input type="checkbox"/> SSO
<input type="button" value="⊕"/>	<input type="checkbox"/> Server Group
<input type="button" value="⊕"/>	<input type="checkbox"/> Stateful 802.1X Authentication
<input type="button" value="⊕"/>	<input type="checkbox"/> Stateful Kerberos Authentication
<input type="button" value="⊕"/>	<input type="checkbox"/> Stateful NTLM Authentication
<input type="button" value="⊕"/>	<input type="checkbox"/> TACACS Server
<input type="button" value="⊕"/>	<input type="checkbox"/> TSM Report Request
<input type="button" value="⊕"/>	<input type="checkbox"/> VIA Client WLAN
<input type="button" value="⊕"/>	<input type="checkbox"/> VPN Authentication
<input type="button" value="⊖"/>	<input type="checkbox"/> Virtual AP
<input type="button" value="⊕"/>	<input type="checkbox"/> default
<input type="button" value="⊕"/>	<input type="checkbox"/> lab1-psk-vap
<input type="button" value="⊕"/>	<input type="checkbox"/> WISPr Authentication

Virtual AP profile: New Profile

Profile name:	<input type="text" value="lab1-mac-vap"/> labX-mac-vap
General	
Virtual AP enable:	<input checked="" type="checkbox"/>
VLAN:	<input type="text" value="120"/> X20
Forward mode:	<input type="text" value="tunnel"/>
> RF	
> Advanced	
> Broadcast/Multicast	

The screenshots show the ArubaOS8 configuration interface for a network named 'lab1'. The left sidebar lists network components: Mobility Master, Managed Network (2), and lab1 (2) which includes Lab1-MM-1, Lab1-MD-1, and Lab1-MD-2.

Screenshot 1: AAA Profile Configuration

- Left Panel:** Shows the 'Configuration' section with 'WLANS' selected. Under 'WLANS', 'Virtual AP' is highlighted with a red box. Below it, 'lab1-mac-vap' is also highlighted with a red box. A note in red text says: '选中labX-mac-vap后，要将AAA和SSID内的Profile换过来' (After selecting labX-mac-vap, swap the profiles in AAA and SSID).
- Right Panel:** The 'Profiles' tab is selected. The 'AAA Profile: lab1-mac-aaa' section shows 'lab1-mac-aaa' selected in a dropdown. Other options include macfailed, authenticated, and guest.

Screenshot 2: SSID Profile Configuration

- Left Panel:** Shows the 'Configuration' section with 'WLANS' selected. Under 'WLANS', 'Virtual AP' is highlighted with a red box. Below it, 'lab1-mac-vap' is also highlighted with a red box. A note in red text says: '选中labX-mac-vap后，要将AAA和SSID内的Profile换过来' (After selecting labX-mac-vap, swap the profiles in AAA and SSID).
- Right Panel:** The 'Profiles' tab is selected. The 'SSID Profile: lab1-mac-ssid' section shows 'lab1-mac-ssid' selected in a dropdown. Other options include lab1-psk-vap and lab1-psk-wan.

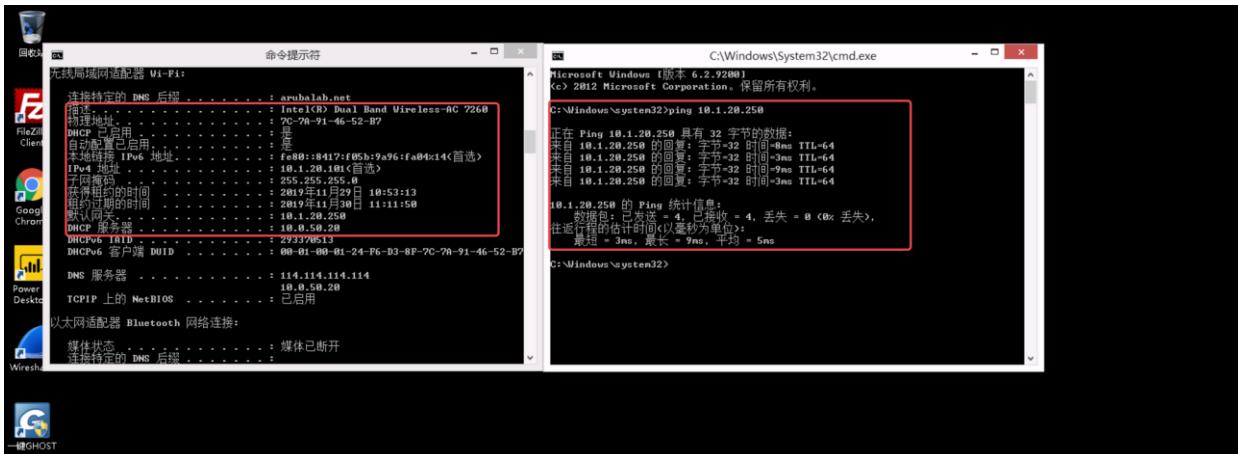
第6步: 在 AP-GROUP labX-group 下, 选择 WLANS, 添加刚做好的 VAP, 然后 submit 并点击右上角的 pending changes 确认配置, AP 即放出 labX-mac 信号可供测试

The screenshot shows the Aruba Network Configuration interface. On the left, there's a sidebar with 'Managed Network > lab1' selected. The main area has tabs for 'Dashboard', 'Configuration', 'WLANS', 'Roles & Policies', 'Access Points', 'AP Group' (which is selected and highlighted in red), 'Authentication', 'Services', 'Interfaces', 'Controllers', 'System', 'Tasks', and 'Maintenance'. In the 'AP Group' section, there's a table with columns 'NAME', 'AP GROUP', 'AIRTIME LIMIT (%)', 'PER-USER LIMIT (KBPS)', and 'PER-RADIO LIMIT (KBPS)'. One row is visible: 'NAME' is 'lab1-psk-vap', 'AP GROUP' is 'lab1-group', and other fields are blank. Below the table is a large red '+' button. To the right of the table is a 'Select WLAN' dialog box. It has a list of 'Virtual-ap': 'default' and 'lab1-mac-vap' (which is checked). At the bottom of the dialog are 'Cancel' and 'Submit' buttons. A red arrow points from the 'AP GROUP' tab to the '+' button. Another red arrow points from the 'AP GROUP' tab to the 'Select WLAN' dialog. A third red arrow points from the 'Select WLAN' dialog to the 'Submit' button.

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。

The screenshot shows a Windows desktop environment. On the left, there's a taskbar with icons for FileZilla Client, Google Chrome, Power BI Desktop, Wireshark, and GHOST. The main window is a network settings screen. It shows a '飞行模式' (Flight Mode) switch set to '关' (Off). Under '连接' (Connections), it lists 'Npcap Loopback Adapter' and '未识别的网络' (Unknown Network), both with '受限' (Restricted) status. In the 'Wi-Fi' section, a list of available networks is shown. The network 'lab1-mac' is highlighted with a red box and a red arrow pointing to its '连接(C)' (Connect) button. Other networks listed include 'selab-wpa2', 'lab1-psk 2', 'lab2-cy', '000-employee', '@Aruba-LiuHao', 'ethersphere-wpa2', 'hpn-byod', and 'lab2-lab2-portal'. The '自动连接' (Automatically connect) checkbox is also highlighted with a red box and a red arrow.



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 Phy	MAC Profile	Name Type	Current switch User Type	Role	Auth AP name	Roaming	Essid	Bssid
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:c1:3f:e0

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的来的 MAC 地址，是否击中了正确的策略名称，是否被 Accept 了。

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	10.1.50.41	RADIUS	a49b4f4419fa	Lab1-Mac	REJECT	2019/11/29 11:09:49
2.	10.1.50.41	RADIUS	7c7a914652b7	Lab1-Mac	ACCEPT	2019/11/29 10:49:54

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

The screenshot shows two views of the ArubaOS8 configuration interface for a managed network named 'Lab1'. The left sidebar lists network components: Mobility Master (Lab1-MM-1), Managed Network (2) (Aruba (0), China (0), US (0), Lab1 (2), Lab1-MD-1, Lab1-MD-2). The 'System' tab is selected.

Top View (Profiles Tab):

- All Profiles:** Shows a list of profiles including Other Profiles, QoS, RF Management, UCC, Wireless LAN, 802.11K, 802.11r, 802.1X Authentication, and AAA. The 'Wireless LAN' section is highlighted with a red box.
- AAA Profile: New Profile:**
 - Profile name:** lab1-1x-aaa (highlighted with a red box)
 - Initial role:** logon
 - MAC Authentication Default Role:** guest
 - 802.1X Authentication Default Role:** authenticated (highlighted with a red box)
 - Download Role from CPPM:** (checkbox)
 - Set username from dhcp option 12:** (checkbox)
 - L2 Authentication Fail Through:** (checkbox)
 - Multiple Server Accounting:** (checkbox)
 - User idle timeout:** (input field set to 300)
 - Max IPv4 for wireless user:** (input field set to 2)
 - RADIUS Roaming Accounting:** (checkbox)
 - RADIUS Interim Accounting:** (checkbox checked with a red arrow pointing to it)
 - RADIUS Acct-Session-Id In Access-Request:** (checkbox)
 - User derivation rules:** -None-
 - Wired to Wireless Roaming:** (checkbox checked with a red arrow pointing to it)
 - Reauthenticate wired user on VLAN change:** (checkbox)
 - Device Type Classification:** (checkbox checked with a red arrow pointing to it)

Pending Changes button is visible at the bottom right.

Bottom View (Profiles Tab):

- All Profiles:** Shows a list of profiles including AAA, 802.1X Authentication, 802.1X Authentication Server Group, MAC Authentication, and MAC Authentication Server Group. The 'lab1-1x-aaa' profile is selected and highlighted with a red box.
- 802.1X Authentication Profile: default:**
 - 802.1X Authentication Profile:** default (highlighted with a red box)
 - Max authentication failures:** 0
 - Enforce Machine Authentication:** guest
 - Machine Authentication Cache Timeout:** 24
 - Blacklist on Machine Authentication Failure:** (checkbox)
 - Machine Authentication: Default User Role:** guest
 - Interval between Identity Requests:** 5
 - Quiet Period after Failed Authentication:** 30
 - Reauthentication Interval:** 86400
 - Use Server provided Reauthentication Interval:** (checkbox)
 - Use the termination-action attribute from the Server:** (checkbox)
 - Multicast Key Rotation Time Interval:** 1800

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

Managed Network > lab1 >

Profiles

SSID Profile: New Profile

- Profile name: lab1-1x-ssid
- SSID enable:
- ESSID: labX-1x
- WPA Passphrase:
- Retype:
- Encryption: wpa2-aes (selected)
- Opmode transition:
- Enable Management Frame Protection:
- Require Management Frame Protection:
- DTIM Interval: 1
- 802.11a Basic Rates: 6, 9, 12, 18, 48, 54
- 802.11a Transmit Rates: 6, 9, 12, 18

ArubaOS8.0.0.0

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

Managed Network > lab1 >

Profiles

Virtual AP profile: New Profile

- Profile name: lab1-1x-vap
- Virtual AP enable:
- VLAN: 120
- Forward mode:

All Profiles

- SSID
- SSO
- Server Group
- Stateful 802.1X Authentication
- Stateful Kerberos Authentication
- Stateful NTLM Authentication
- TACACS Server
- TSM Report Request
- VIA Client WLAN
- VPN Authentication
- Virtual AP
- default
- lab1-mac-vap
- lab1-psk-vap

The screenshots show the ArubaOS8 configuration interface for a network named 'lab1'. The left sidebar shows the network structure with 'lab1 (2)' selected. The main area is under the 'Configuration' tab.

AAA Profile: lab1-1x-aaa

- AAA Profile:** lab1-1x-aaa (highlighted)
- Initial role:** logon
- MAC Authentication Default Role:** guest
- 802.1X Authentication Default Role:** authenticated
- Download Role from CPPM:** (checkbox)
- Set username from dhcp option 12:** (checkbox)
- L2 Authentication Fail Through:** (checkbox)
- Multiple Server Accounting:** (checkbox)
- User idle timeout:** (input field: 2 seconds)
- Max IPv4 for wireless user:** (input field: 2)
- RADIUS Roaming Accounting:** (checkbox)
- RADIUS Interim Accounting:** (checkbox)
- RADIUS Acct-Session-Id In Access-Request:** (checkbox)
- User derivation rules:** (dropdown: -None-)

SSID Profile: lab1-1x-ssid

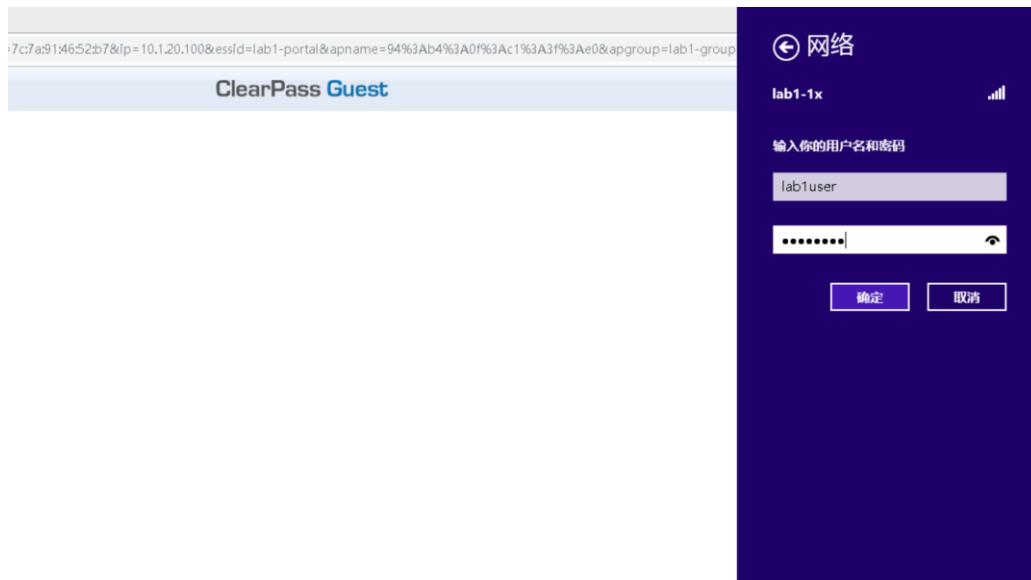
- SSID Profile:** lab1-1x-ssid (highlighted)
- SSID enable:** (checkbox checked)
- ESSID:** lab1-1x
- WPA Passphrase:** (input field)
- WPA passphrase:** (input field)
- Retype:** (checkboxes: xSec, enhanced-open, wpa3-sae-aes, wpa3-aes-ccm-128, wpa3-cnsa, opensystem, static-wep) (checkbox checked)
- Encryption:** (checkbox checked)
- Opmode transition:** (checkbox checked)
- Enable Management Frame Protection:** (checkbox checked)

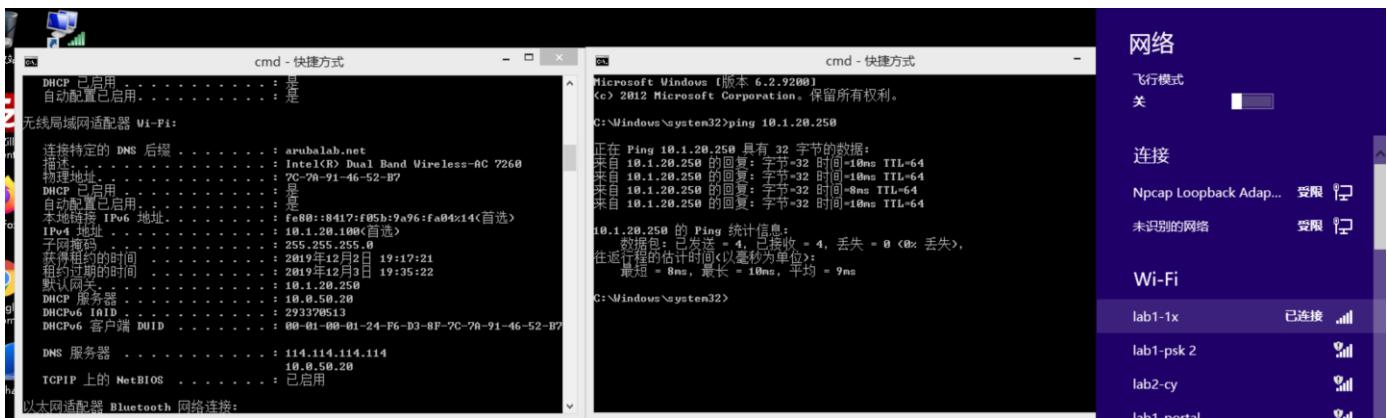
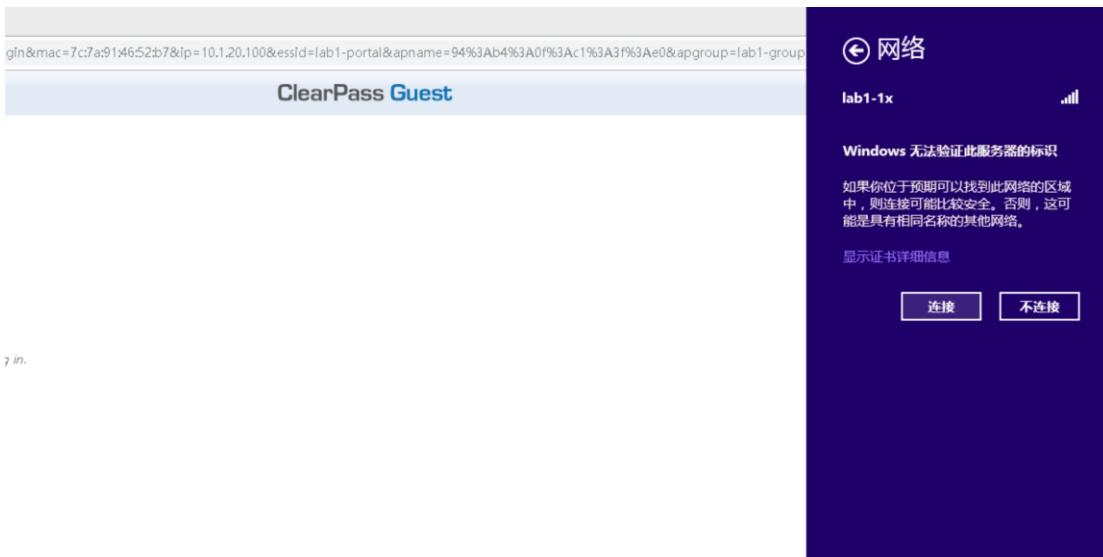
第5步: 在现有的 AP-GROUP labX-group 下, 调用上述 VAP, 放出信号后, 可以开始测试。

NAME	APs	WLANs	AIRTIME LIMIT (%)	PER-USER LIMIT (KBPS)	PER-RADIO LIMIT (KBPS)
lab1-psk-vap	lab1-group		--	--	--
lab1-mac-vap	lab1-group		--	--	--
lab1-vap-profile	lab1-group		--	--	--

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。





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 Phy	MAC Profile	Name Type	Current switch User Type	Role	Auth	AP name	Roaming	Essid	Bssid
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	
				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的 1x 认证，是否击中了正确的策略名称，是否被 Accept 了。

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	10.1.50.41	RADIUS	lab1user	Lab1-1x	ACCEPT	2019/12/02 20:11:08

NOTE 可在过滤器 username 中过滤查询，便于查看结果。

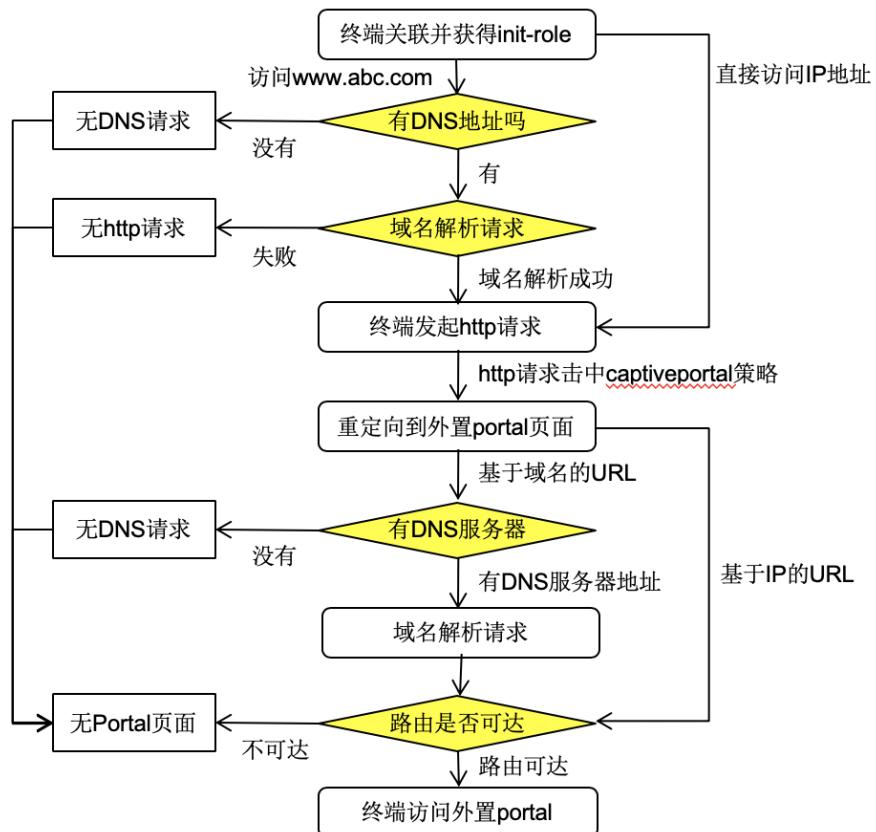
11 外置 PORTAL 认证

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
```

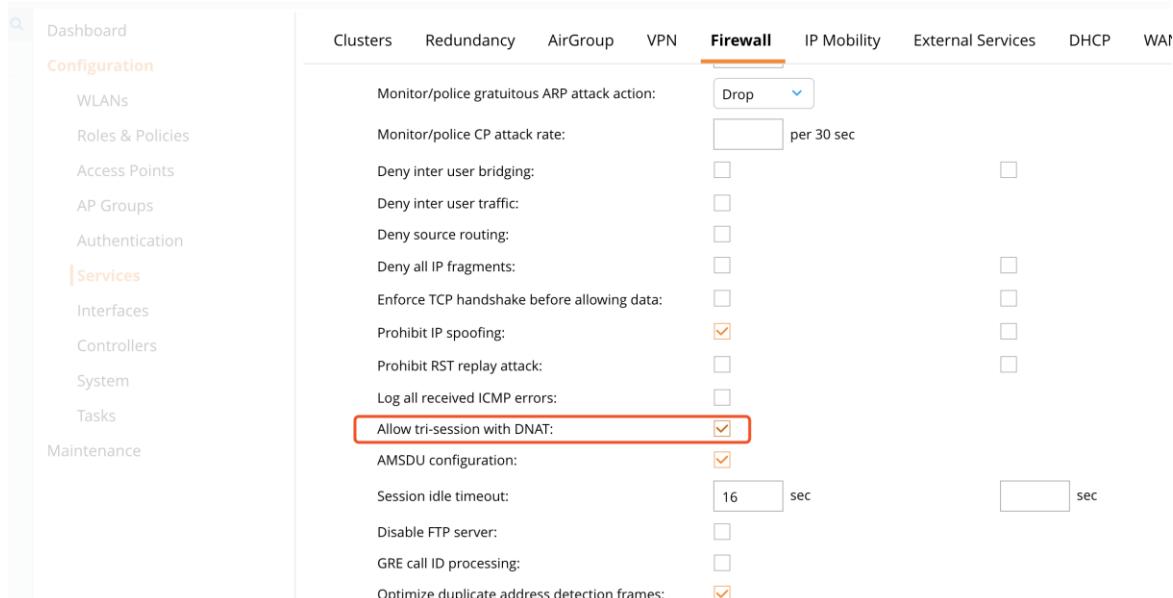
Saving Configuration...

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

Auth Servers

NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SERVER RULES
default	1	--	--	1
internal	1	--	--	1

All Servers

NAME	TYPE	IP ADDRESS / HOSTNAME	SERVER GROUP
Internal	--	--	default internal

第4步：添加 Server Group

Add Server Group

Name:	lab1-cppm
-------	-----------

Cancel **Submit**

第5步：添加 Server

internal	1	--	--	1
lab1-cppm	0	--	--	0

All Servers

NAME	TYPE	IP ADDRESS / HOSTNAME	SERVER GROUP
Internal	--	--	default internal

New Server for CPPM

Add existing server Add new server

Name:	cppm
IP address / hostname:	10.0.50.41
Type:	RADIUS

Cancel **Submit**

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

The screenshot shows the 'All Servers' table with one entry: 'lab1-cppm' (TYPE: RADIUS, IP ADDRESS / HOSTNAME: 10.1.50.41). Below it is the 'Server Options' configuration dialog for 'lab1-cppm'. The configuration fields are as follows:

Name:	lab1-cppm
IP address / hostname:	10.0.50.41
Auth port:	1812
Acct port:	1813
Shared key:
Retype key:

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

The screenshot shows the 'L3 Authentication' tab selected in the navigation bar. On the left, there is a sidebar with various configuration options. The main panel displays a list of authentication profiles under 'L3 Authentication'. A 'Captive Portal Authentication: New Profile' dialog is open on the right, containing a single field: 'Captive Portal Authentication: +'. The '+' button is highlighted with a red box.

2) 填写 Captive Portal Authentication Profile 名称

Captive Portal Authentication Profile: New Profile

Profile name:	<input type="text" value="Lab1-Portalprofile"/>
Default Role:	<input type="text" value="guest"/>
Default Guest Role:	<input type="text" value="guest"/>
Redirect Pause:	<input type="text" value="10"/> sec
User Login:	<input checked="" type="checkbox"/>
Guest Login:	<input type="checkbox"/>
Logout popup window:	<input checked="" type="checkbox"/>
Use HTTP for authentication:	<input type="checkbox"/>

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。

Login page:	<input type="text" value="http://10.0.50.41"/>
Welcome page:	<input type="text" value="/auth/welcome.htm"/>
Show Welcome Page:	<input checked="" type="checkbox"/>

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

The screenshot shows the 'L3 Authentication' tab selected in the top navigation bar. On the left, there's a tree view with 'Captive Portal Authentication', 'Lab1-Portalprofile', 'Server Group' (which is selected and highlighted in orange), 'default', and 'Stateful Kerberos Authentication'. On the right, under 'Server Group: lab1-cppm', there are dropdown menus for 'Server Group' (set to 'lab1-cppm'), 'Fail Through' (unchecked), and 'Load Balance' (unchecked).

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

The screenshot shows the 'Configuration' menu on the left with 'Roles & Policies' selected. The main area has tabs for 'Roles' (highlighted with a red box), 'Policies', 'Applications', and 'Aliases'. The 'Roles' table lists 13 roles with columns for 'NAME' and 'RULES': logon (32 Rules), guest (11 Rules), ap-role (35 Rules), stateful-dot1x (0 Rules), guest-logon (27 Rules), sys-ap-role (23 Rules), sys-switch-role (24 Rules), and switch-logon (1 Rules). A large blue plus sign button at the bottom left of the table is highlighted with a red box.

NAME	RULES
logon	32 Rules
guest	11 Rules
ap-role	35 Rules
stateful-dot1x	0 Rules
guest-logon	27 Rules
sys-ap-role	23 Rules
sys-switch-role	24 Rules
switch-logon	1 Rules

- 2) 新建 initial role 名称

New Role

Name: portal-initial

Cancel Submit

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

voice 41 Rules

portal-initial 0 Rules

portal-initial

Show Advanced View

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	
------------	--------	-------------	---------------------	--------	--

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

admin ^

Preferences

Preferences

Show advanced profiles:

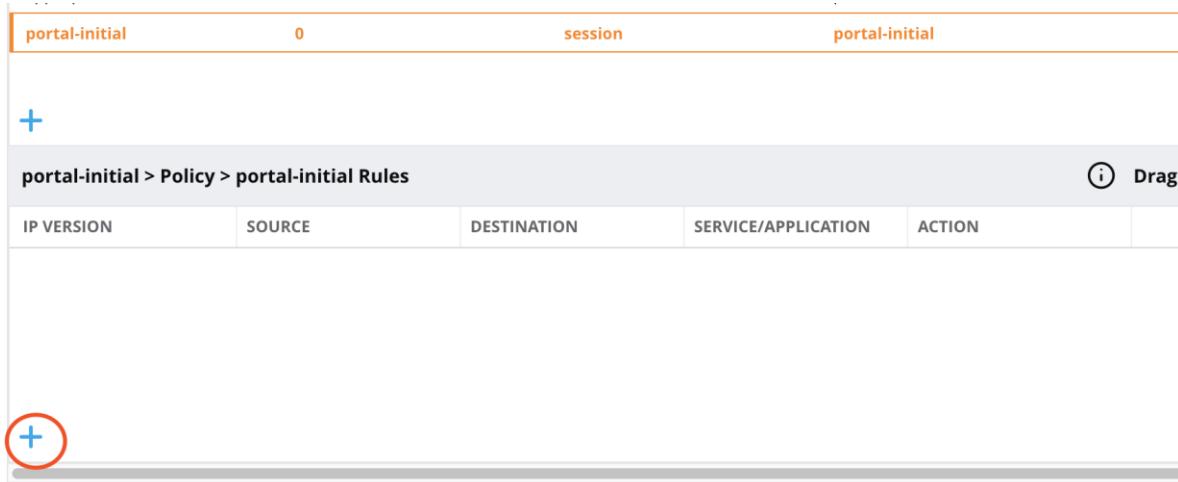
4) 新建 role 默认策略如下:

portal-initial 0 Rules

portal-initial Policies Bandwidth Captive Portal More Show Basic View

NAME	RULES COUNT	TYPE	POLICY USAGE	
global-sacl	0	session	logon, guest, ap-role, stateful-d...	
apprf-portal-initial-sacl	0	session	portal-initial	
portal-initial	0	session	portal-initial	

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”

New Rule for portal-initial

Rule type: Access control Application

Cancel **OK**

7) 添加外置 Portal 服务器地址，选择 permit 并提交

portal-initial > portal-initial > New forwarding Rule

IP version:	IPv4
Source:	User
Destination:	Host
IPv4 address:	10.0.50.41
Service/app:	Any
Action:	Permit
TOS:	

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

New Policy

Add an existing policy Create a new policy

Policy type:

Session

Policy name:

logon-control

Position:

Cancel

Submit

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

New Policy

Add an existing policy Create a new policy

Policy type:

Session

Policy name:

captiveportal

Position:

Cancel

Submit

10) 完成 portal initial role 策略如下，点击提交。

portal-initial		14 Rules		
		+		
portal-initial	Policies	Bandwidth	Captive Portal	More
apprf-portal-initial-sacl	0		session	portal-initial
portal-initial	1		session	portal-initial
logon-control	7		session	logon, guest-logon, portal-initial
captiveportal	6		session	logon, guest-logon

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。

portal-initial Policies Bandwidth Captive Portal More

- > Network
- > VPN
- ▼ Authentication

IDP profile:	-None-
Stateful NTLM profile:	-None-
Stateful Kerberos profile:	-None-
WISPr profile:	-None-
Captive portal profile:	Lab1-Portalprofile
Captive portal check for accounting:	<input checked="" type="checkbox"/>

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

AAA Profiles	
	AAA
	NoAuthAAAProfile
	default
	default-dot1x
	default-iap-aaa-profile...
	default-mac-auth
	default-open
	default-tunneled-use...
	default-xml-api
	lab1-psk-aaa

AAA Profile: New Profile

1) 填写 profile 名称，勾选 initial role

AAA Profile: New Profile

Profile name:	aaa-portal
Initial role:	portal-initial
MAC Authentication Default Role:	guest
802.1X Authentication Default Role:	guest
Download Role from CPPM:	<input type="checkbox"/>
Set username from dhc option 12:	<input type="checkbox"/>

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

The screenshot shows the Aruba Mobility Network configuration interface. On the left, there's a navigation tree under 'Configuration' with sections like WLANs, Roles & Policies, Access Points, AP Groups, Authentication, Services, Interfaces, Controllers, System (which is selected), Tasks, and Maintenance. The 'Profiles' tab is active at the top right. In the main pane, under 'All Profiles', several profiles are listed: 'meair', 'Other Profiles', 'QoS', 'RF Management', 'UCC', 'Wireless LAN' (which is highlighted in orange), '802.11K', '802.11r', '802.1X Authentication', and 'AAA'. Below this, there's a note about 'AMOD 3GPP Cellular Networks'.

Profiles

- Management Authentication
- RADIUS Server
- RFC 3576 Server
- RRM IE
- Radius Modifier
- SSID**
- default

SSID Profile: New Profile

SSID Profile: +

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

SSID Profile: New Profile

Profile name:	lab1-portal
SSID enable:	<input checked="" type="checkbox"/>
ESSID:	lab1-portal
WPA Passphrase:	WPA passphrase:
Encryption:	Retype: <input type="checkbox"/> xSec <input type="checkbox"/> enhanced-open <input type="checkbox"/> wpa3-sae-aes <input type="checkbox"/> wpa3-aes-ccm-128 <input type="checkbox"/> wpa3-cnsa <input checked="" type="checkbox"/> opensystem <input type="checkbox"/> static-wep
Opmode transition:	<input checked="" type="checkbox"/>
Enable Management Frame Protection:	<input type="checkbox"/>

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)

Profile name:	lab1-portal-vap
Virtual AP enable:	<input checked="" type="checkbox"/>
VLAN:	120
Forward mode:	tunnel

- > RF
- > Advanced
- > Broadcast/Multicast

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

The screenshot shows the ArubaOS8 configuration interface with several panels:

- Virtual AP Profile:** A list of profiles including "Virtual AP", "default", "lab1-portal-vap", "802.11K", "AAA", "Anyspot", "Hotspot 2.0", "SSID", and "WMM Traffic management". "lab1-portal-vap" is selected.
- All Profiles:** A list of profiles including "TACACS Server", "TSM Report Request", "VIA Client WLAN", "VPN Authentication", "Virtual AP", "default", "lab1-portal-vap", "802.11K", "AAA", "Anyspot", and "Hotspot 2.0". "AAA" is selected.
- AAA Profile: aaa-portal:** Configuration for the selected AAA profile. It includes fields for "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:", and "User idle timeout:".
- SSID Profile:** Configuration for the selected SSID profile. It includes fields for "SSID enable:", "ESSID:", "WPA Passphrase:", and "Encryption:".
- WMM Traffic management:** A section showing configuration for WMM Traffic management.

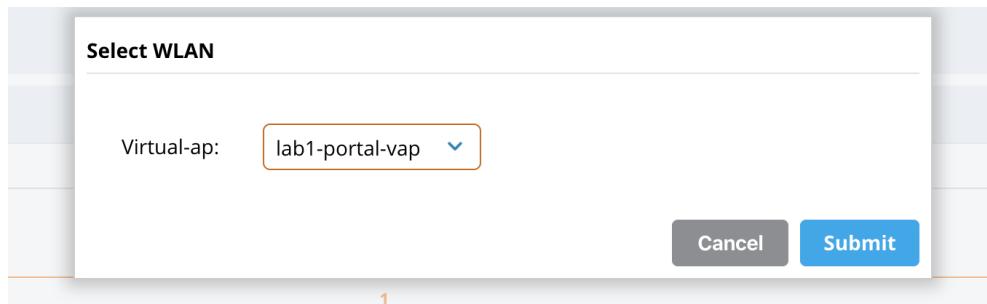
第12步:配置 AP Group: 创建 AP Group 或者在现有 AP Group 添加 portal Virtual AP profile。 Mobility

Network- >LabX- > Configuration -> AP Groups

NAME	APs
default	--
NoAuthApGroup	--
lab1-group	1

NAME	AP GROUP	AIRTIME LIMIT (%)
lab1-psk-vap	lab1-group	--

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
```

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

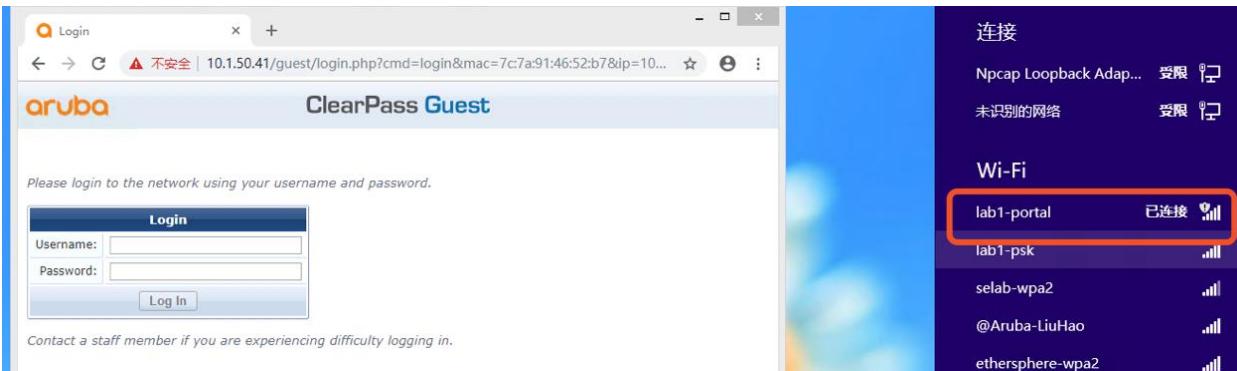
第2步：查看 SSID 是否释放

```
(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 Profile	Name	Role	Age(d:h:m)	Auth	VPN link	AP name	Roaming	Essid/Bssid/Phy
			Forward mode	Type			Host Name	User Type	
10.1.20.100	b4:0f:93:fe:12/a-VHT	labX-portal-logon	tunnel	00:00:00			Wireless		lab1-portal/94:

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 Profile	MAC Forward mode	Name Role	Age(d:h:m) Type	Auth Host Name	VPN link User Type	AP name	Roaming	Essid/Bssid/Phy
10.1.20.100 /94:b4:0f:93:fe:12/a-VHT	7c:7a:91:46:52:b7 labXcauser	authenticated	00:00:00 tunnel	Web aaa	94:b4:0f:c1:3f:e0 tunnel	Wireless AP name	lab1-portal	

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]

The screenshot shows the 'Profiles' tab in the 'System' section of the Aruba MM-VA interface. On the left, there's a sidebar with navigation links like Dashboard, Configuration, WLANs, Roles & Policies, Access Points, AP Groups, Authentication, Services, Interfaces, Controllers, System (which is selected), Tasks, and Maintenance. The main panel has tabs for General, Admin, AirWave, CPSec, Certificates, SNMP, Logging, Profiles (selected), and More. Under the Profiles tab, there's a 'All Profiles' list containing various profiles such as Wireless LAN, 802.11K, 802.11r, 802.1X Authentication, and several AAA profiles. One specific AAA profile, 'lab1-mac-caching', is highlighted with an orange box. To the right, a detailed configuration window titled 'AAA Profile: New Profile' is open. It shows fields for 'Profile name' (set to 'lab1-mac-caching'), 'Initial role' (set to 'lab1-portal-logon'), and 'MAC Authentication Default Role' (set to 'authenticated'). Red arrows point from the text '1、新建aaa profile name' to the profile name field, '2、修改initial role:' to the initial role dropdown, and '3、修改mac认证成功role' to the MAC authentication default role dropdown. At the bottom right of the configuration window are 'Cancel' and 'Submit' buttons.

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”

This screenshot shows the 'MAC Authentication Profile' configuration screen. The left sidebar is identical to the previous one. The main panel shows the 'Profiles' tab selected. In the 'All Profiles' list, the 'MAC Authentication' profile is highlighted with an orange box. To the right, a configuration window titled 'MAC Authentication Profile: lab1-mac' is displayed. It lists settings for 'Delimiter' (set to 'none'), 'Case' (set to 'lower'), 'Max Authentication failures' (set to '0'), 'Reauthentication' (unchecked), 'Reauthentication Interval' (set to '86400 sec'), and 'Use Server provided Reauthentication Interval' (unchecked). A red box highlights the 'MAC Authentication Profile' dropdown, which is set to 'lab1-mac'.

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”

Managed Network > lab1 >

Pending Changes

General Admin AirWave CPSEC Certificates SNMP Logging **Profiles** More

All Profiles

- LDAP Server
- MAC Authentication
- Management Authentication
- RADIUS Server
- RFC 3576 Server
- RRM IE
- Radius Modifier
- SSID**
- default
- lab1-1x-ssid
- lab1-mac-caching-ssi...
- lab1-mac-ssid
- lab1-portal-ssid
- lab1-psk-ssid

SSID Profile: New Profile

Profile name: lab1-mac-caching-ss

SSID enable:

ESSID: aruba-ap

WPA Passphrase:

WPA passphrase:

Retype:

Encryption:

Opmode transition:

Enable Management Frame Protection:

Cancel **Submit**

ArubaMM-WA, 8.4.0.0

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”

Managed Network > lab1 >

Pending Changes

General Admin AirWave CPSEC Certificates SNMP Logging **Profiles** More

All Profiles

- TACACS Server
- TSM Report Request
- VIA Client WLAN
- VPN Authentication
- Virtual AP**
- default
- lab1-1x-vap
- lab1-mac-caching-vap
- lab1-mac-vap
- lab1-portal-vap
- lab1-psk-vap

Virtual AP profile: New Profile

Profile name: lab1-mac-caching-vap

Virtual AP enable:

VLAN: 120

Forward mode: tunnel

> General

> RF

> Advanced

> Broadcast/Multicast

Cancel **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”

The screenshot shows the 'Profiles' tab selected in the top navigation bar. On the left, a sidebar lists various configuration categories like WLANs, Roles & Policies, and AP Groups. The main panel displays a list of 'All Profiles' under the 'AAA' category. One profile, 'lab1-mac-caching-aaa', is highlighted with a red border. The right side shows the configuration details for this profile, including fields for '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', 'Max IPv4 for wireless user', and 'RADIUS Roaming Accounting'. The 'AAA Profile' dropdown at the top is also highlighted with a red border.

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

This screenshot shows the 'Profiles' tab selected. The left sidebar and profile list are identical to the previous screenshot. The right panel shows the configuration for the 'SSID Profile: lab1-mac-caching-ssid'. It includes fields for 'SSID enable' (checked), 'ESSID' (set to 'lab1-mac-caching'), 'WPA Passphrase', 'Retype', 'Encryption' (with 'wpa3-sae-aes' checked), and 'Opmode transition'. The 'SSID Profile' dropdown at the top is highlighted with a red border.

第10步:点击右上角的“Pending Changes”,保存配置

The screenshot shows the bottom navigation bar of the Aruba interface. It includes the Aruba logo, the mobility master name 'MOBILITY MASTER Lab1-MM-1', user information ('admin'), and a 'Pending Changes' button with a circular arrow icon. The 'Pending Changes' button is highlighted with a red border.

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 Profile	Name	Role Forward mode	Age(d:h:m)	Auth Type	VPN link Host Name	AP name User Type	Roaming	Essid/Bssid/Phy
10.1.20.100	7c:7a:91:46:52:b7	labX-portal-logon	lab1-mac-caching-aaa	00:00:00	tunnel	Win 8	94:b4:0f:c1:3f:e0	Wireless	lab1-mac-caching-aaa

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 /Phy	MAC Profile	Name	Role	Age(d:h:m)	Auth Type	VPN link Host Name	AP name User Type	Roaming	Essid/Bssid
10.1.20.100	7c:7a:91:46:52:b7	guest1@arubalab.net	authenticated	00:00:01	Web	ab1-mac-caching/94:b4:0f:93:fe:14/a-VHT	lab1-mac-caching-aaa tunnel	Win 8	94:b4:0f:c1:3f:e0 Wireless 1 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。

IP /Phy	MAC Profile	Name	Role	Age(d:h:m)	Auth Type	VPN link Host Name	AP name User Type	Roaming	Essid/Bssid
10.1.20.100	7c:7a:91:46:52:b7	guest1@arubalab.net	authenticated	00:00:00	MAC	ab1-mac-caching/94:b4:0f:93:fe:14/a-VHT	lab1-mac-caching-aaa tunnel	Win 8	94:b4:0f:c1:3f:e0 Wireless 1 WIRELESS

User Entries: 1/1

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

-----全文完-----