

Aruba 动手实验手册

ArubaOS 8 网络优化和故障诊断

V2.0.0-Final

杨正鑫/马景浩

1	无线	网络优化	6
1.	.1	用户需求	6
1	2	立 和 用 路	6
	-		
1.	.3		7
	1.3.1	版本、备份恢复相关(CLI)	7
	1.3.2	版本、备份恢复相关(GUI)	15
	1.3.3	虚拟机相关(CLI)	21
	1.3.4	LACP 链路聚合(CLI)	23
	1.3.5	LACP 链路聚合(GUI)	24
	1.3.6	Jumbo Frame (CLI)	26
	1.3.7	Jumbo Frame (GUI)	27
	1.3.8	MTU (CLI)	29
	1.3.9	MTU (GUI)	29
	1.3.10	0 NTP Server (CLI)	
	1.3.1	1 NTP Server (GUI)	31
	1.3.17	2 Spanning-Tree (CLI)	32
	1.3.13	3 Spanning-Tree (GUI)	32
	1.3.14	4 ADP (CLI)	33
	1.3.1	5 VRRP (CLI)	33
	1.3.1	6 VRRP (GUI)	34
	1.3.1	7 CPSec (CLI)	36
	1.3.18	8 CPSec (GUI)	36
	1.3.19	9 IPv6 (CLI)	37
	1.3.20	0 IPv6 (GUI)	37
1.	.4	射频层面的优化项	
	1.4.1	2.4Ghz 频宽(CLI)	
	1.4.2	2.4Ghz 频宽(GUI)	
	1.4.3	5Ghz 频宽(CLI)	40
	1.4.4	5Ghz 频宽(GUI)MM+MD 架构	40
	1.4.5	5Ghz 频宽(GUI)Standalone 架构	41
	1.4.6	DFS (CLI)	41
	1.4.7	DFS (GUI)	43
	1.4.8	Basic-rates (CLI)	43



1.4.9	Basic-rates (GUI)	45					
1.4.10	AP 接收灵敏度(CLI)						
1.4.11	AP 接收灵敏度(GUI)						
1.4.12	2 802.11h (CLI)						
1.4.13	802.11h (GUI)	48					
1.4.14	ARM/WIDs (CLI)	49					
1.4.15	ARM/WIDs (GUI)	49					
1.4.16	802.11b/g (CLI)	50					
1.4.17	802.11b/g (GUI)	51					
1.4.18	802.11b/g(HT) (CLI)	51					
1.4.19	802.11b/g(HT) (GUI)	52					
1.4.20	室外 AP	53					
1.4.21	室外 AP(GUI)	53					
1.4.22	最大关联数(CLI)	54					
1.4.23	最大关联数(GUI)	55					
1.4.24	AP 扫描(CLI)	55					
1.4.25	Clientmatch (CLI)	56					
1.4.26	空口整形(CLI)	56					
1.4.27	空口整形(GUI)	57					
1.5 应	Z用层面的优化项	59					
1.5.1	无线侧组播广播(CLI)	59					
1.5.2	无线侧组播广播(GUI)	59					
1.5.3	有线侧组播广播(CLI)	60					
1.5.4	有线侧组播广播(GUI)	60					
1.5.5	VMM (CLI)	61					
1.5.6	VMM (GUI)	62					
1.6 岁	安全层面的优化项	64					
1.6.1	Basic-acl (CLI)	64					
1.6.2	Basic-acl (GUI)	65					
1.6.3	user-table (CLI)	75					
1.6.4	user-table (GUI)	76					
1.6.5	控制器访问控制(CLI)	80					
1.6.6	控制器访问控制(GUI)	81					
1.6.7	用户隔离(CLI)	88					
1.6.8	用户隔离(GUI)	89					
1.6.9	端口阻断(CLI)	90					



	1.6.1	ⅠO 端口阻断(GUI)	91
2	高级	及故障诊断	<u>98</u>
	2.1	用户需求	.98
	2.2	实现思路	.98
	2.3	诊断故障的流程	.98
	2.4	终端层面诊断	.99
	2.5	AP 层面诊断1	115
	2.6	控制器层面诊断1	130
	2.7	搜集重要信息来联系 TAC1	163



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
1.0.0-Final	2020/03/30	最初发布
2.0.0-Final	2020/07/01	更新 LAB2.0 拓扑,实验内
		容相关调整



1 无线网络优化

1.1 用户需求

大多数客户在部署完Aruba的无线网络后,随着用户数和各种应用业务的增加以及周边射频 环境的变化,或者是因为AP部署点位的变化(比如扩容或者增加了AP点位等),用户希望能够对 现有的无线网络的参数进行相关的优化和调整,除了能够满足各种应用场景下的网络使用外,在现 有的网络环境下,还能够进行性能的提升,从而让您的网络体验度更好,尤其是在高密度的场景下, 通过优化网络参数能够更好地满足该场景下的用户接入体验。

1.2 实现思路

我们会将无线网络的设计容量分为低密度和中高密度场景:

基于低密度场景下802.11ac/ax能力的AP设计规则: 建议AP间距约15米(即每隔15米放置一颗AP),每颗AP的两个radio的总关联用户数建议40-60人,如果客户端的密度高于这个,AP 应该部署的更密集。

基于中高密度场景下802.11ac/ax能力的AP设计规则:建议AP间距约15米以内,所谓无线网 络中/高密度场景,是指在单一物理空间内的无线用户数量与网络流量都远超过普通无线网络设计的 预期,即在单个RF冲突域里(所谓冲突域,就是相互间信号干扰区域,即我们说的ap干扰半径为 802.11 preamble can be decoded SNR >= 4dB,比实际的覆盖半径多出12倍左右)有500个或 以上的无线客户端,通常可达1000-2000,甚至更多.每个cell微蜂窝(即AP的单个radio)需要提 供至少40-60个以上的终端接入(40个以上是中高等密度,60个以上是超高密度)。主要场景:大 型会议室,演讲厅和礼堂,会议中心会议厅,酒店宴会厅,室内和室外体育馆,运动场和球场,剧 场和竞技场,赌场,公共交通的等候大厅,客机和邮轮,宗教活动场所,金融交易大厅等。

因此针对以上各种场景,我们会考虑对无线网络进行相关参数的优化,这些参数的修改是基于默认配置基础上的调优,也是我们希望在一些使用环境中,初始化配置完成后,就对这些参数进行一个适当的调优。



通常默认的参数可以满足大多数场景下的需求和使用,我们的调优是建立在默认参数基础之上,同时优化网络很多时候是需要循环渐进的过程,并不是简单的把所有参数一起设置下,就能够达到最终的理想效果。同时不同的AP点位,不同客户环境场景,不同的应用需求,不同的终端类型等,我们所采用的优化参数和优化方向也是不相同的,需要大家根据平时所学习到的理论知识,项目经验以及结合本手册中所描述的配置参数,来选择性地进行相关优化,每做一次优化调整,需要做好变更记录,同时进行验证和测试,看看对当前的业务是否有大的影响,如果没有影响,那么我再进行下一阶段的参数优化,每次优化内容尽可能做到只对一个功能性的内容进行调整,比如我们调整AP的发射功率时,就不要同时调整裁剪低速率的动作。当所有优化项内容完成后,再进行一次验证和测试,看看对当前业务是否进行改善和提升,是否带来其他业务的影响,所以优化网络是一个长时间验证的过程。

那么接下来,我们就从四个层面(方向)来完成一个无线网络的优化设置。

1.3 架构层面的优化项

1.3.1 版本、备份恢复相关 (CLI)



无线控制器当前运行的 AOS 版本是否是 Aruba 原厂推荐的最佳版本,如果不是,请尽快升级到厂商 SE 推荐的最佳版本。有条件的话,先备份配置和授权,等升级后强烈建议采用 write erase all 方法先清空所有的配置和内置数据库内容,然后重新初始化控制器并采用重新贴入命令的方式来部署一遍(强烈推荐方式)或者采用导入原备份配置文件的方式来恢复(相对比较快速恢复网络)。

注意点:不管是 MM 还是 MD 控制器的两个分区的 image 最佳部署方式:全都是版本 6.x, 或者全都是版本 8.x。不建议一个分区是 6.x 版本,另外一个分区是 8.x 版本).另外就是当你从 8.X 降级版本时,一定需要在降级后,检测当前系统配置是否部分丢失,如果丢失的话,请尽快重 新配置上去。

千万别说今天没有问题,就不要升级了,今天没有问题,不代表客户环境和业务不变化,也 许就会某时某刻触发已知 bug.

举一个真实客户案例:

之前客户采用 MPLS VPN 线路, MTU 可以满足 1500, 从而 AP305 可以正常通过专线实现 IPSec 到控制器, 实现 Remote AP 的部署, 可是随着 MPLS VPN 线路开始改造(需要变成 SD-WAN)后, 用户仅仅测试了 AP105 是正常工作的, 此时运营商告知他们的线路满足的 MTU 最大 只能 1300, 客户仅仅测试了 AP105 能够在 SD-WAN 上正常工作, 以为其他 AP 型号应该也没有 问题, 可是当后期大规模部署时, 发现仅仅是 AP305 和控制器之间的 IPSec VPN 无法建立, 客户 当前的版本是 AOS6.5.1.9, 而正巧赶上了这个 AP305 型号触发了已知的 bug, 就是这么巧合, 客户之前一直没有问题时, 不希望升级, 可是触发问题了, 就希望我们尽快解决, 如果升级是一个 常态, 那结果又如何呢?

当前LabX 系统环境和配置层次如下 (AOS版本V8.6.0.x)

(LabX-MM-1) [md] <mark>#show configuration node-hierarchy</mark>			
Default-node is not configured. Autopark is disabled.			
Configuration node hierarchy			
Config Node	Type Name		
/	System		

Page 8 of 171



/md	System
/md/labX	Group
/md/labX/00:0c:29:82:71:b4	Device labX-md1
/md/labX/00:0c:29:ea:9a:d9	Device labX-md2
/mm	System
/mm/mynode	System

在MM控制器上显示当前系统版本镜像分区,注意default boot 表示当前正在运行的系统版

本

(LabX-MM-1) [mynode] (config) <mark>#show image version</mark>					
Partition	: 0:0 (/mnt/disk1)				
Software Version	: ArubaOS 8.4.0.5 (Digitally Signed SHA1/SHA256 - Production Build)				
Build number : 72830					
Label	: 72830				
Built on	: Tue Oct 22 08:43:27 UTC 2019				
Partition	: 0:1 (/mnt/disk2) <mark>**Default boot**</mark>				
Software Version : ArubaOS 8.6.0.3 (Digitally Signed SHA1/SHA256 - Production Build)					
Build number	: 74788				
Label	: 74788				
Built on	: Fri Mar 20 11:07:28 UTC 2020				

在MM控制器上显示当前停靠的MD控制器正在运行软件版本信息,原则上我们是建议您的 MM控制器软件版本和MD一致最佳,当然您的MM版本也可以高于MD(但是不要超过2个大版本, 例如mm是8.5,md是8.2 是不行的),不建议MM低于MD的版本来运行。

(LabX-MM-1) [mynode] #show switches

All Switches

IP Address IPv6 Address Name Location Type Model Version Status Configuration State Concerned Time (sec) Config ID					guration State Config Sy	
10.2.50.11 None 0 46	LabX-MM-1 B	uilding1.floor1 ma	ster ArubaMl	M-VA <mark>8.6.0</mark>	<mark>).3_74788</mark> up	UPDATE SUCCESSFUL
10.2.10.12 None 10 46	labX-md2 Bui	ilding1.floor1 MD	ArubaMC-\	VA <mark>8.6.0.3</mark> _	<mark>74788</mark> up	UPDATE SUCCESSFUL
10.2.10.11 None 8 46	labX-md1 Bui	ilding1.floor1 MD	ArubaMC-\	VA <mark>8.6.0.3_</mark>	<mark>74788</mark> up	UPDATE SUCCESSFUL

你也可以分别MDConnect到每台MD控制器上show image version, 查看两个分区的镜像版本。

(labX-md1) [MDC] <mark>#show image version</mark>				
Partition	: 0:0 (/mnt/disk1) **Default boot**			
Software Version : ArubaOS 8.6.0.3 (Digitally Signed SHA1/SHA256 - Production Build)				
Build number	: 74788			
Label	: 74788			
Built on	: Fri Mar 20 14:07:12 UTC 2020			
Partition	: 0:1 (/mnt/disk2)			
Software Version : ArubaOS 8.6.0.3 (Digitally Signed SHA1/SHA256 - Production Build)				
Build number	: 74788			
Label	: 74788			
Built on	: Fri Mar 20 14:07:12 UTC 2020			



(labX-md2) [MDC] #show image version					
Partition	: 0:0 (/mnt/disk1) **Default boot**				
Software Version : ArubaOS 8.6.0.3 (Digitally Signed SHA1/SHA256 - Production Build)					
Build number : 74788					
Label	: 74788				
Built on	: Fri Mar 20 14:07:12 UTC 2020				
Partition	: 0:1 (/mnt/disk2)				
Software Version : ArubaOS 8.6.0.3 (Digitally Signed SHA1/SHA256 - Production Build)					
Build number	: 74788				
Label	: 74788				
Built on	: Fri Mar 20 14:07:12 UTC 2020				

备份配置(在MM控制器上的/mm/mynode节点下备份配置即可,无需在MD控制器上备份配置,因为配置都是从MM控制器同步给MD的,MD上仅仅只要初始化配置即可)

(LabX-MM-1) [mynode] <mark>#backup config</mark>

Please wait while we take the config backup......

File configbackup.tar.gz created successfully on flash.

Please copy it out of the controller and delete it when done.

备份授权,在MM控制器上的/mm/mynode节点下备份中心化授权即可。

(LabX-MM-1) [mynode] #license export license-mynode.lic

Successfully exported 5 licenses from the license database to license-mynode.lic

(LabX-MM-1) [mynode] #dir

- -rw-r--r-- 1 root root 7323 Mar 24 13:52 AUDITTRAIL-HISTORY.log
- -rw-r--r-- 1 root root 37108 Mar 24 13:52 AUDITTRAIL-LOGIN_OUT-HISTORY.log
- -rw-r--r-- 1 root root 152 Mar 24 13:58 blimits



-rw-rr	1 root	root	40 Mar 24 13:28 bmap
-rw-rr	1 root	root	40298 Mar 24 15:25 <mark>configbackup.tar.gz</mark>
-rw-rr	1 root	root	24532 Mar 24 13:54 default.cfg
drwxr-xr-x	4 root	root	4096 Mar 24 13:08 fieldCerts
-rw-rr	1 root	root	12521 Jan 8 10:59 license-backup-2020
-rw-rr	1 root	root	12604 Mar 24 15:33 license-mynode.lic
-rw-rr	1 root	root	18 Mar 24 13:54 mac_addr.cfg
-rw-rr	1 root	root	39868 Mar 24 13:51 reboot_config_backup.tar.gz
drwxr-xr-x	2 root	root	4096 Mar 24 13:10 upgrade-2020-03-24_13-10-02
-rw-rr z	1 root	root	51746 Mar 24 12:57 upgrade_config_backup_8.4.0.5_to_8.6.0.3_2020-03-24-12_57_14.tar.g
-rw-rr	1 root	root	5 Mar 24 13:50 vclock.time

恢复配置(仍然在 /mm/mynode 节点下恢复即可)

(LabX-MM-1) [mynode] #restore config

恢复授权(仍然在 /mm/mynode 节点下恢复即可)

(LabX-MM-1) [mynode] #license import license-mynode.lic

注意:当然有些场景下,客户会利用控制器来实现 Remote AP 和 IAP 的远程接入,甚至会采用内置的 internal db 作为用户认证 源,

请及时备份相关的RAP白名单和internal db数据,备份internal db数据

(LabX-MM-1) [mynode] #local-userdb export localdb

Successfully exported 0 users and 1 CPSec Whitelist 0 RAP whitelist entries from the Internal User Database to localdb

(LabX-MM-1) [mynode] #dir

-rw-rr	1 root	root	7323 Mar 24 13:52 AUDITTRAIL-HISTORY.log
--------	--------	------	--

-rw-r--r-- 1 root root 37108 Mar 24 13:52 AUDITTRAIL-LOGIN_OUT-HISTORY.log

-rw-r--r-- 1 root root 152 Mar 24 13:58 blimits

-rw-r--r-- 1 root root 40 Mar 24 13:28 bmap



-rw-rr 1 root	root	40298 Mar 24 15:25 configbackup.tar.gz
-rw-rr 1 root	root	24532 Mar 24 13:54 default.cfg
drwxr-xr-x 4 root	root	4096 Mar 24 13:08 fieldCerts
-rw-rr 1 root	root	12521 Jan 8 10:59 license-backup-2020
-rw-rr 1 root	root	12604 Mar 24 15:33 license-mynode.lic
-rw-rr 1 root	root	31127 Mar 24 15:40 <mark>localdb</mark>
-rw-rr 1 root	root	18 Mar 24 13:54 mac_addr.cfg
-rw-rr 1 root	root	39868 Mar 24 13:51 reboot_config_backup.tar.gz
drwxr-xr-x 2 root	root	4096 Mar 24 13:10 upgrade-2020-03-24_13-10-02
-rw-rr 1 root z	root	51746 Mar 24 12:57 upgrade_config_backup_8.4.0.5_to_8.6.0.3_2020-03-24-12_57_14.tar.g
-rw-rr 1 root	root	5 Mar 24 13:50 vclock.time

导入备份的数据库文件

(LabX-MM-1) [mynode] #local-userdb import localdb

查看当前系统的白名单数据库,并将所有记录贴入到电脑的文本文件中

(LabX-MM-1) [mynode] <mark>#show whitelist-db rap</mark>		
AP-entry Details		
Name AP-Group AP-Name Full-Name Date-Added Enabled Remote-IP Remote-IP	ne Authen-Username Revoke-Text Al IPv6 Cluster-InnerIP Cert-type	P_Authenticated Description
11:12:13:14:15:16 default 11:12:13:14:15:16 0 Yes 0.0.0.0 :: 0.0.0.0 NA	Provisioned	Tue Mar 24 15:43:26 202
AP Entries: 1		

恢复系统的内置白名单数据库 (事先将命令行编辑好,一起贴入)



(LabX-MM-1) [mynode] (config) #whitelist-db rap add mac-address 11:12:13:14:15:16 ap-group default

(LabX-MM-1) [mynode] (config) #whitelist-db rap add mac-address 11:12:13:14:15:17 ap-group default

查看所有在线和离线的AP数据库信息,方便后期查看曾经掉线的AP信息(特别是以位置来命名的AP)。

```
(LabX-MM-1) [mynode] #show ap database long
AP Database
_____
Name Group
              AP Type IP Address Status Flags Switch IP Standby IP Wired MAC Address Serial # Port
FQLN Outer IP User
             _____ ___
                                                   LAB2-AP1 lab2-group 205 10.2.12.101 Up 2h:13m:37s 10.2.10.11 10.2.10.12 94:b4:0f:cc:4d:68 CM0219527
  N/A N/A
Flags: 1 = 802.1x authenticated AP use EAP-PEAP; 1+ = 802.1x use EST; 1- = 802.1x use factory cert; 2 = Using IKE versi
on 2
   B = Built-in AP; C = Cellular RAP; D = Dirty or no config
   E = Regulatory Domain Mismatch; F = AP failed 802.1x authentication
   G = No such group; I = Inactive; J = USB cert at AP; L = Unlicensed
   M = Mesh node
   N = Duplicate name; P = PPPoe AP; R = Remote AP; R- = Remote AP requires Auth;
   S = Standby-mode AP; U = Unprovisioned; X = Maintenance Mode
   Y = Mesh Recovery
   c = CERT-based RAP; e = Custom EST cert; f = No Spectrum FFT support
   i = Indoor; o = Outdoor; s = LACP striping; u = Custom-Cert RAP; z = Datazone AP
   p = In deep-sleep status
   4 = WiFi Uplink
   r = Power Restricted; T = Thermal ShutDown
Total APs:1
```



1.3.2 版本、备份恢复相关 (GUI)

1) 当前 LabX 无线系统环境下配置节点层次(AOS 版本 V8.6.0.x):

CTUDO MOBILITY MASTI Lab2-MM-1	R	$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	admin 🐱		
Managed Network > lab2 >			😒 Search 🔍		
Mobility Master Lab2-MM-1 Managed Network (2) Lab2-20 Lab2-20	Dashboard Overview Infrastructure Traffic Analysis Services Configuration Maintenance	CLIENTS Grouped by health ~ $\fill \ Show W$ Show W There is no client to display right now.	WLANS Show WLANs with most clients V		
	ArubaMM-VA,8.6.0.3	USAGE Show Tx & Rx	S d by channel quality V CODD e is no radio to display right now.		

 进入到 Mobility Master -> Lab^X-MM-1,点击 "Maintenance->Software Management",点击 Upgrade 选项卡,在 MM 控制器上显示当前系统版本镜像分区,两个分区的版本是否都在 8.x 下,注 意 default boot 表示当前正在运行的系统版本。

ALAPSA MOBILITY MAST Lab2-MM-1	ER	CONTROLLERS ⊘ 2 ⊙ 0	ACCESS POINTS	CLIENTS	ALERTS		⑦ admin ✓
Mobility Master > Lab2-MM-1							(⁴)
 Mobility Master Mobility Master Managed Network (2) Iab2 (2) Iab2-md1 Iab2-md2 	Configuration Diagnostics Maintenance Software Management Configuration Management	Upgrade using: Server IP address Image file name: Partition to upgr Reboot controller Current Partition Software Version Build Number Label Built On	boot Boot P. s. ade: r after upgrade: ion Usage PARTITION 0 0:0/(mnt/disk1) ArubaOS 8.4.0.5 (Production Build) 72830 72830 72830 Tue Oct 22 08:43:	TFTP TFTP Partition 0 Digitally Signed SHA*	rvice Module Pr	About About PARTITION 1 (DEFAULT BOOT) O.1(/mmt/disk2) ArubaOS 8.6.0.3 (Digitally Signe Production Build) 74788 74788 Fri Mar 20 11:07:28 UTC 2020	ed SHA1/SHA256 -

3) 进入到 Managed Netowrk->Dashboard->Infrastructure",点击 Controllers 选项,在 MM 控制器上显示当前停靠的 MD 控制器的正在运行软件版本信息,原则上我们是建议您的 MM 控制器软件版本和 MD 一致最佳,当然你的 MM 版本也可以高于 MD,不建议低于 MD 的运行版本。

Orubo MOBILITY MASTE Lab2-MM-1	R	CONTROLLERS ⊘ 2 ○ 0	ACCESS POINT	CLIENTS	5 ALE ◎ 0 🛆	RTS 2		admin 🗸
🗲 Managed Network >							🏟 Sea	rch 🔍
Image: Constraint of the system Image: Constraint of the system <t< th=""><th>Dashboard Overview Infrastructure Traffic Analysis Security Services Configuration Maintenance</th><th>Grouped by statu</th><th>2 ontrollers</th><th>• • •</th><th>Up (2) Down (0) work Map</th><th>ACCESS DEVICES Grouped by status</th><th>ss point to di</th><th>splay right now.</th></t<>	Dashboard Overview Infrastructure Traffic Analysis Security Services Configuration Maintenance	Grouped by statu	2 ontrollers	• • •	Up (2) Down (0) work Map	ACCESS DEVICES Grouped by status	ss point to di	splay right now.
	ArubaMM-VA,8.6.0.3	WAN Uplinks grouped I	uplink to dis	play right no	ow.	CLUSTERS Show dusters with I lab2-cluster 0 25	nighest AP load	 Active Standby Free
ACTUDO MOBILITY MASTE Lab2-MM-1	R	CONTROLLERS ⊘ 2 ① 0	ACCESS POINTS	CLIENTS	ALEF	2 2		admin 🗸
Managed Network >							🏟 Sear	rch 🔍
C Q ➢ Mobility Master ☞ Lab2-MM-1 ➢ Managed Network (2) ➢ lab2 (2) ☞ lab2-md1 ☞ lab2-md2	Dashboard Overview Infrastructure Traffic Analysis Security Services Configuration Maintenance	Controllers 2 NAME A > lab2md1 > lab2md2	STATUS Ο υρ Ο υρ	Access Devices	UPTIME 11h 11m	software 8603 8603	ACCESS POIN 0 0	CUENTS O O

4) 进入到 Managed Netowrk->labX ->labx-md1->Dashboard->Infrastructure",你可以分别在每台 MD 控制器节点上,查看当前运行镜像版本和两个分区的版本情况。点击下图的 labX-md1 蓝色字体,会进入到详细内容展示。



Orubo MOBILITY MAST Lab2-MM-1	ER	CONTROLLERS ACCES	S POINTS CLIENTS	ALERTS 2	admin 🛩
← Managed Network > lab2 > lab2	2-md1				🔄 Search 🔍
Ck Q Mobility Master E Lab2-MM-1 E Managed Network (2) E Iab2 (2) E Iab2-md1 E	Dashboard Overview Infrastructure Traffic Analysis Services Configuration Maintenance	CONTROLLER Show controller information I a b2 Status Up O Heath Good III	on 2-md1 Software 8.0.03_74788 Model ArubaMC-VA Paddess 10.2.10.11 Software M	ACCESS DEVI Grouped by sta	cess point to display right now.
	AnubaMM-VAR.0.0.3 R	WAN Uplinks grouped by statue	to display right now.	ALERTS	admin 🛩
Managed Network > lab2 > lab2	-md1		0 0 0 0 0 0	△ 2	🔄 Search 🔍
<u>с</u> , с	Dashboard	1			
C Mobility Master	Overview		Access Devices	0 uplinks	0
Lab2-MM-1	Infrastructure	DETAILS Name lab2-md1	Model ArubaMC-VA	Uptime 11h 18m	Group Iab2
lab2 (2)	Fonticos	IP address	Boot partition	Country	Serial number
🖾 lab2-md1	Configuration	10.2.10.11	ArubaOS 8.6.0.3 74788	CN	MC18271AA
lab2-md2	Maintenance	MAC address 00:0c:29:82:71:b4	Backup partition ArubaOS 8.6.0.3 74788		
		PORTS Hover a port for more details.	° į́ ∧	à	✓ Up Down A Admin disabled

5) 点击下图的 labX-md2 蓝色字体, 会进入到详细内容展示。



ALADO MOBILITY MASTE	R	CONTROLLERS ⊙ 2 ① 0	ACCESS POINTS	CLIENTS	ALERTS		admin 🗸
← Managed Network > lab2 > lab2	-md2					🚱 Search	0,
 ► Mobility Master ■ Lab2-MM-1 ► Managed Network (2) ► lab2 (2) ■ lab2.md1 ■ lab2-md2 	Dashboard Overview Infrastructure Traffic Analysis Services Configuration Maintenance	CONTROLLER Show controller int Up O Health Good III	formation Iab2-md2 Software Softw	3_74788 MC-VA 50.12	ACCESS DEVI Grouped by sta	cess point to displa	y right now.
MOBILITY MASTE Lab2-MM-1 Managed Network > lab2 > lab2	Anubet/ML VA.B.6.0.3	CONTROLLERS	plink to displa	y right now. CLIENTS で 0 ゆ 0	ALERTS	🖗 Search	admin 🛩
€ k Q	Dashboard		â 0,	rs Devices			
Mobility Master Lab2-MM-1	Overview	DETAILS		SI DEVICES	- Quints		0
🔁 Managed Network (2)	Traffic Analysis	ame ab2-md2	Model ArubaMC	-VA	Uptime 11h 22m	Group lab2	
🔁 lab2 (2)	Services 1	address 0.2.10.12	Boot partiti- ArubaOS	on 8.6.0.3 74788	Country CN	Serial number MC2EA9ACF	
📼 lab2-md1	Configuration	IAC address	Backup part	ttion			
⊡ lab2-md2	Maintenance 0	PORTS Hover a port for more Orubio Anter Mark	details.	× A	2		Up Down Admin disabled

 6) 进入到 Mobility Master->LabX-MM-1 ->Maintenance->Configuration Management",点击
 Backup 选项卡,你可以在 MM 控制器上备份配置(仅仅在 MM 控制器上备份配置即可,无需在 MD 上备份配置,因为配置都是从 MM 控制器同步给 MD 的)



ALAPSA MOBILITY M Lab2-M	MASTER M-1	CONTROLLERS ACCESS POINTS CLIENTS ALERTS ② ○	
Mobility Master > Lab2-MM	-1		٩
 Mobility Master Lab2-MM-1 Managed Network (2) lab2 (2) lab2-md1 lab2-md2 	Configuration Diagnostics Maintenance Software Management	Backup Restore Clear Configuration Synchronize Database WMS Database Select what to backup: Flash	

7) 进入到 Mobility Master->Configuration>License",点击 License Usage 选项卡,备份授权,仅仅 在 MM 控制器上备份中心化授权即可(注意:这里只能查看,不能拷贝和粘贴到文本文件中,建议大家 还是采用 cli 的 show license 来输出并拷贝到电脑本地的文本文件中)。

ALADZA MOBILITY MASTE Lab2-MM-1	ER	CONTROL ② 2	LERS ACCES: ○ 0 ○ 0	5 POINTS ① 0 ⑦	CLIENTS 0 2 0	ALERTS					⑦ admin	~
← Mobility Master >												¢
 Mobility Master > Mobility Master Monaged Network (2) Iab2.701 Iab2.md1 Iab2.md2 	Configuration Roles & Policies Authentication Services Interfaces Controllers System License Redundancy	License management: () License Uzage Control Control	Aruba Support AP Asses Parts 0/2048 AP Per-AP 2048 0 2048	Portal (ASP) PEF Parig-freeman PEF Per-AP 2048 0 2048	Disternal lio RF Protect Wegesinguese Byperses Protect Migesinguese Protect Migesinguese Per-AP 2048 0 2048	ACR ACR Anarad Cysopathy 0.0 ACR III Per-Session 0 0 0	Manual WebCC WebCC WebCC WebCC I Per-AP 0 0 0 0	VIA Vinue Internet Access 0.00 VIA VIA VIA Per-Session 0 0 0	MM Materity Materi 2/50 MM M Per-Device 50 0 0 50	MC-VA-RW Regarding to the second antonio MC-VA-RW M MC-VA-RW M Per-Device 0 0 1000		\$
		Licenses Used	0	0	0	0	0	0	2	0		
		Licenses Remaining Available	2048	2048	2048	0	0	0	48	1000		
		Expired/Expiring Licenses for Global Pool										
		KEY			FEATU	RE C	OUNT	USED	TYPE	EXPIRA	non	819-
		8pJuOzvH-IBSqZWY9-DV1WsY6d-aSTIEf52-Prpymnao-CY745	i6M6-x8FUS068-HqR	LmZrz-zWRGSRmo-Jit	D AP	2	0.48	0	Eval	Apr 23	20.20	0
		Q0t2Bdje-pA10QrH8-XG5/wH7A-M1cV2Ive-+g8fTiLn-QLMS	(7uf-0m8hbhg)-k5G2	p/B1-wHfMimfl-M+k	PEFNG	2	048	0	Eval	Apr 23	20.20	0
		pmXhaWz-URtjW9K/-CAhn94P5-IULEpjNN-xlauP8Rg-INmuB	M8w-fAhRepkQ-N5a	cT7Xo-8xvb8u3Y-AQg	RFP	2	048	0	Eval	Apr 23	20.20	0
		6nKTh6Gn-GVBo7rot-8OwT2b8w-QklyuWCI-UWa1SGue-irA	201jF-p7W08Xyb-gg8	CDYrU-nKKgk5pr-Yal	MM NM	5	0	0	Eval	Apr 23	20.20	0
		a9u///BeFQ-1KWDAM3s-IOwaTDKb-2IpXxXII-cLYMUJsb-FaAz	ZKxp-ipUCsAWD-CiC	PU92T-g3jFKRpV-M/g	MC-VA	-RW 1	000	0	Eval	Apr 23	20.20	0
	ArubaM M-VA, 8.6.0.3									1	Cancel	Submit

8) 恢复配置

进入到 Mobility Master->LabX-MM-1 ->Maintenance->Configuration Management",点击 Restore 选项 卡,选择 Configuration 来 Restore.



ALADZA MOBILITY MAST Lab2-MM-1	ER	CONTROLLERS ACCESS POINTS CLIENTS ALERTS ∅ 2 ○ 0 ○ 0 ♠ 0 ▲ 2	(?) admin ~
Mobility Master > Lab2-MM-1			¢
 Mobility Master > Lab2-MM-1 Mobility Master Lab2-MM-1 Managed Network (2) Tab2 (2) Tab2 (2) Tab2-md1 Tab2-md2 	Configuration Diagnostics Maintenance Software Management Configuration Management	Clear Configuration Synchronize Database WMS Database Figure Configuration Configuration This will restore the contents of configbackup, targ z A reboot will be required once this is completed. Freetore	\$
	AntraMMVA 8.6.0.3		

9) 恢复授权 (重新贴入之前备份的授权 key 即可) 进入到 Mobility Master->Configuration>License", 点击 License Inventory 选项卡,点击+ 按钮来添加 license。

ALAB2-MM-1	ER	CONTROLLERS ⊘ 2 ○ 0	ACCESS POINTS CL ○ 0 ○ 0 ○ 0 ○ 0	IENTS ALERTS		0	admin 🗸
🗲 Mobility Master >							Ŷ
Che a	Configuration	License management:	🔿 Aruba Support Porta	al (ASP)	e server 🔘 Manual		
Mobility Master	Roles & Policies	License Usage License	Inventory				+
Managed Network (2)	Authentication Services	LICENSE	DESCRIPTION	STATUS	EXPIRATION	INSTALLED to this Mobility Master	
🗁 lab2 (2)	Interfaces	AP	Access Points	A Partially Expiring - Expires in 29 da	Apr 23 2020	2048	
📼 lab2-md1	Controllers	PEFNG	Policy Enforcement Firewall	A Partially Expiring - Expires in 29 da	Apr 23 2020	2048	
Iab2-md2	Controllers	RFP	RF Protect(WIP,Spectrum,Multi-z	A Partially Expiring - Expires in 29 da	Apr 23 2020	2048	
1802-1102	System	ACR	Advanced Cryptography	 Not Licensed 	Not Licensed	0	
	License	WebCC	Web Content Classification	 Not Licensed 	Not Licensed	0	
	Redundancy	MM	Mobility Master Virtual Appliance	A Partially Expiring - Expires in 29 da	Apr 23 2020	50	
		MC-VA-RW	Controller Virtual Appliance(RW)	A Partially Expiring - Expires in 29 da	Apr 23 2020	1000	
		MC-VA-EG	Controller Virtual Appliance(EG)	 Not Licensed 	Not Licensed	0	
		MC-VA-II	Controller Virtual Appliance(IL)	(-) Not Licensed	Not Licensed	0	-



To ii	nstall new licenses you will need:
~	The Serial Number of this Mobility Master: MMEAB5AB3
\checkmark	The License Key for each service you wish to activate
\checkmark	License Passphrase: MMEAB5AB3-jfYP9LIG-edTJ7Sjy-Agbgkf8b-umyz+KO
Obt	ain License Keys from HPE Aruba My Networking Portal
Ente	er the license keys in the text box below, one key per line.
Ι	
	//
	Cancel

1.3.3 虚拟机相关 (CLI)

针对 Aruba Mobility Master Virtual Appliance 的虚拟机安装,请按照官方安装向导的要求,对虚拟机硬件资源进行优化,针对不同虚拟机型号平台的服务器硬件资源相关优化项如下(下面是基于 AOS8.6 平台的要求,如果有新版本,请参考对应新版本的虚拟机型号平台的服务器硬件资源):

1)	MM-VA-50	(3 vCPUs,	6GB Memory,	6GB Flash/Disk)
----	----------	-----------	-------------	-----------------

- 2) MM-VA-500 (6 vCPUs, 8GB Memory, 8GB Flash/Disk)
- 3) MM-VA-1K (8 vCPUs, 32GB Memory, 32GB Flash/Disk)
- 4) MM-VA-5K (10 vCPUs, 64GB Memory, 64GB Flash/Disk)

5) MM-VA-10K (16 vCPUs, 128GB Memory, 128GB Flash/Disk)

注意: Aruba recommends using Intel Xeon E5-2650 v4 @ 2.2GHz enterprise grade CPUs for optimum performance. Ensure the number of sockets and threads is always one and the value of cores is the same as the current allocation.

- MC-VA-10 (4 vCPUs, 6GB Memory, 6GB Flash/Disk)
 MC-VA-50 (4 vCPUs, 6GB Memory, 6GB Flash/Disk)
 MC-VA-250 (5 vCPUs, 8GB Memory, 8GB Flash/Disk)
- 4) MC-VA-1K (6 vCPUs, 16GB Memory, 16GB Flash/Disk)



5) MC-VA-4K (12 vCPUs, 48GB Memory, 48GB Flash/Disk)

6) MC-VA-6K (14 vCPUs, 64GB Memory, 64GB Flash/Disk)

注意: Aruba recommends using Intel Xeon E5-2670 v3 @ 2.3GHz enterprise grade CPUs for optimum performance.Ensure the number of sockets and threads is always one and the value of cores is the same as the current allocation.

如果不知道自己的 VMM/VMC 平台型号,请使用 show inventory 进行查看。

(LabX-MM-1) [mynode] #show inventory

Mgmt Port HW MAC Addr : 00:0C:29:AB:5A:B3

HW MAC Addr : 00:0C:29:AB:5A:BD

Product key# : MMEAB5AB3

Activate license : Not Applicable

Active device type : MM-VA-50

对于当前系统的磁盘空间资源查看命令是 show storage,关注 /dev/sdb1 的 size 大小 (即 Flash/Disk 的空间大小).

(LabX-MM-1) [myn	node] #s	how stora	age		
Filesystem	Size	Used Av	ailable Use% Mounted on		
none	3.0G	14.1M	3.0G 0% /tmp		
/dev/sdb1	5.8G	1.0G	4.5G 18% /flash	(对应的是虚拟机中的 Hard Disk2)	
/dev/sda5	1.4G	387.9M	1015.1M 28% /mnt/disk1	(对应的是虚拟机中的 Hard Disk1)	
/dev/sda6	1.4G	420.1M	982.9M 30% /mnt/disk2	(对应的是虚拟机中的 Hard Disk1)	

对于当前系统的虚拟 CPU 数和内存大小的查看命令是 show version. (由于下面的 CLI 是 基于 demo 设备的演示,并不代表以下设备硬件资源是满足实际场景需求的使用,仅仅提供参考 和学习使用)

(LabX-MM-1) [mynode] #show version



Aruba Operating System Software. ArubaOS (MODEL: ArubaMM-VA), Version 8.6.0.3 Website: http://www.arubanetworks.com (c) Copyright 2020 Hewlett Packard Enterprise Development LP. Compiled on 2020-03-20 at 11:07:28 UTC (build 74788) by p4build BIOS Version: Phoenix Technologies LTD, 6.00 Built: 07/30/2013 Switch uptime is 1 hours 58 minutes 37 seconds Reboot Cause: User reboot (Intent:cause: 86:50) Supervisor Card Processor(s): Total CPUs : 3, Sockets : 1, Cores Per CPU : 3 Socket 0: Intel(R) Core(TM) i5-4250U CPU @ 1.30GHz 5703M bytes of memory

4096M bytes of Supervisor Card system flash.

1.3.4 LACP 链路聚合 (CLI)

MD 控制器的上联口和核心交换机互联的端口是需要使用 LACP 链路聚合(有带宽需求的话, 强烈建议设计和使用两条 10G 的链路上联核心交换机)

(LabX-MM-1) [00:0c:29:82:71:b4] (config) #interface gigabitethernet 0/0/1

(LabX-MM-1) ^[00:0c:29:82:71:b4] (config-submode)#trusted

(LabX-MM-1) ^[00:0c:29:82:71:b4] (config-submode)#lacp group 0 mode active

(LabX-MM-1) ^[00:0c:29:82:71:b4] (config-submode)#exit

(LabX-MM-1) ^[00:0c:29:82:71:b4] (config) #interface gigabitethernet 0/0/2

(LabX-MM-1) ^[00:0c:29:82:71:b4] (config-submode)#trusted

(LabX-MM-1) ^[00:0c:29:82:71:b4] (config-submode)#lacp group 0 mode active

(LabX-MM-1) ^[00:0c:29:82:71:b4] (config-submode)#exit

(LabX-MM-1) ^[00:0c:29:82:71:b4] (config) #interface port-channel 0



(LabX-MM-1) ^[00:0c:29:82:71:b4] (config-submode)#trusted

(LabX-MM-1) ^[00:0c:29:82:71:b4] (config-submode)#trusted vlan 1-4094

(LabX-MM-1) ^[00:0c:29:82:71:b4] (config-submode)#switchport mode trunk

(LabX-MM-1) ^[00:0c:29:82:71:b4] (config-submode)#switchport trunk allowed vlan all

1.3.5 LACP 链路聚合 (GUI)

1) 在 labX-md1 下,选择 Configuration > Interfaces,在 Ports 选项卡中,选择需要做端口聚合的物理端口 GE-0/0/1,在下面的详细设置菜单中,勾选 Trust,点击 Submit 按钮。

OCUDO MOBILITY MASTER Lab2-MM-1	CONTROLLERS ACCESS POINTS CLIENTS ALERTS ② 2 ○ 0 ○ 0 ○ 0 ◇ 0 △ 2	3 admin ~
Managed Network > lab2 > lab2-md1		¢
Managed Network > lab2 > lab2-md1 Dashboard Lab2-MM-1 Lab2-MM-1 Lab2-MM-1 Lab2-MM-1 Lab2-MM-1 Lab2-MM-1 Lab2-MM-1 Lab2-MM-1 Lab2-MM-1 Lab2-md1 Lab2-md1 System Lab2-md2 Lab2-md1 Lab2-m	• • • • • • • • • • • • • • •	
	VLAN trust:	
AnihaMMAVA, R 60 3		Cancel

2) 在 labX-md1 下,选择 Configuration>Interfaces,在 Ports 选项卡中,找到 Port Channel 窗口,点击+按钮,弹出 Port Channel ID 选择框,选择 PC 0,点击 Submit 按钮。



Aruba Mobility Mast Lab2-MM-1	ER	CON ©	TROLLERS	ACCESS F		CLIENTS 〒 0 №	ALER	TS 2				(2) ad	dmin 🗸	
Anaged Network > lab2 > lab2 Anaged Network > lab2 > lab2 Anaged Network > lab2 > lab2 Mohility Master S Lab2-MM-1 Managed Network (2) E lab2 (2) D tab2 = dt	Pashboard P Configuration WLANS Roles & Policies Access Points	Orts VLA Port Chanr NAME	2 0 0	⊙ 0 utes IF	© 0 2v6 Neighbo PROTOCOL	rs GRE	0 🛆 Tunnels	2 Pool Manag PoLICY	gement (MODE	DSPF M	lulticast NATIVE VLAN	I TRUNK I	/Lans [¢
C lab2-md1 C lab2-md2	AP Groups Authentication Services Interfaces Controller System	Ports PORT GE-0/0/0	ADMIN ST	TRUSTED	POLICY	MODE	NATIVE V	ACCESS V	TRUNK VL	SPANNIN	MONITOR	DESCRIPT	E	
	Tasks Redundancy Maintenance	GE-0/0/1 GE-0/0/2 + GE-0/0/0 Admin.st	Disabled Disabled	-	Not-defined Not-defined	access access	1	1	1-4094 1-4094					
	ArubaMM-VA, 8.6.0.3											Cancel	Su	



3) 进入到 PC 0 配置界面,按照图中所示的参数进行相关配置即可,最后点击 Submit 按钮和 pending change 按钮。



			ii nouces ii	IPv6 Neight	oors GRE	lunneis	Pool Mana	gement	OSPF Mu	lticast						
		PC-0														-
		Port channel II	D: PC-0													
		Protocol:	LACP 💙													
		LACP mode:	active 🗸													
		Deut members	GE-0/0/0.GE-0	0/0/1 Edit												
		Admin state:	M													
		Trust:	М													
		Policy:	Not-defined		-											
		Mode	Touck	٦												
		Mode.	Trunk													
Allowed Valies: Note: Description:		Native VLAN:	1 ~													
		Allowed VLANS	Allow all		~											
		Description														
		Description.			le la											
		Jumbo MTU:														
																1.
	S	Show advanced op Ports	otions													
		PORT	AD MIN STATE	TRUSTED	POLICY	MODE	NA	IVE VLAN	ACCESS VLAN	TRUN K VLAN	5 SPANNING	S TREE MONI	TORING D	ESCRIPTION	m	
		GE-0/0/0	Enabled	~	Not-defined	trunk	1		1	1-4094	-	-	-			
GE 002 Diabled Nocidefind access 1 1 1.024 n <		GE-0/0/1	Disabled	2	Not-defined	access	1		1	1-4094		-	G	E0/0/1		
WallTY MASTR CONTROLLES CONTROLES CONTROLLES CONTROLLES CONTROLLES CONTROLLES CONTROLLES CONTROLL		GE-0/0/2	Disabled	-	Not-defined	access	1		1	1-4094		-			_	-
Perding Changed Managed Network (> lab2) bb2-md1 Mathematication System Tasks Redundancy Maintenance Post Numater Numater Numater Numater Numater Numater Numater		ITY MASTER 2-MM-1				c	ONTROLLERS	ACCESS POIN	TS CLIEN	TS ALERTS					()	admin v
Amage Network \$ 1802 > 1802-1801 Pathodd Ports VLANs Ports						(2 0 0	00	0 0	∞ 0 <u>∆</u> 2					Paudia	changes
Nable Value Ports VLANs IP Routes IP Route	 Managed Network > lab; 	2 > lab2-md1													Pendin	ng Changes
Instruction Port Name Port Name Port of Columnation Port of Colum	Mobility Master	Configu	ard	Por	ts VLANs	IP Routes	IPv6 Neighbo	rs GRE Tun	nels Pool Ma	anagement C	SPF Multica	st				
Managed Network (2) Roles & Policies Name Members PROTOCOL TRUSED POLY More Name Name TRUNK VAANS <	🖘 Lab2-MM-1	WLA	Ns		Port Channel											
Access Points Access Points Rcd - LACP - Nacdefined tount 1 1-404 A Droups Authentication	Hanaged Network (2)	Role	s & Policies		NAME	MEMBER	15	PROTOCOL	TRUST	ED	POLICY	MODE		NATIVE V LAN	TRUNK VLA	INS (
AP Groups AP Groups A Mathemication Authemication Specifies Authemication Interfaces Interfaces Controller Fort System Geboro Tasks Geboro Redundaryy Geboro Maintenance + + +	🔁 lab2 (2)	Acce	ess Points		PC-0	-		LACP	~		Not-defined	trunk		1	1-4094	
Authentication Services Authentication Interfaces Interfaces Controller Forts Tasks Foot Nos-defined FC-0 1 1 1-094 - - 62000 Exection E Redundarry GE00/2 Dassied - Nos-defined Rctess 1 1 1-094 - - 6200/0 - - 6200/0 - - 6200/0 - - 6200/0 - - 6200/0 - - 6200/0 - - 6200/0 - - 6200/0 - - 6200/0 - - - 6200/0 - - 6200/0 - - - 6200/0 -	🕞 lab2-md1	AP (āroups													
Services Interface System Poter ADMIN State TBUSTED NATIVE VIAN ACCESS VIAN TBUNKVLANS SPANNING TREE MONITORING DESCRPTION Controller System Poter ADMIN State TBUSTED PoLLEY NOTO NATIVE VIAN ACCESS VIAN TBUNKVLANS SPANNING TREE MONITORING DESCRPTION C Tasks GE-00:0 Basiled I Not-defined RC 1 1 1-4094 - - GE-00:0 Redundaryy GE-00:1 Dassiled I Not-defined Rcess 1 1 1-4094 - - GE-00:0 Maintenance I Not-defined Rcess 1 1 1-4094 - - - -	🕒 lab2-md2	Auti	nentication													
Controller Perts System Foot ADMIN STATE TBUSTED POLICY MADE NATIVE VLAN ACCESS VLAN TBUNKVLANS SPANNING TEEE MONTORING DESCRIPTION TE Tasks GE-00-0 Enabled - Ibos-defined FC-0 1 1 1-4094 - - GE-00-0 Redundancy GE-00-1 Dabatied - Nos-defined Rccess 1 1-4094 - - GE-00-0 Maintenance - Nos-defined excess 1 1-4094 - - -		linte	rfaces		+											
System Poet ADMIN State TBUSTE POLCY MODE NATIVE VLAM ACCESS VLAM TBUNT VLAMS SPANNING TREE MONTORING DESCRIPTION DESCRIPTION <thdescription< th=""> DESCRIPTION</thdescription<>		Con	troller		Ports											
Tasks GE-00:0 Enabled • Noc-defined FC-0 1 1 1-494 - - GE00:0 Redundancy GE-00:0 Daskied • Noc-defined FC-0 1 1 1-494 - - GE:00:0 Redundancy GE-00:0 Daskied • Noc-defined access 1 1 1-494 - - GE:00:0 Maintenance + - Noc-defined access 1 1 1-494 - - -		Syst	em		PORT	ADMIN STATE	TRUSTED	POLICY	MODE	NATIVE VLAN	ACCESS VLAN	TRUNK VLANS	SPANNING TREE	MONITORING	DESCRIPTION	f
Redundancy GE-00/2 Disabled - Not-defined rc-or 1 1-4094 - - GE-00/1 Maintenance + - - - - - - -		Task	(S		GE-0/0/0	Enabled		Not-defined	PC-0	1	1	1-4094			GE0/0/0	
Maintenance +		Pad	undancy		GE-0/0/2	Disabled	-	Not-defined	access	1	1	1-4094			12EW0/1	
+		Red														
		Mainter	ance													
		Mainter	ance		+											
		Mainter	lance		÷											
		Mainter	lance		÷											

1.3.6 Jumbo Frame (CLI)

AP 和控制器中间互联的所有有线交换机强烈建议开启 Jumbo Frame,控制器需要全局开 启 Jumbo Frame,并在和核心交换机的上联口上开启 Jumbo Frame (开启 Jumbo 前,需要先 确认和评估对现网 OSPF 路由环境的影响,因为会改变 MTU 大小)

(LabX-MM-1) [labX] (config) #firewall



```
(LabX-MM-1) ^[labX] (config-submode)#jumbo mtu 9216
(LabX-MM-1) [00:0c:29:82:71:b4] (config) #interface gigabitethernet 0/0/1
(LabX-MM-1) ^[00:0c:29:82:71:b4] (config-submode)#jumbo
(LabX-MM-1) [00:0c:29:82:71:b4] (config) #interface port-channel 0
(LabX-MM-1) [00:0c:29:82:71:b4] (config-submode)#jumbo
```

1.3.7 Jumbo Frame (GUI)

1) 在 labX 下,选择 Configuration > Services,在 Firewall 选项卡中,勾选 Jumbo frames processing

ACTOR MOBILITY MASTI Lab2-MM-1	ER	CONTROLLES ACCESS POINTS CLIENTS ALERTS ○ 2 ○ 0 ○ 0 ○ 0 ○ 0 △ 2	🕐 admin 🛩
Managed Network > lab2 > Managed Network > lab2 > Mobility Master Lab2-MM-1 Managed Network (2) Lab2-MM-1 Managed Network (2) Lab2-MM-1 Managed Network (2) Lab2-MM-1 Managed Network (2) Bab2-md2	IR Configuration WLAYS Roles & Policies Access Points A Address Points A Address Points Interfaces Controllers System	CUISTERS ACCESS POINTS CLIENTS ALERTS © 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	 admin > أي المحمد الم المحمد المحمد المحم المحمد ال
	Tasks Redundancy Maintenance	Rate limit CP AIC transfig (ppg) Rate limit CP I2 protocolidver traffic (ppg) Rate limit CP I2 and process traffic (ppg) Rate limit CP IXE traffic (ppg) Jumbo frames processing Mark management frames: Enable deep packet Inspection: Enable web content classification: Drop packets during web content cache miss: > ACL White List	Carcel Education

2) 自动显示隐藏菜单 Jumbo MTU bytes,默认设置 9216 bytes,最后点击 Submit.



Clusters AirGroup VPN Firewall IF	Mobility External Services DHCP WAN	
Pata limit CB untructed usart traffic (apc):		4
Race infine CP unit usted dease traine (pps).		
Rate limit CP untrusted mcast traffic (pps):		
Rate limit CP trusted ucast traffic (pps):		
Rate limit CP trusted mcast traffic (pps):		
Rate limit CP route traffic (pps):		
Rate limit CP session mirror traffic (pps):		
Rate limit CP VRRP traffic (pps):		
Rate limit CP ARP traffic (pps):		
Rate limit CP I2 protocol/other traffic (pps):		
Rate limit CP auth process traffic (pps):		
Rate limit CP IKE traffic (pps):		
Jumbo frames processing:	M	
Jumbo MTU bytes:	9216 bytes	
Mark management frames:		
Enable firewall visibility:		
Enable deep packet inspection:		
Enable web content classification:	0	- 11
Drop packets during web content cache miss:		
	Cancel	mit

3) 在 labX-md1 下,选择 Configuration>Interfaces,在 Ports 选项卡中,选择 GE-0/0/0,在下面出现 详细编辑窗口,勾选 Jumbo MTU,最后点击 Submit 按钮。

aruba	MOBILITY MAST Lab2-MM-1	TER			CONTROLLERS	ACCESS PO	INTS	CLIENTS ALE	ERTS					admin ~
🗲 Managed Netw	ork > lab2 > lab	2-md1												Pending Changes (
Ek.	۹	Dashboard	Ports VLAN	s IP Rout	tes IPvő Neighb	ors GRE Tu	unnels Po	ol Management	OSPF N	Aulticast				
🔁 Mobility Master		Configuration	PORI	AU 1011 31A	IL INVOILD	POLICI	MODE	INVESTIGE VERM	ALLESS VERI	INVER VENES	SPANNING INC.	MONTOKING	DESCRIPTION	ш
🕒 Lab2-MM-1		WLANs	GE-0/0/0	Enabled	~	Not-defined	trunk	1	1	1-4094				
🔁 Managed Netwo	ork (2) 🛛 🕂	Roles & Policies	GE-0/0/1	Disabled	-	Not-defined	access	1	1	1-4094		-		
🔁 lab2 (2)		Access Points	GE-0/0/2	Disabled	-	Not-defined	access	1	1	1-4094		-		
🕞 lab2-m	nd1	AP Groups												
🕒 lab2-m	nd2	Authentication	+											
		Services	GE-0/0/0											
		Interfaces	Admin stat	E.	м									
		Controller	Speed:		auto 💙 Mbps									
		System	Duplex:		auto 💙									
		Tasks	PoE:											
		Redundancy	Trust:		M									
		Maintenance	Policy:		Not-defined	~								
			Mode:		Trunk 👻									
			Native VLA	4:	1 👻									
			Allowed VL	ANS:	Allow all	~								
			Description	c		li:								
			Tunneled n	ode:										
			Jumbo MTU	1:	M									
			(i) The current s	et of pending o	hanges must be deplo	yed or discarde	d before chang	es to this page can be	e made.				I	Cancel Submit

4) 在 labX-md1 下,选择 Configuration>Interfaces,在 Ports 选项卡中,选择 PC-0,在下面出现详细 编辑窗口,勾选 Jumbo MTU,最后点击 Submit 按钮。

ALADO MOBILITY MASTER Lab2-MM-1	R		CONTROLLERS ⊘ 2 ○ 0	ACCESS POINTS	CLIENTS ALE	RTS 2			adm	iin ¥
Managed Network > lab2 > lab2-	-md1								Pending C	hanges 🗘
Mobility Master Managed Network (2) Plab2 (2) Clab2-md2	Dashbaard Configuration WLANS Roles & Policles Access Points A P Groups Authentication Services Interfaces Controller System Tasks Redundancy Maintenance	VLANS II NAM FCO FCO FCO Port channel ID: Port members: Administra: Noise: Native VLAN: Description:	P Routes IPv6 Neighbo MEMBES 	rs GRETunnels PROTOCOL LKCP	Pool Management IBURTED	OSPF Multicast POLICY Not-defined	MODE	T	TRINK VLAVS 5-054	
	ArubaMMAVA, 8.6.0.3	L							Cancel	Submit

1.3.8 MTU (CLI)

如果有线网络没有使用 Jumbo Frame,强烈建议将 AP-system-profile 中的 SAP MTU 手动指定为 1500。

(LabX-MM-1) [labX] (config) #ap system-profile mtu-1500

(LabX-MM-1) ^[labX] (AP system profile "mtu-1500") #mtu 1500

1.3.9 MTU (GUI)

1) 在 lab<mark>X</mark>下,选择 Configuration>System,在 Profiles 选项卡中,选择 AP system,点击 AP system profile 右边的+ 按钮。



ACTUDO MOBILITY MAST Lab2-MM-1	ER	CONTROLLERS ACCESS ⊘ 2 ○ 0 ⊘ 0	SPOINTS CLIENTS ALERTS ○ 0 ○ 0 ▷ 0 △ 2	admin ~
Managed Network > lab2 >				Ŷ
C <u>k</u> Q	Dashboard	Canaral Admin AidMana CDCas Cartificates		
🔁 Mobility Master	Configuration	deneral Admin Anwave Criset Certificates	s sinne Logging Fromes more	
🖾 Lab2-MM-1	WLANS	All Profiles	AP system profile: New Profile	
🔁 Managed Network (2)	Roles & Policies	AP LACP LMS map information		
🔁 lab2 (2) 🛛 🕂 🖉 🔟	Access Points	AP LLDP	AP system profile:	
🖘 lab2-md1	AP Groups	AP LLDP-MED Network Policy		
lab2-md2	Authentication	AP multizone		
	Services	\ominus 🕞 AP system		
	Interfaces			
	Controllers	🕀 🖻 default		
	System	AP wired port		
	Tasks	Dump collection		
	Redundancy	EDCA Parameters (AP)		
	Maintenance	EDCA Parameters (Station)		
		MU EDCA Parameters		
		Regulatory Domain		
		🔄 Spectrum Local Override		
4	ArubaMM-VA, 5.6.0.3			

2) 进入到 Ap system profile 新增窗口, 输入 Profile name 名称和 SAP MTU=1500, 最后点击 Submit 按钮和 pending Changes 按钮。

AP LACP LMS map information	Profile name: mtu-1500		
AP LLDP	V General		
AP LLDP-MED Network Policy			
AP multizone	RF Band:	g 💙	
\ominus 📑 AP system	RF Band for AM mode scanning:	all 👻	
① I NoAuthApSystem	Native VLAN ID:	1	
(+) 🕒 default	WIDS AMPDU Optimization:		
⊕ G AP wired port	Session ACL:	ap-uplink-acl	
Dump collection			
EDCA Parameters (AP)			
EDCA Parameters (Station)			
① MU EDCA Parameters	Corporate DNS Domain:		
① Regulatory Domain			
🕒 Spectrum Local Override	-	+	
	SNMP sysContact:		
	LED operating mode (11n/11ac APs only):	normal 👻	
	LED override:		
	Driver log level:	warnings 🗸	
	Console log level:	emergencies 💙	
	SAP MTU:	1500 bytes	

1.3.10 NTP Server (CLI)



MM+MD 控制器集群架构下的每台设备的初始化国家代码、时区和时间需要同步,当前的时间是否一致,强烈建议设置 NTP Server:

(LabX-MM-1) [mynode] #show country

Country:CN

Model:ArubaMM-VA

Regulatory Domain:Unrestricted

(上述配置中的 Country: CN 是在系统初始化阶段配置好的,如果发现 MM 和 MD 控制器之间的国家代码不匹配,强烈建议重新初始化设置成一致,无法在系统运行状态下设置,而你通过设置 regular-domain-profile 中的 country code 也是无用的)

Cd /mm ---针对 主备两台 MM 控制器设置 ntp server

(LabX-MM-1) [mm] # ntp server 114.4.50.17

Cd /md/labX ---针对 labX 下的所有 md 控制器设置 ntp server

(LabX-MM-1) [labX] (config) #ntp server 114.4.50.17

1.3.11 NTP Server (GUI)

1) 在 labX 下,选择 Configuration > System,在 General 选项卡中,选择 Clock。

Cruba MOBILITY M. Lab2-MM	ASTER 1-1		CONTROLLERS ACCE	SS POINTS CLIENTS ○ 0 ○ 0 ○ 0	ALERTS		🕐 ad	min ¥
Managed Network > lab2 >								Ŷ
Mobility Master Lab2-MM-1 Managed Network (2)	Q Dashboard Configuration WLANS Bolar & Belizier	General Admin Basic Info	AirWave CPSec Certifica	es SNMP Logging	Profiles More			
☐ lab2 (2) ☐ lab2-md1 ☐ lab2-md2	Access Points AP Groups Authentication	Set clock: Time zone:	Using NTP Choose a timezone	×				
	Services		IR ADDRESS	IRLINST MODE	AUTHENTICATION VEV ID			
	Controllers System Tasks			NORT MODE	AUTHENTICATION RETTO	UU.		
	Maintenance		+					
		Use NTP authentication:)					
		> Domain Name System	1					
		 Controller IP address 						
	ArubeMM-VA, 8.6.0.3						Cancel	Submit



 2) 设置 Time zone 为 China:Asia/Shanghai (UTC+08:00),在 NTP Servers 窗口中点击+ 按钮,在 Add NTP Serve 窗口中,输入 IP address 为您的 NTP 服务器地址(这里参数仅仅是演示,请根据实际环境 中来设置),最后点击 Submit 按钮和 pending Changes 按钮。

Set clock:	Using NTP 💙				
Time zone:	China: Asia/Shanghai (UTC+08:00)	*			
	NTP Servers				
	IP ADDRESS	IBURST MODE	AUTHENTICATION KEY ID	=	
	+				
	+ Add NTP Server				
	Add NTP Server				
	Add NTP Server IP version: IPv4 IP address: 114.4.50.17				
	H Add NTP Server IP version: IPv4 ♥ IP address: 114.4.50.17 Iburst mode: I				

1.3.12 Spanning-Tree (CLI)

硬件 MD 控制器采用旁挂方式和核心交换机互联时(即单臂部署模式下),强烈建议全局 下关闭 Spanning-Tree 协议

(LabX-MM-1) [labX] (config) #no spanning-tree

Spanning tree disabled at system level, Interface/vlan level spanning-tree configuration will not be effective

1.3.13 Spanning-Tree (GUI)

1) 在 labX 下,选择 Configuration > System,在 More 选项卡中,选择 Spanning Tree。将 Enable spanning tree 设置关闭 (默认系统是开启的),点击 Submit 按钮和 Pending Changes 按钮。





ADDILITY MASTER Lab2-MM-1	CONTROLLERS ACCESS POINTS CLIENTS ALERTS ∅ 2 ◯ 0 ◯ 0 ◯ 0 ∅ 0 № 0 ▲ 2) admin 🛩
← Managed Network > lab2 >		Pending Changes 🗘
 Construction Construction	General Admin AirWare CP Sec Certificates S NMP Logging Profiles LoCP Capacity Thresholt Phone Home General Mobility Manager Server S MTP S MTP Mobility Manager Server S MTP S MTP Mobility Manager Server Mobility Manager Server Mobility Manager S	Cancel

1.3.14 ADP (CLI)

AP 如果采用 DHCP, DNS 或者静态方式发现控制器,强烈建议全局下关闭 ADP 协议

(LabX-MM-1) [labX] (config) #no adp discovery

(LabX-MM-1) ^[labX] (config) #no adp igmp-join

可以 mdconnect 到每台 md 上,使用 show adp config 来查看当前配置是否是 disable 状态(注意系统默认是开启的):

(labX-md1) [MDC] #show adp config

ADP Configuration

key value

discovery disable

igmp-join disable

igmp-vlan-id 0

1.3.15 VRRP (CLI)

针对 Aruba 控制器之间创建的 Cluster VRRP VID 信息,在同一个 vlan 下,请注意我们的 VID 和用户已有有线网络中的 VRRP VID 不能有冲突,否则会导致 VRRP 的 抖动和脑裂。注意点: 我们的控制器之间创建的 VRRP 冗余集群,会建立和设置 VID 号,针对 AOS6.x 可以自己设置指 定 VID,而针对 AOS8.x 的 Cluster 集群,如果启用了 Cluster VRRP IP 设置,那么系统默认就会 自动使用 VRRP ID=220,221...一直到 255,在 AOS8.4 之前(含 v8.4)不支持修改起始 VRRP ID 号,在 AOS8.5 及以上时可以支持自定义 VRRP VID 的开始 ID 号)。另外针对 AOS8.4 及之前版 本,解决办法:必须使用两个 cluster,那么强烈建议设计两个不同的 VLAN 管理段,或设计其中 一个集群关闭 Cluster VRRP IP 功能(但仍然可以建立 Cluster,但是 Cluster 下就无法使用 AAA 的 CoA 和 XML API 功能)

(LabX-MM-1) [labX] (config) #lc-cluster group-profile labX-cluster

(LabX-MM-1) [labX] (Classic Controller Cluster Profile "labX-cluster") #controller 10.2.10.11 priority 128 mcast-vlan 0 vrr p-ip 10.2.10.21 vrrp-vlan 30 group 0

(LabX-MM-1) [labX] (Classic Controller Cluster Profile "labX-cluster") # controller 10.2.10.12 priority 128 mcast-vlan 0 vrr p-ip 10.2.10.22 vrrp-vlan 30 group 0

(LabX-MM-1) [labX] (Classic Controller Cluster Profile "labX-cluster") #vrrp-id 100

1.3.16 VRRP (GUI)

1) 在 labX 下,选择 Configuration > Services,在 Clusters 选项卡中,点击+ 按钮,进入到新建 Cluster 界面

ALADO MOBILITY MAST Lab2-MM-1	ER		CONTROLLERS ACCESS POINT: ⊘ 2 ○ 0 ○ 0 ○ 0	S CLIENTS ALERTS 0 ○ 0 ▲ 2		③ admin ~
Managed Network > lab2 >						
Ck Q	Dashboard Configuration	Clusters AirGroup	VPN Firewall IP Mobility E	ternal Services DHCP WAN		
Lab2-MM-1	WLANs	Clusters (1)				
Managed Network (2)	Roles & Policies	NAME	CONTROLLERS	FIRMWARE VERSION	UPGRADE STATUS	t
🔁 lab2 (2)	Access Points	lab2-cluster	2	8.6.0.3_74788	N/A	
😑 lab2-md1	AP Groups					
lab2-md2	Authentication					
	Services	+				
	Interfaces					
	Controllers					
	System					
	Tasks					
	Redundancy					
	Maintenance					
	ArubaMM-VA, 8.6.0.3					

 输入 name 为 cluster 名称, Starting VRRP ID=100, 这个就是我们设置的起始 VRRP ID 号, 系统会 自定创建从 VID 100 开始的 VRRP Instance, 如果您不设置的话, 系统自动将从 ID 220 开始计算, 点击+ 按钮, 进入到新增 Controllers 界面。



AME	CONTROLLER5	FIRMWARE VERSION	UPGRADE STATUS	Œ
p2-cluster	2	8.6.0.3 <u>7</u> 4788	<u>N/A</u>	
w Cluster Profile				
Name: lab2-cluster				
Controllers				
IP ADDRESS GROUP	VRRP-IP VRRP-	VLAN RAP PUBLIC IP MCAST-V	VLAN	
+				
Starting VRRP ID: 100				

3) 分别将两台 MD 控制器加入到该 Cluster 中,设置 IP address, VRRP IP, VRRP VLAN 和 Priority 等, 点击 OK 按钮,完成添加。

Add Controller	
IP version:	IPv4 💙
IP address:	10.2.10.11 👻
Group:	-None- 💙
VRRP IP:	10.2.10.21
VRRP VLAN:	30 🗸
RAP public IP:	
MCast VLAN:	
Priority:	128
	Cancel OK



isters (1)								
ME		CONTROLLERS	F	IRMWARE VERSION	U	PGRADE STATUS		
2-cluster		2	8	.6.0.3_74788	N	<u>I/A</u>	C	₽ Ç
ister Profile > la	o2-cluster							
Basic								
Name:	lab2-cluste	r						
Controllers								
IP ADDRES	S GROUP	VRRP-IP	VRRP-VLAN	RAP PUBLIC IP	MCAST-VLAN	Ē		
10.2.10.11		10.2.10.21	30	0.0.0.0				
10.2.10.12		10.2.10.22	30	0.0.0.0				
+								
	ID: 100							
Starting VRRF								
Starting VRRF								

4) 添加完成后,看到下面的信息,最后点击 Submit 按钮和 Pending Changes 按钮。

1.3.17 CPSec (CLI)

如果没有对 AP 的控制和管理信令的安全加密要求时,我们不建议开启 CPSec 功能,该功能会让每个 AP 和控制器建立 IPSec 隧道,用于封装 AP 和控制器之间的管理和控制流量。

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

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

1.3.18 CPSec (GUI)

在 labX 下,选择 Configuration>System,在 CPSec 选项卡中,在 Control Plane Security 下将 Enable CPSec 开关设置为关闭状态,最后点击 Submit 按钮和 Pending Changes 按钮。




	LITY MASTER b2-MM-1	CONTROLLERSACCESS POINTSCLIENTSALERTS \oslash 2 \odot 0 \odot 0 \odot 0 \diamondsuit 0 \bigtriangleup 2	admin ~
🗲 Managed Network > lal	b2 >		Ś
 Mobility Master Lab2-MM-1 Managed Network (2) Lab2 (2) Lab2-md1 Lab2-md2 	Configuration WLANS Roles & Policies Access Points AP Groups Authentication Services Interfaces Controllers System Tasks Redundancy Maintenance	eral Admin AirWare PSec Certificates SNMP Logging Profiles More	Cancel
	ArubaMM-VA, 8.6.0.3		

1.3.19 IPv6 (CLI)

在 IPv6 的部署环境中,由于 AOS8.X CLuster 架构设计需要用户网关指向到上层核心交换 机,也就是 2 层的部署模式,在这个模式下,上层的路由设备会提供含有 IPv6 Prefixes 前缀的路 由宣告 RA 给到客户端,当一个客户端连接网络时,它将开始发送广播的路由恳求或者 DHCP IPv6 请求,在使用路由宣告的 SLAAC 无状态地址自动配置的环境中,上层路由器能够或者响应单 播的路由器宣告或者响应组播的路由宣告,无论什么时候,新的客户端加入网络时,都会收到一个 单播或者一个组播的路由宣告,如果它是一个组播的路由宣告报文,那么对于其他已经关联的客户 端也会收到该组播的路由宣告,这样会导致网络流量的增加,我们可以采用 IPv6 Proxy RA 来侦 听进来的路由宣告报文,并代理单播转发给指定的客户端,从而减少网络中的无用开销流量。

(LabX-MM-1) [labX] (config) #ipv6 proxy-ra

1.3.20 IPv6 (GUI)

在 labX 下,选择 Configuration > Services,在 Firewall 选项卡中,勾选 IPv6 proxy RA,最后点击 Submit 按钮和 Pending Changes 按钮。







1.4 射频层面的优化项

1.4.1 2.4Ghz 频宽 (CLI)

对于 2.4G 的频宽,任何场景下,都是 20Mhz,特殊场景下也可以选择性地将部分 AP 的 2.4G radio 关闭或者变成 AM/SM 模式或者全部禁用,减少同频和邻频的干扰



1.4.2 2.4Ghz 频宽 (GUI)

在 labX 下,选择 Configuration>System,在 Profiles 选项卡中,选择 RF Management >2.4GHz radio>labX-11g-radio-profile,取消勾选 Radio enable,选择 Mode 为 am-mode/spectrum-mode,最后点 击 Submit 按钮和 Pending Changes 按钮。

MOBILITY MASTI Lab2-MM-1	ER	CONTROLLERS ACCESS P ⊘ 2 ○ 0 ○	OINTS CLIENTS ALERTS ○ 0 ○ 0 ▷ 0 ▲ 2			admin ×
← Managed Network > lab2 >						Ġ
Managed Network > lab2 > Mobility Master Lab2-MM-1 Managed Network (2) Isb2 (2) Isb2 (2) Isb2-md1 Isb2-md2	Dashboard Configuration WLANS Roles & Policies Access Points AP Groups Authentication Services Interfaces Controllers [System Tasks Redundancy	General Admin AirWave CPSec Certificates All Profiles C Tother Profiles C Policy Domain C COS C RF Management C 2.4 GHz radio C default Adaptive Radio Management (ARM) Adaptive Radio Management (ARM) High-throughput radio	SNMP Logging Profiles More 2.4 GHz radio profile; lab2-11g:radio-profile C General Radio enable: Mode High throughput enable (radio): High efficiency enable (radio): High efficiency enable (radio): Non-Wi-Fi Interference Immunty: Spectrum Monitoring: Max Channel Bandwidth:	Image: spectrum-mode spectrum-mode spectrum-mode l 2 l 2		e
	Maintenance	Image: Second	Min ERP: Max ERP: ERP offset: Deploy changes daily at: Association Boost: > Advanced	200442 • 6 • 12 • • • • •	dBm dB 30 hrs Cancel	submit As



1.4.3 5Ghz 频宽 (CLI)

对于 5G 的频宽,高密度场景下仅使用 20Mhz,中低等密度下可以考虑用 40Mhz,但仍然不建议使用 80Mhz。

针对 MM+MD 架构下,是在 dot11a-radio-profie 下设置

(LabX-MM-1) [labX] (config) #rf dot11a-radio-profile labX-11a-radio-profile

Warning: If there is an entry for a radio in 'ap spectrum local-override' profile on the local controller that terminates the AP, that entry will override the mode selection in the radio profile.

(LabX-MM-1) ^[labX] (802.11a radio profile " labX-11a-radio-profile ") #min-channel-bandwidth 20MHz

(LabX-MM-1) ^[labX] (802.11a radio profile " labX-11a-radio-profile ") #max-channel-bandwidth 40MHz

针对 Standalone 架构下,是在 arm-profie 下设置

(LabX-md2) [mynode] (config) #rf arm-profile labX-11a-arm-profile

(LabX-md2) ^[mynode] (Adaptive Radio Management (ARM) profile " labX-11a-arm-profile ") #no 80MHz-support

Or

(LabX-md2) ^[mynode] (Adaptive Radio Management (ARM) profile " labX-11a-arm-profile ") #40MHz-allowed-bands none

1.4.4 5Ghz 频宽 (GUI) MM+MD 架构

在 labX 下,选择 Configuration>System,在 Profiles选项卡中,选择 RF Management >5 GHz radio>labX-11a-radio-profile(没有的话,请新建一个),选择 Max Channel Bandwidth为 40MHz,最后点 击 Submit 按钮和 Pending Changes 按钮。



ALADZA MOBILITY MASTI Lab2-MM-1	ER	CONTROLLERS ACCES ⊘ 2 ○ 0 ⊘ 0	S POINTS CLIENTS ALERTS ○ 0 ○ 0 ♪ 0 ▲ 2			() adr	min 🛩
Managed Network > lab2 >							¢)
Managed Network > lab2 > Add the second se	Dashboard Configuration WLANS Roles & Policies Access Points AP Groups Authentication Services Interfaces Controllers System Tasks Redundancy Maintenance	Q Q Q Q General Admin AirWave CPSec Certificate All Profiles Q Policy Domain Q Q OS P Folicy Domain Q Q S P Folicy Domain Q T Schur radio Q T Schur radio Q T Schur radio Q T Promonitoria Q T Procen-a Q T Poscan-a Q T Schur radio	Constant of the second se	✓ ap-mode ✓ ✓ ✓ 22 200/HZ ✓ 15 21 0 0	88m 88m 98 90 hrs		\$
			> Advanced				Ţ
	ArubaMM-VA.8.6.0.3				Cancel	mit Subr	mit As

1.4.5 5Ghz 频宽 (GUI) Standalone 架构

在 labX-MC2-Standalone 下,选择 Configuration>System,在 Profiles 选项卡中,选择 Adaptive Radio Management (ARM) >labX-11a-arm-profile, 取消勾选 80MHz support,选择 Allowed bands for 40MHz channel 为 None,最后点击 Submit 按钮和 Pending Changes 按钮。

aruba	MOBILITY CONTROLLER Lab2-MC2-Standalone	ACCESS POINTS CLIENTS ALERTS ○ 0 ① 1 □ 0 ▲ 1	admin ~
Mobility Control	er > Lab2-MC2-Standalone		Pending Changes 🗘
Dashboard	General Admin AirWave CPSec Certificates	SNMP Logging Profiles Whitelist More	
WLANS	All Profiles	Adaptive Radio Management (ARM) profile: lab2-11a-arm-profile	
Roles & Policies	RF Management	✓ General	
Access Points	2.4 GHz radio		
AP Groups	GHz radio	Assignment: single-band	
Authentication	802.11 60GHz radio	80MHz support:	
Services	802.11a secondary radio	Allowed bands for 40MHz channels: None 💙	
Interfaces	AM Scanning	160MHz-support: None 🗸	
System	Adaptive Radio Management (ARM)	Min Tx EIRP: 9 🗸	
Tasks	🕒 arm-maintain	Max Tx EIRP: 127 ¥	
Redundancy	🕒 arm-scan		
Diagnostics	🕒 default-a		
Maintenance	🕒 default-g	> Advanced	
	🖻 lab2-11a-arm-profile 👘	> Scanning	
	High-throughput radio		
	RF Event Thresholds		
Aruba7010, 8.6.0.	2		Cancel Submit Submit As

1.4.6 DFS (CLI)

如果周边存在雷达信号,强烈建议 5G 频段下移除 DFS 信道 (52,56,60,64 在中国属于 DFS)



(LabX-MM-1) [labX] (config) #ap regulatory-domain-profile remove-dfs-domain-p	orofile
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") #	country-code CN
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") #	valid-11g-channel 1
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") #	valid-11g-channel 6
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") #	valid-11g-channel 11
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") #	valid-11a-channel 36
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") #	valid-11a-channel 40
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") #	valid-11a-channel 44
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") #	valid-11a-channel 48
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") #	valid-11a-channel 149
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") #	valid-11a-channel 153
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") #	valid-11a-channel 157
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") #	valid-11a-channel 161
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") #	valid-11a-channel 165
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") #	valid-11g-40mhz-channel-pair 1-5
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") #	valid-11g-40mhz-channel-pair 7-11
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") #	valid-11a-40mhz-channel-pair 36-40
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") #	valid-11a-40mhz-channel-pair 44-48
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") # 53	valid-11a-40mhz-channel-pair 149-1
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") # 61	valid-11a-40mhz-channel-pair 157-1
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") # 48	valid-11a-80mhz-channel-group 36-
(LabX-MM-1) [labX] (Regulatory Domain profile "remove-dfs-domain-profile") # -161	valid-11a-80mhz-channel-group 149
(LabX-MM-1) [labX] (config) #ap-group test-group	
(LabX-MM-1) ^[labX] (AP group "test-group") #regulatory-domain-profile remov	ve-dfs-domain-profile



1.4.7 DFS (GUI)

在 labX 下,选择 Configuration>System,在 Profiles 选项卡中,选择 AP>Regulatory Domain>remove-dfs-domain-profile,取消 Channel 52-64 相关的所有信道,最后点击 Submit 按钮和 Pending Changes 按钮。

aruba "	Lab2-MM-1	R		CONTROLLERS ACCESS ⊘ 2 ○ 0 ○ 0	POINTS CLIENTS ALERTS ○ 0 ○ 0 ▷ 0 △ 2	⑦ admin ∨
← Managed Network >	lab2 >					Pending Changes $ \varphi \rangle$
C Mobility Master	۹	Dashboard Configuration	General	Admin AirWave CPSec Certificates	SNMP Logging Profiles	More
🖼 Lab2-MM-1		WLANS	All Prof	iles	Regulatory Domain profile: remove-d	fs-domain-profile
Managed Network (2))	Roles & Policies		AP LACP LMS map information	Country Code:	CN - China 👻
🗁 lab2 (2)		Access Points	(G AP LLDP		▶ 1 2 3 4 5 ▶ 6 7 8
😑 lab2-md1		AP Groups	(AP LLDP-MED Network Policy	Valid 802.11g channel:	9 10 🔽 11 12 13
😑 lab2-md2		Authentication	(AP multizone		✓ 36 ✓ 40 ✓ 44 ✓ 48 52 56 60
		Services	(AP system	Valid 802.11a channel:	64 M 149 M 153 M 157 M 161 M 165
		Interfaces	(AP wired port		✓ 1.5 2.6 3.7 4.8 5.9 6.10 ✓ 7.11
		Controllers	(Dump collection	Valid 802.11g 40MHz channel pair:	8-12 9-13
		System	(EDCA Parameters (AP)		26.40 × 44.48 52.56 60.64 × 149.152
		Tasks	(+) EDCA Parameters (Station)	Valid 802.11 a 40MHz channel pair:	✓ 157-161
		Redundancy		G Description Description		Mana Ulan Mana
		Maintenance			Valid 802.11a 80MHz channel group:	36-48
				🕞 remove-dfs-domain-or 📾	Valid 802.11a 160MHz channel group	36-64
				Spectrum Local Override		
		Anical II VA 9 6 0 3				Cancel Submit As

1.4.8 Basic-rates (CLI)

在默认的 EIRP 发射功率下(2.4G 是 6-12,5G 是 15-21),如果同频和邻频干扰严重的话(在 没有无线终端使用时,即空闲状态下,AP 的 Channel Utilization 在 20%左右且 RX Time 比重较 高),可以继续裁剪 SSID 下的低速率,来避免同频和邻频干扰:

802.11a/g Transmit Rates ==设置 802.11 数据帧传输的匹配速率,通常最低传输速率应该 要比 beacon 速率小一位(禁用低速率也可以帮助消除终端的粘滞现象--即总是连接到最远的 AP 上)

802.11a/g Basic Rates ==设置 802.11 控制帧和管理帧的最低速率

802.11a/g Beacon Rate ==设置 Beacon 帧的最低速率,即等于最低位的 Basic Rate

注意:必须针对全网中所有广播的 ssid 信号,进行该裁剪配置,不能放过一个,否则无优化效果。

在保证终端收到最低-65dBm 信号强度覆盖要求下,使用越少的 SSID、在同一个信道中越少的 AP 数量、越高的 Beacon Rate、越高的 Basic Rate,从而节省更多的空口 Airtime,无线性能越好。

在相对 AP 部署密集环境中,控制 co-channel interference (CCI) and adjacent channel interference (ACI)干扰的影响。

裁减以下低速率时,请保持现有的无线信号发射功率不变下进行,且建议从低密度场景的参数 开始进行采集,每采集完成后,观察下当前无线网络的干扰程度。一步一步,逐渐采集其他的低速 率。AP 密度越高,被裁剪的低速率越多。

低密度场景(AP 间距 15-20 米左右)--覆盖为主的设计(注意:任何场景下,强烈推荐大家 先从这步开始裁剪,这也是绝大多数办公场景下都可以采用该配置项进行部署,然后观察一段时间 网络运行情况)

(LabX-MM-1) [labX] (config) #wlan ssid-profile opt-ssid-profile

(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	essid low-density-ssid
(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	a-basic-rates 6 12
(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	g-basic-rates 6 12
(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	g-tx-rates 6 9 12 18 24 36 48 54
(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	g-beacon-rate 6
(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	a-beacon-rate 6

中高等密度场景(AP 间距 10-15 米左右) -容量和覆盖兼顾的设计

(LabX-MM-1) [labX] (config) # wlan ssid-profile opt-ssid-profile					
(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	essid middle-density-ssid				
(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	a-basic-rates 18 24				
(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	a-tx-rates 12 18 24 36 48 54				
(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	g-basic-rates 18 24				
(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	g-tx-rates 12 18 24 36 48 54				
(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	g-beacon-rate 18				
(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	a-beacon-rate 18				

超高密场景(AP间距 5-10米左右)--容量为主的设计

(LabX-MM-1) [labX] (config) #wlan ssid-profile opt-ssid-profile



(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	essid high-density-ssid
(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	a-basic-rates 24 36
(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	a-tx-rates 18 24 36 48 54
(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	g-basic-rates 24 36
(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	g-tx-rates 18 24 36 48 54
(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	g-beacon-rate 24
(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #	a-beacon-rate 24

1.4.9 Basic-rates (GUI)

在 lab<mark>X</mark>下,选择 Configuration>System,在 Profiles 选项卡中,选择 Wireless LAN>SSID>optssid-profile,根据不同场景下,设置不同的 802.11a/g Transmit Rates, 802.11a/g Basic Rates 和 802.11a/g Beacon Rate 组合(参考 CLI 参数值),最后点击 Submit 按钮和 Pending Changes 按钮。

	Y MASTER -MM-1	CONTROLLEI ⊙ 2 ○	ACCESS POINTS CLIENTS ALERTS 0 ○ 0 ○ ○ △ <th></th> <th></th> <th></th> <th>(2) ac</th>				(2) ac
lanaged Network > lab2	D						Pending
bilty Master Lab2-MM-1 maged Network (2) lab2 (2) c lab2-md2 c lab2-md2	Configuration WLANS Roles & Policies Access Polints A droups Authentication Services Interfaces (System) Tasis Redundancy Maintenance	General Admin AirWave CPSec Certificates	SIMP Logging Profiles More SID enable: • ESSD: WRA Parsphrase: Encryption: Comode transition: Enable Management frame Protection (for WPA2 opmodes): Require Management Frame Protection (for WPA2 opmodes): DTIM Interval: • 802.11a Transmit Rates: • 802.11a Transmit Rates: • 802.11a Transmit Rates:	✓ Nigh-density-sold With passphrase: Retype:	static-mep dynamic-wep wpaskip wpaskip wpask-kes wpask-kes		
				1 2	5 6 9	□ 11 □ 12	

1.4.10 AP 接收灵敏度 (CLI)

通过上一步的裁剪低速率的操作,如果同频和邻频干扰仍然无法得到明显改善的话,我们接 着采用降低AP的接受灵敏度来提升信道复用的可能,记住在这步中,我们仍然保持现有的EIRP值 不变,我们的调优是循环渐进,不能在同一时间同时调整多个优化参数,规避产生无法预期的效果。 降低AP的接受信号的灵敏度 6-10 dB 是比较靠谱的,可以每次增加3dB向上调整.(Increase CCA idle frequency by filtering low-SINR PLCP preambles and data payloads)通过过滤掉低SINR 的PLCP前导帧和数据开销,从而提升同频信道空闲复用的指数,避免空间内的同频干扰的发生。

参考: The threshold is about received signal strength (notSNR) above -95 dBm. If you put in 20, it means any transmissi on with lower than -75 dBm will not be processed by the radio regardless of wifi/non-wifi transmissions.Depending on how dense your typical 2.4 Ghz would be, value from 6-10 is quite safe and you may need 20-25 for quite dense deploy ment example, Shopping mall with big void and multi-floors of open spaces

我们的计算模型是按照-95dBm,如果你设置20,意味着低于-75dBm强度的任何数据包都会 被AP忽略掉,通常设置6-10是比较安全的,如果你的网络比较密集可以调整到20-25,请从10来 时,每次逐渐增加3dB,每次观察AP的channel busy是否降低。

(LabX-MM-1) [labX] (config) #rf dot11g-radio-profile labX-11g-radio-profile

(LabX-MM-1) [labX] (802.11g radio profile "labX-11g-radio-profile") #cell-size-reduction 10

(LabX-MM-1) [labX] (config) #rf dot11a-radio-profile labX-11a-radio-profile

(LabX-MM-1) [labX] (802.11a radio profile "labX-11a-radio-profile") #cell-size-reduction 10

1.4.11 AP 接收灵敏度 (GUI)

1) 在 labX 下,选择 Configuration>System,在 Profiles选项卡中,选择 RF Management>2.4 GHz radio>labX-11g-radio-profile,点击 Advanced 展开设置项,Reduce Cell Size 设置为 10,最后点击 Submit 按钮和 Pending Changes 按钮。



	TER 1	CONTROLLERS ⊘ 2 ○ 0	ACCESS POINTS CLIENTS ALERTS ○ 0 ○ 0 ○ 0 ○ 0 △ 2		() admin ~
Managed Network > lab2 >					Pending Changes
 Managed Network > Int2 > Molity Master Lab2.4M1 Managed Network (2) Int2.2(2) Int2.2(2)<!--</th--><th>Dashboard Configuration WLNIS Roles & Policies Access Points A Groups Authentication Services Interfaces Controllers System Tasks</th><th>General Admin AirWave CPSec C All Profiles © © QOS © # RF Management © © 2.4 GH2 radio © © 1.6 AM Scanning © manating © © p-manating</th><th>Certificates SNMP Logging Profiles More 2.4 GHz radio profile: lab2.11p.radio-profile 2.4 GHz radio profile: lab2.11p.radio-profile 3. General 4. Advenced Advenced Advenced 5. GasCount: 5. GasC</th><th>4 4 1 1 1 100 msec</th><th>Pending Changes</th>	Dashboard Configuration WLNIS Roles & Policies Access Points A Groups Authentication Services Interfaces Controllers System Tasks	General Admin AirWave CPSec C All Profiles © © QOS © # RF Management © © 2.4 GH2 radio © © 1.6 AM Scanning © manating © © p-manating	Certificates SNMP Logging Profiles More 2.4 GHz radio profile: lab2.11p.radio-profile 2.4 GHz radio profile: lab2.11p.radio-profile 3. General 4. Advenced Advenced Advenced 5. GasCount: 5. GasC	4 4 1 1 1 100 msec	Pending Changes
	Redundancy Maintenance	Imparations Imparation Imparation Imparation	Beacon Regulate: ARLWWDS Override: • Reduce Cell Size (Rt: Sensthrity): Energy Detect Threshold Offset: Management Frame Throttle Interval: Management Frame Throttle Limit: Management Frame Throttle Limit: Masimum Distance: Rt: Sensthrity Threshold:	0 F V 10 d0 0 d0 1 sec 30 sec 0 meters 0 d8	Cancel Schutz As

2) 在 labX 下,选择 Configuration>System,在 Profiles 选项卡中,选择 RF Management>5 GHz radio>labX-11a-radio-profile,点击 Advanced 展开设置项,Reduce Cell Size 设置为 10,最后点击 Submit 按钮和 Pending Changes 按钮。

	CONTROLLERSACCESS F⊘ 2○ 0⊘ 0	POINTS CLIENTS ALERTS ○ 0 ○ 0 ○ 0 △ 2			⑦ admin ∽
← Managed Network > lab2 >					Pending Changes
Ck Q Dashboard Configuration	General Admin AirWave CPSec Certificates	SNMP Logging Profiles More			
🖙 Lab2-MM-1 WLANs	All Profiles	5 GHz radio profile: lab2-11a-radio-profile			
Managed Network (2) Roles & Policies Access Points Access Points Access Points	C QOS FF Management	> General			
 a cloups a cloups<		AM tx mute (radio):			
Services	🕀 🖻 default	Spur Immunity:	0		
Interfaces	\ominus 🕞 lab2-11a-radio-profi 💼	Enable CSA:			
Controllers	AM Scanning	CSA Count:	4		
System	Adaptive Radio Management (ARM)	Smart Antenna:			
Tasks	🕒 High-throughput radio	Advertise 802.11d and 802.11h Capabilities:			
Redundancy		spectrum Load Balancing.			
Maintenance	Trp-monitor-a	Beacon Period:	100	msec	
	F rp-scan-a	Beacon Regulate:			
		ARM/WIDS Override:	OFF 💙		
	⊕	Reduce Cell Size (Rx Sensitivity):	10	dB	
		Energy Detect Threshold Offset:	0	dB	
		Management Frame Throttle interval:	1	sec	
		Management Frame Throttle Limit:	30		
		Maximum Distance:	0	meters	
Arubel/MAVA.8.6.0.3				Cancel	Submit Submit As

1.4.12 802.11h (CLI)



802.11h 涉及两种技术,一种是动态频率选择(DFS),它用于检测在一个信道上有其他信号出现,当这样的信号被检测到时,就会自动将网络转移到另一个信道。另一种技术是传输功率控制(TPC),它主要是减少网络传输的无线频率输出功率,使系统间干扰最小,而且还可以达到更好的网络性能。

(LabX-MM-1) [labX] (config) #rf dot11g-radio-profile labX-11g-radio-profile

(LabX-MM-1) ^[labX] (802.11g radio profile " labX-11g-radio-profile ") #dot11h

And

(LabX-MM-1) [labX] (config) #rf dot11a-radio-profile labX-11a-radio-profile

(LabX-MM-1) ^[labX] (802.11a radio profile " labX-11a-radio-profile ") #dot11h

1.4.13 802.11h (GUI)

1) 在 labX 下,选择 Configuration>System,在 Profiles选项卡中,选择 RF Management>2.4 GHz radio>labX-11g-radio-profile,点击 Advanced 展开设置项,勾选 Advertise 802.11d and 802.11h Capabilities,最后点击 Submit 按钮和 Pending Changes 按钮。

	Y MASTER -MM-1	CONTROLLERSACCESS☉20○0	POINTS CLIENTS ALERTS ③ 0 ⑦ 0 ∅ 0 △ 2			admin ~
← Managed Network > lab2	:>					Pending Changes
🛱 Mobility Master	Q Dashboard	General Admin AirWave CPSec Certificates	SNMP Logging Profiles More			
🖘 Lab2-MM-1	WLANS	All Profiles	2.4 GHz radio profile: lab2-11g-radio-profile			
Managed Network (2)	Roles & Policies Access Points	QOS RF Management	> General			
lab2-md1	AP Groups Authentication	C 2.4 GHz radio C default	AM tx mute (radio):			
	Services	⊖ 🕞 lab2-11g-radio-profi 💼	Enable CSA:			
	Interfaces	G AM Scanning	Smart Antenna:	4		
	Controllers	Adaptive Radio Management (ARM) High-throughput radio	 Advertise 802.11d and 802.11h Capabilities: 	М		
	Tasks	⊕ 🕞 rp-maintain-g	Spectrum Load Balancing:			
	Redundancy	Trp-monitor-g	Beacon Period:	100	msec	
	Maintenance	The second	ARM/WIDS Override:	OFF 🗸		
		 ⊕ ⊆ 3 Gr2 rabio ⊕ ⊆ 802.11 60GHz radio 	 Reduce Cell Size (Rx Sensitivity): 	10	dB	
		⊕	Energy Detect Threshold Offset:	0	dB	
			Management Frame Throttle interval:	1	sec	
			Management Frame Throttle Limit:	30		
			Maximum Distance:	0	meters	
			RX Sensitivity Threshold:	0	dB	
	ArubaMM-VA, 8.6.0.3				Cancel	Submit Submit As



2) 在 labX 下,选择 Configuration>System,在 Profiles选项卡中,选择 RF Management>5 GHz radio>labX-11a-radio-profile,点击 Advanced 展开设置项,勾选 Advertise 802.11d and 802.11h Capabilities,最后点击 Submit 按钮和 Pending Changes 按钮。

	CONTROLLERSACCESS∅20∅	POINTS CLIENTS ALERTS ○ 0 ○ 0 ○ 0 △ 2			admin ~
← Managed Network > lab2 >					Pending Changes
Configuration	General Admin AirWave CPSec Certificates	SNMP Logging Profiles More			
🖘 Lab2-MM-1 WLANS	All Profiles	5 GHz radio profile: lab2-11a-radio-profile			
Managed Network (2) Roles & Policies Access Points ab2(2) Access Points Access Points	 () □ QOS () □ RF Management () □ 2.4 (Hz radio 	> General			
ab2-md2 Authentication	G G	AM tx mute (radio):			
Services	G default	Spur Immunity:	0		
Interfaces	\ominus 🕞 lab2-11a-radio-profi 💼	Enable CSA:			
Controllers	AM Scanning	CSA Count:	4		
System	Adaptive Radio Management (ARM)	Smart Antenna:			
Tasks	High-throughput radio	Advertise 802.11d and 802.11h Capabilities:	M		
Redundancy	F rp-maintain-a	Spectrum Load Balancing:			
Maintenance	Trp-monitor-a	Beacon Period:	100	msec	
	🕀 📑 rp-scan-a	Beacon Regulate:			
		ARM/WIDS Override:	OFF 💙		
		 Reduce Cell Size (Rx Sensitivity): 	10	dB	
		Energy Detect Threshold Offset:	0	dB	
		Management Frame Throttle interval:	1	sec	
		Management Frame Throttle Limit:	30		
		Maximum Distance:	0	meters	
ArubeMMAVA, 8.6.0.3				Cancel	Submit Submit As

1.4.14 ARM/WIDs (CLI)

动态调整 ARM 和 WIDs 的进程调度,提升 AP 的处理效率.系统默认是一直开启 ARM 和 WIDs 处理进程, AP 存在一定的处理性能开销。

(LabX-MM-1) [labX] (config) #rf dot11g-radio-profile labX-11g-radio-profile

(LabX-MM-1) ^[labX] (802.11g radio profile " labX-11g-radio-profile ") #disable-arm-wids-functions dynamic

And

(LabX-MM-1) [labX] (config) #rf dot11a-radio-profile labX-11a-radio-profile

(LabX-MM-1) ^[labX] (802.11a radio profile " labX-11a-radio-profile ") #disable-arm-wids-functions dynamic

1.4.15 ARM/WIDs (GUI)

 在 labX下,选择 Configuration>System,在 Profiles选项卡中,选择 RF Management>2.4 GHz radio>labX-11g-radio-profile,点击 Advanced 展开设置项, ARM/WIDS Override 选择 Dynamic, 最后点击 Submit 按钮和 Pending Changes 按钮。



ALAPSA MOBILITY MASTE	R	CONTROLLERS ACCESS	POINTS CLIENTS ALERTS ○ 0 ○ 0 ○ 0 △ 2			admin ~
Managed Network > lab2 >						Pending Changes
C Q	Dashboard Configuration	General Admin AirWave CPSec Certificates	SNMP Logging Profiles More			
Lab2-MM-1	WLANs	All Profiles	2.4 GHz radio profile: lab2-11g-radio-profile			
Managed Network (2)	Roles & Policies	 Qos 	> General			
🕞 lab2-md1	AP Groups	C 2.4 GHz radio	Advanced			
lab2-md2	Authentication	🕀 🕒 default	AM tx mute (radio):			
	Services	\ominus 🕞 lab2-11g-radio-profi 💼	Enable CSA:			
	Interfaces	🕒 AM Scanning	CSA Count:	4		
	Controllers	G Adaptive Radio Management (ARM)	Smart Antenna:			
	System	🕒 High-throughput radio	 Advertise 802.11d and 802.11h Capabilities: 	м		
	Tasks	Trp-maintain-g	Spectrum Load Balancing:			
	Redundancy	Trp-monitor-g	Beacon Period:	100	msec	
	Maintenance	Trp-scan-g	Beacon Regulate:	11		
		⊕ 5 GHz radio	ARM/WIDS Override:	Dynamic 💙		
		802.11 60GHz radio	 Reduce Cell Size (Rx Sensitivity): 	10	dB	
		B02.11a secondary radio	Energy Detect Threshold Offset:	0	dB	
			Management Frame Throttle interval:	1	sec	
			Management Frame Throttle Limit:	30		
			Maximum Distance:	0	meters	
			RX Sensitivity Threshold:	0	dB	
	ArubaMM-VA, 8.6.0.3				Cancel	Submit As

 在 labX 下,选择 Configuration>System,在 Profiles 选项卡中,选择 RF Management>5 GHz radio>labX-11a-radio-profile,点击 Advanced 展开设置项, ARM/WIDS Override 选择 Dynamic, 最后点击 Submit 按钮和 Pending Changes 按钮。

ALADZAMOBILITY MAST Lab2-MM-1	TER	CONTROLLERS ACCESS	S POINTS CLIENTS ALERTS ○ 0 ○ 0 ○ 0 △ 2			admin ~
← Managed Network > lab2 >						Pending Changes
Ck Q	Dashboard Configuration	General Admin AirWave CPSec Certificates	s SNMP Logging Profiles More			
Lab2-MM-1	WLANS	All Profiles	5 GHz radio profile: lab2-11a-radio-profile			
Managed Network (2) (2) lab2 (2) (2) lab2-md1	Roles & Policies Access Points AP Groups	C C QOS C RF Management C R 2.4 GHz radio	> General			
lab2-md2	Authentication		AM tx mute (radio):			
	Services	default	Spur Immunity:	0		
	Interfaces	\ominus 🕞 lab2-11a-radio-profi 💼	Enable CSA:			
	Controllers	AM Scanning	CSA Count:	4		
	System	Adaptive Radio Management (ARM)	Smart Antenna:			
	Tasks	🕒 High-throughput radio	 Advertise 802.11d and 802.11h Capabilities: 	M		
	Redundancy	Trp-maintain-a	Spectrum Load Balancing:			
	Maintenance	Trp-monitor-a	Beacon Period:	100	msec	
		Trp-scan-a	Beacon Regulate:			
			ARM/WIDS Override:	Dynamic 👻		
		B02.11a secondary radio	 Reduce Cell Size (Rx Sensitivity): 	10	dB	
			Energy Detect Threshold Offset:	0	dB	
			Management Frame Throttle interval:	1	sec	
			Management Frame Throttle Limit:	30		
			Maximum Distance:	0	meters	
	ArubaMM-VA, 8.6.0.3				Cancel	Submit As

1.4.16 802.11b/g (CLI)

没有802.11 b/g协议的无线终端使用场景,为了减少AP对11b协议的保护处理开销,从而可以提升无线网络整体性能。

注意:请一定要确定客户的使用场景下没有 11b/g 协议的终端接入到无线网络的需求。关闭对 11b 的保护后, 11b 和 11g 的终端可以同时发送数据, 会导致系统传输冲突。推荐结合关闭 Legacy stations 功能一起使用。

仅仅在 dot11g-radio-profie 下设置

(LabX-MM-1) [labX] (config) #rf dot11g-radio-profile labX-11g-radio-profile

(LabX-MM-1) ^[labX] (802.11g radio profile " labX-11g-radio-profile ") #no dot11b-protection

WARNING: Disabling protection violates the 802.11 standard and may cause interoperability issues.

1.4.17 802.11b/g (GUI)

在 labX 下,选择 Configuration>System,在 Profiles选项卡中,选择 RF Management>2.4 GHz radio>labX-11g-radio-profile,点击 Advanced 展开设置项,取消勾选 Protection for 802.11b Clients,最 后点击 Submit 按钮和 Pending Changes 按钮。

ALAPSON AND AND AND AND AND AND AND AND AND AN	ER	CONTROLLERS ACCESS P	OINTS CLIENTS ALERTS ○ 0 ○ 0 ▷ 0 △ 2			⑦ admin ∽
← Managed Network > lab2 >						Pending Changes
Managed Network > lab2 > Cit Qit Mobility Master Lab2-MM-1 Managed Network (2) Image: Lab2-MM-1 Image: Lab2-MM-1 Image: Lab2-MM-1 Ima	Dashboard Configuration WLANS Roles & Policies Access Points AP Groups Authentication Services Interfaces Controllers Tasks Redundancy Maintenance	General Admin AirWave CPSec Certificates © Policy Domain © QOS © RF Management © 124 GHz radio © 244 GHz radio © 124 GHz radio © 14004 Tig cadeo groft. © 44504 Readio Management (ARIO) — High-throughput radio — High-throughput radio — T-p-maintain-g — © 1-p-conteg — © 1-p-conteg — © 1-p-conteg — © 1-p-conteg	SMMP Logging Profiles More Advanced At to mute (radio): Enable GA: GA Count Smart Antenna: Advertise 802.11d and 802.11h Capabilities: Spectrum Load Balancing: Beacon Regulate: Beacon Regulate: Re	 4 100 100 1 30 0 0 0 0 0 0 0	msec dB dB sec meters dB	Pending Changes
	ArubaMM-VA, 8.6.0.3				Cancel	ubmit Submit As

1.4.18 802.11b/g(HT) (CLI)

不允许 802.11 b/g 协议的非 HT 无线终端关联到 SSID 上,由于低速率占用更多的空口资源,从而导致整体无线网络性能下降。



注意:常规环境中谨慎使用,仅仅在客户环境中确实没有11b/g协议的无线终端下使用时,才可以

设置该选项。同时一定告知客户该选项会导致所有 11b/g 协议的旧无线终端无法关联无线网络。

(LabX-MM-1) [labX] (config) # wlan ht-ssid-profile no-legacy-station-ht-ssid

(LabX-MM-1) [labX] (High-throughput SSID profile "no-legacy-station-ht-ssid") # no legacy-stations

And

(LabX-MM-1) [labX] (config) #wlan ssid-profile no-legacy-station-ssid-profile

(LabX-MM-1) [labX] (SSID Profile " no-legacy-station-ssid-profile") # ht-ssid-profile no-legacy-station-ht-ssid

1.4.19 802.11b/g(HT) (GUI)

1) 在 labX 下,选择 Configuration>System,在 Profiles 选项卡中,选择 Wireless LAN>Highthroughput SSID>no-legacy-station-ht-ssid,点击 Advanced 展开设置项,取消勾选 Legacy stations,最后点击 Submit 按钮和 Pending Changes 按钮。

ACTUDO MOBILITY MAST Lab2-MM-1	ER	CONTROLLERS ACCESS ⊘ 2 ○ 0 ○ 0	POINTS CLIENTS ALERTS ① 0 ⑦ 0 P 0 △ 2	③ admir
Managed Network > lab2 >				Pending Cha
← Managed Network > lab2 > ← Managed Network > lab2 + ← Mobility Master ○ Lab2-4MM-1 ← Managed Network (2) ○ Lab2 + MM-1 ○ Lab2 + M	Dashboard Configuration WLANS Roles & Policies Access Points AP Groups Authentication Services Interfaces Controllers System Tasks Redundancy	General Admin AirWave CPSec Certificates All Profiles	5 SNMP Logging Profiles More High-throughput SSID profile: no-legacy-station-ht-ssid > Second Station-ht-ssid > General • Second Station-ht-ssid > Advanced - Second Station-ht-ssid > Advanced - - Advanced - - Low-density Enable: - - Low-density Parity Check: Maximum number of spatial streams usable for STBC reception: Maximum number of spatial streams usable for STBC transmission: MPDU Aggregation:	M M I I I I I
	AnodeMMVA 8603	ACC Authentication Acc Authentication	Max received A-MPDU size: Max transmitted A-MPDU size: Min MPDU start spacing: Short guard interval in 20 MHz mode: Short guard interval in 80 MHz mode: Short guard interval in 80 MHz mode: Supported MCS set VHT - Supported MCS map:	65535 v 65535 bytes 0 v M 0-31 9,9,9,9,9,9,9,9 Cancel Submit Submit

2) 在 labX 下,选择 Configuration>System,在 Profiles选项卡中,选择 Wireless LAN>SSID>optssid-profile>High-throughput SSID,在 High-throughput SSID profile 中选择之前创建好的 nolegacy-station-ht-ssid,最后点击 Submit 按钮和 Pending Changes 按钮。



	CONTROLLERS ACCESS POINTS CLIENTS ALERTS ∅ 2 ₀ ₀ ₀ ₀ ₀ ₀ ₀ ₀ ☺ ₀ ₀ ₀ ₀ ₀ ₀ ₀ ₀ ໖ ₀ ₀ △ △ △ △ △ △ △ △ △ △ △ △ △ △ △ △ △	⑦ admin ~
Managed Network > lab2 >		Pending Changes
 Managed Network > lab2 > Mobility Master Lab2-MM-1 Managed Network (2) Lab2-md1 Lab2-md1 Lab2-md1 Lab2-md2 Dashboard Configuration WLANs Access Points Access Points Authentication Services Interfaces Controllers System Tasks Redundancy Maintenance 	General Admin AirWave CPSec Certificates SNMP Logging Profiles More All Profiles • Badius Modifier • General • Operside profile • Operside profile profile profile profile	Pending Changes
AV084MVA.8.6.3		Cancel Submit As

1.4.20 室外 AP

如果使用室外型 AP270/370/365 等系列部署在室内环境使用时,请将该类型的 AP 的安装 模式设置为 indoor,增加 5G 可用信道资源数到 13 个,即增加了(ch36--ch64)

1.4.21 室外 AP (GUI)

1) 在 labX 下,选择 Configuration > Access Points,在 Campus APs 选项卡中,勾选你要设置的 AP name,点击 Provision 按钮,进入到配置页面。

	MASTER M-1			CONTROLLERS ACCES ⊙ 2 ⊙ 0 ⊙ 0	S POINTS CLIENT	S ALERTS				admin	~
Managed Network > lab2 >											¢
Ck Mobility Master	Q Dashboard	Campus APs Remo	te APs Mesh APs	Whitelist Provisioning	Rules						
Contraction (2)	WLANS	Campus APS 1									۹
Managed Network (2)	Roles & Policies	APNAME	AP GROUP	IPV4 ADDRESS	IPV6 ADDRESS	SWITCH IP	MAC ADDRESS	SERIAL #	TYPE	FLAGS	
i⇒ lab2(2) lab2-md1	Access Points AP Groups	AP-205	lab4-group	192.168.101.1		10.2.10.12	94:04:01:00:40:58	CM0219527	205	UG	
lab2-md2	Authentication										
	Services										
	Interfaces										
	Controllers	Provision								50 🛩 <	>
	System	Flags:									
	Tasks	U = Unprovisioned, N = Dup BAP, 1 = 802.1x authenticate Custom EST cert. p = in dee	licate name. G = No such group. U d'AP use EAP.PEAP. 1+ = 802.1k u p-sieep status. 4 = Using WiFi upli	.= Unlicensed, I = Inactive, D = Dirt se EST, 1 = 802.1x use factory cert k, r = Power Restricted, I = Therm	y or no config. E = Regulatory D 2 = Using IKE version 2, u = Cu al ShutDown, F = AP failed 802	omain Mismatch, X – Maintenai stom-Cert RAP, S = Standby-mor Ix authentication	nce Mode, P = PPPoE AP, B = Built-i de AP, J = USB cert at AP, f = No Spe	n AP, s = LACP striping, R = Remo ctrum FFT support, I = Indoor, o	te AP, R- = Remote AP requ = Outdoor, M = Mesh node	ves Auth, C = Cellular RAR c = CERT , Y = Mesh Recovery z = Detazone i	T-based AP, e =
	Redundancy										
	Maintenance										

2) 在配置页面左下角,点击 Show advanced options 按钮。出现隐藏菜单,选择 Coverage area 为 indoor,最后点击 Submit 按钮和 Pending Changes 按钮。



ampus APs 1								
APNAME	AP GROUP	IPV4 AD DRESS	IPV6 ADD RESS	SWITCH IP	MAC ADDRESS	SERIAL #	TYPE	FLAGS
AP-205	lab4-group	192.168.101.1	-	10.2.10.12	94:b4:Df:cc:4d:68	CM0219527	205	UG
provision								50 🗸
\P-205								
MAC address:	94:b4:0f:cc:4d:68							
Name:	AP-205							
AP group:	lab4-group	~						
Controller discovery:	 Use AP discove 	ry proto col (ADP)	Static					
IP:	• DHCP	Static						
Deployment: Wi-Fi uplink:	Campus	○ Remote ○ Mesł	h 🔿 Remote mesh	1 portal				
vanced options			2.4aa					Cancel
vanced options	s Mesh APs W lab4-group	hitelist Provisioning (192168-101.1	Rules -	10.2.10.12	94 bi 95cc-4668	CM0219527	205	Cancel
vanced options pus APs AP205 Provision	s Mesh APs W Iebłgroup	hitelist Provisioning f 192168.101.1	Rules -	10.2.10.12	94349£cc-4658	CMR19527	285	Cance UG 50 ~ (1
Vanced options pus APs Remote AP AP-205 Provision	s MeshAPs W lab4group	hitelist Provisioning I 192168.101.1	Rules -	10.2.10.12	943405cc4d58	CM1219527	205	Cancel UG 50 ~ (1
Vanced options pus APs Remote AP AP205 Provision P205 MAC address:	s MeshAPs W lab4group 94b40fcc4d68	hitelist Provisioning f 192168.101.1	Rules -	10.2.10.12	943405xc-4658	CMI2:19527	205	Cancel UG 50 ~ (1
Pus APs Remote AP AP205 Provision Provision Provision MAC address: Name:	s Mesh APs W lab4group 94b40frc4df8 AP-205	hitelist Provisioning f 192168.101.1	Rules -	10.2.10.12	945405xc-4658	CMI2:19527	205	UG 50 ~ (1
Nanced options Pus APs AP205 Provision Page 200 Provision AP 200	s Mesh APs W lab4group 94b40fcc4d58 AP-205 lab4group	hitelist Provisioning f 192168.101.1	Rules -	10.2.10.12	943405cc4d58	CM2/1957	205	UG 50 ~ (1
Nanced options Pus APs AP205 Provision Page AP AP205 AP205 AP205 AP205 AP205 Controller discovery:	s Mesh APs W lab4goup 94b40fcc4d58 AP-205 lab4group @ Use AP discore	hitelist Provisioning f 192168.101.1	Rules -	10.2.10.12	94 bil9fxc-4658	CM2/19527	25	Cancd UG 50 ~ (1
Nanced options Pus APs AP205 Provision Pageoup: Controller discovery: IP:	5 Mesh APs W lab4group 94b40fcc4d68 AP-205 lab4group @ Use AP discove @ DHCP ()	hitelist Provisioning / 1921681011	Rules - Static	10.2.10.12	953455254658	CMR219527	25	UG 50 ~ (1
Nanced options Puss APs AP203 Provision Provision Provision AP group: Controller discovery: IP: Deployment: Wi-Fi uplink:	s Mesh APs W bbł group 94b40fcc4di58 AP-205 bb4group @ Use AP discove @ DHCP (@ Campus	hitelist Provisioning (192168.101.1	Rules	10.2.10.12	943495xc-4658	CMI219527	25	UG 50 ~ (1
Nanced options Pus APs AP205 Provision Provision MAC address: Name: AP group: Controller discovery: IP: Deployment: Wi-Fi uplink: Coverage area:	s Mesh APs W Iob4 group 94b40fcc4d68 AP-205 Iob4 group @ Use AP discove @ DHCP C @ Campus Indoor \vee	hitelist Provisioning f 192168.101.1	Rules - Static	10.2.10.12	9436562-4658	CMI219527	25	UG 50 v C 1
Nanced options Pus APs AP205 Provitation Provitation AP group: Controller discovery: IP: Deployment: Wi-Fi uplink: Coverage area: Single chain mode:	s Mesh APs W Isb4-group 94.b40fcc4d68 AP-205 Isb4-group @ Use AP discove @ DHCP C @ Campus Indoor ~ Radio 0	hitelist Provisioning f 192168.101.1	Rules - Static	10.2.10.12	94.5405.cc.4458	ONR/19527	205	UG 50 ~ (1
Provision Provision AP-205 Provision AP-205 MAC address: Name: AP group: Controller discovery: IP: Deployment: Wi-Fi uplink: Coverage area: Single chain mode: Uplink authentication:	s Mesh APs W bbł group 94b40fxc4d58 AP-205 bb4group @ Use AP discove @ Campus Indoor ~ Radio 0 @ None _ EAP-PEAP _ EAP-PEAP	hitelist Provisioning f 1921641011	Rules - Static n O Remote mesh	10.2.10.12	943458.000	CMI219527	25	UG 50 ~ (1
Nanced options Pus APs AP205 Provitation Provitation Provitation AP group: Controller discovery: IP: Deployment: Wi-Fi uplink: Coverage area: Single chain mode: Uplink authentication: SNMP system location:	s Mesh APs W Isb4-group 94.b40fcc4d68 AP-205 Isb4-group @ Use AP discove @ DHCP C @ Campus Indoor V Radio 0 @ None EAP-RAP EAP-TLS 	hitelist Provisioning f 192168.101.1	Rules -	10.2.10.12	94540522-4458	ONR/19527	25	UG 50 ~ (1

1.4.22 最大关联数 (CLI)

在中高密度场景下,由于终端接入数的剧增,我们需要及时调整单个 SSID 下的关联用户数 的最大限制,系统默认是 64,如果终端数超过了 64,会导致部分终端无法关联 AP。

(LabX-MM-1) [labX] (config) # wlan ssid-profile opt-ssid-profile

(LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #max-clients 255

1.4.23 最大关联数 (GUI)

1) 在 labX 下,选择 Configuration>System,在 Profiles 选项卡中,选择 Wireless LAN>SSID>optssid-profile,设置 Max Associations=255,最后点击 Submit 按钮和 Pending Changes 按钮。

ANDBILITY MASTER Lab2-MM-1	CONTROLLERS ACCESS FOINTS CLEMTS ALERTS ∅ 2 ₀ ₀ ₀ 1 ♥ ₀ ♠ ₀ ▲ 2) admin 👻
Managed Network > lab2 >		
Kanaged Interork > IB2 > Dathbard Mobility Matter Databbard Configuration WLNB Roles A Places Access Primes Datbard Configuration WLNB Roles A Places Access Primes Services Interfaces Controllers Controllers Redundancy Maintenance	General Admin A Wave Cfsc Certificates SUMP Logging Frome Interview In	
4 ArubaMAFVA, 8603	Cancel	Submit As

1.4.24 AP 扫描 (CLI)

在中高密度场景下,为了提升 AP 的性能,我们可以降低 AP 主动扫描周边射频环境的时间间隔,但是不代表你可以设置一个最大值,从而就貌似关闭了 AP 的扫描功能,记住,AP 扫描周边射频环境信息是非常重要的,我们的 MM 控制器需要这些信息来完成 ClientMatch 和 Airmatch 的精准计算,从而能够更好地优化整个无线网络的射频环境。这里我们推荐的是当所有的 AP 上线后,并且获得了各自的适合的信道,那么我们就可以将扫描周期提升到 30s 最佳。

(LabX-MM-1) [labX] (config) #rf arm-profile labX-11a-arm-profile

(LabX-MM-1) ^[labX] (Adaptive Radio Management (ARM) profile "labX-11a-arm-profile") #scan-interval 30

(LabX-MM-1) [labX] (config) #rf dot11a-radio-profile labX-11a-radio-profile

(LabX-MM-1) [labX] (802.11a radio profile "labX-11a-radio-profile") #arm-profile labX-11a-arm-profile

(LabX-MM-1) [labX] (config) #rf arm-profile labX-11g-arm-profile



(LabX-MM-1) ^[labX] (Adaptive Radio Management (ARM) profile "labX-11g-arm-profile") #scan-interval 30 (LabX-MM-1) [labX] (config) #rf dot11g-radio-profile labX-11g-radio-profile (LabX-MM-1) ^[labX] (802.11g radio profile "labX-11g-radio-profile") #arm-profile labX-11g-arm-profile

1.4.25 Clientmatch (CLI)

在中高密度场景下,尤其是每房间一颗 AP 的部署场景, cm-band-g-max-signal 和 cmband-a-min-signal 成对使用的,表示双频能力的终端正连在 2.4G 上,同时 AP 的 2.4G Radio 感知终端信号强度在-45dBm 以下且 5G Radio 感知终端信号强度在-65dBm 以上时,才将该终端 持续地导引到 5G 频段,当终端的 2.4G 信号强度高于-45dBm 或者 5G 信号强度低于-65dBm 时, 不做导引。我们需要调整的是 cm-band-g-max-signal 参数,因为高密度场景通常在 2.4G 信号 强度下,终端很容易获得-30 到 -45dBm 之间的信号强度,那这样 Clientmatch 就会停止对该终 端继续导引到 5G 频段,从而降低了 11ac AP 的使用效率。

双频终端当前关联在 2.4G 上目在 2.4G 信号强度大于-10dBm,不导引到 5G。那基本上终端关联到 2.4G radio 上的信号强度不会在-10dBm 以上,所以相当于只要双频能力终端关联到 2.4G 上, Clientmatch 就会持续地导引到 5G 频段下。

(LabX-MM-1) [labX] (config) #rf arm-profile labX-11a-arm-profile

(LabX-MM-1) [labX] (Adaptive Radio Management (ARM) profile "labX-11a-arm-profile") #cm-band-g-max-signal 10

(LabX-MM-1) [labX] (config) #rf dot11a-radio-profile labX-11a-radio-profile

(LabX-MM-1) [labX] (802.11a radio profile "labX-11a-radio-profile") #arm-profile labX-11a-arm-profile

(LabX-MM-1) [labX] (config) #rf arm-profile labX-11g-arm-profile

(LabX-MM-1) ^[labX] (Adaptive Radio Management (ARM) profile "labX-11g-arm-profile") # cm-band-g-max-signal 10

(LabX-MM-1) [labX] (config) #rf dot11g-radio-profile labX-11g-radio-profile

(LabX-MM-1) ^[labX] (802.11g radio profile "labX-11g-radio-profile") #arm-profile labX-11g-arm-profile

1.4.26 空口整形 (CLI)

设置空口流量整形为公平访问机制,如果同时需要设置不同 SSID 的空口资源占用百分比时, 该 fair-access 的功能必须同时开启

(LabX-MM-1) [labX] (config) #wlan traffic-management-profile fair-access



(LabX-MM-1) ^[labX] (Traffic management profile "fair-access") #shaping-policy fair-access

(LabX-MM-1) [labX] (config) #ap-group lab2-group

(LabX-MM-1) ^[labX] (AP group "lab2-group") #wlan traffic-management-profile fair-access

1.4.27 空口整形 (GUI)

 在 lab<mark>X</mark>下,选择 Configuration>System,在 Profiles 选项卡中,选择 QOS>Traffic management, 点击 Traffic management profile 后的+号,进入到新建页面。

	MASTER IM-1	CONTROLLERS O	ACCESS POINTS CLIENTS ALERTS ⊘ 0 ○ 1 ♀ 0 ѝ 0 ▲ 2	admin ~
Managed Network > lab2 >				(¢)
Ck Mobility Master	Q Dashboard	General Admin AirWave CPSec Cert	ficates SNMP Logging Profiles More	
🖾 Lab2-MM-1	WLANs	All Profiles	Traffic management profile: New Profile	
🔁 Managed Network (2)	Roles & Policies	⊕ AP		
🔁 lab2 (2)	Access Points	AirGroup		
📼 lab2-md1	AP Groups	G Cluster Cluster		
🖘 lab2-md2	Authentication	G Controller Profile		
	Services	EST Profile		
	Interfaces	⊕ □		
	Controllers	🕀 🕒 Mesh		
	System	Other Profiles		
	Tasks	Policy Domain		
	Redundancy	O 🕒 qos		
	Maintenance	\ominus 🕒 Traffic management		
		🕒 fair-access		
		WMM Traffic management		
		RF Management	•	

2) 在新建页面中, 输入 Profile name 和 选择 Station Shaping Policy 为 fair-access。最后点击 Submit 按钮和 Pending Changes 按钮。



General Admin AirWave CPSec Certificates	SNMP Logging Profiles More
All Profiles	Traffic management profile: New Profile
• • • AP	Profile name: fair-access
AirGroup	General
Guster Cluster Cluster	
Controller Profile	Station Shaping Policy: fair-access 🗸
🕀 📑 EST Profile	> Advanced
🕀 🖻 Mesh	
Other Profiles	
Policy Domain	
\ominus 🕒 Traffic management	
📑 fair-access	
WMM Traffic management	
🕀 📑 RF Management	
· - · · ·	

Cancel



1.5 应用层面的优化项

1.5.1 无线侧组播广播 (CLI)

在所有使用到的 virtual ap profile 下,开启 Drop Broadcast and Unknown Multicast (没有组播应用的场景下,对来自无线侧的报文,丢弃未知的组播和广播报文,例如由客户端上的 某些 APP 产生的 SSDP, mDNS, DLNA 和 NetBIOS 组播服务被丢弃,但是 ARP 和 DHCPv4/v6 广播报文仍然放行且转单播, IPv6 的 ND, NS 和 RA 也放行,如果有已知的组播业务应用时,请 结合 Airgroup 协议使用)

注意: 该配置必须和 Convert Broadcast ARP requests to unicast 同时使用, Convert

Broadcast ARP requests to unicast 系统默认就是 enable 开启的。

(LabX-MM-1) [labX] (config) #wlan virtual-ap no-broadcast-vap

(LabX-MM-1) ^[labX] (Virtual AP profile "no-broadcast-vap") #broadcast-filter all

Warning: broadcast-filter arp should be enabled with this option. Otherwise ARP requests will be dropped!

1.5.2 无线侧组播广播 (GUI)

在 labX 下,选择 Configuration>System,在 Profiles 选项卡中,选择 Wireless LAN>Virtual AP 新 增一个 no-broadcast-vap 配置,点击进入到 Broadcast/Multicast,勾选 Drop Broadcast and Multicast。 最后点击 Submit 按钮和 Pending Changes 按钮。





1.5.3 有线侧组播广播 (CLI)

在所有使用到的无线用户 VLAN 接口编辑下, 启用 Enable BCMC Optimization (没有组播应用的场景下, 必须针对所有使用的无线用户的 VLAN ID 下进行配置, 对来自有线侧的报文, 丢弃未知的组播和广播报文----例如由客户端上的某些 APP 产生的 SSDP, mDNS, DLNA 和 NetBIOS 组播服务被丢弃, 但是 ARP 和 DHCPv4/v6 广播报文仍然放行且转单播, IPv6 的 ND, NS 和 RA 也放行, VRRP 报文也放行, 如果有已知的组播业务 mDNS 应用时, 请结合 Airgroup 协议使用)

注意:所有使用到的无线用户 VLAN 接口,都要开启
(LabX-MM-1) [labX] (config) #interface vlan <mark>X</mark> 20
(LabX-MM-1) ^[labX] (config-submode)#bcmc-optimization

1.5.4 有线侧组播广播 (GUI)

1) 在 labX 下,选择 Configuration > Interfaces,在 VLANs 选项卡中,选择你用到的用户 VLAN ID,点击 IPv4 选项卡,点击 Other Option.



	ITY MASTER 02-MM-1	CONTROLLERS ACCESS POINTS CLIENTS ALERTS ∅ 2 0 ∅ 0 0 1 ♀ 0 ๗ Δ 2	⑦ admin ∨
🗲 Managed Network > la	b2 >		¢)
 Managed Network > la Mobility Master Lab2-MM-1 Managed Network (2) Lab2 (2) Lab2-md1 Lab2-md2 	Dashboard Configuration WLANS Roles & Policles Access Points AP Groups Authentication Services Controllers System Tasks Redundancy	VLANS IP Routes GRE Tunnels Pool Management OSPF Multicast VLANS ID(5) -	
	Maintenance	Port Members IPv6 More > IP Address Assignment > IGMP ✓ Other Option NAT inside:	Cancel Submit

2) 在 Other Option 菜单下,勾选 BCMC Optimization. 最后点击 Submit 按钮和 Pending Changes 按 钮。

Port Members IPv4 IPv6	xe	
> IP Address Assignment		
> IGMP		
 Other Option 		
NAT inside:		
NAT outside:		
Local-proxy ARP:		
Inter-VLAN routing:		
BCMC optimization:		
Bandwidth contract:	v	
ACL:	-None-	
Enable ospf:	0	
		_
	Cancel	bmit

1.5.5 VMM (CLI)

如果需要优化语音和视频等流量,则需要开启 WMM + DSCP VO/VI/BE/BK (56-voice,40-video,24-best effort,8-background, DSCP的值在这里是参考,请根据具体环境需求来调整值),有语音或者视频应用时,

那么建议启用WMM,这是从视频层面优化应用,当然你必须要结合QoS相关配置来一起提升语音和视频的服务 等级(相信你之前已经学会了如何基于语音和视频流量的QoS设置)

(LabX-MM-1) [labX] (config) #wlan ssid-profile opt-ssid-profile (LabX-MM-1) [labX] (SSID Profile "opt-ssid-profile") #wmm-vo-dscp 56 (LabX-MM-1) ^[labX] (SSID Profile "opt-ssid-profile") #wmm-vi-dscp 40 (LabX-MM-1) ^[labX] (SSID Profile "opt-ssid-profile") #wmm-be-dscp 24 (LabX-MM-1) ^[labX] (SSID Profile "opt-ssid-profile") #wmm-be-dscp 24

1.5.6 VMM (GUI)

在 labX 下,选择 Configuration>System,在 Profiles 选项卡中,选择 Wireless LAN>SSID>optssid-profile,勾选 WMM,并分别设置 voice,video,best-effort 和 background 的 dscp 值(具体该值需 要根据实际环境中的有线网络一起联合定义,这里只是给大家一个参考设置),最后点击 Submit 按钮和 Pending Changes 按钮。

aruba	MOBILITY MASTER Lab2-MM-1	CONTROLL ⊙ 2 (ACCESS POINTS CLIENTS ALERTS 0 Image: Comparison of the second seco		admin ~
🗲 Managed Netwo	ork > lab2 >				¢
C Mobility Master	Q Dashboard Configuration	General Admin AirWave CPSec Certificates	SNMP Logging Profiles More		
Lab2-MM-1	WLANS	All Profiles	SSID Profile: opt-ssid-profile		
Managed Network Participation	rk (2) Roles & Policies Access Points	Management Authentication	 Advanced 		
🖘 lab2-me	d1 AP Groups	RADIUS Server	SSID enable:		
🖘 lab2-me	d2 Authentication	RFC 35/6 Server	ESSID:	high-density-ssid	
	Services	G Radius Modifier	WPA Passphrase:	WPA passphrase:	
	Interfaces Controllers System Tasks Redundancy Maintenance	C © SSD C = default C = default	Encryption: Opmode transition: Enable Management Frame Protection (for WPA2 opmodes):	Retype: Sec opensystem wpa3-ese enhanced-open static wep wpa3-ase-aes dynamic-wep wpa3-ase-com-128 wpa3-ases wpa3-ases wpa3-ases wpa3-ases mpik-aes wpa3-ases mpik-aes wpa3-ases to 5sec-226 wpa-psk-aes	
			DTIM Interval:	1 hearon nerioris	
			802.11a Basic Rates:		
			 802.11a Transmit Rates: 	6 9 12 ✓ 18 ✓ 24 ✓ 36 ✓ 48 ✓ 54	
		()			÷.
	AnihaMM-VA 8603			Cancel Subr	iit Submit As



• Wireless Multimedia (WMM):	
Wireless Multimedia U-APSD (WMM-UAPSD) Powersave:	
WMM TSPEC Min Inactivity Interval:	0 msec
WMM DSCP Mapping Control:	\checkmark
 DSCP mapping for WMM voice AC (0-63): 	56
 DSCP mapping for WMM video AC (0-63): 	40
 DSCP mapping for WMM best-effort AC (0-63): 	24
 DSCP mapping for WMM background AC (0-63): 	8



1.6 安全层面的优化项

1.6.1 Basic-acl (CLI)

强烈建议配置一套基本的安全策略 basic-acl, 被每个认证后的用户角色中调用, 尤其是常用的 employee role (我们需要在所有允许访问外网的角色中都需要调用下面的安全策略控制的, 注意 position 的顺 序, 按照从上到下优先匹配原则.)

(LabX-MM-1) [labX] (config) #ip access-list	session ipv4-basic-acl		
(LabX-MM-1) ^[labX] (config-submode)#	user any udp 68 deny p	position 1	I
(LabX-MM-1) ^[labX] (config-submode)#	any any svc-dhcp permit	position	2
(LabX-MM-1) ^[labX] (config-submode)#	any any svc-dns permit	position	3
(LabX-MM-1) ^[labX] (config-submode)#	any any svc-icmp permit	position	4
(LabX-MM-1) [labX] (config) #ip access-list	session ipv6-basic-acl		
(LabX-MM-1) ^[labX] (config-submode)#	ipv6 user any udp 546	deny	position 1
(LabX-MM-1) ^[labX] (config-submode)#	ipv6 any any svc-v6-dhcp	permit	position 2
(LabX-MM-1) ^[labX] (config-submode)#	ipv6 any any svc-dns	permit	position 3
(LabX-MM-1) ^[labX] (config-submode)#	ipv6 any any svc-v6-icmp	permit	position 4
(LabX-MM-1) [labX] (config) #user-role em	ployee		
(LabX-MM-1) [labX] (config-submode)# a	ccess-list session ipv4-bas	ic-acl	position 3
(LabX-MM-1) ^[labX] (config-submode)#	access-list session ra-guar	ď	position 4
(LabX-MM-1) ^[labX] (config-submode)#	access-list session ipv6-ba	asic-acl	position 5
(LabX-MM-1) ^[labX] (config-submode)#	access-list session allowal	I	position 6
(LabX-MM-1) ^[labX] (config-submode)#	access-list session v6-allow	wall	position 7

(阻止无线用户私设 IPv4 的 dhcp server) (阻止无线用户私设 IPv6 的 dhcp server)



1.6.2 Basic-acl (GUI)

1) 在 labX 下,选择 Configuration > Roles & Policies,在 Policies 选项卡中,点击+按钮来新增两个 Policy。

aruba	MOBILITY MASTER Lab2-MM-1		CONTROLLERSACCES⊙ 2⊙ 0⊙ 0	S POINTS CLIENTS ALERTS ① 1 □ 0 0 ▲ 2		admin ~
🗲 Managed Netwo	ork > lab2 >					Ŷ
C Mobility Master	Q Dashboard Configuration WLANs	Roles Policies Applications	s Aliases			
🗁 Managed Netwo	rk (2) Roles & Policies	NAME	RULES COUNT	TYPE	POLICY USAGE	E
🗁 lab2 (2)	Access Points	validuserethacl	1	eth	-	
🕒 lab2-m	d1 AP Groups	global-sacl	0	session	-	
📼 lab2-m	d2 Authentication	sdn-acl	0	session		
	Services	sys-control	12	session	-	
	Interfaces	sys-ap-act	1	session		
	Controllers	sys-switch-ad	12	session	-	
	System	+	12			v
	Tasks					
	Redundancy					
	Maintenance					

2) Policy 1= ipv4-basic-acl, 点击 Submit 按钮, 然后在 Policies 中找到 ipv4-basic-acl, 继续点击+ 按钮来添加多个规则, Rule type 类型选择 Access Control.

4	
	Cancel Submit
	session
0	session
12	session
11	session
1	session
10	
	0 0 12 11 1



Ro	les Policies Applications	Aliases						
	Policies							
	NAME	RULES COUNT	TYPE		POLICY USAGE			
	logon-control	7	session		logon, guest-logo	n		A
	jabber-acl	2	session		voice			
	ipv6-controller-if-acl	1	session		contractor			
	ipv6-basic-acl	4	session		employee			
	ipv4-controller-if-acl	1	session		contractor			
-	ipud-basic-acl-1	0	session					
L	ipv4-basic-acl	4	session		employee		0	· · · · · · · · · · · · · · · · · · ·
	+							
	Policy > ipv4-basic-acl Rules							 Drag rows to re-order
	IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	N	ACTION		
	lpv4	user	any	68		deny_opt		
	lpv4	any	any	svc-dhcp		permit		
	Ipv4	any	any	svc-dns		permit		
-	Ipv4	any	any	svc-icmp		permit		
L	+							

	New Rule for ipv4-basic-acl		_
Roles Policies Appli	cation Rule type: 🖲 Access control	○ Application	
Policies			
NAME		Cancel	ОК
logon-control	7	session	
jabber-acl	2	session	
ipv6-controller-if-acl		session	
ipv6-basic-acl	4	session	
ipv4-controller-if-acl	1	session	
ipv4-basic-acl-1	0	session	
ipv4-basic-acl	4	session	
+			
Policy > ipv4-basic-acl kul	es		
IP VERSION	SOURCE	DESTINATION	SERVICE
lpv4	user	any	68
Ipv4	any	any	svc-dhc
Ipv4	any	any	svc-dns
Inut	2017	2010	ave icro



olicy > ipv4-basic-acl Rule	5				 Drag rows to re-ore
VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	
•					
v4-basic-acl > New forwa	rding Rule				
IP version:	IPv4 ¥				
Source:	User 👻				
Destination:	Any 💙				
Service/app:	UDP 💙				
Min/max nort:	68 68				
Source destu					
Source dest.					
Action:	Deny				
TOS:					
Time range:	- None - V Reset				
802.1p priority:	v				
Options	Log Mirror Blackli	st Disable scanning			
options.					
Queue:					

:v > ipv4-basic-acl Rule:	s				Drag rows to re-on
ERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	0
	user	any	68 68	deny_opt	
-basic-acl > New forwa	rding Rule				
IP version:	IPv4 💙				
Source:	Any 👻				
Destination:	Any 👻				
Service/app:	Service 💙				
Services alias:	svc-dhcp 👻				
Action:	Permit 👻				
TOS:					
Time range:	- None - 🗸 🗸 Reset				
802.1p priority:	~				
Options:	Log Mirror Blacklist	Disable scanning			
Queue:	~				



Policy > ipv4-basic-acl Rule	5				Drag rows to re-or
IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	0.0
lpv4	user	any	68 68	deny_opt	
lpv4	any	any	svc-dhcp	permit	
+ pv4-basic-acl > New forwa	arding Rule				
IP version:	IPv4 💙				
Source:	Any 👻				
Destination:	Any 🗸				
Sanica (anni	Seniro X				
Service/app:	Service				
Services alias:	svc-dns 🗸				
Action:	Permit 💙				
TOS:					
Time range:	- None - 🗸 🖌 Reset				
802.1p priority:	~				
Options:	Log Mirror Blacklist	Disable scanning			
Queue:	~				
s Policies Applic.	ations Allases				Cancel
s Policies Applica	ations Aliases				Cancel
s Policies Applic F	ations Aliases \$				Cancel
s <mark>Policies</mark> Applic F olicy > ipv4-basic-acl Rule P VERSION	ations Aliases \$	DESTINATION	SERVICE/APPLICATION	ACTION	Cancel
s Policies Applic ► Volicy > ipv4-basic-acl Rule P VERSION Ipv4	ations Aliases s SOURCE USEF	DESTINATION any	SERVICE/APPLICATION 68 68	ACTION deny_opt	Cancel
s Policies Applica b volicy > ipv4-basic-acl Rule P VERSION pv4 pv4	ations Aliases s SOURCE user any	DESTINATION any any	SERVICE/APPLICATION 68 68 svc-dhcp	ACTION dery_opt permit	Cancol
s Policies Applica Policy > jpv4-basic-acl Rule P VERSION pv4 pv4	ations Aliases s SOURCE user any any	DESTINATION any any any	SERVICE/APPLICATION 68 68 svc-dhcp svc-dns	ACTION deny_opt permit permit	Cancel
s Policies Applic. - olicy > ipv4-basic-acl Rule P VERSION pv4 pv4 - -	ations Allases 5 SOURCE user any any	DESTINATION any any any	SERVICE/APPLICATION 68 68 svc-dhcp svc-dns	ACTION deny_opt permit permit	Cancel
s Policies Applica olicy > ipv4-basic-acl Rule p VERSION pv4 pv4 wv4-basic-acl > New forwa	ations Aliases S SURCE User any any rding Rule	DESTINATION any any any	SERVICE/APPLICATION 68 68 svc-dhcp svc-dns	ACTION dery_opt permit permit	Cancol
s Policies Applica policy > jpv4-basic-acl Rules p VERSION pv4 pv4 pv4 pv4 pv4 pv4 pv4 pv4	ations Aliases SOURCE USEr any any rding Rule	DESTINATION any any any	SERVICE/APPLICATION 68 68 svc-dhcp svc-dns	ACTION deny_opt permit permit	Cancol
s Policies Applic. olicy > jpv4-basic-acl Rules P VERSION pv4 pv4 pv4 pv4 iP Version: Source:	ations Aliases SOURCE USEr any any any rding Rule	DESTINATION any any any	SERVICE/APPLICATION 68 68 svc-dhcp svc-dns	ACTION deny_opt permit permit	Cancel
s Policies Applic. olicy > jpv4-basic-acl Rule p vERSION pv4 pv4 pv4 pv4 pv4 pv4 pv4 pv4	ations Aliases SOURCE USET any any any Any Y	DESTINATION any any any	SERVICE/APPLICATION 68.68 svc-dhcp svc-dns	ACTION deny_opt permit permit	Cancel
s Policies Applic olicy > ipv4-basic-acl Rule P VERSION pv4 pv4 pv4 pv4 iP version: Source: Destination: Service/app:	ations Allases	DESTINATION any any any	SERVICE/APPLICATION 68 68 svc-dhcp svc-dns	ACTION deny_opt permit permit	Cancel
s Policies Applic. olicy > ipv4-basic-acl Rule P VERSION pv4 pv4 bv4-basic-acl > New forwa Version: Source: Destination: Service/app: Services alias:	ations Allases	DESTINATION any any any	SERVICE/APPLICATION 68 68 svc-dhcp svc-dns	ACTION deny_opt permit permit	Cancel
s Policies Applic. solicy > ipv4-basic-acl Rule P VERSION pv4 pv4 pv4 bv4-basic-acl > New forwa F version: Source: Destination: Service/app: Service/app: Services alias: Action:	ations Allases	DESTINATION any any any	SERVICE/APPLICATION 68 68 svc-dhcp svc-dns	ACTION dery_opt permit permit	Cancel
s Policies Applic. olicy > ipv4-basic-acl Rule: P VERSION pv4 pv4 bv4-basic-acl > New forwa IP version: Source: Destination: Service/app: Services alias: Action: TOS:	ations Allases	DESTINATION any any any	SERVICE/APPLICATION 68 68 svc-dhcp svc-dns	ACTION dery_opt permit permit	Cancel
s Policies Applica picy > jpv4-basic-acl Rules p vESSION pv4 pv4 pv4 pv4 pv4 pv4 pv4 pv4	ations Aliases SOURCE USEr any any any rding Rule IPv4 Y Any Service Service V Permit V Reset	DESTINATION any any any	SERVICE/APPLICATION 68 68 svc-dhcp svc-dns	ACTION deny.opt permit permit	Cancal
s Policies Applica olicy > ipv4-basic-acl Rule p Version pv4 pv4 pv4 pv4 pv4 pv4 pv4 pv4	ations Allases	DESTINATION any any any	SERVICE/APPLICATION 68 68 svc-dhcp svc-dns	ACTION deny_opt permit permit	Cancel
s Policies Applica olicy > ipv4-basic-acl Rule P VERSION pv4 pv4 pv4 pv4 Pv4 Pv4 Pv4 Pv4 Pv4 Pv4 Pv4 P	ations Aliases	DESTINATION any any any any Disable scanning	SERVICE/APPLICATION 68 68 svc-dhcp svc-dns	ACTION deny_opt permit permit	Cancol

3) Policy 2= ipv6-basic-acl, 点击 Submit 按钮, 然后在 Policies 中找到 ipv6-basic-acl, 继续点击+ 按钮来添加多个规则, Rule type 类型选择 Access Control.



	New Policy		
es Policies Applicatio	r Policy type: Policy name:	Session V Ipv6-basic-acl	
NAME		Cancel Submit	POLICY USAGE
apprf-sys-ap-role-sacl	0	session	sys-ap-role
apprf-sys-switch-role-sacl	0	session	sys-switch-role
apprf-employee-sacl 🍂	0	session	employee
apprf-contractor-sacl	0	session	contractor
ipv6-basic-acl	0	session	employee
deny-cry-antivirus	6	session	-
ipv4-controller-if-acl	1	session	contractor

Roles Policies Applications	Aliases				
Policies					
NAME	RULES COUNT	TYPE	POLICY	USAGE	E
icmp-acl	1	session	guest,	voice	A
ipv4-basic-acl	4	session	employ	/ee	
ipv4-controller-if-acl	1	session	contra	tor	
ipv6-basic-acl	0	session	emplo	yee	Ū.
ipv6-controller-if-acl	1	session	contra	tor	
jabber-acl	2	session	voice		
logon-control	7	session	logon,	guest-logon	*
+					
Policy > ipv6-basic-acl Rules					 Drag rows to re-order
IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	
_					
+					





	SOURCE	DESTINATION	SEDVICE/ADDI (CATICAL	ACTION	
IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	
+					
ipv6-basic-acl > New forward	ing Rule				
IP version:	IPv6 💙				
Source:	User 👻				
Destination:	Anv 👻				
Service/app;					
Servicerapp.					
Min/max port:	540 540				
Action:	Dany				
	Deny -				
105:					
Time range:	- None - 🗸 🗸	Reset			
000 1					
802.1p priority:					
Options.		Disable scatting			
Queue:	-				
					Cancel
es Policies Applicat	ions Allases				Cancel
es Policies Applicat	ions Aliases				Cancel
es <mark>Policies</mark> Applicat Policy > jpy5-basic-acl Rules IP VERSION	ions Aliases SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	Cancel
es <mark>Policies</mark> Applicat Policy > ipv5-basic-acl Rules IP VERSION Ipv5	ions Aliases SOURCE user	DESTINATION any	SERVICE/APPLICATION 546 546	ACTION dery_opt	Cancel
es <mark>Policies</mark> Applicat Policy > jpv6-basic-acl Rules IP VERSION Ipv6	ions Allases SOURCE user	DESTINATION any	SERVICE/APPLICATION 546 546	ACTION deny_opt	Cancel
es <mark>Policies</mark> Applicat Policy > jpv6-basic-acl Rules IP VERSION Ipv6	ions Allases SOURCE user	DESTINATION any	SERVICE/APPLICATION 546 546	ACTION deny_opt	Cancel
es <u>Policies</u> Applicat Policy > jpv6-basic-acl Rules IP VERSION Ipv6	ions Allases SOURCE USEr	DESTINATION any	SERVICE/APPLICATION 546 546	ACTION deny_opt	Cancel
es <u>Policies</u> Applicat Policy > jpv6-basic-acl Rules IP VERSION Ipv6 + ipv6-basic-acl > New forward	ions Aliases SOURCE USEr	DESTINATION any	SERVICE/APPLICATION 546 546	ACTION deny_opt	Cancel
es <u>Policies</u> Applicat Policy > jpv6-basic-acl Rules IP VERSION Ipv6 + Ipv6-basic-acl > New forward	ions Aliases SOURCE USEr ing Rule	DESTINATION any	SERVICE/APPLICATION 546 546	ACTION deny_opt	Cancel
es <u>Policies</u> Applicat Policy > jpv6-basic-acl Rules IP VERSION Ipv6 + ipv6-basic-acl > New forward	ions Aliases SOURCE USER ing Rule	DESTINATION any	SERVICE/APPLICATION 546 546	ACTION deny_opt	Cancel
es <u>Policies</u> Applicat Policy > jpv6-basic-acl Rules IP VERSION Ipv6 + ipv6-basic-acl > New forward IP version: Source: Source:	ions Aliases SOURCE USEr ing Rule	DESTINATION any	SERVICE/APPLICATION 546 546	ACTION deny_opt	Cancel
es <u>Policies</u> Applicat Policy > jpv6-basic-acl Rules IP VERSION Ipv6 Ipv6 IPversion: Source: Destination:	ions Aliases SOURCE USEr ing Rule IPv6 V Any V Any V	DESTINATION any	SERVICE/APPLICATION 546 546	ACTION deny_opt	Cancel
es Policies Applicat Policy > jpv5-basic-acl Rules IP VERSION Ipv6	ions Aliases SOURCE USEr ing Rule IPv6 V Any V Any V Service V	DESTINATION any	SERVICE/APPLICATION 546 546	ACTION deny_opt	Cancel
es Policies Applicat Policy > jpv6-basic-acl Rules IP VERSION Ipv6 Ipv6 IPversion: Source: Destination: Service/app: Services alias:	ions Aliases SOURCE USEr ing Rule IPv6 ~ Any ~ Service ~ Service ~	DESTINATION any	SERVICE/APPLICATION 546 546	ACTION deny_opt	Cancel
es Policies Applicat Policy > jpv6-basic-acl Rules IP VERSION Ipv6 Ipv6 IPversion: Source: Destination: Service/app: Services alias: Action:	ions Aliases SOURCE USEr ing Rule IPv6 ~ Any ~ Service ~ Service ~ Service ~	DESTINATION any	SERVICE/APPLICATION 546 546	ACTION deny_opt	Cancel
es Policies Applicat Policy > jpv6-basic-acl Rules IP VERSION Ipv6	ions Aliases SOURCE USEr ing Rule IPv6 ~ Any ~ Service ~ Service ~ Service ~ Permit ~	DESTINATION any	SERVICE/APPLICATION 546 546	ACTION deny_opt	Cancel
es Policies Applicat Policy > jpv6-basic-acl Rules IP VERSION Ipv6 Ipv6 Ipv6-basic-acl > New forward Ipversion: Source: Destination: Source: Service/app: Service alias: Action: TOS: Time range:	Ions Allases SOURCE USEr Ing Rule IPAG V Any V Any V Service V Service V Service V Service V Service V Service V	DESTINATION any	SERVICE/APPLICATION 546 546	ACTION deny_opt	Cancel
es Policies Applicat Policy > ipv6-basic-acl Rules IP VERSION Ipv6 Ipv6 Ipv6-basic-acl > New forward Ipv6-basic-acl > Ne	ions Aliases SOURCE user ing Rule IPv6 ~ Any ~ Service ~ Service ~ Service ~ Permit ~ . None - ~	any Reset	SERVICE/APPLICATION 546 546	ACTION deny_opt	Cancel
es Policies Applicat holicy > ipv6-basic-acl Rules IP VERSION Ipv6 + pv6-basic-acl > New forward Pversion: Source: Destination: Service/app: Service/app: Service/app: Services allas: Action: TOS: Time range: 802.1p priority: Options:	Ions Allases SOURCE User Ing Rule IPv6 V Any V Service V Service V Permit V Permit V	DESTINATION any Reset	SERVICE/APPLICATION 546 546	ACTION deny_opt	Cancel
es Policies Applicat Policy > ipv6-basic-acl Rules IP VERSION Ipv6 Policy > ipv6-basic-acl Rules IP VERSION Ipv6 Policy > ipv6-basic-acl Rules Ipv6-basic-acl > New forward Source: Destination: Service-allas: Action: ToS: Time range: B02.1p priority: Options: Queue:	Ions Allases SOURCE User Ing Rule IPv6 V Any V Service V Service V Service V Permit V I None - V I Log Mirror E	e DESTINATION any Reset Blacklist Disable scanning	SERVICE/APPLICATION 546 546	ACTION deny_opt	Cancel

Cancel

4



olicy > ipv6-basic-acl Rule	25				 Drag rows to re-o
P VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	
pv6	user	any	546 546	deny_opt	
рvб	any	any	svc-v6-dhcp	permit	
-					
ov6-basic-acl > New forwa	rding Rule				
IP version:	IPv6 💙				
Source:	Any 👻				
Destination:	Any 💙				
Service/app:	Service 💙				
Services alias:	svc-dns 🗸				
Action:	Permit 👻				
TOS:					
Time range:	- None - 🗸 🗸 Reset				
802.1p priority:	~				
Options:	Log Mirror Blacklist	Disable scanning			

Policy > ipv6-basic-acl Ru	les			 Drag rows to re
IP VERSION	SOURCE DE	STINATION SERVICE/APPLICAT	ION ACTION	
Іруб	user an	y 546 546	deny_opt	
Іруб	any an	y svc-v6-dhcp	permit	
Іриб	any an	y svc-dns	permit	
<u>т</u>				
т				
ipv6-basic-acl > New forw	varding Rule			
IP version:	IPv6 💙			
Source:	Any 👻			
Destination:	Anv.			
Destination.	Zuy			
Service/app:	Service 💙			
Services alias:	svc-v6-icmp 💙			
Action:	Permit 💙			
TOS:				
Time range:	- None - 🗸 🖌 Reset			
802.1p priority:	~			
Options:	Log Mirror Blacklist Disa	ble scanning		



4) 在 labX下,选择 Configuration>Roles & Policies,在 Roles 选项卡中,找到认证后的上网角色 employee(没有的话,可以新增一个),来调用之前创建好的两个策略 policies 和一个系统自带的 ra-guard 策略(另外请注意该角色的最后需要有你自己定义的其他策略的调用)。最后点击 Submit 按钮和 Pending Changes 按钮。

Crubo MOBILITY MASTER Lab2-MM-1	co ©	ONTROLLERS ACCESS POINTS CLIENTS ALERTS 0 2 0 0 0 1 \diamondsuit 0 \bigstar 2	admin ~
← Managed Network > lab2 >			¢
Mobility Master Managed Network (2) Dabboard Configuration WLAts Managed Network (2) Dabband1 Dabband1 Dabband2 Debband2 Atchentication Services Interfaces Controllers System Tasks Redundancy Maintenance	Policies Applications Alases Roles 10 NAME	RULES 32 Rules 11 Rules 33 Rules 0 Rules 22 Rules 23 Rules 24 Rules	

S Policies Application Name: employed Oldes 16 Cancel Submit Oggon 32 Rules sprole 35 Rules stateful-dot1x 0 Rules sprole 27 Rules sys-p-rol 23 Rules	S Policies Application Name: employed Cancel Submit Cancel Submit ogon 32 Rules ryuest 11 Rules sp-role 35 Rules tateful-dot1x 0 Rules ryus-logon 27 Rules sys-ap-rol 23 Rules	New Role	
Submit Cancel Submit ogon 32 Rules guest 11 Rules ap-role 35 Rules stateful-dot1x 0 Rules guest-logon 27 Rules sys-p-rol 23 Rules	Cancel Submit IAME Cancel Submit oggon 32 Rules guest 11 Rules sp-role 35 Rules tateful-dot1x 0 Rules guest-logon 27 Rules sys-ap-role 23 Rules	s Policies Application Name:	employee
AAME Calles Source Sour	AAME Calles Submit Solution Strategy States Strategy States Strates St	oles 16	Cancol
oogon 32 Rules guest 11 Rules ap-role 35 Rules stateful-dot1x 0 Rules guest-logon 27 Rules sys-ap-rol 23 Rules	ogon 32 Rules guest 11 Rules ap-role 35 Rules stateful-dot1x 0 Rules guest-logon 27 Rules tys-ap-roly 23 Rules	NAME	Cancel Submit
guest 11 Rules ap-role 35 Rules stateful-dot1x 0 Rules guest-logon 27 Rules sys-ap-rol 23 Rules	guest 11 Rules hp-role 35 Rules datateful-dot1x 0 Rules guest-logon 27 Rules zys-ap-rol 23 Rules	ogon	32 Rules
ap-role 35 Rules stateful-dot1x 0 Rules guest-logon 27 Rules sys-ap-rol 23 Rules	ap-role 35 Rules stateful-dot1x 0 Rules guest-logon 27 Rules gys-ap-rol 23 Rules	guest	11 Rules
tateful-dot1x 0 Rules guest-logon 27 Rules ys-ap-rol 23 Rules	tateful-dot1x 0 Rules guest-logon 27 Rules ys-ap-rol 23 Rules	ap-role	35 Rules
guest-logon 27 Rules ys-ap-rol 23 Rules	guest-logon 27 Rules ys-ap-role 23 Rules	stateful-dot1x	0 Rules
rys-ap-rol 23 Rules	ys-ap-rol 23 Rules	guest-logon	27 Rules
		sys-ap-rol	23 Rules
rys-synch-role 24 Rules	sys-switch-role 24 Rules	sys-syntch-role	24 Rules


Roles 16					
NAME		RULES			
denyall		1 Rules			
default-via-role		3 Rules			
default-vpn-role		4 Rules			
authenticated		4 Rules			
voice		43 Rules			
contractor		5 Rules			
+					_
employee					Show Advance
Global Rules					
IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	
+					
Rules of this Role only	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	
+ Rules of this Role only IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	
+ Rules of this Role only IP VERSION Ipv4 Iov6	SOURCE any any	DESTINATION any any	SERVICE/APPLICATION any any	ACTION permit	

New Text Document (4) tyt - Notenard

Roles Policies Applic	ations Aliases			
Roles 16				
NAME		RULES		
denyall		1 Rules		<u>م</u>
default-via-role		3 Rules		
default-vpn-role		4 Rules		
authenticated		4 Rules		
voice		43 Rules		
contractor		5 Rules		
employee		3 Rules		
+				
employee Policies	Bandwidth Captive Portal More			Show Basic View
NAME	RULES COUNT	TYPE	POLICY USAGE	
global-sacl	0	session	logon, guest, ap-role, stateful-dot1x, guest-lo	
apprf-employee-sacl	0	session	employee	
allowall	2	session	default-iap-user-role, default-via-role, defaul	
v6-allowall	1	session	default-via-role, default-vpn-role, authenticat	
+				



	New Policy				
	licevitoney				
s Policies Applicatio	Add an existing po	olicy O Create a new p	olicy		
Roles 16	Policy type:	Session ¥			
NAME					
	Policy name:	ipv4-basic-acl			
lenyall	Position:	3			
lefault-via-role					
lefault-vpn-role			Cancel Submit		
utnenticated		(2 Dulas			
ontractor		43 Kules			
employee	1	3 Rules			
-					
/	,				
mployee Policies B	Bandwidth Captive Portal	More			Show Basic V
NAME	RULES COUN	Т	TYPE	POLICY USAGE	
(lobal-sacl	0		session	logon, guest, ap-role, stateful-dot1x, guest-lo	
apprf-employee-sacl	0		session	employee	
allowall	2		session	default-iap-user-role, default-via-role, defaul	
US allowall	1		session	default-via-role default-von-role authenticat	





	New Policy			Pending Ch
es Policies Application	Add an existing policy Create a new pc	licy		
Roles 16	Policy type: Session 👻			
NAME	Policy name: ipv6-basic-acl	~ ·		
denyall	Porition: 5			
default-via-role	Position: 5			
default-vpn-role		Cancel		
authenticated		Cancer		
voice	43 Rules			
contractor	5 Rules			
employee	8 Rules			
-				
	dwidth Captive Portal More			Show Ba
employee Policies Ba	RULES COUNT	ТҮРЕ	POLICY USAGE	
employee Policies Bai NAME				
employee Policies Bai NAME global-sacl	0	session	logon, guest, ap-role, stateful-dot1x, guest-l	
employee Policies Bar NAME global-sacl apprf-employee-sacl	0 0	session session	logon, guest, ap-role, stateful-dot1x, guest-l employee	
employee Policies Bai NAME global-sacl apprf-employee-sacl ipv4-basic acl	0 0 4	session session session	logon, guest, ap-role, stateful-dot1x, guest-l employee employee	

1.6.3 user-table (CLI)

不希望非无线用户的子网地址段进入到控制器的 user-table, 定义可以加入 user-table 的无线用户子网 地址段白名单范围(阻止用户私设静态 IP 地址和后台的 DNS, DHCP, RADIUS 等应用服务器的地址冲突,导 致无线用户业务的故障)

首先定义 IPv6 和 IPv6 的无线用户 IP 地址段别名,如果用户网络环境发生变化,新增了用户 vlan 子网, 请提醒客户及时更新该别名。(这里的 IPv6 地址段没有具体含义,仅仅是配置参考)

(LabX-MM-1) [labX] (config) #netdestination6 user-net-ipv6

(LabX-MM-1) ^[labX] (config-submode)#network 2001:da8::/32

(LabX-MM-1) [labX] (config) #netdestination user-net-ipv4

(LabX-MM-1) ^[labX] (config-submode)#network 10.x.20.0 255.255.255.0

(LabX-MM-1) [labX] (config) #ip access-list session validuser

(LabX-MM-1) ^[labX] (config-submode)#no any any permit

(LabX-MM-1) ^[labX] (config-submode)#no ipv6 any any permit

(LabX-MM-1) ^[labX] (config-submode)#alias user-net-ipv4 any any permit position 6

(LabX-MM-1) ^[labX] (config-submode)#any any any deny position 7

(LabX-MM-1) ^[labX] (config-submode)#ipv6 alias user-net-ipv6 any any permit position 12

(LabX-MM-1) ^[labX] (config-submode)#ipv6 any any any deny position 13

(LabX-MM-1) ^[labX] (config-submode)#end



注意: 该 position x 是根据系统默认的 validuser 中的策略来定义的位置顺序。

1.6.4 user-table (GUI)

 在 labX 下,选择 Configuration > Roles & Policies,在 Aliases 选项卡中,点击+按钮来新增无线用 户 IP 子网地址池的别名,包括 IPv4 和 IPv6 的(IPv6 地址段这里只是示意,lab 环境中目前还不具备 IPv6)。最后点击 Submit 按钮和 Pending Changes 按钮。

aruba	MOBILITY MASTER Lab2-MM-1		CONTROLLERS ∅ 2 0 0	ACCESS POINTS CLIENTS ○ 0 ○ 1 ○ 0 0 0	ALERTS) admin ~
🗲 Managed Networl	k > lab2 >						Ŷ
C Mobility Master	Q Dashboard Configuration WLANS	Roles Policies Applicatio	ns Aliases				
Anaged Network	(2) Roles & Policies	NAME	ITEMS	DESCRIPTION	IP VERSION	INVERT	
🗁 lab2 (2)	Access Points	mswitch	1		IPv4		A
📼 lab2-md1	AP Groups	controller	1		IPv4		
📼 lab2-md2	Authentication	vrrp_ip	1	-	IPv4	-	
	Services	any	1		IPv4		
	Interfaces	localin	1	-	IPv4		
	Controllers	auth-google	2		IPv4		
	System	ÐŬ					
	Tasks						
	Redundancy	Service Aliases					
	Maintenance						

	Add New Destination				_			
es Polici	Rule type:	Network 💙						
controller	IP address:	10.2.20.0			IPv4	-		
vrrp_ip	Network mark:	255 255 255 0			IPv4	-		
any	Network mask.	255.255.255.0			IPv4	-		
localip				Cancel	OK IPv4			
auth-goog	e 2				IPv4			
\backslash								
Destina	on user-net-ipv4		/					
Destina	on user-net-ipv4 IP version: IPv4 ✓ Name: user-net-	ipv4	/	/				
Destina	on user-net-ipv4 IP version: IPv4 ~ Name: user-net- Description:	ipv4	/	-				
Destina	on user-net-ipv4 IP version: IPv4 ✓ Name: user-net- Description: Invert:	ip/4	/	-				
Destina	on user-net-ipv4	1pv4	/	•				



	© 2	0 0 0 1 0 0	☆ 0 ≠ 0 ▲ 2			
	Add New Destination					
Roles Polici Iocalip auth-goog	e Rule type: IP address: Network mask:	Network 2001:da8:: 32		IPv4 IPv4		
Dettinat	ti		Cancel OK			
Ì	IP version: IPv6 👻 Name: user-net-	pv6				
	Description:	_/				
	Items					
	ТҮРЕ	IP ADDRESS		NETMASK/RAN GE/OFFSET		=
Service Aliase	+ /					
						Cancel

2) 在 labX 下,选择 Configuration>Roles & Policies,在 Policies 选项卡中,点击 validuser 策略, 按照下面操作步骤,最后点击 Submit 按钮和 Pending Changes 按钮。

删除 ipv4 和 IPv6 的 any any any permit 两条策略。



A						
AME	RULES COUNT	TYPE		POLICY USAGE		
5-http-aci	1	session		guest		
5-https-acl	1	session		guest		
i-icmp-acl	1	session		guest		
5-logon-control	7	session		logon, guest-logon		
aliduser	11	session			()	
liduserethacl	1	eth				
nware-acl	5	session				
licy > validuser Rules						 Drag rows to re-or
VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION		
v4	240.0.0.0 240.0.0.0	any	any	deny_opt		
v4	any	any	any	permit		
/6	fe80::	any	any	deny_opt		
/6	fc00::/7	any	any	permit		
/6	fe80::/64	any	any	permit		
vб	ipv6-reserved-range	any	any	deny_opt		
v6	any	any	any	permit		
iduser > forwarding Pu	le .					
iliduser > forwarding Ru • Policies Appli	le ications Aliases				-	Cancel
liduser > forwarding Ru Policies Appli S-https-acl	le Ications Aliases	session		guest		Cancel
Iiduser > forwarding Ru Policies Appli Https-acl Hcmp-ad Hoeon-control	le Ications Aliases	session session session		guest guest logon, guest-logon		Cancel
Iiduser > forwarding Ru Policies Appli -https=acl -dcmp=acl -logon-control -liduser	le lications Aliases	session session session session		guest guest logon, guest-logon	0	Cancel
Ilduser > forwarding Ru Policies Appli -https-acl -icmp-acl -logon-control Mduser Iduserethacl	le Lications Aliases	session session session session eth		guest guest logon, guest-logon	Ō	Cancel
Hiduser > forwarding Ru Policies Appli https-acl -dogen-acl -dogenetacl Hiduser Hiduser Hiduseretacl	le Ications Aliases I I I I I I I I I I I I I I I I I I	session session session session eth session		guest guest logon, guest-logon 	Ō	Cancel
Iiduser > forwarding Ru Policies Appli -httpsacl -dagan.control Iduserethacl hware.acl	le ications Aliases 1 1 7 7 11 1 5	session session session eth session		guest guest logon, guest-logon 	0	Cancel
Iduser > forwarding Ru Policies Appli Apple Appl	le ications Aliases 1 1 1 7 1 1 1 5	session session session session eth session		guest guest logon, guest-logon 	0	Cancel
iiduser > forwarding Ru Policies Appli Attips-acl Jogon-control Iduserethacl Iduserethacl Iduserethacl Iduserethacl Version	le Ications Aliases 1 1 7 1 1 5 source	session session session eth session DESTINATION	SERVICE/APPLICATION	guest guest logon.guest-logon ACTION	0	Cancel
liduser > forwarding Ru Policies Appli Antips-acl Acorp-acl Acorp-acl Acorp-acl Iduserethacl Itiuserethacl Itiuser	le ications Aliases	session session session eth session deth session	SERVICE/APPLICATION	guest guest logon guest-logon 	٥	Cancel
IIduser > forwarding Ru Policies Appli Apple App	le ications Aliases	session session session eth session deth session any any	SERVICE/APPLICATION any any	guest guest logon, guest-logon 	0	Cancel
liduser > forwarding Ru Policies Appli Apple App	le ications Aliases	session session session eth session eth session session any any	SERVICE/APPLICATION any any any	guest guest logon, guest-logon 	0	Cancel
liduser > forwarding Ru Policies Appli Appli Apple App	le ications Aliases 1 1 1 7 1 1 5 SOURCE 240.00.0 2400.00 any fe80:: fc00:7	session session session eth session eth session dth session any any any any	SERVICE/APPLICATION any any any any any	guest guest logon,guest-logon 	•	Cancel
liduser > forwarding Ru Policies Appli App	le iccations Aliases 1 1 7 1 1 5 source 240.0.0.0 240.0.0 any fe80:: fc00:/7 fe80::64	session session session eth session eth session any any any any any any any	SERVICE/APPLICATION any any any any any any any	guest guest logon, guest-logon 	0	Cancel
liduser > forwarding Ru Policies Appli Compact Compact Compact Compact Policies Poli	le iccations Aliases	session session session eth session eth session ary any any any any any any any any any	SERVICE/APPLICATION any any any any any any any any any	guest guest logon.guest-logon 	٥	Cancel
liduser > forwarding Ru Policies Appli Apple App	le ications Aliases 1 1 1 7 1 1 5 SOURCE 240.0.0 2400.0.0 any res0:: rco0:77 res0::/7 res0::/7 res0::/7 res0::- res0:: any	session session session eth session eth session any any any any any any any any any an	SERVICE/APPLICATION any any any any any any any any any any	guest guest logon,guest-logon 	٠	Cancel
liduser > forwarding Ru Policies Appli Apple App	le	session session session eth session eth session any any any any any any any any any an	SERVICE/APPLICATION any any any any any any any any any any	guest guest logon,guest-logon 	•	Cancel
Iduser > forwarding Ru Policies Appli Apple Appl	le ications Aliases	session session eth session eth session any any any any any any any any any an	SERVICE/APPLICATION any any any any any any any any any any	guest guest logon, guest-logon 	0	Cancel
liduser > forwarding Ru Policies Appli Apple App	le ications Aliases	session session eth session eth session any any any any any any any any any an	SERVICE/APPLICATION any any any any any any any any any any	guest guest logon, guest-logon 	0	Cancel
liduser > forwarding Ru Policies Appli Apple App	le	Session Session Session eth session eth session any any any any any any any any any an	SERVICE/APPLICATION any any any any any any any any any any	guest guest logon, guest-logon 	0	Cancel

新增基于 IPv4 的 alias user-net-ipv4 any any permit 和 any any any deny 两条策略



			۷		
New Rule	e for validuser				Pending Changes
es Policie Rulet	type: (Access control	Application			
Policies		Cancel	POLICY USAG	E	Ē
v6-http-aci	1	session			4
v6-https-acl	1	session			
v6-icmp-acl	1	session			
v6-logon-control	7	session			
validuser	9	session			
validuserethacl		eth			
vmware-aci	5	session			
Policy > validuser Rules					i Drag rows to re-order
IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	6
Ipv4	127.0.0.0 255.0.0.0	any	any	deny_opt	
Ipv4	169.254.0.0 255.255.0.0	any	any	deny_opt	
Ipv4	224.0.0.0 240.0.0.0	any	any	deny_opt	
Ipv4	255.255.255.255	any	any	deny_opt	
Ipv4	240.0.0.0 240.0.0.0	any	any	deny_opt	
Ipv6	fe80::	any	any	deny_opt	
Ipv6	fc00::/7	any	any	permit	

validuser > New forwarding Rule

IP version:	IPv4 🗸	
Source:	Alias 🗸	
Source alias:	user-net-ipv4	~
Destination:	Any 💙	
Service/app:	Any 💙	
Action:	Permit	~
TOS:		
Time range:	- None - 🗸	Reset
802.1p priority:	V Mirror	Placklic
Options:	Log Mirror	DIackiis
Queue.	•	

Cancel Sub

user > New forwarding R	ule			
IP version:	IPv4 👻			
Source:	Any 🗸			
Destination:	Any 🗸			
Service/app:	Any 👻			
Action:	Deny 🗸			
ros:)		
l'ime range:	- None - 🗸 Reser	:		
802.1p priority:	~			
Options:	Log Mirror Blackl	st Disable scanning		
Queue:	~			



P version:	IPv6 🗸	
Source:	Alias 👻	
ource alias:	user-net-ipv6 🗸	
Destination:	Any 💌	
ervice/app:	Any 👻	
Action:	Permit 👻	
'OS:		
ime range:	- None - 🗸 Reset	
02.1 p priority:	v	
)ptions:	Log Mirror Biecklist Disable scanning	
lueue:	· ·	
	Cancel	
ser > New forwarding R	Cancel	
ser > New forwarding R P version:	Cancel	
ser > New forwarding R P version: Source:	Cancel ule	
ser > New forwarding R IP version: Source: Destination:	Cancel	
Ser > New forwarding R P version: Source: Destination: Service/app:	Le IP/6 V Any V Any V	
ser > New forwarding R P version: Source: Destination: Service/app: Action:	Leve Cancel	
ser > New forwarding R P version: jource: Destination: Service/app: Action: TOS:	Cancel ule IPV6 ~ Any ~ Any ~ Deny ~ I	
ser > New forwarding R P version: Source: Destination: Service/app: Action: TO S: Lime range:	Le Prof V Any V Any V Deny V Le None - V Reset	
ser > New forwarding R P version: Source: Destination: Service/app: Action: TO 5: Time range: 100 - 10 priority:	Lee IP6 Any · · Any · · Deny · · None - · Reset	
ser > New forwarding R P version: Source: Destination: Service/app: Action: TOS: Time range: S02.1 p priority: Options:	Ule IP/6 ~ Any ~ Any ~ Deny ~ Deny ~ Image: Second Seco	
ser > New forwarding R P version: Source: Destination: Service/app: Action: TO 5: Time range: 302.1 p priority: Dptions: Queue:	ule Image: PV6 Image: P	

新增基于 IPv6 的 ipv6 alias user-net-ipv6 any any permit 和 ipv6 any any any deny 两条策略

1.6.5 控制器访问控制 (CLI)

不希望无线用户可以直接访问控制器的管理界面,在指定认证后的用户角色中调用下面的策略 xxcontroller-if-acl。注意:必须是认证后的无线用户 role 以及默认的 authenticanted role,针对 Portal 认证前 的用户角色谨慎使用。

(LabX-MM-1) [labX] (config) #netdestination v4-controller-interfaces (LabX-MM-1) [labX] (config-submode)# host 10.2.10.11



(LabX-MM-1) [labX] (config-submode)# host 10.2.10.12
(LabX-MM-1) [labX] (config-submode)# host 10.2.10.21
(LabX-MM-1) [labX] (config-submode)# host 10.2.10.22
(LabX-MM-1) [labX] (config-submode)# host 10.2.10.10
(LabX-MM-1) [labX] (config-submode)# host 10.2.50.11
(LabX-MM-1) [labX] (config) #netdestination6 v6-controller-interfaces
(LabX-MM-1) [labX] (config-submode)# host 2001:da8:8000:151::13
(LabX-MM-1) [labX] (config) #ip access-list session ipv4-controller-if-acl
(LabX-MM-1) ^[labX] (config-submode)#user alias v4-controller-interfaces any deny position 1
(LabX-MM-1) [labX] (config) #ip access-list session ipv6-controller-if-acl
(LabX-MM-1) ^[labX] (config-submode)#ipv6 user alias v6-controller-interfaces any deny position 1
(LabX-MM-1) ^[labX] (config) #user-role contractor
(LabX-MM-1) ^[labX] (config-submode)# access-list session ipv4-controller-if-acl position 3
(LabX-MM-1) ^[labX] (config-submode)# access-list session ipv6-controller-if-acl position 4
(LabX-MM-1) ^[labX] (config-submode)# access-list session allowall position 5
(LabX-MM-1) ^[labX] (config-submode)# access-list session v6-allowall position 6

1.6.6 控制器访问控制 (GUI)

1) 在 labX 下,选择 Configuration>Roles & Policies,在 Aliases 选项卡中,点击+ 按钮来新增控制 IP 地址池的别名,包括 IPv4 和 IPv6 的 (IPv6 地址这里只是示意,lab 环境中目前还不具备 IPv6)。最后 点击 Submit 按钮和 Pending Changes 按钮。

aruba "	IOBILITY MASTER Lab2-MM-1			ACCESS POINTS CLIENTS ○ ○ ① 1 ○ 0 0 0	ALERTS		admin ~
← Managed Network	> lab2 >						Ŷ
C Mobility Master	Q Dashboard Configuration WLANS	Roles Policies Application	Aliases				
Managed Network (2)	2) Roles & Policies	NAME	ITEMS	DESCRIPTION	IP VERSION	INVERT	
🗁 lab2 (2)	Access Points	mswitch	1	-	IPv4	-	<u>^</u>
🗂 lab2-md1	AP Groups	controller	1	-	IPv4	-	
📼 lab2-md2	Authentication	vrrp_ip	1	-	IPv4		
	Services	any	1	-	IPv4	-	
	Interfaces	user	1		IPv4		
	Controllers	auth-google	2	-	IPv4		
	System Tasks	E					
	Redundancy						
	Maintenance	Service Allases					





ith-facebook					
icalling block	3	-	IPv4		
icaling block	2		IPv4		
-controller-interfaces	2	-	IPV4	-	
er-net	1		IPV4		
ntroller6	1		IPV6		
o-reserveu-range	1		IP-V0		
controller-interiaces	1		IPVO	**	
stination v4-controller-ir	terfaces				
IP version: Ipv-	1				
Description:					
Invert:					
Items					
ТҮРЕ		IP ADDRESS	NETMASK/RANGE/OF	FSET	
host		10.2.10.11			
host		10.2.10.12			
host		10.2.10.21			
host		10.2.10.22	-		
+					
Policies Applicati	ons Aliases				
Policies Applicati	ons Aliases		10×-4		
Policies Application	Aliases	-	IPv4 IPv4		
Policies Applicati auth-facebook wificalling-block	Aliases		IPv4 IPv4 IPv4		
Policies Applicati auth-facebook wificalling-block v4-controller-interfaces	Aliases		1Pv4 1Pv4 1Pv4 1Pv4		
Policies Applicati auth-facebook wrificalling-block v4-controller-interfaces user-net controller6	Aliases 3 2 5 1		1Py4 1Py4 1Py4 1Py4 1Py6		
Policies Applicati auth-facebook wrficalling-block v4-controller-interfaces user-net controller6 ins/freserved-canpe	Aliases 3 2 5 1 1 1		1Py4 1Py4 1Py4 1Py4 1Py6 1Py6		
Policies Applicati auth-facebook wifcalling-block v4-controller-interfaces user-net controller6 jpx6-reserved-range v4-controller-interfaces	aliases 3 2 5 1 1 1 1		1Pv4 1Pv4 1Pv4 1Pv4 1Pv6 1Pv6		
Policies Applicati auth-facebook wrificalling-block v4-controller-interfaces user-net controller6 jox6-reserved-range v6-controller-interfaces	aliases 3 2 5 1 1 1 1 1	- - - - - - - - -	1Pv4 1Pv4 1Pv4 1Pv6 1Pv6 1Pv6 1Pv6		
Policies Applicati auth-facebook wificalling-block v4-controller-interfaces user-net controller6 jox6-reserved-range v4-controller-interfaces + Destination v6-controlle	Aliases 3 2 5 1 1 1 1 1 		1Pv4 1Pv4 1Pv4 1Pv6 1Pv6 1Pv6 1Pv6		
Policies Applicati auth-facebook wi-faciling-block v4-controller-interfaces user-net controller of user-net v6-controller-interfaces v6-controller-interfaces v6-controller-interfaces v6-controller-interfaces	Aliases		IPv4 IPv4 IPv4 IPv6 IPv6 IPv6		
Policies Applicati auth-facebook wificalling-block v4-controller-interfaces user-net controller-interfaces iox6-reserved-range v6-controller-interfaces i Destination v6-controlle Persion: Description: Invert:	Aliases		1Pv4 1Pv4 1Pv4 1Pv6 1Pv6 1Pv6 1Pv6		
Policies Applicati auth-facebook wifcalling-block v4-controller-interfaces user-net controller-interfaces user-net v4-controller-interfaces postination v6-controller IP version: Description: Invert: Items	Aliases		1Pv4 1Pv4 1Pv4 1Pv6 1Pv6 1Pv6 1Pv6		
Policies Applicati auth-facebook wifcalling-block v4-controller-interfaces user-net controller-interfaces ipx6-reserved-range v4-controller-interfaces ipv6-contro	ns Aliases	 	IРч4 IРч4 IРч4 IРч6 IРч6 IРч6 IРч6 IРч6	L/OFFSET	
Policies Applicati auth-facebook wifcalling-block v4-controller-interfaces user-net controller-interfaces user-net ovef-controller-interfaces person: Description: Invert: Items TYPE host	Aliases	 	IРч4 IРч4 IРч4 IРч6 IРч6 IРч6 IРч6 IРч6 IРч6 IРч6		

2) 在 labX 下,选择 Configuration > Roles & Policies,在 Policiess选项卡中,点击+按钮来新增两个策略。

ipv4-controller-if-acl 和 ipv6-controller-if-acl。最后点击 Submit 按钮和 Pending Changes 按钮。



CIUDO MOBILITY MA Lab2-MM	ASTER I-1		CONTROLLERS A ⊗ 2 ○ 0	CCESS POINTS CLIENTS ALERT	rs 2		admin ¥
← Managed Network > lab2 >							Ġ
Ck Mobility Master	Q Dashboard	Roles Policies Applications	Aliases				
C Lab2-MM-1	WLANS	Policies					
Managed Network (2)	+ Roles & Policies	NAME	RULES COUNT	TYPE	POLICY USAGE		
😂 lab2 (2)	Access Points	deny-cry-antivirus	6	session	-		*
lab2-md1	AP Groups	ipv4-controller-if-acl	1	session	contractor		.
lab2-md2	Authentication	ipv4-basic-ad	4	session	employee		
	Services	ipv6-controller-if-acl	1	session	contractor		
	Interfaces	uplink-lb-cfg-racl	0	routing	-		
	Controllers	uplink-lb-sys-raci	0	routing	-		
	Surtem	master-boc-traffic	0	routing	-		*
	System						
	Tasks						
	Redundancy	Policy > Ipv4-controller-it-aci Rules					 Drag rows to re-order
	Maintenance	IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	
		Ipv4	user	v4-controller-interfaces	any	deny_opt	
		+					



	ster 1		CONTROLLERS A ⊙ 2 ○ 0 0	CCESS POINTS CLIENTS ALE 0 0 1 0 0 Δ	ERTS 2		⑦ admin ♥
Managed Network > lab2 >							Ŷ
C C C	Dashboard Configuration	Roles Policies Applications	Aliases				
Lab2-MM-1	WLANs	Policies					
Managed Network (2)	Roles & Policies	NAME	RULES COUNT	TYPE	POLICY US	AGE	
🔁 lab2 (2)	Access Points	deny-cry-antivirus	6	session			^
🖾 lab2-md1	AP Groups	ipv4-controller-if-acl	1	session	contractor		
lab2-md2	Authentication	ipv4-basic-acl	4	session	employee		
	Services	ipv6-controller-if-acl	1	session	contractor		÷
	Interfaces	uplink-lb-cfg-racl	0	routing			
	Controllers	uplink-lb-sys-racl	0	routing	-		
	Conditioners	master-boc-traffic	0	routing	-		÷
	System	Ŧ					
	Tasks						
	Redundancy	Policy > ipvö-controller-if-acl Rules	5				 Drag rows to re-order
	Maintenance	IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	
		lpv6	user	v6-controller-interfaces	any	deny_opt	
		т					



IP version:	IPv6 💙	
Source:	User 👻	
Destination:	Alias 👻	
Destination alias:	v6-controller-interfaces ¥	
Service/app:	Any 👻	
Action:	Deny Y	
TOS:		
Time range:	- None - 🗸 Reset	
802.1p priority:	×	
Options:	Log Mirror Blacklist Disable scanning	
Queue:	▼	

3) 在 labX 下,选择 Configuration>Roles & Policies,在 Roles 选项卡中,找到认证后的上网角色 contractor(没有的话,可以新增一个),来调用之前创建好的两个策略 policies, ipv4-controller-if-acl 和 ipv6-controller-if-acl (另外请注意该角色的最后需要有你自己定义的其他策略的调用)。最 后点击 Submit 按钮和 Pending Changes 按钮。

Crubo MOBILITY MASTER Lab2-MM-1		CONTROLLERS ACCESS POINTS CLIENTS ALERTS ⊘ 2 ○ 0 ○ 1 ♀ 0 △ 2	(b) admin ~
Managed Network > lab2 >			\$
Managed Network 2 lab2 2 Mobility Master Lab2-MM-1 Managed Network (2) Dab2(2) Dab2-md1 Configure Lab2-md1 A	paraton LANS Dels & Policies Applications / LANS Dels & Policies P Groups B G Groups B G Groups B G Groups B G G B G B	Ilases RULES RULES SRules SRules SRules RULES RULES	
Ta Ri Maint	isks edundancy enance		



Cancel Sub

oles Policies Application Name:	contractor
Roles 16 NAME	Cancel Submit
logon	32 Rules
guest 7	11 Rules
ap-role	35 Rules
stateful-dot1x	0 Rules
guest-logon	27 Rules
sys-ap-role	23 Rules
sys-switch-role	24 Rules

Roles 16					
NAME		RULES			
denyall		1 Rules			
default-via-role		3 Rules			
default-vpn-role		4 Rules			
authenticated		4 Rules			
voice		43 Rules			
contractor		5 Rules			
employee		12 Rules			
contractor					Show Advance
Global Rules					
IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	
+					
Rules of this Role only					
IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	





oles 16						
IAME		RULES				
lenyall		1 Rules				
lefault-via-role		3 Rules				
lefault-vpn-role		4 Rules				
uthenticated		4 Rules				
oice		43 Rules				
ontractor		a modern				
		5 Kules				
mployee		12 Rules				
ontractor Policies Banc	dwidth Captive Portal	12 Rules				Show Basi
ontractor Policies Banc	dwidth Captive Portal RULES COUNT	12 Rules	түре	POLICY USAGE		Show Basi
mployee ontractor IAME Jobal-sacl	dwidth Captive Portal RULES COUNT 0	12 Rules	TYPE session	POLICY USAGE logon, guest, ap-role.	stateful-dot1x, guest-l	Show Basi
mployee Policies Banc IAME Jobal-sacl ipprf-contractor-sacl	dwidth Captive Portal RULES COUNT 0 0	12 Rules	TYPE session session	POLICY USAGE logon, guest, ap-role, contractor	stateful-dot1x, guest-L	Show Basi
mployee Policies Banc JAME jobal-sacl pprf-contractor-sacl ove-controller-if-acl	dwidth Captive Portal RULES COUNT 0 1	3 Kules 12 Rules More	TYPE Session session session	POLICY USAGE logon, guest, ap-role, contractor contractor	stateful-dottx, guest-L	Show Basi





	⊘ 2 ① 0	Ø 0 0 1 ₹	≈ 0 ≠ 0 🛆 2	
New	Policy			
oles Policies Application	 Add an existing policy 	/ Create a new poli	cy	
Roles 16	Policy type:	Session 💙		
NAME	Policy name:	ipv6-controller-if-acl	×	
denyall default-via-role	Position:	4		
default-vpn-role				
authenticated		I		
voice		43 Rules		
contractor		5 Rules		
employee +		12 Rules		
contractor Policies Bandwid	lth Captive Portal	More		
NAME	RULES COUNT		TYPE	POLICY USAGE
global-sacl	0		session	logon, guest, ap-role, stateful-dot1x, guest-l
apprf-contractor-sacl	0		session	contractor
ipv4-coptroller-if-acl	1		session	contractor
ipv6-controller-if-acl +	1		session	contractor

1.6.7 用户隔离 (CLI)

不希望无线用户之间可以互相访问,即使在同一个 VLAN 下,也需要阻止用户间的相互访问。 注意:如果环境中需要有 Bonjour 等组播应用,不能关闭该选项。AOS8.6 开始完美地增加了基于 rolebased 的 acl 来灵活控制同一个 VLAN 下不同用户角色之间的互访(<mark>请参考 role-based 的 acl 章节设置)</mark>。

全局模式下阻止 L2 层用户间的相互访问配置
(LabX-MM-1) ^[labX] (config) #firewall
(LabX-MM-1) ^[labX] (config-submode)#deny-inter-user-bridging (阻止两层的非 IP 帧流量)
(LabX-MM-1) ^[labX] (config-submode)#deny-inter-user-traffic (阻止 3 层的 IP 数据流量)
(LabX-MM-1) ^[labX] (config) #ipv6 firewall
(LabX-MM-1) ^[labX] (config-submode)#deny-inter-user-bridging
如果需要针对单个 SSID 下的无线用户,为了阻止终端之间的互访以及 P2P 应用等,
(LabX-MM-1) [labX] (config) #wlan virtual-ap no-broadcast-vap



(LabX-MM-1) ^[labX] (Virtual AP profile "no-broadcast-vap") #deny-inter-user-traffic

1.6.8 用户隔离 (GUI)

1) 在 labX 下,选择 Configuration > Services,在 Firewall 选项卡中,勾选 Deny inter user bridging 和 Deny inter user traffic。最后点击 Submit 按钮和 Pending Changes 按钮。

	TY MASTER 2-MM-1		CONTROLLERS ACCESS POINTS ∅ 2 0 0 1 3	CLIENTS ALERTS) admin ~
Managed Network > lab2	2 >				Pending Changes
🛱 Mobility Master	Configuration	Clusters AirGroup VPN Firewall	Mobility External Services DHCP	WAN	
🖾 Lab2-MM-1	WLANS	 Global Settings 			
Managed Network (2)	Roles & Policies		IPV4	IPV6	
🔁 lab2 (2)	Access Points	Monitor ping attack:	per 30 sec	per 30 sec	
🖾 lab2-md1	AP Groups	Monitor TCP SYN attack rate:	per 30 sec	per 30 sec	
lab2-md2	Authentication	Monitor IR receiper attack	per 20 ser	ner 20 ser	
	Services	Monitor/police.non.gratuitous ARP attacks:	0	per so sec	
	Interfaces	Meniteripelice analyticus ABB attack rate	50 per 20 per		
	Controllers	Monitor/police gratuitous ARP attack rate:	50 per 30 sec		
	System	Monitor/police gratuitous ARP attack action:	Drop 👻		
	Tasks	Monitor/police CP attack rate:	per 30 sec		
	Redundancy	 Deny inter user bridging: 			
	Maintenance	Deny inter user traffic:			
		Deny source routing:			
		Deny all IP fragments:			
		Prohibit IP receiptor			
		Prohibit RST replay attack:			
		Log all received ICMP errors:			
		Allow tri-session with DNAT:			
		AMSDU configuration:			
		Session idle timeout:	16 sec	sec	
		Disable FTP server:			
		GRE call ID processing:			
		Optimize duplicate address detection frames:			
					Cancal
	ArubaMM-VA, 8.6.0.3				Cancer

2) 在 labX 下,选择 Configuration>System,在 Profiles选项卡中,找到 Wireless LAN>Virtual AP >no-broadcast-vap,在 Advanced中,勾选 Deny inter user traffic。最后点击 Submit 按钮和 Pending Changes 按钮。



aruba	MOBILITY MASTER Lab2-MM-1	CONTRO © 2	LLERS ACCESS POINTS CLIENTS ALERTS ○ 0 ○ 0 ○ 1 ○ 0 △ 2		admin ~
🔶 Managed Netwo	ork > lab2 >				Pending Change:
Ck Mobility Master	Configuration	General Admin AirWave CPSec Certificates	SNMP Logging Profiles More		
Lab2-MM-1	WLANS	All Profiles	Virtual AP profile: no-broadcast-vap		
Managed Networ	rk (2) Roles & Policies	⊕	> General		
□ Iab2 (2)	Access Points	Server Group	> RF		
	AP Groups	Stateful 802.1X Authentication	Y Advanced		
	Authentication	Stateful Kerberos Authentication			
	Services	Stateful NTLM Authentication	Cellular handoff assist:		
	Interfaces	TACACS Server	Upennow Enable:		
	Controllers	TSM Report Request	Authentication Failure Blacklist Times	3600	
	System	VIA Client WLAN	Addrendradon Palidre Blackisc Time.	3000 sec	
	Tasks	OPN Authentication	Blacklist Time:	3600 sec	
	Redundancy	\ominus 📑 Virtual AP	Deny inter user traffic:		
	Maintenance	default	Deny time range:	-None-	
		⊖ 🗗 no-broadcast-vap 👘	DoS Prevention:		
			HA Discovery on-association:		
		• 🕒 AAA 👻 👻	Mobile IP:		
			Preserve Client VLAN:		
			Remote-AP Operation:	standard 👻	
			Station Blacklisting:		
			Strict Compliance:		
			VLAN MODIIITY:		
			WAN Operation mode:	always	
			FDB Update on Assoc:		
			 Broadcast/Multicast 		
	ArubaMM-VA, 8.6.0.3				Cancel Submit Submit As

1.6.9 端口阻断 (CLI)

阻止无线终端在内部感染和传播勒索病毒。

1) 先定义 policy 策略

(LabX-MM-1) [labX] (config) #ip access-list session deny-cry-antivirus					
(LabX-MM-1) ^[labX] (config-submode)#	any any tcp 135 deny	position 1			
(LabX-MM-1) ^[labX] (config-submode)#	any any tcp 137 139 deny	position 2			
(LabX-MM-1) ^[labX] (config-submode)#	any any tcp 445 deny	position 3			
(LabX-MM-1) ^[labX] (config-submode)#	any any udp 135 deny	position 4			
(LabX-MM-1) ^[labX] (config-submode)#	any any udp 137 139 deny	position 5			
(LabX-MM-1) ^[labX] (config-submode)#	any any udp 445 deny	position 6			

2) 然后在认证的角色中进行策略调用。

(LabX-MM-1) [labX] (config) #user-role employee (LabX-MM-1) [labX] (config-submode)# access-list session deny-cry-antivirus position 3 (LabX-MM-1) ^[labX] (config-submode)# access-list session allowall position 4



1.6.10 端口阻断 (GUI)

1) 在 labX 下,选择 Configuration > Roles & Policies,在 Policiess选项卡中,点击+按钮来新增一个策略。

deny-cry-antivirus。最后点击 Submit 按钮和 Pending Changes 按钮。

Cruba MOBILITY MAST Lab2-MM-1	TER		CONTROLLERS ⊘ 2 ○ 0	ACCESS POINTS CLIENTS ○ 0 ① 1	ALERTS Z) admin 🛩
← Managed Network > lab2 >							Pending Changes 🗘
C Q	Dashboard Configuration	Roles Policies Applications	Aliases				
Lad2-MM-1	WLANs	Policies					
Managed Network (2)	Roles & Policies	NAME	RULES COUNT	TYPE	POLICY USA	GE	=
🗂 lab2 (2)	Access Points	apprf-sys-ap-role-sacl	0	session	sys-ap-role		*
	AP Groups	apprf-sys-switch-role-sacl	0	session	sys-switch-ro	ble	
	Authentication	apprf-employee-sacl	0	session	employee		
	Services	apprf-contractor-sacl	0	session	contractor		
	Interfaces	ipv6-basic-acl	4	session	employee		
	Internaces	deny-cry-antivirus	6	session			<u> </u>
	Controllers	ipv4-controller-if-acl	1	session	contractor		*
	System	+					
	Tasks						
	Redundancy	Policy > deny-cry-antivirus Rules					 Drag rows to re-order
	Maintenance	IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION	
		Ipv4	any	any	135	deny_opt	A
		Ipv4	any	any	137 139	deny_opt	
		Ipv4	any	any	445	deny_opt	
		Ipv4	any	any	135	deny_opt	*
		+					

NAME POLICY USAGE cplogout 1 Session demy-cry-antivius 0 Session Session demy-cry-antivius 0 Session Session Session Session	olicies		Cancel			
cplogout 1 session - demy-cry-entivitus 0 session - 0	IAME			POLICY USAG	E	
deny-of-shtrorus o session - te deny-all 2 session denyall	plogout	1	session			
deryal eession oeryal dirp-ad 1 session guest, voic dns-ad 1 session guest, voic global-ad 4 session voice global-ad 0 session logon, guest, aprole, stateful-dottx, guest-L Policy>deny-cry-antivers Rules O pag rows to re-or IP VERSION SOURCE DESTINATION SERVICE/APPLICATION ACTION ACTION	eny-cry-antivirus		session	-		
dirsped i accusation getex, total dirsped 1 acession getex, total facetime-acl 4 acession volce global-sacl 0 acession logon, guest, ap-role, stateful-dottx, guest-L Policy> deny-cry-antity us Rules Policy> deny-cry-antity us Rules Image: Comparison of the	lenyali Ibco-acl		session	denyali duest voice		
Acetime ad 4 session voice global-sad 0 session logon, guest, ap-role, stateful-dot1x, guest-l Policy > deny-cry-antiv/Lis Rules	Ins-acl		session	guest voice		
global-sacl 0 session logon, guest, ap-role, stateful-dot1x, guest-L + * * * Policy>deny-cry-antiv/Lis Rules * * p VERSION SOURCE DESTINATION SERVICE/APPLICATION ACTION	acetime-acl	4	session	voice		
Policy > deny-cry-antivus Rules IP VERSION SOURCE DESTINATION SERVICE/APPLICATION ACTION	lobal-sacl	0	session	logon, guest,	ap-role, stateful-dot1x, guest-l	
IP VERSION SOURCE DESTINATION SERVICE/APPLICATION ACTION	olicy > deny-cry-antivirus Rule	s				 Drag rows to re-o
	VERSION	SOURCE	DESTINATION S	ERVICE/APPLICATION	ACTION	



y-cry-antivirus > New	r forwarding Rule
IP version:	IPv4 💙
Source:	Any 💙
Destination:	Any 💙
Service/app:	ТСР 🗸
Min/max port:	 135 135
Source dest:	0
Action:	Deny 👻
TOS:	
Time range:	- None - 💙 Reset
802.1p priority:	▼
Options:	Log Mirror Blacklist Disable scanning
Queue:	~

deny-cry-antivirus > New forwarding Rule

IP version:	IPv4 💙
Source:	Any 💙
Destination:	Any 💙
Service/app:	тср 🗸
Min/max port:	 137 139
Source dest:	0
Action:	Deny 👻
TOS:	
TOS: Time range:	- None - V Reset
TOS: Time range:	- None - V Reset
TOS: Time range: 802.1p priority:	- None - V Reset
TOS: Time range: 802.1p priority: Options:	None - Reset Log Mirror Blacklist Disable scanning
TOS: Time range: 802.1p priority: Options: Queue:	None - Reset Log Mirror Blacklist Disable scanning

eny-cry-antivirus > New for	warding Rule
IP version:	IPv4 💙
Source:	Any 👻
Destination:	Any 👻
Service/app:	TCP 👻
Min/max port:	 445 445
Source dest:	0
Action:	Deny 👻
TOS:	
Time range:	- None - 👻 Reset
802.1p priority:	v
Options:	Log Mirror Blacklist Disable scanning
Queue:	▼

ry-antivirus > New f	orwarding Rule
IP version:	IPv4 💙
Source:	Any 💙
Destination:	Any 💙
Service/app:	UDP 👻
Min/max port:	 135 135
Source dest:	0
Action:	Deny 👻
TOS:	
Time range:	- None - 💙 Reset
902 1p priority	
Options:	Log Mirror Blacklist Disable sca



deny-	cry-antivirus > New forwa	arding Rule
Γ	IP version:	IPv4 👻
	Source:	Any 🗸
	Destination:	Any 🗸
	Service/app:	UDP 🗸
	Min/max port:	 137 139
	Source dest:	0
Ŀ	Action:	Deny
	TOS:	
	Time range:	- None - 🗸 Reset
	802. Ip priority:	Log Niccor Dicable comping
	Quaua:	
	Queue.	

ny-cry-antivirus > New	forwarding Rule
IP version:	IPv4 💙
Source:	Any 👻
Destination:	Any 👻
Service/app:	UDP 💙
Min/max port:	 445 445
Source dest:	0
Action:	Deny 🗸
TOS:	
Time range:	- None - 💙 Reset
802.1p priority:	
Options:	Log Mirror Blacklist Disable scanning
Queue:	✓

2) 在 labX 下,选择 Configuration>Roles & Policies,在 Roles 选项卡中,找到认证后的上网角色 contractor (没有的话,可以新增一个),来调用之前创建好的两个策略 policies, deny-cry-antivirus,设置 position=3 (表示该策略最靠上,优先执行。另外请注意该角色的最后需要有你自 己定义的其他策略的调用)。最后点击 Submit 按钮和 Pending Changes 按钮。

Crubo MOBILITY MA Lab2-MM	ISTER I-1		CONTROLLERS ACCESS POINTS CLIENTS ALERTS ○ 2 ○ 0 ○ 1 ○ 0 ○ 2 △ 2	admin ~
← Managed Network > lab2 >				Ŷ
Mobility Master Lab2-MM-1 Managed Network (2) Lab2(2)	Dashboard Configuration WLANS Roles & Policies	Roles Policies Applications Aliases	s RULES 23 Poler	
C lab2-md1 C lab2-md2	Access Points AP Groups Authentication Services Interfaces Controllers System Tasks	ogen guest aprole stateful-dottx guest-kogon sys-aprole sys-antol+ole ₽	24 Rules 11 Rules 35 Rules 0 Rules 27 Rules 28 Rules 24 Rules	·
	Redundancy Maintenance			



RULES 1 Rules * 3 Rules de 4 Rules 4 Rules 43 Rules 12 Rules 5 Rules 12 Rules Show Advanced
Notes
1 Rules le 3 Rules le 4 Rules le 4 Rules la 4 Rules la 4 Rules la 2 Rules la
le 3 Rules Je 4 Rules 4 Rules 4 Rules 5 Dules 12 Rules 5 Dules 5 Due Advanced
de 4 Rules 4 Rules 43 Rules 5 Rules 12 Rules Show Advanced
4 Rules 43 Rules 12 Rules 12 Rules 5 Now Advanced
43 Rules 5 Bules 12 Rules Show Advanced
S Rules
12 Rules Show Advanced
Show Advanced
Show Advanced
Show Advanced
SOURCE DESTINATION SERVICE/APPLICATION ACTION
vale only





NAME		RULES		
denyall		1 Rules		
default-via-role		3 Rules		
default-vpn-role		4 Rules		
authenticated		4 Rules		
voice		43 Rules		
contractor		5 Rules		Ū
employee		12 Rules		
+				
contractor Policies Band	width Captive Portal More	•		Show Basic V
	RULES COUNT	TYPE	POLICY USAGE	
NAME	0	session	logon, guest, ap-role, stateful-dot1x, guest-l	
global-saci		rorrigo	contractor	
NAME global-sacl apprf-contractor-sacl	0	26221011		
NAME global-sacl apprf-contractor-sacl ipv4-controller-if-acl	0	session	contractor	

NAME authenticated default-tap-user-role de		⊘ 2 ① 0	○ 0 ① 1 ⑦ 0 ₱ 0 ▲ 2		U III
es Policies Application Roles 10 NAME aprole authenticated Gefault-van-role default-van-role default-van-rol		New Policy			
AMAE aprole aprole authenicated contractor default-iaprone	es Policies Application	 Add an existing policy Policy type: 	Create a new policy		
addreidaed default-lap-use-role default-lap-role default-lap-ro	NAME ap-role	Policy name: Position:	deny-cry-antivirus		
default-rynole 4 Rules default-rynole 4 Rules default-rynole 1 Rules terrator Policie Andrew Portal NAME RULES COUNT TYPE gobal-saci 0 session gobal-saci 0 session gobal-saci 1 session	contractor default-iap-user-role		Cancel Submit		
ontractor Policie Andwidth Captive Portal More Show Basi NAME RULES COUNT TYPE POLICY USAGE Show Basi global-saci 0 session logon, guest, ap-role, stateful-dot1x, guest-l Show Basi global-saci 0 session contractor ontractor gord-control-Lif-saci 1 session contractor contractor gord-control-Lif-saci 1 session contractor contractor	default-via-role default-vpn-role denyall	1	3 Kules 4 Rules 1 Rules		
Policie Policie Policie Policie Policie Policie Policie Policie Show Basi NAME RULES COUNT TYPE Policie USAGE Policie USAGE <td< td=""><td>+</td><td></td><td></td><td></td><td></td></td<>	+				
NAME RULES COUNT TYPE POLICY USAGE global-sad 0 session logon, guest, ap-role, stateful-dot1x, guest-L. apprf-contract/Red 0 session contractor ipu4-contract/Red 1 session contractor ipu4-contract/Red 1 session contractor ipu6-contract/Red session contractor	contractor Policies	andwidth Captive Portal 1	llore		Show Basic V
global-sacl 0 session logon, guest, ap-role, stateful-dot ix, guest-l appr/contracturation 0 session contractor ipu4-controler-if-acl 1 session contractor up-6-controler-if-acl 1 session contractor	NAME	RULES COUNT	TYPE	POLICY USAGE	
apprf-contract_radad 0 session contractor ipu-4-contract_radad 1 session contractor ipu-6-controller-if-ad 1 session contractor ipu-6-controller-if-ad 1 session contractor	global-sacl	0	session	logon, guest, ap-role, stateful-dot1x, guest-l	
ipu4-contro 4-1Facil 1 session contractor ipu6-controller-1Facil 1 session contractor +	apprf-contractorsacl	0	session	contractor	
ipr6-g-croiler:iFad 1 session contractor	ipv4-controver-if-acl	1	session	contractor	
	ipv6-controller-if-acl	1	session	contractor	



oles Polici	es Applic	ations Alias	ies						
Roles 16									
NAME		*		RULES					⊞
ap-role				35 Rules					
authenticated				4 Rules					
contractor				11 Rules				Ū	
default-iap-use	er-role			2 Rules					
default-via-role	2			3 Rules					
default-vpn-rol	le			4 Rules					
denyall				1 Rules					
+									
1 - C									
contractor	Policies	Bandwidth	Captive Portal	More				Show Basic \	/iew
NAME		RIII	ES COUNT		TYPE	POLICYUSAG	F		Ē
apprf-contract	or-sacl	0			session	contractor		1	
deny-cry-antivi	irus	6			session	contractor			
ipv4-controller	-if-acl	1			session	contractor			
ipv6-controller	-if-acl	1			session	contractor			
allowall		2			session	default-iap-us	er-role, default-via-role, def		
llewolle av		1			rorrion	dofault via rol	la dafaultivon rola authon		•
+									
									_
1									an P



2 高级故障诊断

2.1 用户需求

希望能够对无线网络的异常情况进行故障的分析和诊断,能够尽快找到问题的原因,并及时解决问题。

2.2 实现思路

我们会通过各个层面的相关内容的采集和分析,结合过去的相关经验的总结,来初步给出大概问题的原因,并及时帮助客户解决常规遇到的各种疑难问题,提升 Aruba 无线网络的上网体验度。另外这一章节,我们仅仅提供 CLI 的查看和分析命令,不提供图形化 GUI。

2.3 诊断故障的流程

通常我们需要5个阶段来分析无线终端问题



而通常无线问题集中最多的是在关联和认证阶段, 802.11 WiFi 终端 使用无线网络的标准上 网过程如下:

1) 首先是Probe request (主动发起, 分为广播Probe和特定SSID Probe) 和Beacon (被动接受AP 的) 的交互



- 2) 发送关联请求 (AP是否关联成功)
- 3) 发送认证请求 (认证服务器是否正常响应)
- 4) DHCP获取IP地址过程 (DHCP服务器是否正常提供IP)
- 5) 通过DNS解析域名过程 (DNS是否正常解析IP)
- 6) 最后上网通信 (角色策略是否正确,经过三层路由和网关出口线路等)



802.11 Negotiation

- > 对于一个新建的网络,大多数故障集中在配置问题,网络物理层问题(线路,水晶头)等
- 对于一个成熟运行的网络,大多数问题集中在终端驱动更新问题,新终端和协议标准使用,网络物 理层问题(线路,水晶头),射频环境变化,有线网络环境变化等
- > 对于一个老旧的网络,大多数问题集中在网络物理层问题(线路,水晶头),硬件故障等。

2.4 终端层面诊断

第1步:登录到 MM 控制器上,观察全网所有在线用户的状态信息,可以查看当前无线终端所停 靠的 UAC (Current Switch), MAC 地址,角色,认证用户名,认证方式,终端类型和所 关联的 AP name 等信息。

查看所有用户的状态信息

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

Global Users
IP MAC Name <mark>Current switch</mark> Role Auth <mark>AP name</mark> Roaming Essid Bssid Phy Pr
ofile Type User Type
80 g-HT aruba-test_aaa_prof Android WIRELESS
172.16.200.1337c:01:91:a8:a2:aa10.2.10.12authenticatedLAB2-AP1Wireless aruba-test94:b4:0f:44:d6:90a-VHTaruba-test_aaa_profiPhoneWIRELESS
192.168.100.2 7c:01:91:a8:a2:aa 10.2.10.12 authenticated LAB2-AP1 Wireless aruba-test 94:b4:0f:44:d6:9 0 a-VHT aruba-test_aaa_prof iPhone WIRELESS

基于这个用户的 mac 地址来过滤查询,在 MM 上可以快速定位一个用户所停靠的 UAC 和当前所关联的 AP name.

(LabX-MM-1) [mynode] #show global-user-table list mac-addr 7c:01:91:a8:a2:aa					
Global Users					
IP MAC Name <mark>Current switch</mark> Role Auth <mark>AP name</mark> Roaming Essid <mark>Bssid</mark> Phy Prof ile Type User Type					
192.168.100.27c:01:91:a8:a2:aaemployee10.2.10.12employee802.1xLAB2-AP1Wirelessaruba-test94:b4:0f:44:d6:90a-VHTaruba-test_aaa_profiPhoneWIRELESS					
Total entries = 1					

基于这个 ESSID 来过滤查询,在 MM 上可以快速定位一组用户所停靠的 UAC

(LabX-MM-1) [mynode] #show global-user-table list essid aruba-test



Global Users
IP MAC Name Current switch Role Auth AP name Roaming Essid Bssid Phy Prof ile Type User Type
 192.168.100.2 7c:01:91:a8:a2:aa employee 10.2.10.12 employee 802.1x LAB2-AP1 Wireless aruba-test 94:b4:0f:4 4:d6:90 a-VHT aruba-test_aaa_prof iPhone WIRELESS
192.168.100.150:a7:2b:5b:25:17employee10.2.10.11employee802.1xLAB2-AP1Wirelessaruba-test94:b4:0f:44:d6:80g-HTaruba-test_aaa_profAndroidWIRELESSTotal entries = 2
第2步: 登录到终端所停靠的 MD 控制器上(UAC),所关联的 AP name 下面的所有终端信息(其中就有自己的终端信息),包括当前关联状态、关联时长、关联速率(上下行)、客户端 SNR 信噪比(上下行),重传次数,空间流和 Client health 值等。
假设终端收到的信号强度是-65dBm,而此时的无线网络环境底噪是-95dBm,那么该终端的 SNR 值为 95-65=30dB
可以通过 show user mac <mark>7c:01:91:a8:a2:aa</mark> 来查看,通常无线网络环境底噪在-85dBm 到 -95dBm 都是正常范围,越低越好
可以通过 show user mac <mark>7c:01:91:a8:a2:aa</mark> 来查看,通常无线网络环境底噪在-85dBm 到 -95dBm 都是正常范围,越低越好 理想的无线终端的 SNR 值要大于等于 25dB,SNR=50 为最佳,小于 20dB 通常是不可用状态。
可以通过 show user mac <mark>7c:01:91:a8:a2:aa</mark> 来查看,通常无线网络环境底噪在-85dBm 到 -95dBm 都是正常范围,越低越好 理想的无线终端的 SNR 值要大于等于 25dB,SNR=50 为最佳,小于 20dB 通常是不可用状态。 <mark>Tx_Rate反映的是终端下行速率,Rx_Rate反映的是终端上行速率,</mark> 这两个速率不能相差太大,通常是动态不断变化的。
可以通过 show user mac <mark>7c:01:91:a8:a2:aa</mark> 来查看,通常无线网络环境底噪在-85dBm 到 -95dBm 都是正常范围,越低越好 理想的无线终端的 SNR 值要大于等于 25dB,SNR=50 为最佳,小于 20dB 通常是不可用状态。 Tx_Rate反映的是终端下行速率,Rx_Rate反映的是终端上行速率,这两个速率不能相差太大,通常是动态不断变化的。 (labX-md1) [MDC] #show ap debug client-table ap-name LAB2-AP1
可以通过 show user mac <mark>7c:01:91:a8:a2:aa</mark> 来查看,通常无线网络环境底噪在-85dBm 到 -95dBm 都是正常范围,越低越好 理想的无线终端的 SNR 值要大于等于 25dB, SNR=50 为最佳,小于 20dB 通常是不可用状态。 Tx_Rate反映的是终端下行速率,Rx_Rate反映的是终端上行速率,这两个速率不能相差太大,通常是动态不断变化的。 (labX-md1) [MDC] #show ap debug client-table ap-name LAB2-AP1 Client Table
可以通过 show user mac <mark>7c:01:91:a8:a2:aa</mark> 来查看,通常无线网络环境底噪在-85dBm 到 -95dBm 都是正常范围,越低越好 理想的无线终端的 SNR 值要大于等于 25dB, SNR=50 为最佳,小于 20dB 通常是不可用状态。 Tx_Rate反映的是终端下行速率,Rx_Rate反映的是终端上行速率,这两个速率不能相差太大,通常是动态不断变化的。 (labX-md1) [MDC] #show ap debug client-table ap-name LAB2-AP1 Client Table
可以通过 show user mac 7c:01:91:a8:a2:aa 来查看,通常无线网络环境底噪在-85dBm 到 -95dBm 都是正常范围,越低越好 理想的无线终端的 SNR 值要大于等于 25dB,SNR=50 为最佳,小于 20dB 通常是不可用状态。 Tx_Rate反映的是终端下行速率,Rx_Rate反映的是终端上行速率,这两个速率不能相差太大,通常是动态不断变化的。 (labX-md1) [MDC] #show ap debug client-table ap-name LAB2-AP1 Client Table
可以通过 show user mac 7c:01:91:a8:a2:aa 来查看,通常无线网络环境底噪在-85dBm 到 -95dBm 都是正常范围,越低越好 理想的无线终端的 SNR 值要大于等于 25dB,SNR=50 为最佳,小于 20dB 通常是不可用状态。 Tx_Rate反映的是终端下行速率,Rx_Rate反映的是终端上行速率,这两个速率不能相差太大,通常是动态不断变化的。 (labX-md1) [MDC] #show ap debug client-table ap-name LAB2-AP1 Client Table
可以通过 show user mac 7c:01:91:a8:a2:aa 来查看,通常无线网络环境底噪在-85dBm 到 -95dBm 都是正常范围,越低越好 理想的无线终端的 SNR 值要大于等于 25dB,SNR=50 为最佳,小于 20dB 通常是不可用状态。 Tx_Rate反映的是终端下行速率,Rx_Rate反映的是终端上行速率,这两个速率不能相差太大,通常是动态不断变化的。 (labX-md1) [MDC] #show ap debug client-table ap-name LAB2-AP1 Client Table



7c:01:91:a8:a2:aa aruba-test 94:b4:0f:44:d6:90 Associated AWvSsEe 0x1 Power-save (0,0,0,0,N/A,0) (0,0) 455 78 9 0 866 866 42 43 6 Sat Mar 28 14:36:18 2020 Sat Mar 28 14:36:18 2020 (0,0) 71/71 2[0x3] 0 50:a7:2b:5b:25:17 aruba-test 94:b4:0f:44:d6:80 Associated sb 0x1 Power-save (0,0,0,0,N/A,0) (0,0) 1328 2028 0 117 72 1 39 40 2[0x3] Sat Mar 28 14:35:17 2020 Sat Mar 28 14:36:02 2020 (0,0) 16 96/78 Num of associated clients: 2 UAPSD:(VO,VI,BK,BE,Max SP,Q Len) TWT:(iTWT sessions num, bTWT groups num) HT Flags: A - LDPC Coding; B - TX STBC; D - Delayed BA; G - Greenfield I - HT40 Intolerant: M - Max A-MSDU: N - A-MPDU disabled Q - Static SM PS; R - Dynamic SM PS; S - Short GI 40; W - 40 MHz b - RX STBC; s - Short GI 20; t - turbo-rates (256-QAM) VHT Flags: C - 160MHz/80+80MHz; E - Beamformee; V - Short GI 160 c - 80MHz; e - Beamformer; v - Short GI 80 HT State shows client's original capabilities (not operational capabilities) MFP Status: C - 1 if the station is MFP capable; R - 1 if the station has negotiated MFP

查看当前 AP 下,所有终端的关联时长,判断终端是否存在频繁关联和掉线问题,通常这些问题终端的关联时长不会超过 2 分钟。

可以查看单个终端的关联时长,也可以查看当前 AP 下的所有终端关联时长,便于分析和判断问题。

(lab2-md1) [MDC] #show ap association ap-name lab2-ap1

The phy column shows client's operational capabilities for current association

Flags: A: Active, B: Band Steerable, H: Hotspot(802.11u) client, K: 802.11K client, M: Mu beam formee, R: 802.11R client, W: WMM client, w: 802.11w client, V: 802.11v BSS trans capab le, P: Punctured preamble, U: HE UL Mu-mimo, O: OWE cli



ent, S: SAE client, E: Enterprise client, m: Agile Multiband client, C: Cellular Data Capable - network available, c: Cellular Data Capable - network unavailable, p: Pending GSM activation, T: Individual TWT client, t: Broadcast TWT client PHY Details: HT : High throughput; 20: 20MHz; 40: 40MHz; t: turbo-rates (256-QAM) VHT : Very High throughput; 80: 80MHz; 160: 160MHz; 80p80: 80MHz + 80MHz HE : High Efficiency; 80: 80MHz; 160: 160MHz; 80p80: 80MHz + 80MHz <n>ss: <n> spatial streams Association Table _____ bssid auth assoc aid l-int essid vlan-id tunnel-id phy assoc. time num as Name mac soc Flags Band steer moves (T/S) phy_c ap ---- ---- --- -----_____ lab2-ap1 84:d4:7e:fe:45:56 7c:7a:91:46:24:18 y y 1 250 lab2-AG-1x 220 0x10009 a-VHT-80sqi-2ss 7h:25 <mark>m:49s</mark> 1 WAB 0/0 a-VHT -80sgi-2ss Num Clients:1 Total num of dual-band capable clients:1 Total num of dual-band capable clients in 2.4G band:0 Total num of dual-band capable clients in 5G band:1 Total num of single-band only clients:0

查看终端和 AP 之间的关联过程 (参考日志中的 50:a7:2b:5b:25:17 是无线终端的 mac 地址, 94:b4:0f:44:d6:80 是 BSSID,关联请求和关联响应成对出现,表示正常)

(labX-md1) [MDC] #show ap remote debug mgmt-frames ap-name LAB2-AP1

Traced 802.11 Management Frames



Timestamp	stype	SA	DA	BSS	signal Misc	
<mark>Mar 29 20:19:34</mark>	.215 assoc	-resp 9	94:b4:0f:44:d6:80	50:a7:2b:5b:25:1	17 94:b4:0f:44:d6:80 1	1 <mark>5 Success</mark>
<mark>Mar 29 20:19:34</mark>	.215 assoc	<mark>-req 5</mark>	0:a7:2b:5b:25:17	94:b4:0f:44:d6:8	0 94:b4:0f:44:d6:80 0	-
Mar 29 20:19:34	.212 auth	94:	b4:0f:44:d6:80 5	0:a7:2b:5b:25:17	94:b4:0f:44:d6:80 15	Success (seq num 0)
Mar 29 20:19:34	.212 auth	50:	a7:2b:5b:25:17 9	4:b4:0f:44:d6:80	94:b4:0f:44:d6:80 0	-
Mar 29 17:53:32 nticated (seq nu	617 deau ım 357)	th 50):a7:2b:5b:25:17	94:b4:0f:44:d6:80	0 94:b4:0f:44:d6:80 0	STA has left and is deauthe
<mark>Mar 29 17:20:11</mark>	.817 assoc	-resp 9	94:b4:0f:44:d6:80	50:a7:2b:5b:25:1	17 94:b4:0f:44:d6:80 1	15 Success
<mark>Mar 29 17:20:11</mark>	.817 assoc	<mark>-req 5</mark>	<mark>0:a7:2b:5b:25:17</mark>	94:b4:0f:44:d6:8	0 94:b4:0f:44:d6:80 0) <mark>-</mark>
Mar 29 17:20:11	.813 auth	94:	b4:0f:44:d6:80 5	0:a7:2b:5b:25:17	94:b4:0f:44:d6:80 15	Success (seq num 0)
Mar 29 17:20:11	.813 auth	50:	a7:2b:5b:25:17 9	4:b4:0f:44:d6:80	94:b4:0f:44:d6:80 0	-
Mar 29 15:46:26 nticated (seq nu	.465 deau ım 239)	th 50):a7:2b:5b:25:17	94:b4:0f:44:d6:80	0 94:b4:0f:44:d6:80 0	STA has left and is deauthe
<mark>Mar 29 15:13:05</mark>	.804 assoc	-resp S	9 <mark>4:b4:0f:44:d6:80</mark>	50:a7:2b:5b:25:1	17 94:b4:0f:44:d6:80 1	15 Success
<mark>Mar 29 15:13:05</mark>	.804 assoc	req 5	<mark>0:a7:2b:5b:25:17</mark>	94:b4:0f:44:d6:8	0 94:b4:0f:44:d6:80 0) <mark>-</mark>
Mar 29 15:13:05	.802 auth	94:	b4:0f:44:d6:80 5	0:a7:2b:5b:25:17	94:b4:0f:44:d6:80 15	Success (seq num 0)
Mar 29 15:13:05	.802 auth	50:	a7:2b:5b:25:17 9	4:b4:0f:44:d6:80	94:b4:0f:44:d6:80 0	-
Mar 29 15:05:26 nticated (seq nu	5.386 deau im 122)	th 50):a7:2b:5b:25:17	94:b4:0f:44:d6:80) 94:b4:0f:44:d6:80 0	STA has left and is deauthe
Mar 29 14:30:24	.040 assoc	-resp 9	94:b4:0f:44:d6:80	50:a7:2b:5b:25:1	17 94:b4:0f:44:d6:80 1	1 <mark>5 Success</mark>
Mar 29 14:30:24	.040 assoc	req 5	0:a7:2b:5b:25:17	94:b4:0f:44:d6:8	0 94:b4:0f:44:d6:80 0	•
Mar 29 14:30:24	.035 auth	94:	b4:0f:44:d6:80 5	0:a7:2b:5b:25:17	94:b4:0f:44:d6:80 15	Success (seq num 0)
Mar 29 14:30:24	.035 auth	50:	a7:2b:5b:25:17 9	4:b4:0f:44:d6:80	94:b4:0f:44:d6:80 0	-
Mar 29 14:30:19 nticated (seq nu	0.765 deau 1m 93)	th 50):a7:2b:5b:25:17	94:b4:0f:44:d6:80	0 94:b4:0f:44:d6:80 0	STA has left and is deauthe
<mark>Mar 29 14:28:41</mark>	.491 assoc	<mark>-resp S</mark>	9 <mark>4:b4:0f:44:d6:80</mark>	50:a7:2b:5b:25:1	17 94:b4:0f:44:d6:80 1	15 Success
<mark>Mar 29 14:28:41</mark>	.491 assoc	<mark>-req 5</mark>	<mark>0:a7:2b:5b:25:17</mark>	94:b4:0f:44:d6:8	0 94:b4:0f:44:d6:80 0	<mark>) -</mark>



 Mar 29 14:28:41.488 auth
 94:b4:0f:44:d6:80 50:a7:2b:5b:25:17 94:b4:0f:44:d6:80 15
 Success (seq num 0)

 Mar 29 14:28:41.488 auth
 50:a7:2b:5b:25:17 94:b4:0f:44:d6:80 94:b4:0f:44:d6:80 0

第3步:登录到终端所停靠的 MD 控制器上(UAC),根据之前看到的终端 MAC 地址,可以查看该 终端的更多详细关联信息(例如终端的角色和 VLAN 是怎么获得的,采用的是什么认证方式 和认证服务器),终端无线网卡能力,漫游轨迹,环境底噪和 SNR 值等。

(labX-md2) [MDC] #show user mac 7c:01:91:a8:a2:aa

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

Name: employee, IP: 192.168.100.2, MAC: 7c:01:91:a8:a2:aa, Age: 00:00:01

Role: employee (how: ROLE_DERIVATION_DOT1X_VSA), ACL: 94/0

Authentication: Yes, status: successful, method: 802.1x, protocol: EAP-PEAP, server: clearpass

Authentication Servers: dot1x authserver: clearpass, mac authserver:

Bandwidth = No Limit

Bandwidth = No Limit

Role Derivation: ROLE_DERIVATION_DOT1X_VSA

VLAN Derivation: Default VLAN

Idle timeout (global): 300 seconds, Age: 00:00:00

Mobility state: Wireless, HA: Yes, Proxy ARP: No, Roaming: No Tunnel ID: 0 L3 Mob: 0

Flags: internal=0, trusted_ap=0, I3auth=0, mba=0, vpnflags=0, u_stm_ageout=1

Flags: innerip=0, outerip=0, vpn_outer_ind:0, download=1, wispr=0

IP User termcause: 0

phy_type: a-VHT-80, l3 reauth: 0, BW Contract: up:0 down:0, user-how: 1

Vlan default: 100, Assigned: 100, Current: 100 vlan-how: 1 DP assigned vlan:0

Mobility Messages: L2=0, Move=0, Inter=0, Intra=0, Flags=0x0

SlotPort=0x2100, Port=0x1000f (tunnel 15)

Essid: aruba-test, Bssid: 94:b4:0f:44:d6:90 AP name/group: LAB2-AP1/lab2-group Phy-type: a-VHT-80 Forward Mode: tu nnel

AP IP: 10.2.12.101



RadAcct sessionID:n/a RadAcct Traffic In 495/63844 Out 285/115364 (0:61185/63844:0:0:0,0:7425/49828:1:0:0) Timers: L3 reauth 0, mac reauth 0 (Reason:), dot1x reauth 0 (Reason:) Profiles AAA:aruba-test_aaa_prof, dot1x:aruba-test_dot1_aut, mac: CP:n/a def-role:'logon' via-auth-profile:'' ncfg flags udr 0, mac 0, dot1x 1, RADIUS interim accounting 0 IP Born: 1585378863 (Sat Mar 28 15:01:03 2020) Core User Born: 1585378859 (Sat Mar 28 15:00:59 2020) Upstream AP ID: 0, Downstream AP ID: 0 User Agent String: Mozilla/5.0 (iPhone; CPU iPhone OS 13 3 1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Geck o) Mobile/15E148 HTTP based device-id info - Index: 46, Device: iPhone Overall device-id info - Index: 6, Device: iPhone By: Auth-UA-Str Max IPv4 users: 2 L3-Auth Session Timeout from RADIUS: 0 Mac-Auth Session Timeout Value from RADIUS: 0 Dot1x Session Timeout Value from RADIUS: 0 Dot1x Session Term-Action Value from RADIUS: Default CaptivePortal Login-Page URL from RADIUS: N/A Reauth-interval from role: 0 Number of reauthentication attempts: mac reauth 0, dot1x reauth 0 mac auth server: N/A, dot1x auth server: clearpass Address is from DHCP: yes ipuser notify action:NoAction/NoAction RTTS disabled: rtts_throughput 554240 rtts_discard 0 rtts_reest 0 rtts_keepalive 0 Repkey-ready: 1, Repkey: 8, uuid: 000c29ea9ad9000000070001, bucket: 160 nasip 0.0.0.0 User added to cluster bucket-map: Yes The phy column shows client's operational capabilities for current association



Flags: A: Active, B: Band Steerable, H: Hotspot(802.11u) client, K: 802.11K client, M: Mu beam formee, R: 802.11R client, W: WMM client, w: 802.11w client, V: 802.11v BSS trans capable, P: Punctured preamble, U: HE UL Mu-mimo, O: OWE cli ent, S: SAE client, E: Enterprise client, m: Agile Multiband client, C: Cellular Data Capable - network available, c: Cellular D ata Capable - network unavailable, p: Pending GSM activation, T: Individual TWT client, t: Broadcast TWT client

PHY Details: HT : High throughput; 20: 20MHz; 40: 40MHz; t: turbo-rates (256-QAM) VHT : Very High throughput; 80: 80MHz; 160: 160MHz; 80p80: 80MHz + 80MHz HE : High Efficiency; 80: 80MHz; 160: 160MHz; 80p80: 80MHz + 80MHz <n>ss: <n> spatial streams Association Table _____ Name bssid auth assoc aid l-int essid vlan-id tunnel-id phy assoc. time num ass mac oc Flags Band steer moves (T/S) phy cap _____ LAB2-AP1 94:b4:0f:44:d6:90 7c:01:91:a8:a2:aa y y 1 20 aruba-test 100 0x1000f a-VHT-80sgi-2ss 1m:19s 1 WVAB 0/0 a-VHT-80sgi-2ss-V 7c:01:91:a8:a2:aa-94:b4:0f:44:d6:90 Stats -----Value Parameter ____ _____ Channel 60 Channel Frame Retry Rate(%) 5 (信道帧重传率,越高表明信道越繁忙) Channel Frame Low Speed Rate(%) 0 Channel Frame Non Unicast Rate(%) 0 Channel Frame Fragmentation Rate(%) 0 Channel Frame Error Rate(%) 0 Channel Bandwidth Rate(kbps) 258 Channel Noise 89 (当前信道的底噪, 2.4G>85, 5G >90)



Client Frame Retry Rate(%) 5 (客户端数据帧的重传率,越小越好)						
Client Frame Low Speed R	ate(%) 0						
Client Frame Non Unicast	Rate(%) 0						
Client Frame Fragmentation Rate(%) 0							
Client Frame Receive Error	Rate(%) 6						
Client Bandwidth Rate(kbp	os) 258						
Client Tx Packets	1308						
Client Rx Packets	255						
Client Tx Bytes	104834						
Client Rx Bytes	113793						
Client SNR	<mark>45</mark> (终端的 SNR 值=当前信道底噪- <mark>终端收到的 RSSI</mark>)						
A2c_SM SeqNum, Old Sec	Nums 5 0						
Client non-preferred chan	nels Disabled						

查看一个终端在不同 AP 间漫游的详细轨迹记录(以下数据并非来自 lab 环境,仅供参考):

nternal ageout 表示用户漫游切换到其他的新 AP 上,于是旧的 AP 就内部发送一个 internal ageout 信息,将该用户相关表项从 ∃ AP 上删除掉。 Deauth 原因就是需要进行 AP 的切换,同样也表现在同一颗 AP 的 2.4G 和 5G 频段之间的切换。					
(xx-7240XM-MD1) [MDC] *#show ap client trail-info d8:63:75:bb:d4:75					
Client Trail Info					
MAC BSSID ESSID <mark>AP-name</mark> VLAN Deauth Reason Alert					
d8:63:75:bb:d4:75 00:24:6c:ac:6b:31 shisu_free SJ-1JXL-WS1F-120 920 Unspecified Failure STA has roamed to anoth er AP					
Deauth Reason					


Reason	Timestamp
Unspecified Failure	Mar 30 17:22:14
AP aged out STA; did not get ASSOC	Mar 30 17:16:17
Sapcp Ageout (internal ageout)	Mar 30 17:11:32
AP aged out STA; did not get ASSOC	Mar 30 17:08:17
Disassociated; Auth frame from STA that	was already associated Mar 30 17:04
Disassociated; Auth frame from STA that	was already associated Mar 30 17:01
Disconnect User	Mar 30 17:00:10
Sapcp Ageout (internal ageout)	Mar 30 16:29:20
Disconnect User	Mar 30 16:24:34
Disconnect User	Mar 30 07:51:11
Num Deauths:10	
Alerts	
Reason Timestamp	
STA has roamed to another AP Mar 30 17	<mark>7:23:40</mark>
STA has roamed to another AP Mar 30 17	<mark>7:19:38</mark>
STA has roamed to another AP Mar 30 17	<mark>7:10:18</mark>
STA has roamed to another AP Mar 30 17	<mark>7:10:14</mark>
STA has roamed to another AP Mar 30 17	<mark>7:06:53</mark>
STA has roamed to another AP Mar 30 17	<mark>7:06:46</mark>
STA has roamed to another AP Mar 30 17	<mark>7:06:34</mark>
STA has roamed to another AP Mar 30 17	<mark>7:05:28</mark>



STA has roamed to another AP Mar 30 17:05:09
STA has roamed to another AP Mar 30 17:02:22
Num Alerts:10
Mobility Trail
BSSID ESSID AP-name VLAN Timestamp
00:24:6c:ac:6b:31 shisu_free SJ-1JXL-WS1F-120 920 Mar 30 17:23:40
80:8d:b7:ac:4d:c1 shisu_free SJ-JXL-2-W2F-OUTDOOR1 920 Mar 30 17:23:40
00:24:6c:ac:6b:31 shisu_free SJ-1JXL-WS1F-120 920 Mar 30 17:23:40
80:8d:b7:ac:4d:c1 shisu_free SJ-JXL-2-W2F-OUTDOOR1 920 Mar 30 17:22:26
80:8d:b7:ac:4d:c1 shisu_free SJ-JXL-2-W2F-OUTDOOR1 920 Mar 30 17:22:26
00:24:6c:ac:6b:31 shisu_free SJ-1JXL-WS1F-120 920 Mar 30 17:22:14
00:24:6c:ac:6b:31 shisu_free SJ-1JXL-WS1F-120 920 Mar 30 17:21:21
00:24:6c:ac:6b:31 shisu_free SJ-1JXL-WS1F-120 920 Mar 30 17:21:21
00:24:6c:ac:6b:31 shisu_free SJ-1JXL-WS1F-120 920 Mar 30 17:19:38
44:48:c1:79:dd:61 shisu_free SJ-TWXXL-NW7F-J718 920 Mar 30 17:19:38
Num Mobility Trails:10

查看一个终端获得角色的详细轨迹记录:

(labX-md1) [MDC] #show aaa debug role user mac 50:a7:2b:5b:25:17

Role Derivation History

0: I2 role->logon, mac user created

1: I2 role->employee, station Authenticated with auth type: 802.1x



2: I2 role->employee, station Authenticated with auth type: 802.1x

查看一个终端获得的 employee 角色里面所定义的相关策略内容:

(lab2-md1) [MDC] #show rights employee
Valid = 'Yes'
CleanedUp = 'No'
Derived Role = 'employee'
Up BW:No Limit Down BW:No Limit
L2TP Pool = default-l2tp-pool
PPTP Pool = default-pptp-pool
Number of users referencing it = 0
Periodic reauthentication: Disabled
DPI Classification: Enabled
Youtube education: Disabled
Web Content Classification: Enabled
IP-Classification Enforcement: Enabled
ACL Number = 130/0
Openflow: Enabled
Max Sessions = 65535
Check CP Profile for Accounting = TRUE
Application Exception List
Name Type
Application BW-Contract List

Page 111 of 171



Name Type BW Contract Id Direction	
Position Name Type Location	
1 global-sacl session	
2 apprf-employee-sacl session	
3 allowall session	
dobal-sac	
Priority Source Destination Service Application Action TimeRange Log Expired Queue TOS 8021P Blacklist Mir	ro
1 any any applync permit Low 1 1 4	
2 any any applying permit $10w 11 = 6$	
apprt-employee-saci	
Priority Source Destination Service Application Action TimeRange Log Expired Queue TOS 8021P Blacklist Min	ro
r DisScan IPv4/6 Contract	
allowall	
Priority Source Destination Service Application Action TimeRange Log Expired Queue TOS 8021P Blacklist Mir r DisScan IPv4/6 Contract	ro



1	any	any	any	permit	Low	4	
2	any	any	any-v6	permit	Low	6	
Ехрії	red Poli	cies (du	e to time cons	traints) = 0			

查看一个终端当前所发生的 session 会话表信息:

(lab2-md1) [MDC] #show datapath session table 10.2.20.101
Datapath Session Table Entries
Flags: F - fast age, S - src NAT, N - dest NAT
D - deny, R - redirect, Y - no syn
H - high prio, P - set prio, T - set ToS
C - client, M - mirror, V - VOIP
Q - Real-Time Quality analysis
u - Upstream Real-Time Quality analysis
I - Deep inspect, U - Locally destined
E - Media Deep Inspect, G - media signal
r - Route Nexthop, h - High Value
A - Application Firewall Inspect
J - SDWAN Default Probe stats used as fallback
B - Permanent, O - Openflow
L - Log, o - Openflow config revision mismatched
Source IP or MAC Destination IP Prot SPort DPort Cntr Prio ToS Age Destination TAge Packets Bytes Flags CPU ID



10.2.20.255 7	10.2.20.101	17	137	137	0/0	0	0	109	9 tunnel 9	58	d9 0	0	FY	
124.239.239.2 7	228 10.2.20.101	6	5 80	5606	5 0/0) () () <i>·</i>	1 tunnel 9) 17	25	1460) F	
10.2.20.101 7	239.255.255.2	250 1	17 58	146 19	0 00	/0	0	0	0 tunne	19	f 4	644	FDCO	
172.16.2.254	10.2.20.101	6	443	56068	0/0	0	0	0	tunnel 9	3	0	0	YA	
10.2.20.101 7	172.16.2.254	6	5606	4 4 4 3	0/0	0	0	1	tunnel 9	19	2	104	YCA	
172.16.2.254 7	10.2.20.101	6	443	56066	0/0	0	0	1	tunnel 9	12	0	0	YA	
172.16.2.254	10.2.20.101	6	443	56067	0/0	0	0	0	tunnel 9	b	0	0	YA	
10.2.20.101 7	10.2.20.255	17	137	137	0/0	0	0	0	tunnel 9	58d	a 56742	2 442	26308 FC	
172.16.2.254 7	10.2.20.101	6	443	56064	0/0	0	0	1	tunnel 9	19	0	0	YA	
10.2.20.101 7	172.16.2.254	6	5606	8 443	0/0	0	0	0	tunnel 9	4	2	104	YCA	
10.2.20.101 7	172.16.2.254	6	5606	6 443	0/0	0	0	1	tunnel 9	12	2	104	YCA	
10.2.20.101 7	172.16.2.254	6	5606	7 443	0/0	0	0	1	tunnel 9	b	2	104	YCA	
10.2.20.101 7	239.255.255.2	250 1	17 58	485 37	02 0	/0	0	0	1 tunne	19	58da 1	2551	13931610 F	С

查看控制器 MD 上, 2.4G 和 5G 终端的分布比例,以及双频能力的终端仍然停靠在 2.4G 频段的数量,当然是占所有双频能力终端的比例越小越好(该数据是第三方的,并非 lab 环境中, 仅供大家学习和参考) (WLAN_HD_AC_Aruba_1) #show ap association | begin Num
Num Clients:1286
Total num of dual-band capable clients:970
Total num of dual-band capable clients in 2.4G band:356
Total num of dual-band capable clients in 5G band:614
Total num of single-band only clients:316
(WLAN_HD_AC_Aruba_1) #show ap association ap-group local10-d1jx | begin Num
Num Clients:257
Total num of dual-band capable clients in 2.4G band:14
Total num of dual-band capable clients in 2.4G band:14
Total num of dual-band capable clients in 5G band:186
Total num of single-band only clients:57

2.5 AP 层面诊断

第1步:登录到 MM 控制器上,观察全网中所有的 AP 在线状态是否正常(即处于 Up 的状态), 目前 Flag 标志位有什么,可以查看每颗 AP 的当前停靠控制器 IP (switch ip AAC) 和备援 停靠控制器 IP (standby IP S-AAC)

(LabX-MM-1) [mynode] #show ap database long
AP Database
Name Group AP Type IP Address Status Flags <mark>Switch IP Standby IP</mark> Wired MAC Address Serial # Port FQLN Outer IP User
LAB2-AP1 lab4-group 205
Flags: 1 = 802.1x authenticated AP use EAP-PEAP; 1+ = 802.1x use EST; 1- = 802.1x use factory cert; 2 = Using IKE versi on 2



```
B = Built-in AP; C = Cellular RAP; D = Dirty or no config
E = Regulatory Domain Mismatch; F = AP failed 802.1x authentication
G = No such group; I = Inactive; J = USB cert at AP; L = Unlicensed
M = Mesh node
N = Duplicate name; P = PPPoe AP; R = Remote AP; R- = Remote AP requires Auth;
S = Standby-mode AP; U = Unprovisioned; X = Maintenance Mode
Y = Mesh Recovery
c = CERT-based RAP; e = Custom EST cert; f = No Spectrum FFT support
i = Indoor; o = Outdoor; s = LACP striping; u = Custom-Cert RAP; z = Datazone AP
p = In deep-sleep status
4 = WiFi Uplink
r = Power Restricted; T = Thermal ShutDown
```

```
Total APs:1
```

如果存在 Flags 标记,可以在相关的解释中获得当前 AP 工作状态的问题,比如这里显示的 UG,U 表示还没有配置,G 表示没有相关的 AP Group 存在,因为 Aruba 的 AP 是记忆存储上一 次获得的 AP Group 名称在本地的 flash 上,AP 会一直和上一次 AP Group 名称进行通讯,如果 当前控制器将之前的 AP Group 名称删除后,就出现了 G 标签。

另外一个原因是,license 超过或者过期了(控制器或者 MM 的),AP 在控制器上显示是 up,但是 flag 中有 IL,表示非激活且无授权,该现象发生在 AP 现场无信号,wlan 灯不亮,客户 反映现场无信号。

AC 上看到 AP 标识为 I=inactive. 可能的原因有:

(1)virtual AP 没有配置或不正确的 VLAN ID.例如 AP has a tunneled SSID of VLAN2 but your controller doesn't have VLA N2.

(2) master AC 上给 virtual AP 配置了 VLAN Pool name 但 local 上没有 vlan pool 的映射;

(3) Unknown AP Group.

(4) Duplicate AP Name.

(5) AP not provisioned with external antenna gain. Only applies to APs that have external antenna.



(6) Both Radios disabled.

- (7) No Virtual AP's defined.
- (8) Profile errors. Use 'show profile errors' .
- (9) GRE blocked at firewall after AP is already up.
- (10) 配置冲突. Single radio but dual-band AP. AP System Profile RF Band says 11g but VAP says 11a.
- (11) RAP fails to move between VPN Client, RAP_ROLE, and standard AP Role.
- (12) VAP in wrong forwarding mode. Campus AP without CPSEC enabled only supports tunnel mode forwarding.

第2步:登录到每个 MD 控制器上,观察当前所有的 AP 工作状态是否正常,释放正确的 ESSID 信号,其中"Clients"为显示当前关联在每个 AP 的不同 Radio 上的终端数量, "Band Ch/EIRP/MaxEIRP"栏目下显示每个 Radio 的当前工作协议、工作信道和频宽、当前发射 功率、被允许的最大发射功率等参数。

(labX-md2) [MDC] #show ap bss-table

fm (forward mode): T-Tunnel, S-Split, D-Decrypt Tunnel, B-Bridge (s-standard, p-persistent, b-backup, a-always), n-anys pot

cluster (cluster role): U-UAC, A-AAC, sU-Standby UAC, sA-Standby AAC

Aruba AP BSS Table

bss ess port ip phy type ch/EIRP/max-EIRP cur-cl ap name in-t(s) tot-t mtu acl-state acl fm flags cluster datazone

____ __

9<mark>4:b4:0f:44:d6:80 aruba-test N/A 10.2.12.101 g-HT</mark> ap 11/9.0/20.0 0 LAB2-AP1 0 1h:9m:40s 1500 -2 T A no

<mark>94:b4:0f:44:d6:90 aruba-test N/A 10.2.12.101 a-VHT</mark> ap 60E/18.0/23.0 0 LAB2-AP1 0 1h:9m:40s 1500 - 2 T A no

Channel followed by "*" indicates channel selected due to unsupported configured channel.

"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:2

Num Associations:0



Flags: K = 802.11K Enabled; W = 802.11W Enabled; 3 = WPA3 BSS; O = Enhanced-open BSS with transition mode; o = Enhanced-open transition mode open BSS; M = WPA3-SAE mixed mode BSS; E = Enhanced-open BSS without transiti on mode; m = Agile Multiband (MBO) BSS; c = MBO Cellular Data Capable BSS; I = Imminent VAP Down; T = Individual TWT Enabled; t = Broadcast TWT Enabled

(labX-md2) [MDC] #show ap active

Active AP Table

Name Group IP Address AP Type Flags Uptime Outer IP Cluster Role Radio 0 Band Ch/EIRP/MaxEIRP/Clients Radio 1 Band Ch/EIRP/MaxEIRP/Clients Radio 2 Band Ch/EIRP/MaxEIRP/Clients

LAB2-AP1 lab2-group 10.2.12.101 205 a 4m:52s N/A A AP:5GHz-VHT:60E/18.0/23.0/0 AP:2.4G Hz-HT:11/9.0/20.0/0

Flags: 1 = 802.1x authenticated AP; 2 = Using IKE version 2;

A = Enet1 in active/standby mode; B = Battery Boost On; C = Cellular;

D = Disconn. Extra Calls On; E = Wired AP enabled; F = AP failed 802.1x authentication;

H = Hotspot Enabled; K = 802.11K Enabled; L = Client Balancing Enabled; M = Mesh;

N = 802.11b protection disabled; P = PPPOE; R = Remote AP;

S = AP connected as standby; X = Maintenance Mode;

a = Reduce ARP packets in the air; d = Drop Mcast/Bcast On; u = Custom-Cert RAP;

i = Provisioned as Indoor; o = Provisioned as Outdoor;

p = Restriction mode in POE-AF/AT;r = 802.11r Enabled; f = No Spectrum FFT support;

Q = DFS CAC timer running; T = Flex Radio Mode is 2.4GHz+5GHz; t = Tri-Radio Mode Enabled;

U = Flex Radio Mode is 5GHz; V = Flex Radio Mode is 2.4GHz; e = custom EST cert; W = Dual 5GHz Mode Enabled; 4 = Using WiFi Uplink

Channel followed by "*" indicates channel selected due to unsupported configured channel.

"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Channel flags: +/- = 40 MHz, E = 80 MHz, S = 160 MHz, E+E = 80 + 80 MHz (i.e. 36E+149E)

Cluster Role: U = UAC, A = AAC, SU = Standby UAC , SA = Standby AAC

Page 118 of 171



Num APs:1

另外,还有该 AP 当前工作在线时长,当前 md 控制器的 cluster role 等信息

VHT---表示工作在 11ac 协议, HT---表示工作在 11n 协议

第3步:登录到每个 MD 控制器上,观察当前所有的 AP 连接状态是否正常。

查看 Bootstraps 的数量是否远大于 Reboots 的数量,其中 Bootstraps (Total) 表示 AP 的进程重启次数,也即是软重启,表示因为 GRE 心跳丢失导致,通常因为网线、水晶头或者网络通讯不稳定等原因。 Reboots 表示 AP 的完全硬重启次数,通常因为 PAPI 心跳丢失,断电故障,手动重启等。

(labX-md2) [MDC] #show ap debug counters
AP Counters
Name Group IP Address Configs Sent Configs Acked AP Boots Sent AP Boots Acked <mark>Bootstraps (Total) Rebo</mark> <mark>ots</mark> Crash Current License counter Global License counter GSM Info for AP
LAB2-AP1 lab2-group 10.2.12.101 3 2 0 0 1 (3) 3 N 1/0/1/0/0/0 6/5/6/5/0/0/0 40/4/0/0
Current License Counter : Increment/Decrement/Active-Increment/Active-Decrement/Standby-Increment/Standby-Decr ement
Global License counter : G-Increment/G-Decrement/G-Active-Increment/G-Active-Decrement/G-Standby-Increment/G- Standby-Decrement
GSM Info for AP : AP-Flags/HA-Flags/AP-Flag-Standby/HA-Flag-Standby
Total APs :1

查看 AP 的软重启和硬重启的历史记录和原因分析:

(labX-md2) [MDC] #show ap debug system-status ap-name LAB2-AP1

Reboot Information (硬重启信息)



AP rebooted Sun Mar 29 14:15:18 CST 2020; SAPD: Reboot requested by controller
Rebootstrap Information (软重启信息)
Date Time Reason (Latest 10)
2020-03-29 14:19:06 Power report failed: UNKNOWN_AP
HA Failover Information
Date Time Reason (Latest 10)
(none found)
Cluster Failover Information
Date Time <mark>Reason (Latest 10)</mark>
2020-03-29 14:21:15 Standby 10.2.10.12 is up, fail-over to it, since Missed heartbeats: Last Sequence Generated=7 Sent =7 Rcvd=0; eth Sent=256 Drop=0; gre Sent=145 Drop=0 First=1; tun Sent=0 Drop=0
2020-03-29 14:21:20 Standby 10.2.10.11 is up, fail-over to it, since Missed heartbeats: Last Sequence Generated=8 Sent =5 Rcvd=0; eth Sent=266 Drop=0; gre Sent=150 Drop=0 First=1; tun Sent=0 Drop=0
2020-03-29 14:21:23 Standby 10.2.10.12 is up, fail-over to it, since Missed heartbeats: Last Sequence Generated=8 Sent =8 Rcvd=0; eth Sent=272 Drop=0; gre Sent=153 Drop=0 First=1; tun Sent=0 Drop=0
2020-03-29 14:21:28 Standby 10.2.10.11 is up, fail-over to it, since Missed heartbeats: Last Sequence Generated=8 Sent =5 Rcvd=0; eth Sent=282 Drop=0; gre Sent=158 Drop=0 First=1; tun Sent=0 Drop=0
2020-03-29 14:21:31 Standby 10.2.10.12 is up, fail-over to it, since Missed heartbeats: Last Sequence Generated=8 Sent =8 Rcvd=0; eth Sent=288 Drop=0; gre Sent=161 Drop=0 First=1; tun Sent=0 Drop=0



2020-03-29 14:21:36 Standby 10.2.10.11 is up, fail-over to it, since Missed heartbeats: Last Sequence Generated=8 Sent =4 Rcvd=0; eth Sent=297 Drop=0; gre Sent=166 Drop=0 First=1; tun Sent=0 Drop=0

2020-03-29 14:21:39 Standby 10.2.10.12 is up, fail-over to it, since Missed heartbeats: Last Sequence Generated=7 Sent =7 Rcvd=0; eth Sent=302 Drop=0; gre Sent=169 Drop=0 First=1; tun Sent=0 Drop=0

2020-03-29 14:21:44 Standby 10.2.10.11 is up, fail-over to it, since Missed heartbeats: Last Sequence Generated=7 Sent =4 Rcvd=0; eth Sent=311 Drop=0; gre Sent=174 Drop=0 First=1; tun Sent=0 Drop=0

2020-03-29 14:21:47 Standby 10.2.10.12 is up, fail-over to it, since Missed heartbeats: Last Sequence Generated=7 Sent =7 Rcvd=0; eth Sent=316 Drop=0; gre Sent=177 Drop=0 First=1; tun Sent=0 Drop=0

2020-03-29 14:21:52 Standby 10.2.10.11 is up, fail-over to it, since Missed heartbeats: Last Sequence Generated=7 Sent =4 Rcvd=0; eth Sent=325 Drop=0; gre Sent=182 Drop=0 First=1; tun Sent=0 Drop=0

Recent Control Messages from AP to Controller

Date Time Message Description

Sun Mar 29 14:21:53 2020(0 secs ago): SENT REQ type=AP_READY len=25 peer=10.2.10.12 seq_num=1 num_attempts= 1 rtt=0 secs 0400000014040000000105C0A865010400803E810400000001

Rebootstrap LMS

(none found)

Crash Information

(none found)



关于不同的硬和软重启原因归纳如下(一下日志仅供参考,并非 lab 环境所具备):

1) AP rebooted Tue Apr 29 10:22:30 PST 2008: SAPD: Unable to contact switch. Called by sapd_hello_cb:4

说明 ap 在和交换机通信时出现问题, 排查 L2 或 L3 路由可达问题。

2) AP rebooted Tue Apr 29 10:25:31 PST 2008: SAPD: Rebooting after provisioning

说明 ap 重启是由于被 provision 或者 reprovisioned。Indicates that the AP rebooted after being provisioned or reprovisio ned.

3) AP rebooted Tue Apr 29 10:41:55 PST 2008: SAPD: Reboot requested by controller

说明 ap 被从控制器的 WebUI 上重启或者通过 CLI 的 apboot 命令硬重启。

4) AP rebooted Fri Dec 31 16:05:23 PST 1999: SAPD: Reboot after image upgrade

说明 ap 是由于更新 image 而重启。

5) 2008-04-29 10:33:42 Missed heartbeats on radio 0 VAP 0 Missed 8 heartbeats; rebootstrapping

这个例子说明 ap 重启是由于丢失心跳信息(去查看下 GRE 心跳是否被网络阻塞),是由于网络通讯原因造成的,

是否 AP 和控制器之间存在防火墙或者上网行为设备或者其他具有 acl 设备等,将 GRE (IP 47)流量给阻塞了?

GRE 心跳是双向的 (AP 发给控制器,控制器也发给 AP, IP 47),超时后,导致 rebootstrap 次数增加,软重启,主要用于 Tun nel mode SSID)

PAPI 心跳是单向的(AP 发给控制器, UDP8211, 超时后,导致 reboot 次数增加,硬重启。主要用于 bridge mode SSID)

PAPI 端口如果一开始就被 ACL 阻断的话, 会导致 AP 无法在控制器上线, 什么 AP 信息都没有。

GRE 端口如何一开始被 ACL 阻断的话, AP 会在 ac 上线, 但是一会 up, 一会 down (有该 AP 的 down 信息)。

AP 仅仅通过 PAPI 心跳来感知并从主 AC 切换到备 AC

6) ap reboot caused by cold HW reset(power loss)

Ap 突然电源丢失, 冷启动了

7) 有的时候不显示任何重启原因, 是由于 ap 没有时间向 flash 中写信息。

Reboot Information

(none found)



Rebootstrap Information

(none found)

这个通常是由于 ap 的内核软件崩溃。

第4步:登录到 AP 所停靠的 MD 控制器上(即 AAC),观察特定 AP 的连接状态是否异常,并 且详细查看该 AP 和控制器之间的会话状态信息内容,通常这个也是用来判断 AP 无法注册 到控制器的基本诊断方法。

(labX-md2) [MDC] #show ap database AP Database _____ Name Group AP Type IP Address Status Flags Switch IP Standby IP ----- ------ ------LAB2-AP1 lab2-group 205 10.2.12.101 Up 3h:35m:18s 10.2.10.12 10.2.10.11 Flags: 1 = 802.1x authenticated AP use EAP-PEAP; 1+ = 802.1x use EST; 1- = 802.1x use factory cert; 2 = Using IKE versi on 2 B = Built-in AP; C = Cellular RAP; D = Dirty or no configE = Regulatory Domain Mismatch; F = AP failed 802.1x authentication G = No such group; I = Inactive; J = USB cert at AP; L = Unlicensed M = Mesh nodeN = Duplicate name; P = PPPoe AP; R = Remote AP; R- = Remote AP requires Auth; S = Standby-mode AP; U = Unprovisioned; X = Maintenance Mode Y = Mesh Recoveryc = CERT-based RAP; e = Custom EST cert; f = No Spectrum FFT support i = Indoor; o = Outdoor; s = LACP striping; u = Custom-Cert RAP; z = Datazone AP p = In deep-sleep status



4 = WiFi Uplink

r = Power Restricted; T = Thermal ShutDown

Total APs:1

正常通讯状态下,你会发现 AP 和 AAC (当前停靠的控制器)之间会有 GRE (IP 47)和 PAPI (UDP 8211)端口的通讯流量。

而 AP 和控制器之间通讯异常导致无法注册时,或者由于网络中 GRE 端口被屏蔽了,一直 心跳丢失导致 Bootstraps 值持续增加。

采用这个方法可以非常容易定位 AP 和 AC 之前的故障是因为网络通讯问题导致。

<mark>(labX-md2) [</mark> MDC] #show datapath session table <mark>10.2.12.101</mark> (这里是 AP 的 IP 地址)
Datapath Session Table Entries
Flags: F - fast age, S - src NAT, N - dest NAT
D - deny, R - redirect, Y - no syn
H - high prio, P - set prio, T - set ToS
C - client, M - mirror, V - VOIP
Q - Real-Time Quality analysis
u - Upstream Real-Time Quality analysis
I - Deep inspect, U - Locally destined
E - Media Deep Inspect, G - media signal
r - Route Nexthop, h - High Value
A - Application Firewall Inspect
J - SDWAN Default Probe stats used as fallback
B - Permanent, O - Openflow
L - Log, o - Openflow config revision mismatched
Source IP or MAC Destination IP Prot SPort DPort Cntr Prio ToS Age Destination TAge Packets Bytes Flags CPU ID



10.2.10.12	10.2.12.101	17	8222 8211 0/0	0 0	0 0/0/0	3 0	0 FYI	2
10.2.10.12	10.2.12.101	17	8211 8211 0/0	0 0	1 0/0/0	17 0	0 FYI	2
<mark>10.2.12.101</mark>	10.2.10.12	47	0 0 0/0 0	40 0	0/0/0	337b 20380	2592822 FC	2
<mark>10.2.12.101</mark>	10.2.10.12	17	8211 8211 0/0	0 0	0 0/0/0	17 12	4374 FCI	2
10.2.10.12	10.2.12.101	47	0 0 0/0 0	40 0	0/0/0	337c 12954	1289950 F	2
10.2.12.101	10.2.10.12	17	8211 8222 1/0	0 0	0 0/0/0	4 0	0 FYCI	2
10.2.10.12	10.2.12.101	17	8999 8211 0/0	0 0	1 0/0/0	f 1	184 FI	2
10.2.12.101	10.2.10.12	17	8211 8999 0/0	0 0	1 0/0/0	f O	0 FYCI	2

正常通讯状态下, 你会发现 AP 和 S-AAC (当前备援的控制器) 之间会仅有 GRE (IP 47) 端口的通讯流量。

(labX-md1) [MDC] #show datapath session table 10.2.12.101

Datapath Session Table Entries

Flags: F - fast age, S - src NAT, N - dest NAT

- D deny, R redirect, Y no syn
- H high prio, P set prio, T set ToS
- C client, M mirror, V VOIP
- Q Real-Time Quality analysis
- u Upstream Real-Time Quality analysis
- I Deep inspect, U Locally destined
- E Media Deep Inspect, G media signal
- r Route Nexthop, h High Value
- A Application Firewall Inspect
- J SDWAN Default Probe stats used as fallback
- B Permanent, O Openflow
- L Log, o Openflow config revision mismatched



Source IP or CPU ID	MAC Destinat	ion I	ΡP	rot Sl	Port DI	Port	Cntr	Prio To	S Age Destinatio	n TAge Pac	kets	Bytes	Flags
10.2.12.101	10.2.10.11	47	0	0	0/0	0	40 1	0/0/0	33eb 15142	1619198	FC	2	
<mark>10.2.10.11</mark>	10.2.12.101	47	0	0	0/0	0	40 0	0/0/0	33eb 13062	1300850	F	2	

如果在控制器上无法看到任何 AP 的 session 信息,那有可能是 AP PoE 供电问题,无法获得控制器的 IP 地址, AP 自身获取不到 IP 地址, AP 和控制器之间的路由不可达和需要的访问端口 全部被屏蔽了, AP 上缓存其他的错误配置没有被清除,控制器上的授权已经超过最大可用数量, 等等因素。

第5步:登录到每个 MD 控制器上(即当前 AP 所停靠的 AAC),查看当前 AP 的 PoE 供电状态。

(labX-md2) [MDC] #show ap debug system-status ap-name LAB2-AP1 begin "Power Status"							
Power Status							
Item	Value						
Power Supply	: POE	(符合的 802.3af 供电需求)					
LLDP Power	: 0.0W						
Current Operation	al State : No rest	rictions					
HW POE status	: POE						
(labX-md1) [MDC]	#show ap debug	system-status ap-name labX-ap1 begin "Power Status"					
Power Status							
Item	Value						
Power Supply	: POE-AT	(符合的 802.3at 供电需求)					



LLDP Power : Successfully negotiated at 20.2W Current Operational State : No restrictions (Overridden by LLDP) (通过 LLDP 协商到 802.3at 标准) HW POE status : POE-AF 注意, 针对 PoE 交换机设备, 强烈建议开启 LLDP 协议。Aruba AP 默认开启并支持 LLDP 协商。

第6步: 登录到每个 MD 控制器上(即当前 AP 所停靠的 AAC),查看当前 AP 的 Radio 健康状态。

注意,通过 <mark>Total Radio Resets 和 Channel Changes 的次数</mark>,可以了解<mark>当前 AP 的工作健康状态,频繁切换表示 AP 工作异常。</mark>

(labX-md1) [MDC] #show ap debug radio-stats ap-name LAB2-AP1 radio 0

RADIO Stats

Parameter	Value
	General
Total Radio Resets	0
Resets Beacon Fail	0
TX Power Changes	1
Channel Changes	<mark>0</mark>
Failed Channel Changes	0
Radio Band Changes	0
Current Noise Floor	89
Dummy NF pkts on home	channel 0
Dummy NF pkts on scan	hannel 0
11g Protection	0
	Transmit
Tx Time perct @ beacon i	ntvl 000000000000000000000000000000000000
Tx Frames Rcvd	0
Tx Bcast Frames Rcvd	0



0000

x Frames Dropped Rate 1s 0 x Frames Dropped Rate 1s 0 x Bcast Frames Dropped 0 x Frames Transmitted 958 x Bytes Rcvd 0 abX-md1) [MDC] #show ap debug radio-str ADIO Stats arameter Value General otal Radio Resets 0 cesets Beacon Fail 0 x Power Changes 1 channel Changes 0 ailed Channel Changes 0 ailed Channel Changes 0 cadio Band Changes 0 current Noise Floor 85 oummy NF pkts on home channel 0 furmy NF pkts on scan channel 0 1g Protection 1 Transmit x Time perct @ beacon intvl 114444 x Frames Rcvd 1730 x Bcast Frames Rcvd 2 x Frames Dropped 505		
x Frames Dropped Rate 1s 0 x Bcast Frames Dropped 0 x Frames Transmitted 958 x Bytes Rcvd 0 abX-md1) [MDC] #show ap debug radio ADIO Stats arameter Value General otal Radio Resets 0 cesets Beacon Fail 0 x Power Changes 1 hannel Changes 0 ailed Channel Changes 0 ailed Channel Changes 0 ailed Channel Changes 0 adio Band Changes 0 current Noise Floor 85 oummy NF pkts on home channel 0 pummy NF pkts on scan channel 0 1g Protection 1 Transmit x Time perct @ beacon intvl 11444 x Frames Rcvd 1730 x Bcast Frames Rcvd 2 x Frames Dropped 505	Tx Frames Dropped	0
x Bcast Frames Dropped 0 x Frames Transmitted 958 x Bytes Rcvd 0 abX-md1) [MDC] #show ap debug radio ADIO Stats arameter Value General otal Radio Resets 0 esets Beacon Fail 0 X Power Changes 1 hannel Changes 0 ailed Channel Changes 0 ailed Channel Changes 0 ailed Channel Changes 0 adio Band Changes 0 furrent Noise Floor 85 Dummy NF pkts on home channel 0 Dummy NF pkts on scan channel 0 1g Protection 1 Transmit x Time perct @ beacon intvl 114.4 x Frames Rcvd 1730 x Bcast Frames Rcvd 2 x Frames Dropped 505	Tx Frames Dropped Rate	1s 0
x Frames Transmitted 958 x Bytes Rcvd 0 abX-md1) [MDC] #show ap debug radio ADIO Stats arameter Value General otal Radio Resets 0 esets Beacon Fail 0 X Power Changes 0 esets Beacon Fail 0 X Power Changes 1 channel Changes 0 ailed Channel Changes 0 ailed Channel Changes 0 ailed Channel Changes 0 aurrent Noise Floor 85 oummy NF pkts on home channel 0 furrent Noise Floor 85 oummy NF pkts on scan channel 0 1g Protection 1 Transmit x Time perct @ beacon intvl 1 1 4 4 x Frames Rcvd 1730 x Bcast Frames Rcvd 2 x Frames Dropped 505	Tx Bcast Frames Dropped	0
x Bytes Rcvd 0 abX-md1) [MDC] #show ap debug radio ADIO Stats arameter Value General otal Radio Resets 0 cesets Beacon Fail 0 X Power Changes 0 ailed Channel Changes 0 ailed Channel Changes 0 ailed Channel Changes 0 current Noise Floor 85 oummy NF pkts on home channel 0 furrent Noise Floor 85 oummy NF pkts on scan channel 0 furrent Noise Floor 1 current Noise Floor 1 furrent Noise Floor 2 furrent Noise Floor 3 furrent Noi	Tx Frames Transmitted	958
abX-md1) [MDC] #show ap debug radii ADIO Stats	Tx Bytes Rcvd	0
abX-md1) [MDC] #show ap debug radiADIO Stats'arameterValueGeneralotal Radio Resets0esets Beacon Fail0X Power Changes1Channel Changes0ailed Channel Changes0adio Band Changes0Current Noise Floor85Oummy NF pkts on home channel0Oummy NF pkts on scan channel01g Protection1Transmitx Time perct @ beacon intvl1 1 4 4x Frames Rcvd1730x Bcast Frames Rcvd2x Frames Dropped505		
ADIO Stats ADIO S	(labX-md1) [MDC] #show	ap debug
AarameterValueVarameterValueVarameterSearchGeneralOtal Radio Resets0Sesets Beacon Fail0Resets Beacon Fail0X Power Changes1Channel Changes0ailed Channel Changes0ailed Channel Changes0Current Noise Floor85Oummy NF pkts on home channel0Oummy NF pkts on scan channel0Oummy NF pkts on scan channel0Oummy NF pkts on scan channel0Ag Protection11 1 4 4x Time perct @ beacon intvl1 1 4 4x Frames Rcvd1730x Bcast Frames Rcvd2x Frames Dropped505	RADIO Stats	
Parameter Value General otal Radio Resets 0 desets Beacon Fail 0 X Power Changes 1 Channel Changes 0 ailed Channel Changes 0 ailed Channel Changes 0 current Noise Floor 85 Dummy NF pkts on home channel 0 Dummy NF pkts on scan channel 0 1 g Protection 1 Transmit x Time perct @ beacon intvl 1 1 4 4 x Frames Rcvd 1730 x Bcast Frames Rcvd 2 x Frames Dropped 505		
General otal Radio Resets 0 esets Beacon Fail 0 X Power Changes 1 hannel Changes 0 ailed Channel Changes 0 ailed Channel Changes 0 adio Band Changes 0 furrent Noise Floor 85 oummy NF pkts on home channel 0 pummy NF pkts on scan channel 0 1 g Protection 1 Transmit x Time perct @ beacon intvl 1 1 4 4 x Frames Rcvd 1730 x Bcast Frames Rcvd 2 x Frames Dropped 505	Parameter	Value
Generalotal Radio Resets0desets Beacon Fail0X Power Changes1Channel Changes0ailed Channel Changes0adio Band Changes0Current Noise Floor85Oummy NF pkts on home channel0Oummy NF pkts on scan channel01g Protection1Transmitx Time perct @ beacon intvl1 1 4 4x Frames Rcvd1730x Bcast Frames Rcvd2x Frames Dropped505		
Otal Radio Resets0Lesets Beacon Fail0X Power Changes1Channel Changes0ailed Channel Changes0adio Band Changes0Current Noise Floor85Dummy NF pkts on home channel0Dummy NF pkts on scan channel01g Protection1Transmitx Time perct @ beacon intvl1 1 4 4x Frames Rcvd1730x Bcast Frames Rcvd2x Frames Dropped505		General
Lessets Beacon Fail0X Power Changes1Channel Changes0ailed Channel Changes0adio Band Changes0Current Noise Floor85Dummy NF pkts on home channel0Dummy NF pkts on scan channel01g Protection1Transmitx Time perct @ beacon intvl1 1 4 4x Frames Rcvd1730x Bcast Frames Rcvd2x Frames Dropped505	Total Radio Resets	0
X Power Changes1Channel Changes0ailed Channel Changes0adio Band Changes0adio Band Changes0current Noise Floor85Dummy NF pkts on home channel0Dummy NF pkts on scan channel01g Protection1Transmitx Time perct @ beacon intvl1 1 4 4x Frames Rcvd1730x Bcast Frames Rcvd2x Frames Dropped505	Resets Beacon Fail	0
Channel Changes0ailed Channel Changes0adio Band Changes0Current Noise Floor85Oummy NF pkts on home channel0Oummy NF pkts on scan channel01g Protection11g Protection1x Time perct @ beacon intvl1144x Frames Rcvd1730x Bcast Frames Rcvd2x Frames Dropped505	TX Power Changes	1
ailed Channel Changes 0 adio Band Changes 0 Current Noise Floor 85 Dummy NF pkts on home channel 0 Dummy NF pkts on scan channel 0 1g Protection 1 Transmit x Time perct @ beacon intvl 1144 x Frames Rcvd 1730 x Bcast Frames Rcvd 2 x Frames Dropped 505	Channel Changes	0
Radio Band Changes0Current Noise Floor85Dummy NF pkts on home channel0Dummy NF pkts on scan channel01g Protection11g Protection1x Time perct @ beacon intvl1 1 4 4x Frames Rcvd1730x Bcast Frames Rcvd2x Frames Dropped505	Failed Channel Changes	0
Current Noise Floor85Dummy NF pkts on home channel0Dummy NF pkts on scan channel01g Protection11g Protection1* Time perct @ beacon intvl1 1 4 4x Frames Rcvd1730x Bcast Frames Rcvd2x Frames Dropped505	Radio Band Changes	0
Dummy NF pkts on home channel0Dummy NF pkts on scan channel01g Protection11g Protection1Transmitx Time perct @ beacon intvl1 1 4 4x Frames Rcvd1730x Bcast Frames Rcvd2x Frames Dropped505	Current Noise Floor	85
Dummy NF pkts on scan channel01g Protection1Transmitx Time perct @ beacon intvl1 1 4 4x Frames Rcvd1730x Bcast Frames Rcvd2x Frames Dropped505	Dummy NF pkts on home	e channel
1g Protection1Transmitx Time perct @ beacon intvl1 1 4 4x Frames Rcvd1730x Bcast Frames Rcvd2x Frames Dropped505	Dummy NF pkts on scan	channel
Transmit x Time perct @ beacon intvl 1 1 4 4 x Frames Rcvd 1730 x Bcast Frames Rcvd 2 x Frames Dropped 505	11g Protection	1
x Time perct @ beacon intvl 1144 x Frames Rcvd 1730 x Bcast Frames Rcvd 2 x Frames Dropped 505		Transmi
x Frames Rcvd 1730 x Bcast Frames Rcvd 2 x Frames Dropped 505	Tx Time perct @ beacon	intvl 1
x Bcast Frames Rcvd 2 x Frames Dropped 505	Tx Frames Rcvd	1730
x Frames Dropped 505	Tx Bcast Frames Rcvd	2
	Tx Frames Dropped	505



Tx Frames Dropped Rate 1s 0

当前 AP 能够扫描到周边的其他无线信号信息列表。

(labX-md1) [MDC] #show ap monitor ap-list ap-name LAB2-AP1

Monitored AP Table

bssid essid chan ap-type phy-type dos dt/mt ut/it encr nstas avg-snr curr -snr avg-rssi curr-rssi wmacs ibss cl-delay bss-color partial bss color bss color disabled

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

94:b	4:0f:44	:d6:90	aruba-t	est		60E	valio	d 80)211a-VHT-8	30 disable 20537/20537 0/0 wpa2-8021x-aes
0	30	30	65	65	0	no	0			
94:b	4:0f:44	:d6:80	aruba-t	est		11	valic	80	211b/g-HT-2	20 disable 20537/20537 0/0 wpa2-8021x-aes
0	15	15	80	80	0	no	0			
6c:f3	8:7f:7f:6	51:c0 B	aggio-1	03		11	inter	fering 8	80211b/g-HT	-20 disable 20534/20534 0/0 wpa2-psk-aes
2	27	29	67	66	2	no	0			
b4:0 1	f:3b:77 0	c0:a1: 26	Tenda_ 0	77C0A0 69	1	no	2 in 0	terfering 	9 80211b/g- 	-HT-20 disable 20521/3187 35/10 wpa-psk-aes
04:b	d:88:de	e:11:20 65	Baggic 29	-103 30	2	1 no	inte 0	erfering	80211b/g-H	HT-20 disable 20520/3041 4/0 wpa2-psk-aes
01·h	d.88.95	0.5 0.11.20	Baggio	-103	2	1/	19F ir	ntorforin	a 80211a-V	HT-80 dicable 18788/115 321/1 wpa2-psk-aes
2	0	56	0	39	2	no	0			
6c:f3 1	8:7f:7f:6 6 1	61:d0 B	Baggio-1 79 7	103 '9 1	r	36E 10 1	inte	rfering	80211a-VHT 	80 disable 3681/76 54/0 wpa2-psk-aes 0
7c:49	9:eb:a0	:d0:a6	rockrok	o-vacui	um-v	1_mia	pD0A	.66 ir	nterfering 8	0211b disable 1748/508 1/0 open
0	30	30	29	29	0	no	0			
Start	t:0									
Leng	gth:8									



2.6 控制器层面诊断

第1步:在 MM 控制器上总览全网接管的所有控制器情况,相互间的配置同步状态,各个控制器 的版本信息,设备类型,设备型号,设备的主机名,在线状态,配置 ID, crash 信息和控制 器所在节点路径信息等。

(LabX-MM-1) [mynode] #show switches
All Switches
IP Address IPv6 Address <mark>Name</mark> Location <mark>Type</mark> Model <mark>Version</mark> Status Configuration State Config Sy nc Time (sec) Config ID
10.2.50.11 NoneLabX-MM-1 Building1.floor1 master ArubaMM-VA 8.6.0.3_74788 upUPDATE SUCCESSFUL066
10.2.10.12 NonelabX-md2 Building1.floor1 MDArubaMC-VA 8.6.0.3_74788 upUPDATE SUCCESSFUL066
10.2.10.11 NonelabX-md1 Building1.floor1 MDArubaMC-VA 8.6.0.3_74788 upUPDATE SUCCESSFUL066
Total Switches:3
(LabX-MM-1) [mynode] #show switches debug
All Switches
IP Address MAC Name Nodepath Type Model Version Status Uptime CrashInfo Config Syn c Time (sec)
10.2.50.11 00:0c:29:ab:5a:bd LabX-MM-1 /mm/mynode master ArubaMM-VA 8.6.0.3_74788 up 0d 6h 24m no 0



10.2.10.12 00:0c:29	ea:9a:d9 labX-md2	/md/labX	MD	ArubaMC-VA	8.6.0.3_74788	up	0d 6h 25m no	0
10.2.10.11 00:0c:29	9:82:71:b4 labX-md1	/md/labX	MD	ArubaMC-VA	8.6.0.3_74788	up	0d 6h 25m no	0
Total Switches:3								
(LabX-MM-1) [myn	ode] #show configura	ation node-l	nierarch	ıy				
Default-node is no	t configured. Autopar	k is disabled	ł.					
Configuration node	e hierarchy							
Config Node	Type Name							
/ S	ystem							
/md	System							
/md/labX	Group							
/md/labX/00:0c:29:	82:71:b4 Device lab)	K-md1						
/md/labX/00:0c:29:	ea:9a:d9 Device lab>	(-md2						
/mm	System							
/mm/mynode	System							

MM和 MD 之间分别建立了 IPSec 隧道,传输控制和管理信令。

(LabX-MM-1) [mynode] (config) #show datapath tunnel table

Datapath Tunnel Table Entries

Flags: E - Ether encap, I - Wi-Fi encap, R - Wired tunnel, F - IP fragment OK

W - WEP, K - TKIP, A - AESCCM, G - AESGCM, M - no mcast src filtering

S - Single encrypt, U - Untagged, X - Tunneled node, 1(cert-id) - 802.1X Term-PEAP

2(cert-id) - 802.1X Term-TLS, T - Trusted, L - No looping, d - Drop Bcast/Unknown Mcast,



D - Decrypt tunnel, a - Reduce ARP packets in the air, e - EAPOL only										
C - Prohibit new calls, P - Permanent, m - Convert multicast, B - Bgw peer uplink tunnel										
n - Convert RAs to unicast(VLAN Pooling/L3 Mobility enabled), s - Split tunnel	n - Convert RAs to unicast(VLAN Pooling/L3 Mobility enabled), s - Split tunnel									
V - enforce user vlan(open clients only), z - Datazone										
H - Standby (HA-Lite), u - Cluster UAC tunnel, b - Active AAC tunnel, t - Cluster s-AAC tunnel										
c - IP Compression, g - PAN GlobalProtect Tunnel, w - Tunneled Node Heartbeat										
B - Cluster A-SAC Mcast, G - Cluster S-SAC Mcast, I - Tunneled Node user tunnel										
f - Static GRE Tunnels, k- keepalive enabled, Y - Convert BC/MC to Unicast										
# Source Destination Prt Type MTU VLAN Acls BSSID Decaps Encaps Heartbeats Flags EncapKBytes DecapKBytes										
10 SPIFB1A1400out 10.2.10.12 50 IPSE 1500 0 routeDest 000A 0 0 0) 901 T									
9 SPI30BDC600 in 10.2.50.11 50 IPSE 1500 0 routeDest 000A 0 185 0 0	2 0 T									
13 SPIDF663500out 10.2.10.11 50 IPSE 1500 0 routeDest 000A 0 0 0) 1329 T									
14 SPIF741BC00 in 10.2.50.11 50 IPSE 1500 0 routeDest 000A 0 256 0 0	i3 0 T									
(LabX-MM-1) [mynode] (config) #show crypto isakmp sa peer 10.2.10.11										
Initiator IP: 10.2.10.11										
Responder IP: 10.2.50.11	Responder IP: 10.2.50.11									
Initiator: No										
Initiator cookie:25da2fd000b38ba4 Responder cookie:1e3d83b34c7a372e										
SA Creation Date: Sun Mar 29 20:38:35 2020										



Life secs: 28800

Initiator Phase1 ID: IPV4_ADDR:10.2.10.11 Responder Phase1 ID: IPV4_ADDR:10.2.50.11 Exchange Type: IKE_SA (IKEV2) Phase1 Transform:EncrAlg:AES128 HashAlg:HMAC_SHA1_96 DHGroup:2 Authentication Method: Pre Shared Key IPSEC SA Rekey Number: 1 Ipsec-map name: default-local-master-ipsecmap10.2.10.11

第2步:在 MM 控制器上如何查看和管理当前的相关配置内容。

```
如果在配置的提示符下,有个^符号,表示有当前编辑好的配置,还没有 write memory (即推送给 MD 控制器)
(LabX-MM-1) <mark>^[labX] #show configuration pending (查看还没有推送给 md 的配置内容)</mark>
wlan ssid-profile "test-ssid-profile"
  essid "yang-test"
ļ
(LabX-MM-1) ^ [mm] #write me (如果我们输入了 write memory,发现仍然显示^符号,表示你推送的配置节点路径不对)
Saving Configuration...
(LabX-MM-1) ^[mm] #
(LabX-MM-1) ^ [mm] #show configuration unsaved-nodes (可以查看在哪个节点路径下还有配置没有推送)
List of unsaved configuration nodes
_____
Nodename
_____
/md/labX
(LabX-MM-1) ^[mm] #cd /md/labX
                                 (我们需要切换到未保存配置的节点路径,重新推送下配置即可)
(LabX-MM-1) ^[labX] #write me
Saving Configuration...
Page 133 of 171
```

a Hewlett Packard Enterprise company Configuration Saved.

(LabX-MM-1) [labX] #

```
(LabX-MM-1) [labX] #show configuration committed (如何查看在当前节点路径下编辑和提交的相关配置内容)
netdestination v4-controller-interfaces
  host 10.2.10.11
  host 10.2.10.12
  host 10.2.10.21
  host 10.2.10.22
  host 10.2.10.10
ļ
netdestination user-net
  network 192.168.100.0 255.255.255.0
ļ
netdestination6 v6-controller-interfaces
  host 2001:da8:8000:151::13
i
ip access-list session apprf-employee-sacl
i
ip access-list session apprf-contractor-sacl
İ
ip access-list session labX-skype-role
i
ip access-list session ipv6-basic-acl
  ipv6 user any udp 546 deny
```

```
ipv6 any any svc-v6-dhcp permit
```



```
ipv6 any any svc-v6-icmp permit
i
ip access-list session deny-cry-antivirus
  any any tcp 135 deny
  any any tcp 137 139 deny
  any any tcp 445 deny
  any any udp 135 deny
  any any udp 137 139 deny
  any any udp 445 deny
!
ip access-list session ipv4-controller-if-acl
  user alias v4-controller-interfaces any deny
i
ip access-list session apprf-labX-skype-role-sacl
!
ip access-list session ipv4-basic-acl
  user any udp 68 deny
  any any svc-dhcp permit
  any any svc-dns permit
  any any svc-icmp permit
```

ipv6 any any svc-dns permit

如何在指定的节点路径下,查看从哪个节点路径继承来的和从哪个路径提交的配置内容,且 这些内容和你 mdconnect 到 md 上,采用 show running–config 看到的是一致的。

(LabX-MM-1) [mynode] #cd labX-md1

(LabX-MM-1) [00:0c:29:82:71:b4] #show configuration effective detail



crypto-local pki PublicCert master-ssh-pub-cert master-ssh-pub-cert	# inherited from [/]
masterip 10.2.50.11 ipsec ***** interface vlan 30	# local [/md/labX/00:0c:29:82:71:b4]
ip access-list eth validuserethacl	# inherited from [/]
permit any	# inherited from [/]
!	
aaa tacacs-accounting	# inherited from [/]
!	
netservice svc-smb-udp udp 445	# inherited from [/]
netservice vnc tcp 5900 5905	# inherited from [/]
netservice svc-noe udp 32512 ALG noe	# inherited from [/]
netservice svc-cfgm-tcp tcp 8211	# inherited from [/]
netservice svc-netbios-ssn tcp 139	# inherited from [/]
netservice svc-syslog udp 514	# inherited from [/]
netservice svc-citrix tcp 2598	# inherited from [/]
netservice svc-ipp-tcp tcp 631	# inherited from [/]
netservice svc-v6-icmp 58	# inherited from [/]
netservice svc-l2tp udp 1701	# inherited from [/]
netservice svc-http-proxy1 tcp 3128	# inherited from [/]
netservice svc-papi udp 8211	# inherited from [/]

第3步:在 MM 控制器设置相关配置导致 MD 失去通讯, 默认 240s 后, MD 会自动配置回滚。

查看当前 MM 和 MD 的工作状态,正常同步配置								
(LabX-MM-1) [00:0c:29:82:71:b4] #show switches								
All Switches								
IP Address IPv6 Address Name nc Time (sec) Config ID	Location	Туре	Model	Version	Status Configuration State Config Sy			



10.2.50.11 None 0 75	LabX-MM-1 Building1.floor1 ma	ster ArubaMM-VA 8.6.0.3_74788 up	UPDATE SUCCESSFUL
10.2.10.12 None 0 75	labX-md2 Building1.floor1 MD	ArubaMC-VA 8.6.0.3_74788 up	UPDATE SUCCESSFUL
10.2.10.11 None 0 75	labX-md1 Building1.floor1 MD	ArubaMC-VA 8.6.0.3_74788 <mark>up</mark>	UPDATE SUCCESSFUL
Total Switches:3			

我们登陆到 labX-md1 控制器上,模拟误操作将上联端口 0/0/0 shutdown 掉。

(LabX-MM-1) [00:0c:29:82:71:b4] #cd labX-md1

(LabX-MM-1) [00:0c:29:82:71:b4] #configure terminal

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

(LabX-MM-1) [00:0c:29:82:71:b4] (config) #interface gigabitethernet 0/0/0

(LabX-MM-1) [00:0c:29:82:71:b4] (config-submode)#shutdown

(LabX-MM-1) ^[00:0c:29:82:71:b4] (config-submode)#end

(LabX-MM-1) ^[00:0c:29:82:71:b4] #write me

Saving Configuration...

Configuration Saved.

接着我们继续 show switches,发现 labX-md1 的配置状态一直停留在 UPDATE REQUIRED

(LabX-MM-1) [00:0c:29:82:71:b4] #show switches								
All Switches								
IP Address IPv6 Address Name nc Time (sec) Config ID	Location	Туре	Model	Version	Status Configuration State Config Sy			



10.2.50.11 None 0 76	LabX-MM-1 Building1.floor1 master Aruba	aMM-VA 8.6.0.3_74788 up	UPDATE SUCCESSFUL
10.2.10.12 None 0 76	labX-md2 Building1.floor1 MD ArubaN	C-VA 8.6.0.3_74788 up	UPDATE SUCCESSFUL
10.2.10.11 <mark>None</mark>	labX-md1 Building1.floor1 MD ArubaM	C-VA 8.6.0.3_74788 up	UPDATE REQUIRED 0
75			

Total Switches:3

此时我们在mm控制上ping md1,发现已经失去通讯。

(LabX-MM-1) [00:0c:29:82:71:b4] #ping 10.2.10.11

Press 'q' to abort.

Sending 5, 92-byte ICMP Echos to 10.2.10.11, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

接着我们必须先在 mm 上将该 labX-md1 设备节点路径下的配置还原,重新开启 0/0/0 端口,这个操作是必须的,否则一旦 labX-md1 重新回来后,又同步了该节点路径的配置,又会将 0/0/0 端口 shutdown 掉。

另外请注意,这里虽然我们在 mm 上修改了 labX-md2 节点下的配置,由于 md 和 mm 已 经失去通讯,这个配置是无法及时同步到 labX-md2 上的,必须等待 labX-md2 的自身重新配置 回滚,才能再次和 mm 控制器同步配置。

(LabX-MM-1) [00:0c:29:82:71:b4] (config) #interface gigabitethernet 0/0/0

(LabX-MM-1) [00:0c:29:82:71:b4] (config-submode)#no shutdown

(LabX-MM-1) ^[00:0c:29:82:71:b4] (config-submode)#end

(LabX-MM-1) ^[00:0c:29:82:71:b4] #write me

Saving Configuration...

Configuration Saved.

等待 240s 后,我们在 mm 上再次 ping labX-md1,成功 ping 通



(LabX-MM-1) [00:0c:29:82:71:b4] #ping 10.2.10.11

Press 'q' to abort.

Sending 5, 92-byte ICMP Echos to 10.2.10.11, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 3.016/3.406/3.693 ms

在 mm 控制器上,再次查看当前控制器的状态, labX-md1 已经 up 起来。

(LabX-MM-1) [00:0c:29:82:71:b4] #show switches								
All Switches								
IP Address IPv6 Address Name Location Type Model Version Status Configuration State Config Sy nc Time (sec) Config ID								
10.2.50.11 None LabX-MM-1 Building1.floor1 master ArubaMM-VA 8.6.0.3_74788 up UPDATE SUCCESSFUL 0 77								
10.2.10.12 None 0 77	labX-md2	Building1.floor1	MD	ArubaM	C-VA 8.6.0.3	3_74788 up	UPDATE SUCCESSFL	JL
10.2.10.11 None <mark>75</mark>	labX-md1	Building1.floor1	MD	ArubaM	C-VA 8.6.0.3	3_74788 up	UPDATE REQUIRED	0
Total Switches:3								

最后我们登陆到 labX-md1 上,查看配置回滚的相关日志,证明 labX-md1 确实经过了配置回滚的过程。

(LabX-MM-1) [00:0c:29:82:71:b4] #cd labX-md1

(LabX-MM-1) [00:0c:29:82:71:b4] #mdc

Redirecting to Managed Device Shell

(labX-md1) [MDC] #



(labX-md1) [MDC] #show log system 50 | include rollback

Mar 28 09:57:08 :399814: <5419> <DBUG> |cfgm| cfgm_rollback_load_state: State(UNINITIALIZED:UPDATE REQUIRED: CFGID-62:PEND-0:INITCFGID:0) FD=-1:Rollback loading last good id 62, bad reboot id 0

Mar 28 09:57:08 :399814: <5419> <DBUG> |cfgm| cfgm_rollback_recv_config_id: State(UNINITIALIZED:UPDATE REQUI RED:CFGID-62:PEND-0:INITCFGID:0) FD=-1:Rollback ignoring id 62 as it is same as last good id

Mar 28 20:20:09 :399816: <5419> <ERRS> |cfgm| cfgm_rollback_timeout: State(CONNECTINPROGRESS:CONFIG PROP AGATION:CFGID-72:PEND-72:INITCFGID:0) FD=27:Rollback lost connectivity after reciving id 72 moving back to id 71

Mar 28 20:30:01 :399816: <5419> <ERRS> |cfgm| cfgm_rollback_timeout: State(CONNECTINPROGRESS:CONFIG PROP AGATION:CFGID-74:PEND-74:INITCFGID:0) FD=27:Rollback lost connectivity after reciving id 74 moving back to id 73

Mar 28 20:43:10 :399816: <5419> <ERRS> |cfgm| cfgm_rollback_timeout: State(CONNECTINPROGRESS:CONFIG PROP AGATION:CFGID-76:PEND-76:INITCFGID:0) FD=27:Rollback lost connectivity after reciving id 76 moving back to id 75

第4步: 如果 MM 和 MD 失去通讯了,但是 MD 因为各种原因无法配置回滚,那么我们还可以采 用本地强制配置来快速恢复网络。

在 mm 和 md 失去通讯过程中,我们登陆到 labX-md1 控制器上,使用下面的命令,启用本地强制配置,从而可以本地来配置 md 控制器,例如快速设置 port-channel/lacp, STP 等这些容易导致网络通讯故障的配置,当我们重新设置好相关配置后,记住,一定 需要先到 mm 控制器的相关节点路径下(通常就是设备节点),同样的配置方法相同设置一遍(这里就不在演示和介绍),并保存 成功。

(labX-md1) [MDC] #disaster-recovery

off Disable Disaster Recovery Mode

on Enable Disaster Recovery Mode

(labX-md1) [MDC] #disaster-recovery on

Entering disaster recovery mode

(DR-Mode) [MDC] [mm] #

(DR-Mode) [MDC] [mm] #show switches

All Switches

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



	-				
10.2.10.11 None labX-md1 Building1.floor1 MD ArubaMC-VA 8.6.0.3_74788 up <mark>CONFIG DISASTER RECOV</mark> <mark>ERY</mark> 10 77					
Total Switches:1					
(DR-Mode) [MDC] [mm] #configure terminal					
Enter Configuration commands, one per line. End with CNTL/Z					
(DR-Mode) [MDC] [mm] (config) #interface gigabitethernet 0/0/0					
(DR-Mode) [MDC] [mm] (config-submode)#no shutdown					
(DR-Mode) [MDC] [mm] (config-submode)#end					
(DR-Mode) [MDC] [mm] #write me					
Saving Configuration					

最后,在 labX-md1 控制器上,将 disaster-recovery 关闭掉,这样 labX-md1 会立即和 mm 控制器重新完整地同步一次配置。

(DR-Mode) [MDC] [mm] #disaster-recovery off				
(labX-md1) [MDC] #				
(LabX-MM-1) [00:0c:29:82:71:b4] #show switches				
All Switches				
IP Address IPv6 Address Name Location Type Model Version Status Configuration State Config Sy nc Time (sec) Config ID				
10.2.50.11 NoneLabX-MM-1 Building1.floor1 master ArubaMM-VA 8.6.0.3_74788 upUPDATE SUCCESSFUL077				



10.2.10.12 None 0 77	labX-md2	Building1.floor1	MD	ArubaMC-VA	8.6.0.3_74788 up	UPDATE SUCCESSFUL
10.2.10.11 None 0 77	labX-md1	Building1.floor1	MD	ArubaMC-VA	8.6.0.3_74788 up	CONFIG PROPAGATION
Total Switches:3						

第5步:分别在 MM 和 MD 控制器的 CLI 界面输入" show switchinfo"可以读取控制器当前运 行状态数据,其中包括控制器运行版本、在线运行时长、前一次启动原因、启动配置文件名、 启动系统分区号、软件模块健康状态等信息。

(LabX-MM-1) [mynode] #show switchinfo

Hostname is LabX-MM-1

Building1.floor1

System Time: Fri Mar 27 19:08:59 CST 2020

Aruba Operating System Software.

ArubaOS (MODEL: ArubaMM-VA), Version 8.6.0.3

Website: http://www.arubanetworks.com

(c) Copyright 2020 Hewlett Packard Enterprise Development LP.

Compiled on 2020-03-20 at 11:07:28 UTC (build 74788) by p4build

BIOS Version: Phoenix Technologies LTD, 6.00

Built: 07/30/2013

Switch uptime is 9 hours 54 minutes 51 seconds (当前控制器的在线时长)

.

<mark>Reboot Cause: User reboot (Intent:cause: 86:50)</mark> (最近一次重启原因)

Supervisor Card

Processor(s):

Total CPUs: 3, Sockets: 1, Cores Per CPU: 3



Socket 0: Intel(R) Core(TM) i5-4250U CPU @ 1.30GHz 5703M bytes of memory 4096M bytes of Supervisor Card system flash.

Config ID: 62 (启动时,加载的配置文件名称,实际是由 MM 推送过来) Boot Partition: PARTITION 1 (启动时,所使用的分区)

mgmt is administratively down line protocol is down Hardware is Ethernet, address is 00:0C:29:AB:5A:B3

VLAN1 is up line protocol is down

Hardware is CPU Interface, Interface address is 00:0C:29:AB:5A:BD (bia 00:0C:29:AB:5A:BD)

Description: 802.1Q VLAN

IPv6 Router Advertisements are disabled Routing interface is enable, Forwarding mode is enable Directed broadcast is disabled, BCMC Optimization disabled ProxyARP disabled Suppress ARP enable Encapsulation 802, loopback not set MTU 1500 bytes Last clearing of "show interface" counters 0 day 9 hr 54 min 51 sec link status last changed 0 day 9 hr 54 min 51 sec Proxy Arp is disabled for the Interface

switchrole:master (当前控制器的角色)

Configuration unchanged since last save

No AP crash information available.

No controller crash information available. (当前系统是否存在 crash 信息,如果是 no,表示没有。如果是 crash informatio n available ,表示当前系统存在 crash 信息,需要进一步处理)



Reboot Cause: User reboot (Intent:cause: 86:50)

第6步:分别在 MM 和 MD 控制器的 CLI 界面输入"show cpuload"可以读取控制器 CPU 负载数据。下面的 CLI 可以查看每个进程所占用的 CPU 和内存资源情况,可以直接了解是哪个进程占用过多

查看控制面板的 CPU 利用率

(LabX-MM-1) [mynode] #show cpuload

user 9.1%, system 4.4%, idle 86.5%

(labX-md1) [MDC] #show cpuload

user 3.6%, system 4.0%, idle 92.4%

注意: idle 为空闲量,要求空闲的百分比不能持续低于 25%(也就是说观察最近 5 分钟时间内)。

查看当前那个进程占用的 CPU 和内存资源最高以及占用的百分比。

(labX-md1) [MDC] #show cpuload current top2 - 10:17:29 up 22 min, 0 users, load average: 0.33, 0.41, 0.34 Tasks: 217 total, 3 running, 165 sleeping, 0 stopped, 0 zombie Cpu(s): 5.4%us, 4.0%sy, 0.0%ni, 89.1%id, 1.3%wa, 0.0%hi, 0.2%si, 0.0%st Mem: 5840632k total, 3211216k used, 2629416k free, 5228k buffers Swap: 0k total, 0k used, 0k free, 1000828k cached PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND 5170 root 20 0 16.4g 63m 24m S 39 1.1 8:27.57 sos.shumway.elf 50 root 20 0 0 0 0 1 2 0.0 0:00.43 kworker/2:1 5411 root 20 0 399m 195m 192m S 2 3.4 0:46.27 gsmmgr


Aruba 动手实验手册: ArubaOS 8 高级配置

5479 root 20 0 1709m 145m 10m S 2 2.6 0:03.87 fpapps 20 0 19640 2596 2188 R 2 0.0 0:00.01 top2 8249 root 20 0 9632 2288 2180 S 0 0.0 0:00.52 init 1 root 0 0 0 S 0 0.0 0:00.00 kthreadd 2 root 20 0 3 root 0 | 0 0.0 0:00.00 kworker/0:0 20 0 0 0 0 I 0 0.0 0:00.00 kworker/0:0H 4 root 0 - 20 0 0 6 root 0 - 20 01 0 0.0 0:00.00 mm_percpu_wq 0 0 7 root 20 0 0 0 0 S 0 0.0 0:00.25 ksoftirqd/0 8 root 0 R 0 0.0 0:00.51 rcu_sched 20 0 0 0 9 root 0 0 0 I 0 0.0 0:00.00 rcu bh 20 0 0 S 0 0.0 0:00.02 migration/0 10 root RT 0 0 0 11 root 0 P 0 0.0 0:00.00 watchdog/0 20 0 0 0 20 0 12 root 0 S 0 0.0 0:00.00 cpuhp/0 0 0 13 root 0 S 0 0.0 0:00.00 cpuhp/1 20 0 0 0 14 root 0 P 0 0.0 0:00.00 watchdog/1 20 0 0 0 15 root RT 0 0 0 0 S 0 0.0 0:00.02 migration/1 16 root 0 S 0 0.0 0:00.00 ksoftirqd/1 20 0 0 0 0 I 0 0.0 0:00.00 kworker/1:0H 18 root 0 - 20 0 0 19 root 0 S 0 0.0 0:00.00 cpuhp/2 20 0 0 0 20 root 20 0 0 0 0 P 0 0.0 0:00.00 watchdog/2 21 root 0 S 0 0.0 0:00.01 migration/2 RT 0 0 0 22 root 20 0 0 0 0 S 0 0.0 0:00.00 ksoftirqd/2 24 root 0 0 0 I 0 0.0 0:00.00 kworker/2:0H 0 - 20

查看数据转发面板的 CPU 利用率



(labX-md1) [MDC] #show datapath utilization
Datapath Network Processor Utilization
++
Cpu Cpu utilization during past
Type Id 1 Sec 4 Secs 64 Secs
++
<mark>SP 1 1% 1% </mark>
FP 2 2% 2% 2%
DPI 3 1% 1% 1%
Datapath CPU Allocation Summary
Slow Path (SP) : 1, Slow Path Gateway (SPGW) : 0
Fast Path (FP) : 1, Fast Path Gateway (FPGW) : 0
DPI : 1, Crypto (CRYP) : 0
Slow Path Spare (SPSPARE) : 0
注意:要求的利用率百分比不能高于 75%(也就是说观察最近 5分钟时间内)。
第7步: 分别在 MM 和 MD 控制器上查看当前所有进程的当前工作状态(用于查看是否有进程处 于死机状态)





/mswitch/bin/ctrlmgmt	PROCESS_RUNNING -	0	240	3	Sat Mar 28 09:56:27 2020
/mswitch/bin/packet_filter	PROCESS_RUNNING -	0	240	3	Sat Mar 28 09:56:27 2020
/mswitch/bin/cryptoPOST	PROCESS_RUNNING 8	0	240	3	Sat Mar 28 09:56:28 2020
/mswitch/bin/gsmmgr	PROCESS_RUNNING 8	0	240	3	Sat Mar 28 09:56:28 2020
/mswitch/bin/pubsub	PROCESS_RUNNING 8	0	240	3	Sat Mar 28 09:56:28 2020
/mswitch/bin/cfgm	PROCESS_RUNNING 8	0	240	3	Sat Mar 28 09:56:28 2020
/mswitch/bin/rng-mgr	PROCESS_RUNNING -	0	240	3	Sat Mar 28 09:56:28 2020
/mswitch/bin/certmgr	PROCESS_RUNNING -	0	240	3	Sat Mar 28 09:56:29 2020
/mswitch/bin/cfgdist	PROCESS_RUNNING 8	0	240	3	Sat Mar 28 09:56:29 2020
/mswitch/bin/syslogdwrap	PROCESS_RUNNING 8	0	240	3	Sat Mar 28 09:56:29 2020
/mswitch/bin/ <mark>aaa</mark> F	PROCESS_RUNNING 8	0	240	3	Sat Mar 28 09:56:29 2020
/mswitch/bin/fpapps	PROCESS_RUNNING 0	0	240	3	Sat Mar 28 09:56:29 2020
/mswitch/bin/lagm	PROCESS_RUNNING -	0	240	3	Sat Mar 28 09:56:30 2020
/mswitch/bin/pim	PROCESS_RUNNING -	0	240	3	Sat Mar 28 09:56:30 2020
/mswitch/bin/licensemgr	PROCESS_RUNNING -	0	240	3	Sat Mar 28 09:56:30 2020
/mswitch/bin/isakmpd	PROCESS_RUNNING 8	0	240	3	Sat Mar 28 09:56:30 2020
/mswitch/bin/wms	PROCESS_RUNNING -	0	240	3	Sat Mar 28 09:56:30 2020
/mswitch/bin/profmgr	PROCESS_RUNNING -	0	240	3	Sat Mar 28 09:56:31 2020
/mswitch/bin/msghh	PROCESS_RUNNING -	0	240	3	Sat Mar 28 09:56:31 2020
/mswitch/bin/ <mark>auth</mark>	PROCESS_RUNNING -	0	240	3	Sat Mar 28 09:56:31 2020
/mswitch/bin/ <mark>appRF</mark>	PROCESS_RUNNING -	0	240	3	Sat Mar 28 09:56:31 2020
/mswitch/bin/stm	PROCESS_RUNNING -	0	240	3	Sat Mar 28 09:56:32 2020
/mswitch/bin/amon_sende	r PROCESS_RUNNING -	C	240	3	Sat Mar 28 09:56:32 2020
/mswitch/bin/rtpa F	PROCESS_RUNNING -	0	240	3	Sat Mar 28 09:56:32 2020
/mswitch/bin/udbserver	PROCESS_RUNNING -	0	240	3	Sat Mar 28 09:56:32 2020
/mswitch/bin/dhcpdwrap	PROCESS_RUNNING -	0	240	3	Sat Mar 28 09:56:32 2020



如果发现某进程状态出现 stop,我们可以针对单个进程进行 restart,看看是否恢复工作。 如果恢复后,又很快出现 stop,请尽快联系 TAC 进行分析。

(labX-md1) [MDC] #process restart httpd

WARNING: Do you really want to restart process: httpd (y/n):

(labX-md1) [MDC] #process restart aaa

WARNING: Do you really want to restart process: aaa (y/n):

第8步:分别在 MM 和 MD 控制器上查看当前系统内存和存储空间的负载情况。

在控制器 CLI 界面输入"show memory"可以读取控制器内存负载数据。注意:要求 5 分钟时间内,内存使用率小于等于 75%. 在控制器 CLI 界面输入"show storage"可以读取控制器存储空间负载数据。注意:使用率 Use%不能超过 80%

(LabX-MM-1) [mynode] #show memory

Memory (Kb): total: 5840796, used: 2744240, free: 3096556

(LabX-MM-1) [mynode] #show storage (这个是基于 VMC 的控制器输出存储信息,关心 sdb1)

Filesystem Size Used Available <mark>Use%</mark> Mounted on

none 3.0G 13.7M 3.0G 0% /tmp

/dev/sdb1 5.8G 1019.9M 4.5G 18% /flash

/dev/sda5 1.4G 387.9M 1015.1M 28% /mnt/disk1

/dev/sda6 1.4G 420.1M 982.9M 30% /mnt/disk2

(labX-md1) [MDC] #show memory

Memory (Kb): total: 3069168, used: 1192928, free: 1876240

(labX-md1) [MDC] #show storage (这个是基于 7010 控制器输出存储信息,关心 所有 flash 空间)

Filesystem Size Used Available Use% Mounted on

/dev/usb/flash3 1.5G 804.5M 626.4M 56% /flash

(xxx-md1) *#show storage (这个是基于 72xx 控制器输出存储信息,关心 所有 flash 空间)



Filesystem	Size	Used Avai	lable Use% Mounted	or
/dev/usb/flash3	1.5G	268.1M	1.2G 18% /flash	
/dev/usb/flash4	5.6G	656.8M	4.7G 12% /flash1	1

第9步:分别在 MM 和 MD 控制器上查看当前控制器上 CPU 温度,风扇以及电源模块工作状态 (如果是软件的 VMM 和 VMC,则无法查看)

(labX-md1) [MDC] #	show inventory (必须是硬件的 MM 和 MD 控制器,才能查看以下信息,虚拟机不可以)
Supervisor Card slot	: 0
System Serial#	: CG0010616 (Date:10/14/15)
CPU Card Serial#	: AF41032212 (Date:10/14/15)
CPU Card Assembly	# : 2010184C
CPU Card Revision	: (Rev:09.00)
SC Model#	: <mark>Aruba7010</mark>
HW MAC Addr	: 00:0b:86:dd:33:20 to 00:0b:86:dd:33:3f
CPLD Version	: (Rev: 12.8)
PoE Firmware Versio	on : 1.7.0 (Build: 4)
<mark>Power Supply</mark>	: Present
	12V OK : Yes
	56V OK : Yes
<mark>Main Board Temper</mark>	atures :
	U45 - LM95233 Local Temp 24 C (near DDR3)
	Q8 - LM95233 Remote 1 Temp 22 C (near intake right side edge)
	Q12 - LM95233 Remote 2 Temp 24 C (near SFP ports)
	U14 - ADT7476 Local Temp 32 C (near exhaust left side edge)
	U26 - ADT7476 Remote2 Temp 52 C (98DX3036 internal die temp)
Fan 0	: 3372 rpm
Fan 1	: 4150 rpm
Fan 2	: 3876 rpm



Main Board Volta	ges :	
ispPAC_POWR122	20AT8 :	
	: VDD_0V9	0.90V sense 0.922 V
	: VDD_0V85	0.85V sense 0.872 V
	: VDD_1V8	1.80V sense 1.838 V
	: VDD_1V5	1.50V sense 1.538 V
	: VDD_3V3	3.30V sense 3.354 V
	: VDD_SW_1V8	1.80V sense 1.846 V
	: VDD_SW_1V0	1.00V sense 1.018 V
	: VDD_PHY_0V9	0.90V sense 0.924 V
	: 3V3_SB	3.30V sense 3.354 V
	: VDD_CPU	0.88V sense 0.886 V
	: DDR3_VTT	0.77V sense 0.758 V
	: VCC5	5.00V sense 4.998 V

第10步: 如何查询 MD 控制器间的 cluster 工作状态以及如何排除 cluster 在 L2 和 L3 之间 的故障切换

(LabX-MM-1) [mynode] #cd labX-md1

(LabX-MM-1) [00:0c:29:82:71:b4] #

(LabX-MM-1) [00:0c:29:82:71:b4] #mdc

Redirecting to Managed Device Shell

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

Cluster Enabled, Profile Name = "labX-cluster"

Redundancy Mode On

Active Client Rebalance Threshold = 20%

Standby Client Rebalance Threshold = 40%

Unbalance Threshold = 5%

Heartbeat Threshold = 500 msec



AP Load Balancing: Enabled						
Active AP Rebalance Threshold = 20%						
Active AP Unbalance Threshold = 5%						
Active AP Rebalance AP Count = 50						
Active AP Rebalance Timer = 1 minutes						
Cluster Info Table						
Type IPv4 Address Priority Connection-Type STATUS						
self 10.2.10.11 128 N/A CONNECTED (Member)						
peer 10.2.10.12 128 <mark>L2-Connected CONNECTED</mark> (Leader, last HBT_RSP 68ms ago, RTD = 1.764 ms)						

我们模拟仅仅在 labX-md1 节点下新增一个 vlan 1000, 而在 labX-md2 上没有新增该 vlan 1000.

(labX-md1) [MDC] #show vlan					
VLAN CONFIGURA	ATION				
VLAN Description	n Ports	AAA Prof	ile Option-82		
1 Default G	E0/0/0-0/2 Pc0	-7 N/A	Disabled		
30 VLAN0030	GE0/0/0	N/A	Disabled		
100 VLAN0100	GE0/0/0	N/A	Disabled		
220 VLAN0220	GE0/0/0	N/A	Disabled		
1000 VLAN1000	GE0/0/0	N/A	Disabled		
(labX-md2) [MDC]	#show vlan				



VLAN CONFIGURATION

VLAN Description Ports AAA Profile Option-							
1	Default G	E0/0/0-0/2 Pc0-7	N/A	Disabled			
30	VLAN0030	GE0/0/0	N/A	Disabled			
100	VLAN0100	GE0/0/0	N/A	Disabled			
220	VLAN0220	GE0/0/0	N/A	Disabled			

接着,你在 labX-md1 上会发现集群状态变成 L3-Connected

<mark>(labX-md1)</mark> [MDC] #show lc-cluster group-membership
Cluster Enabled, Profile Name = "labX-cluster"
Redundancy Mode On
Active Client Rebalance Threshold = 20%
Standby Client Rebalance Threshold = 40%
Unbalance Threshold = 5%
Heartbeat Threshold = 500 msec
AP Load Balancing: Enabled
Active AP Rebalance Threshold = 20%
Active AP Unbalance Threshold = 5%
Active AP Rebalance AP Count = 50
Active AP Rebalance Timer = 1 minutes
Cluster Info Table
Type IPv4 Address Priority Connection-Type STATUS



self	10.2.10.11	128	N/A CONNECTED (Member)	
peer	10.2.10.12	128	L3-Connected CONNECTED (Leader, last HBT_RSP 50ms ago, RTD = 1.739 ms)	

可以查看到该 labX-md1 出现 L3 Connected 的原因,就是在 VLAN 1000 上有 vlan-

probe	e 失败									
(labX-m	nd1) [MDC] #	show lc-	cluster vl	an-prob	e statu	IS				
Cluster	VLAN Probe	Status								
Type IP OP	v4 Address	REQ-SE	NT REQ-F	AIL ACK	SENT	ACK-F	AIL RE	Q-RCVD A	CK-R	CVD <mark>VLAN_FAIL</mark> CONN-TYPE START/ST
peer	10.2.10.12	42	0 6	0	6	6	<mark>1000</mark>	<mark>L3 Conn</mark>	4/	4

解决办法:在 labX-md1 的设备节点下设置 vlan-probe 排除 vlan 1000

(LabX-MM-1) [00:0c:29:82:71:b4] (config) #lc-cluster exclude-vlan 1000

(LabX-MM-1) ^[00:0c:29:82:71:b4] (config) #write me

重新在 labX-md1 上查看下 vlan-probe 状态,已经变成 L2 Connected 的了

(labX-md1) [MDC] #lc-cluster start-vlan-probe (重新触发一次 vlan probe 请求)	
(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 10.2.10.12 54 0 7 0 7 9 0 <mark>L2 Conn</mark> 3/ 3	

第11步: 如何在建立集群的 MD 控制器上查看用户的 UAC, S-UAC 和负载均衡情况



在当前 labX-md1 控制器上,查看所有以该控制器作为 UAC 的用户信息							
(labX-md1) [MDC] #show aaa cluster essid-all users							
Active Users for ESSID : aruba-test							
BUCKET MAC IP Active UAC Standby UAC							
105 50:a7:2b:5b:25:17 192.168.100.1 10.2.10.11 10.2.10.12							

在当前 labX-md1 控制器上,查看所有以该控制器作为 S-UAC 的用户信息

(labX-md´	1) [MDC] #	#show aaa cl	uster essic	I-all users standby	
Dormant	Users				
ESSID	<mark>BUCKET</mark>	MAC	IP	Active UAC Standby UAC	
<mark>aruba-tes</mark>	s <mark>t 160 7</mark>	<mark>/c:01:91:a8:a2</mark>	aa 192.16:	8.100.2 10.2.10.12 10.2.10.11	

在当前 labX-md1 控制器上,得到了每个用户的 BUCKET ID,就可以了解该用户的选择 UAC 和 S-UAC 的对应关系。

(labX-md1) [MDC] #show sapm-bucketmap						
SAPM Bucketmap						
Item	Value					
Essid	aruba-ap					
Status	Bucketmap not published					



当然你也可以基于特定的 AP 来显示每个用户的 BUCKET ID, 就可以了解该用户的选择 UAC 和 S-UAC 的对应关系。

(labX-md1) [MDC] #show ap remote debug bucketmap sapd ap-name LAB2-AP1

Bucket map for es	sid aruba-test (Rcvd at Sat Mar 28 17:45:15 2020 [15m:22s ago]);gen_num=3
Item	Value
Essid	aruba-test
UAC 0	10.2.10.12
UAC 1	10.2.10.11
Active Map [0-31] 01	00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
Active Map [32-63 01] 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
Active Map [64-95 01] 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00
Active Map [96-12 0 01	7] 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 0
Active Map [128-1 0 01	59] 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 0
Active Map [160-1 0 01	91] 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 0
Active Map [192-2 0 01	23] 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 0
Active Map [224-2 0 01	55] 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 0
Standby Map [0-3 ⁻ 1 00	1] 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 0
Standby Map [32-6 1 00	63] 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 0
Standby Map [64-9 1 00	95] 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 0



Standby Map [96-127] 01 00	01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00	
Standby Map [128-159] 01 00	01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00	
Standby Map [160-191] 01 00	01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00	
Standby Map [192-223] 01 00	01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00	
Standby Map [224-255] 01 00	01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00	
L2 Connectedness [0-31]	111111111111111111111111111111111111111	
L2 Connectedness [32-63]	111111111111111111111111111111111111111	
L2 Connectedness [64-95]	111111111111111111111111111111111111111	
L2 Connectedness [96-127]] 111111111111111111111111111111111	
L2 Connectedness [128-15	9] 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
L2 Connectedness [160-19	1] 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
L2 Connectedness [192-22	71 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
	5]	

在集群中的任何一个 MD 控制器上,可以显示 AP 和 Client 在集群的各个 MD 间的负载情况(由于 lab 环境中的 AP 和 Client 数量有限,仅供参数)

(labX-md1) [MDC] #show lc-cluster load distribution								
Cluster Load Distribution for APs								
Type IPv4 Address Active APs Standby APs								
self	10.2.10.11	0	1					
peer	peer 10.2.10.12 1 0							
Total: Active APs 1 Standby APs 1								



(labX-	abX-md1) [MDC] #show lc-cluster load distribution client								
Cluster Load Distribution for Clients									
Type l	Pv4 Address	Active Clients S	Standby Clients						
self	10.2.10.11	0	1						
peer	10.2.10.12	1	0						
Total: Active Clients 1 Standby Clients 1									

第12步: 如何查看 MM 和 MD 控制器历史的每次重启的时间点和系统原因。

(labX-md1) [MDC] #show boot history	,					
Reboot History Table						
No Description	User	Role	IP	Tin	nestamp)
					-	
1 Reboot Cause: Power Cycle (Intent:	cause: 0:0)	system	-		-	Tue Mar 24 12:56:13 2020
2 Reboot Cause: User reboot (Intent:	cause: 86:50)	system		-	-	Tue Mar 24 13:00:47 2020
3 Controller Reboot initiated.	seamles	ss-logon-	w star	ndard	10.2.5	0.11 Tue Mar 24 13:50:40 2020
4 Reboot Cause: User reboot (Intent:	cause: 86:50)	system		-	-	Tue Mar 24 13:54:26 2020
5 Reboot Cause: Halt reboot (Intent:	ause: 86:50)	system		-	-	Wed Mar 25 10:09:54 2020
6 Reboot Cause: Halt reboot (Intent:	ause: 86:50)	system		-	-	Thu Mar 26 08:49:19 2020
7 Reboot Cause: Halt reboot (Intent:	ause: 86:50)	system		-	-	Fri Mar 27 08:38:54 2020
8 Reboot Cause: Halt reboot (Intent:	ause: 86:50)	system		-	-	Sat Mar 28 09:55:26 2020
9 Reboot Cause: Halt reboot (Intent:	ause: 86:50)	system		-	-	Sun Mar 29 12:44:55 2020

对重启的各种原因做个解释

(xx) #show boot history



Reboot History Table				
No Description	Licor Polo ID	Timost		
No Description	USEI KUIE IF	Timesta	amp	
1 Reboot Cause: User reboot (Intent:cause:reg - <mark>管理员通过 telnet/ssh 重启 AC</mark>	jister 78:86:0)	admin root 10	01.225.89.0	Sat Oct 3 08:41:20 2015
2 Reboot Cause: Power Failure (Intent:cause:re <mark>电源故障</mark>	egister ee:ee:0)	admin root 1	01.225.89.0	Mon Dec 7 09:10:12 2015
3 Controller Reboot initiated from Web-Ul. <mark>理员采用 web Ul(http 浏览器)重启 AC</mark>	adm	in root 192.16	8.89.90 Mor	n Dec 7 09:17:40 2015管
4 Reboot Cause: User reboot (Intent:cause:reg	gister 78:86:0)	admin root 10	01.225.89.0	Mon Dec 7 09:20:05 2015
5 Reboot Cause: License expired (Intent:cause <mark>授权到期,控制自重启</mark>	register bc:86:0) admin root 1	101.225.89.0	Sat Dec 26 00:03:17 2015
6 Reboot Cause: Power Failure (Intent:cause:re	egister ee:ee:0)	admin root 1	01.225.89.0	Thu Feb 18 08:52:26 2016
7 Reboot Cause: Power Failure (Intent:cause:re	egister ee:ee:0)	admin root 1	01.225.89.0	Thu Feb 25 19:31:13 2016
8 Controller Reboot initiated.	admin roo	t serial-console	e Thu Feb 25	20:16:08 2016 <mark>管理员通过</mark>
8 Controller Reboot initiated. <mark>console 串口重启 AC(包括初始化配置后的自动重</mark>	admin roo <mark>i启过程)</mark>	t serial-console	e Thu Feb 25	20:16:08 2016 <mark>管理员通过</mark>
 8 Controller Reboot initiated. console 串口重启 AC (包括初始化配置后的自动重 9 Reboot Cause: User reboot (Intent:cause:reg 	admin roo <mark>启过程)</mark> gister 78:86:0)	t serial-console admin root 10	e Thu Feb 25 01.225.89.0	20:16:08 2016 <mark>管理员通过</mark> Thu Feb 25 20:18:28 2016
 8 Controller Reboot initiated. console 串口重启 AC (包括初始化配置后的自动重 9 Reboot Cause: User reboot (Intent:cause:reg 10 Reboot Cause: User reboot (Intent:cause:reg 	admin roo <mark>i启过程)</mark> gister 78:86:0) gister 78:86:0)	t serial-console admin root 10 admin root 1	e Thu Feb 25 01.225.89.0 01.225.89.0	20:16:08 2016 <mark>管理员通过</mark> Thu Feb 25 20:18:28 2016 Thu Feb 25 20:23:12 2016
 8 Controller Reboot initiated. console 串口重启 AC (包括初始化配置后的自动重 9 Reboot Cause: User reboot (Intent:cause:reg 10 Reboot Cause: User reboot (Intent:cause:reg 11 Controller Reboot initiated. 	admin roo <mark>追己程)</mark> gister 78:86:0) gister 78:86:0) admin roo	t serial-console admin root 10 admin root 1 ot serial-consol	e Thu Feb 25 01.225.89.0 01.225.89.0 le Fri Feb 26	20:16:08 2016 <mark>管理员通过</mark> Thu Feb 25 20:18:28 2016 Thu Feb 25 20:23:12 2016 01:59:46 2016
 8 Controller Reboot initiated. console 串口重启 AC (包括初始化配置后的自动重 9 Reboot Cause: User reboot (Intent:cause:reg 10 Reboot Cause: User reboot (Intent:cause:reg 11 Controller Reboot initiated. 12 Reboot Cause: User reboot (Intent:cause:reg 	admin roo <mark>庐过程)</mark> gister 78:86:0) gister 78:86:0) admin roo gister 78:86:0)	t serial-console admin root 10 admin root 1 ot serial-consol admin root 1	e Thu Feb 25 01.225.89.0 01.225.89.0 le Fri Feb 26 01.225.89.0	20:16:08 2016管理员通过 Thu Feb 25 20:18:28 2016 Thu Feb 25 20:23:12 2016 01:59:46 2016 Fri Feb 26 02:02:06 2016
 8 Controller Reboot initiated. console 串口重启 AC (包括初始化配置后的自动重 9 Reboot Cause: User reboot (Intent:cause:reg 10 Reboot Cause: User reboot (Intent:cause:reg 11 Controller Reboot initiated. 12 Reboot Cause: User reboot (Intent:cause:reg 13 Reboot Cause: Power Failure (Intent:cause:reg 	admin roo 信过程) gister 78:86:0) gister 78:86:0) admin roo gister 78:86:0) register ee:ee:0)	t serial-console admin root 10 admin root 1 ot serial-consol admin root 1 admin root 1	e Thu Feb 25 01.225.89.0 01.225.89.0 e Fri Feb 26 01.225.89.0 101.225.89.0	20:16:08 2016管理员通过 Thu Feb 25 20:18:28 2016 Thu Feb 25 20:23:12 2016 01:59:46 2016 Fri Feb 26 02:02:06 2016 Fri Feb 26 09:44:36 2016
 8 Controller Reboot initiated. console 串口重启 AC (包括初始化配置后的自动重 9 Reboot Cause: User reboot (Intent:cause:reg 10 Reboot Cause: User reboot (Intent:cause:reg 11 Controller Reboot initiated. 12 Reboot Cause: User reboot (Intent:cause:reg 13 Reboot Cause: Power Failure (Intent:cause:reg 14 Reboot Cause: Power Failure (Intent:cause:reg 	admin roo i启过程) gister 78:86:0) gister 78:86:0) admin roo gister 78:86:0) register ee:ee:0)	t serial-console admin root 10 admin root 1 ot serial-consol admin root 1 admin root 1 admin root 1	e Thu Feb 25 01.225.89.0 01.225.89.0 le Fri Feb 26 01.225.89.0 101.225.89.0 101.225.89.0	20:16:08 2016管理员通过 Thu Feb 25 20:18:28 2016 Thu Feb 25 20:23:12 2016 01:59:46 2016 Fri Feb 26 02:02:06 2016 Fri Feb 26 09:44:36 2016 Mon Feb 29 09:22:25 2016
 8 Controller Reboot initiated. console 串口重启 AC (包括初始化配置后的自动重 9 Reboot Cause: User reboot (Intent:cause:reg 10 Reboot Cause: User reboot (Intent:cause:reg 11 Controller Reboot initiated. 12 Reboot Cause: User reboot (Intent:cause:reg 13 Reboot Cause: Power Failure (Intent:cause:reg 14 Reboot Cause: Power Failure (Intent:cause:reg 15 Controller Reboot initiated. 	admin roo i启过程) gister 78:86:0) gister 78:86:0) admin roo gister 78:86:0) register ee:ee:0) register ee:ee:0) admin roo	t serial-console admin root 10 admin root 1 ot serial-consol admin root 1 admin root 1 admin root 1 ot serial-consol	e Thu Feb 25 01.225.89.0 01.225.89.0 (01.225.89.0 (01.225.89.0 (01.225.89.0) (01.225.89.0 (01.225.89.0) (01.225.89.0) (01.225.89.0)	20:16:08 2016管理员通过 Thu Feb 25 20:18:28 2016 Thu Feb 25 20:23:12 2016 01:59:46 2016 Fri Feb 26 02:02:06 2016 Fri Feb 26 09:44:36 2016 Mon Feb 29 09:22:25 2016
 8 Controller Reboot initiated. console 串口重启 AC (包括初始化配置后的自动重 9 Reboot Cause: User reboot (Intent:cause:reg 10 Reboot Cause: User reboot (Intent:cause:reg 11 Controller Reboot initiated. 12 Reboot Cause: User reboot (Intent:cause:reg 13 Reboot Cause: Power Failure (Intent:cause:reg 14 Reboot Cause: Power Failure (Intent:cause:reg 15 Controller Reboot initiated. 16 Reboot Cause: User reboot (Intent:cause:reg 	admin roo 信过程) gister 78:86:0) gister 78:86:0) admin roo gister 78:86:0) register ee:ee:0) register ee:ee:0) admin roo gister 78:86:0)	t serial-console admin root 10 admin root 1 ot serial-consol admin root 1 admin root 1 admin root 1 ot serial-consol admin root 1	e Thu Feb 25 01.225.89.0 01.225.89.0 01.225.89.0 01.225.89.0 101.225.89.0 101.225.89.0 le Mon Feb 2 01.225.89.0	20:16:08 2016管理员通过 Thu Feb 25 20:18:28 2016 Thu Feb 25 20:23:12 2016 01:59:46 2016 Fri Feb 26 02:02:06 2016 Fri Feb 26 09:44:36 2016 Mon Feb 29 09:22:25 2016 29 09:30:20 2016 Mon Feb 29 09:32:42 2016
 8 Controller Reboot initiated. console 串口重启 AC (包括初始化配置后的自动重 9 Reboot Cause: User reboot (Intent:cause:reg 10 Reboot Cause: User reboot (Intent:cause:reg 11 Controller Reboot initiated. 12 Reboot Cause: User reboot (Intent:cause:reg 13 Reboot Cause: Power Failure (Intent:cause:reg 14 Reboot Cause: Power Failure (Intent:cause:reg 15 Controller Reboot initiated. 16 Reboot Cause: User reboot (Intent:cause:reg 17 Reboot Cause: User reboot (Intent:cause:reg 	admin roo 這定过程) gister 78:86:0) gister 78:86:0) admin roo gister 78:86:0) register ee:ee:0) register ee:ee:0) admin roo gister 78:86:0) gister 78:86:0)	t serial-console admin root 10 admin root 1 ot serial-consol admin root 1 admin root 1 admin root 1 ot serial-consol admin root 1 admin root 1	e Thu Feb 25 01.225.89.0 01.225.89.0 01.225.89.0 01.225.89.0 101.225.89.0 101.225.89.0 101.225.89.0 101.225.89.0 01.225.89.0	20:16:08 2016管理员通过 Thu Feb 25 20:18:28 2016 Thu Feb 25 20:23:12 2016 01:59:46 2016 Fri Feb 26 02:02:06 2016 Fri Feb 26 09:44:36 2016 Mon Feb 29 09:22:25 2016 Mon Feb 29 09:32:42 2016 Mon Feb 29 09:31:18 2016
 8 Controller Reboot initiated. console 串口重启 AC (包括初始化配置后的自动重 9 Reboot Cause: User reboot (Intent:cause:reg 10 Reboot Cause: User reboot (Intent:cause:reg 11 Controller Reboot initiated. 12 Reboot Cause: User reboot (Intent:cause:reg 13 Reboot Cause: Power Failure (Intent:cause:reg 14 Reboot Cause: Power Failure (Intent:cause:reg 15 Controller Reboot initiated. 16 Reboot Cause: User reboot (Intent:cause:reg 17 Reboot Cause: User reboot (Intent:cause:reg 18 Controller Reboot initiated. 	admin roo 這定过程) gister 78:86:0) gister 78:86:0) admin roo gister 78:86:0) register ee:ee:0) register ee:ee:0) admin roo gister 78:86:0) gister 78:86:0) admin roo	t serial-console admin root 10 admin root 1 ot serial-consol admin root 1 admin root 1 admin root 1 ot serial-consol admin root 1 admin root 1 ot serial-consol	e Thu Feb 25 01.225.89.0 01.225.89.0 (01.225.89.0) (01.225.89.0) (01.225.89.0) (01.225.89.0) (01.225.89.0) (01.225.89.0) (01.225.89.0) (01.225.89.0) (01.225.89.0) (01.225.89.0) (01.225.89.0)	20:16:08 2016管理员通过 Thu Feb 25 20:18:28 2016 Thu Feb 25 20:23:12 2016 01:59:46 2016 Fri Feb 26 02:02:06 2016 Fri Feb 26 09:44:36 2016 Mon Feb 29 09:22:25 2016 29 09:30:20 2016 Mon Feb 29 09:32:42 2016
 8 Controller Reboot initiated. console 串口重启 AC (包括初始化配置后的自动重 9 Reboot Cause: User reboot (Intent:cause:reg 10 Reboot Cause: User reboot (Intent:cause:reg 11 Controller Reboot initiated. 12 Reboot Cause: User reboot (Intent:cause:reg 13 Reboot Cause: User reboot (Intent:cause:reg 13 Reboot Cause: Power Failure (Intent:cause:reg 14 Reboot Cause: Power Failure (Intent:cause:reg 15 Controller Reboot initiated. 16 Reboot Cause: User reboot (Intent:cause:reg 17 Reboot Cause: User reboot (Intent:cause:reg 18 Controller Reboot initiated. 19 Reboot Cause: User reboot (Intent:cause:reg 	admin roo 這定过程) gister 78:86:0) gister 78:86:0) admin roo gister 78:86:0) register ee:ee:0) register ee:ee:0) admin roo gister 78:86:0) gister 78:86:0) admin roo gister 78:86:0)	t serial-console admin root 10 admin root 1 ot serial-consol admin root 1 admin root 1 admin root 1 admin root 1 admin root 1 admin root 1 ot serial-consol admin root 1	e Thu Feb 25 01.225.89.0 01.225.89.0 01.225.89.0 01.225.89.0 101.225.89.0 101.225.89.0 01.225.89.0 01.225.89.0 01.225.89.0 le Mon Feb 2 01.225.89.0	20:16:08 2016管理员通过 Thu Feb 25 20:18:28 2016 Thu Feb 25 20:23:12 2016 01:59:46 2016 Fri Feb 26 02:02:06 2016 Fri Feb 26 09:44:36 2016 Mon Feb 29 09:22:25 2016 Mon Feb 29 09:32:42 2016 Mon Feb 29 09:41:18 2016



23 Controller Reboot initiated. admin root 192.168.89.6 Wed Apr 20 18:39:20 2016 24 Reboot Cause: User reboot (Intent:cause:register 78:86:0) admin root 101.225.89.0 Wed Apr 20 18:42:05 2016 25 Controller Reboot initiated. admin root 192.168.89.6 Thu Apr 28 16:27:57 2016 26 Reboot Cause: User reboot (Intent:cause:register 78:86:0) admin root 101.225.89.0 Thu Apr 28 16:30:19 2016 27 Controller Reboot initiated from Web-UI. admin root 192.168.89.60 Tue Jun 28 16:02:21 2016 28 Reboot Cause: User reboot (Intent:cause:register 78:86:0) admin root 101.225.89.0 Tue Jun 28 16:04:45 2016 29 Controller Reboot initiated from Web-UI. admin root 116.238.201.168 Sun Jul 3 15:45:53 2016 30 Reboot Cause: User reboot (Intent:cause:register 78:86:0) admin root 101.225.89.0 Sun Jul 3 15:48:17 2016 31 Controller Reboot initiated. admin root 192.168.89.6 Wed Jul 13 13:29:31 2016 32 Reboot Cause: User reboot (Intent:cause:register 78:86:0) admin root 101.225.89.0 Wed Jul 13 13:31:53 2016 33 Reboot Cause: Power Failure (Intent:cause:register ee:ee:0) admin root 101.225.89.0 Tue Aug 30 12:27:32 2016 34 Reboot Cause: Power Failure (Intent:cause:register ee:ee:0) admin root 101.225.89.0 Tue Sep 13 13:35:38 2016 Reboot Cause: Power Failure (Intent:cause:register ee:ee:0) admin root 101.225.89.0 Thu Sep 22 17:40:15 2016 35 36 Reboot Cause: Power Failure (Intent:cause:register ee:ee:0) admin root 101.225.89.0 Sat Oct 8 07:22:37 2016 37 Controller Reboot initiated. admin root 192.168.89.147 Sat Oct 8 07:43:55 2016 38 Reboot Cause: User reboot (Intent:cause:register 78:86:0) Sat Oct 8 07:46:15 2016 admin root 101.225.89.0 39 Upgrade through Web-UI to 6.4.3.7 on partition 1 Successful. admin root 101.85.46.174 Wed Oct 26 18:24:54 20 16 40 Controller Reboot initiated from Web-UI. admin root 101.85.46.174 Wed Oct 26 21:25:30 2016 41 Reboot Cause: User reboot (Intent:cause:register 78:86:0) admin root 101.225.89.0 Wed Oct 26 21:28:15 2016 42 Controller Reboot initiated. admin root 192.168.89.9 Tue Nov 1 12:34:01 2016

43 Reboot Cause: User reboot (Intent:cause:register 78:86:0) admin root 101.225.89.0 Tue Nov 1 12:36:19 2016
44 Upgrade through Web-UI to 6.4.4.10 on partition 0 Successful. admin root 192.168.89.11 Wed Nov 2 19:17:54 2 016

45 Controller Reboot initiated from Web-UI.

admin root 192.168.89.32 Sat Nov 5 08:50:23 2016



46 Reboot Cause: User reboot (Intent:cause:register 78:86:0) admin root 101.225.89.0 Sat Nov 5 08:53:03 2016

47 Upgrade through Web-UI to 6.4.3.10 on partition 1 Successful. admin root 192.168.89.32 Sat Nov 5 09:22:45 20 16

48 Upgrade through Web-UI to 6.4.3.10 on partition 1 Successful. admin root 192.168.89.32 Tue Nov 8 10:48:50 20 16

49 Controller Reboot initiated from Web-UI. admin root 218.3.164.126 Thu Nov 10 20:02:37 2016

50 Reboot Cause: User reboot (Intent:cause:register 78:86:0) admin root 101.225.89.0 Thu Nov 10 20:05:19 2016

第13步: 如何查看 MM 和 MD 控制器的上联口线路或者光模块通讯是否正常。

主要确认下是否有错误的 error 和 CRC 报文,上联端口是否是 TRUSTED.

(labX-md1) [MDC] #show interface gigabitethernet 0/0/0

GE 0/0/0 is up, line protocol is up

Hardware is 10 Gigabit Ethernet, address is 00:0C:29:82:71:B4 (bia 00:0C:29:82:71:B4)

Description: GE0/0/0

Encapsulation ARPA, loopback not set

speed (10 Gbps)

MTU 1500 bytes, BW is 10000 Mbit

Last clearing of "show interface" counters 0 day 4 hr 22 min 7 sec

link status last changed 0 day 4 hr 19 min 23 sec

464046 packets input, 85441353 bytes

Received 24634 broadcasts, 0 runts, 0 giants, 0 throttles

0 input error bytes, 0 CRC, 0 frame

24634 multicast, 439412 unicast

395875 packets output, 73945263 bytes

0 output errors bytes, 0 deferred

0 collisions, 0 late collisions, 0 throttles

This port is TRUSTED



(labX-md1) [MI	DC] #sho	ow por	t stats								
Port Statistics											
Port Packets	In Pack	etsOut	: Bytesl	n Byte	esOut <mark>InputErro</mark>	orBytes	Outpu	<mark>tErrorBy</mark>	tes <mark>CRCE</mark>	rrors RxNoMbuf	
GE 0/0/0 4713	16 40	2390	86697	700 7	5104826 0	0		0	0		
GE 0/0/1 0	0	0	0	0	0	0	0				
GE 0/0/2 0	0	0	0	0	0	0	0				

第14步: 如何查看 MD 控制器和 Radius 服务器之间的通讯是否正常。

(labX-md1) [MDC] #show aaa authentication-server all
Auth Server Table
Name Type FQDN IP addr AuthPort AcctPort Status Requests
Internal Local n/a 10.2.50.11 n/a n/a Enabled 0
clearpass Radius none 10.0.50.41 1812 1813 Enabled 13

采用 aaa test-server 可以测试和外置 Radius 之间通讯是否正常

(labX-md1) [MDC] #aaa test-server mschapv2 lab<mark>X</mark>-cppm lab<mark>X</mark>user lab<mark>X</mark>user

Authentication Successful

可以统计外置 Radius 服务器的平均响应时间(单位 ms,通常建议是低于 100ms 为最佳,并且 Tmout 是不应该持续增加的)

(labX-md1) [MDC] #show aaa authentication-server radius statistics

RADIUS Server Statistics



Server Acct Rq Raw Rq PAP Rq CHAP Rq MSCHAP Rq MSCHAPv2 Rq Mismatch Rsp Bad Auth Acc Rej Acct Rsp Chal Ukn Rsp Tmout AvgRspTm Tot Rq Tot Rsp Rd Err Outstanding Auths Outstanding Requests Acc-RTTS Rq Acc -RTTS Rsp ExpAuthTm Uptime SEQ

clearpass 0 22 0 0 0 12 0 0 6 8 0 20 0 2 1781 34 34 0 57 0:8:43 255/255 0 0 0 0

*AvgRspTm is in msec, Uptime is in d:h:m, SEQ is in Total/Free

Orphaned requests = 0

*ExpAuthTm is in msec and is different from AvgRspTm. ExpAuthTm is a moving average of auth server response time a nd is used in load balancing if enabled in server group in which this auth server is a part of

2.7 搜集重要信息来联系 TAC

第1步:搜集故障相关的信息

- 1) 是否只发生在个别终端还是所有终端上?
 - ----个别终端上,可能与该类型终端网卡的驱动程序有关
 - ----多个终端上,可能与无线侧和网络侧的配置等有关
- 2) 是否只发生在某个地点还是所有区域?
 - -----某个地点,可能与特定区域的 RF 信号强度, RF 周边干扰环境及 AP 的物理层故障等相关
 - -----所有区域,可能与无线侧和网络侧的配置等有关
- 3) 是否只发生在 2.4G 还是 2.4G 和 5G 都存在问题?
 - -----如果 2.4G 不好, 而 5G 正常,则很可能是射频干扰问题
 - -----如果 2.4G 和 5G 都不正常,可能与无线侧和网络侧的配置等有关
- 4) 是否只发生在某组用户?
 - -----可能与 Radius 认证故障相关
- 5) 是否只有某种应用受到影响,其他应用是否正常?



-----可能是 ACL, 路由或服务器性能有关

6) 是否只在特定时间段有影响(如每天的上网高峰期)?

-----可能与防火墙或后台业务服务器性能有关

7) 网络和应用设置最近有什么变化?

-----真实反映网络和应用的变化,有助于快速定位故障

第2步:搜集网络环境相关的信息

1) 无线网络由哪些设备组成?

-----无线控制器和 AP 的型号、版本,以及终端操作系统、无线网卡型号、驱动版本等信息

------提供更详细的网络拓扑图,例如从用户终端到 Aruba 无线控制器之间的所有网络设备的整个拓扑和相关设备厂商和型号, 标明各设备的 IP 地址及互联接口编号

- 2) 用户 VLAN 如何终结, 用户 IP 地址如何获取?
 - -----L2 user vlan, L3 user vlan, internal DHCP Server, external DHCP server
- 3) 如何对无线用户进行认证的,用户认证后的角色策略是否正确?

-----CP auth, MAC auth, 802.1xauth (EAP 方法) 是否设置正确

-----internal DB, external LDAP, external Radius 是否正常工作

----role -- based policy

4) 网络中存在哪种应用?

-----Data access, Voice (Skype or Zoom), Video (Multicast or unicast)

5) 无线控制器与有线网络连接是否正常?

-----从控制器 ping 网关地址,观察是否正常

6) Radius 服务器是否能够正常工作?

-----用" aaa test-server mschap2 <radius-server> <username> <password>" 测试 Radius 认证是否正常,并在 Radius 服务器上观察相应的日志信息

7) DNS/DHCP 服务器是否能够正常工作?

-----将控制器有线端口配置为用户 VLAN, 连接笔记本电脑, 观察是否可以获得 IP 地址

-----将 AP 的有线端口连接笔记本电脑,观察是否可以获得 IP 地址

8) AP 如何发现控制器以及无线控制器与无线 AP 之间是否通讯正常?



----检查防火墙策略是否允许无线控制器与无线 AP 之间通过以下端口/协议进行通信(要求开启这些端口):

FTP (TCP port 21)

TFTP (UDP port 69)

NTP (UDP port 123)

SYSLOG (UDP port 514)

PAPI (UDP port 8211, UDP 8209 for CPSec)

TCP 21/22 (FTP)

GRE (protocol 47)

UDP 4500 (IAP-VPN 和 RAP)

9) 最近整个网络环境中所用到的各个网元配置是否发生变更。

----请先确认当前 Aruba 无线环境的控制器相关配置是否有过变更? 如果有,具体的操作步骤和指令参数是什么?

----请先确认当前的和无线网络有关的有线网络(核心交换机,接入交换机,路由等),认证服务器,防火墙等出口网关设备,D HCP 服务器,DNS 服务器等,最近是否有过变更操作的动作?

第3步:如果此时 MM 和 MD 控制器上发现有 Crash 信息,我们需要在设备重启前,及时将系统中的这些信息保存为文件,并存在本地 flash 闪存中,接着再通过 ftp 协议将该 Crash 文件传输到本地电脑上,便于分析和查看,并可以将该文件发给 Aruba TAC 做进一步分析和处理。

如果发现有 mm 或者 md 控制器发生了 crash 信息或者其他异常故障,不能及时排除时,我们可以到相关控制器上尽快 tar crash ,注意必须是在设备重启前来完成。

首先你要确保您的控制器已经设置了 NTP Server 或者当前的 Clock 时间点是正确的(如果不正确,请给出和北京时间的差异)。 请详细和精确地记录问题第一次发生的时间点和中间经历的过程和问题详细描述。

如果有条件的话,强烈建议设置一台 syslog server 来实施监控和接收控制器的 syslog 日志,便于 TAC 的分析。

(LabX-MM-1) [mynode] #show switches debug

All Switches

IP Address MAC Name Nodepath Type Model Version Status Uptime CrashInfo Config Sync Time (sec)



10.2.50.11 00:0c:29:ab:5a:bd LabX-MM-1 /mm/mynode master ArubaMM-VA 8.6.0.3_74788 up 0d 0h 8m no 0					
10.2.10.12 00:0c:29:ea:9a:d9 labX-md2 /md/labX MD ArubaMC-VA 8.6.0.3_74788 up 0d 0h 9m no 0					
10.2.10.11 00:0c:29:82:71:b4 labX-md1 /md/labX MD ArubaMC-VA 8.6.0.3_74788 up 0d 0h 9m no 0					
如果发现有 mm 或者 md 控制器发生了 crash 信息,我们可以到各自控制器上来 tar crash					
(labX-md1) [MDC] #tar crash					
-rw-rr 1 root root 6710 Jan 5 05:38 AUDITTRAIL-HISTORY.log					
-rw-rr 1 root root 23006710 Jan 5 05:38 crash.tar (自动生成 crash 文件,并保存在本地的 flash 中)					
-rw-rr 1 root root 58 Jan 11 04:24 crash.tar_md5sum.txt					
-rw-rr 1 root root 86928 Jan 11 04:40 default.cfg					
-rw-rr 1 root root 9007 Jun 27 2013 default.cfg.2013-06-27_22-11-20					
-rw-rr 1 root root 9275 Jun 28 2013 default.cfg.2013-06-28_06-23-34					
-rw-rr 1 root root 9339 Mar 18 2014 default.cfg.2014-03-18_05-56-38					
drwxr-xr-x 4 root root 1024 Jan 5 05:41 fieldCerts					
-rw-rr 2 root root 79031 Apr 25 2017 original.cfg					
drwx 2 root root 1024 Nov 29 2016 tpm					
(labX-md1) [MDC] #copy flash: crash.tar ftp: 1.1.1.1 admin 123456 (我们通过 copy 命令,将 crash 文件复制出来到本地 电脑,然后联系 TAC 分析处理)					
上面的操作,同样适合在 mm 控制器上					

第4步:如果此时 MM 和 MD 控制器上发现有 Crash 信息或者出现异常故障,我们同时需要在设备重启前,及时将系统中日志 logs 信息保存为文件,并存在本地 flash 闪存中,接着再通过ftp 协议将该 Crash 文件传输到本地电脑上,便于分析和查看,并可以将该文件发给 Aruba TAC 做进一步分析和处理。

如果发现有 mm 或者 md 控制器发生了 crash 信息或者其他异常故障,不能及时排除时,我们可以到相关控制器上尽快 tar logs t ech-support ,注意必须是在设备重启前来完成。



首先你要确保您的控制器已经设置了 NTP Server 或者当前的 Clock 时间点是正确的(如果不正确,请给出和北京时间的差异)。 请详细和精确地记录问题第一次发生的时间点和中间经历的过程和问题详细描述。

如果有条件的话,强烈建议设置一台 syslog server 来实施监控和接收控制器的 syslog 日志,便于 TAC 的分析。

(LabX-MM-1) [mynode] #tar logs tech-support

(LabX-MM-1) [mynode] #dir

-rw-rr	1 root	root	68737 Mar 28 00:45 AUDITTRAIL-HISTORY.log
-rw-rr	1 root	root	37529 Mar 28 00:45 AUDITTRAIL-LOGIN_OUT-HISTORY.log
-rw-rr	1 root	root	152 Mar 28 11:59 blimits
-rw-rr	1 root	root	40 Mar 24 13:28 bmap
-rw-rr	1 root	root	46384 Mar 27 09:22 configbackup.tar.gz
-rw-rr	1 root	root	24532 Mar 24 13:54 default.cfg
-rw-rr	1 root	root	46384 Mar 27 09:23 default.tar.gz
drwxr-xr-x	4 root	root	4096 Mar 24 13:08 fieldCerts
-rw-rr	1 root	root	12521 Jan 8 10:59 license-backup-2020
-rw-rr	1 root	root	12604 Mar 24 15:33 license-mynode.lic
-rw-rr	1 root	root	31127 Mar 24 15:40 localdb
-rw	1 root	root	5555619 Mar 28 13:28 logs.tar.7z (系统自动生成了该日志文件名)
-rw-rr	1 root	root	18 Mar 28 09:57 mac_addr.cfg
-rw-rr	1 root	root	47500 Mar 27 09:12 reboot_config_backup.tar.gz
drwxr-xr-x	2 root	root	4096 Mar 24 13:10 upgrade-2020-03-24_13-10-02
-rw-rr z	1 root	root	51746 Mar 24 12:57 upgrade_config_backup_8.4.0.5_to_8.6.0.3_2020-03-24-12_57_14.tar.g
-rw-rr	1 root	root	5 Mar 24 13:50 vclock.time
-rw-rr	1 root	root	30575 Mar 25 21:35 wms

(LabX-MM-1) [mynode] #copy flash: logs.tar.7z ftp: 1.1.1.1 admin 123456 (我们通过 copy 命令,将 logs 文件复制出来到 本地电脑,然后联系 TAC 分析处理)



上面的操作,同样适合<mark>在 md 控制器上</mark>

第5步:如果问题发生在特定终端上,请搜集以下的相关信息来提交给 Aruba TAC 做进一步分析 和处理。

1.请提供终端设备的制造商、型号、操作系统版本,包括是否有更新文件或补丁。

2.请提供终端设备无线网卡的制造商、型号、驱动软件信息、配置参数。

- 1) Windows 7 或以上系统
 - a) 运行 CMD, 使用"netsh wlan show drivers"命令
 - b) 运行 CMD, 使用"netsh wlan show interfaces"命令

2) MacOS

- a) 同时点击按键"option"和 Wi-Fi 图标
- b) 选择"Open Wireless Diagnostics"
- c) 点击菜单栏"Window", 并选择"Utilities"
- d) 点击"Logging"图标
- e) 选择"Wi-Fi", "EAPOL", "DHCP", "DNS",并点击 "Collect Logs".
- f) 将桌面上获得的信息文件发送给 Aruba TAC
- 3) Linux 系统
- a) 在命令行中使用"lsmod"命令,针对无线 module name 设置一个记录名称
- b) 在命令行中使用 "modinfo <module name>"
- 3.请在控制器上搜集和查看该特定终端的详细的 802.11 协商报文信息。
 - 1) logging user-debug <client mac address> subcat level debugging
 - 2) show logging level verbose
 - 3) show ap debug mgmt-frames client-mac <client mac address>
 - 4) show log user-debug all | include <client mac address>
 - 5) show log user all | include <client mac address>

当你收集好了 user-debug 日志后,记住一定要关闭掉 logging 设置,这是非常重要的

no logging user-debug <client mac address> subcat level debugging



6) show auth-tracebuf mac <client mac address>

7) packet-capture destination local-filesystem

packet-capture datapath mac <client mac address>

packet-capture copy-to-flash datapath-pcap

第6步:如果问题发生在特定 AP 上,请搜集以下的相关信息来提交给 Aruba TAC 做进一步分析 和处理。

Show profle-errors (查看当前是否有配置错误)

show ap tech-support ap-name <ap name> (请至少收集三次该命令运行结果)

show ap debug system-status ap-name <ap name>

show ap debug radio-status ap-name <ap name> radio 0 advanced (5G 频段下可以查看不同速率上接收到的数据报文量)

show ap debug radio-status ap-name <ap name> radio 1 advanced (2.4G 频段可以查看不同速率上接收到的数据报文量)

有条件的话,可以利用相关工具进行抓包



Aruba 动手实验手册: ArubaOS 8 高级配置



