实验拓扑 1



注意事项:

1、本实验内容采用 6300M 物理交换机,非虚机。6300 和 VSF 共用同一套设备,可能有其他配置,注意辨别。

2、点击 6300 图标即可访问设备。

3、6300 采用 Console 连接,可以做初始化操作。

4、此实验不需要自行添加 NODE 设备,添加任何设备不会和 6300 互联互通。

5、6300只是借用 EVE 平台显示拓扑和链接设备,不要随意删除拓扑内容。

6、6300不能正常点击访问或者误删设备请点击上方菜单栏"重置 EVE"。

7、需要断电重启设备请联系管理员。



如果设备链接出现

这个界面, 需要先点击上方菜单"EVE PC",

打开 PC 远程桌面,浏览器会缓存登录信息 cookie,然后再点击其他设备就正常出现命令行界面。

# 2 UBT 配置

## 2.1 用户需求

要求交换机支持动态隧道技术,根据用户认证的身份信息确定其业务流量是 本地转发还是通过隧道到数据中心进行转发。

### 2.2 实现思路

Aruba CX 6300和6400交换机支持Dynamic Segmentation技术,支持基于用户的动态隧道(User-Based Tunneling)。

UBT可以实现基于用户认证返回的用户角色(LUR),将用户流量通过隧 道转发到Aruba无线控制器,由Aruba无线控制器统一实施防火墙策略,也可以跟 ClearPass配合实现可下载的用户角色(DUR),由ClearPass统一下发用户角色, 无需在交换机本地配置用户角色。

#### UBT支持两种类型的控制器部署模式:

- ✓ Standalone单台控制器部署方式
- ✓ Cluster多台控制器集群部署方式

## 支持的交换机型号:

- ✓ 6300F/M
- ✓ 6400

### 版本要求:

- ✓ 交换机: AOS-CX 10.4或更新
- ✓ 无线控制器: AOS 8.4或更新

#### License要求:

- ✓ 只需要在 MM /Standalone Controller 上安装许可
- ✓ 一台/一个堆叠交换机消耗与一个AP相同的License(AP、PEF)

### UBT主要由两部分组成:

- ✔ 用户角色:
  - ▶ 交换机User-Role: 用户通过交换机端口设置的MAC认证、Dot1X认证等 进行身份验证,获取到交换机User-Role (LUR或者DUR)
  - ▶ 移动控制器User-Role (Gateway Role) : 交换机本地User-Role下设置的 Gateway Role或者通过ClearPass下发的交换机User-Role下带有的Gateway Role
- ✔ 隧道:

- ▶ 交换机与移动控制器之间建立GRE隧道
- 用户通过身份认证获取到交换机User-Role,根据此User-Role下是否设置 了Gateway Role决定用户流量是否通过隧道转发到移动控制器,未设置 Gateway Role用户流量将通过交换机本地转发,设置了Gateway Role用户 流量将通过GRE隧道转发到移动控制器,并在移动控制器上给用户发配 此Gateway Role,由移动控制器实施基于此Role的状态防火墙策略和 AppRF等策略,并在移动控制器上提供此用户的可视化管理。



# 需要配置的内容如下:

 ✓ LabX-CX-CPPM上配置强制执行策略,给交换机下发LUR和DUR(带 gateway role),并创建测试账号:

用户名	密码	说明
wired-user6	123456	dot1x 认证,实现 LUR 下的 ubt
wired-user7	123456	dot1x 认证,实现 DUR 下的 ubt

- ✓ labX-6300-1上配置ubt-client-vlan、ubt zone、LUR (帯gateway role)
- ✓ 通过LabX-CX-MM在vmc1/2上的user-role authentication (gateway role)下配置vlan

#### 2.3 达成目标

熟悉基于LUR的UBT配置,以及ClearPass如何给交换机下发LUR; 熟悉基于DUR的UBT配置,以及ClearPass如何给交换机下发DUR。

## 2.4 基于 LUR 的 UBT 配置

## 2.4.1 ClearPass 配置 (GUI)

通过 EVE PC 访问 ClearPass GUI 界面。https://10.x.40.41/

第1步:添加网络设备。打开 配置 -> 网络 -> 设备 , 点右上角的 添加设

备 链接, 创建一个新的网络设备, 配置如下:

- ▶ 名称: lab<mark>X</mark>-6300
- ▶ IP 或子网地址: 10.X.11.Y(自行在 6300 设备确认 IP 地址)
- > RADIUS 恭喜密钥: aruba123 认证: aruba123
- ▶ TACACS+共享密钥: aruba123 认证: aruba123
- ▶ 供应商名称: Aruba
- ▶ 启用 RADIUS CoA:勾选 RADIUS CoA 端口: 3799

名称:	lab2-6300			
IP 或子网地址:	10.2.11.4			
	(例如, 192.168.1.10、192.3	168.1.1/24、192.168	.1.1-20 或	戊2001:db8:a0b:12f0::1)
设备组:	-			
苗述:				
RADIUS 共享密钥:			验证:	
TACACS+ 共享密钥:			验证:	
供应商名称:	Aruba	*		
言用 RADIUS 动态授权:	≤ 端口: 3799			
启用 RadSec:				

# 第1步:打开 配置 -> 身份 -> 本地用户, 点右上角的 添加用户 链接, 新

增一个用户

用户名	密码			说明			
wired—user6	123456	dot	:1x 认证,	实现 LUR <sup>-</sup>	下的 ubt		
aruba	0 配罟 » 自	份 » 木地田户	ClearPas	ss Policy Ma	nager	0	Menu 🗮
<ul> <li>□ 监视</li> <li>□ 监视</li> <li>○ 監視</li> <li>○ 配置</li> <li>- ○ 此处开始</li> <li>- ○ 服务</li> <li>● 认证</li> </ul>	● 本地用 ● ClearPas	s Policy Manager	r lists all local us	ers in the Local Us	ers page.		<ul> <li>承加用户</li> <li>▲ 导入用户</li> <li>▲ 导出用户</li> <li>▲ 导出用户</li> <li>              Account Settings      </li> </ul>
□ ② 身份)	Dn (SSO)	用户 ID	\$ 包含\$		🕂 Go Clear F	ilter	显示 20 ᅌ 记录
<ul> <li>○ 端点</li> <li>○ 静态主机列表</li> <li>○ 角色</li> <li>○ 角色映射</li> <li>添加本地用户</li> </ul>				30-			→ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○
用户 ID:	wir	ed-user6					
名称:	wir	ed-user6					
密码:	•••						
认证密码:							
启用用户:		(选中可启用本	、地用户)				
更改密码:		Check to for	ce change p	assword on n			
角色:	[0	ther]		¢			
			属性				
属性	Y		值				
1. Click to ad	d						

第2步:打开 配置 -> 强制执行-> 配置文件, 点右上角的 添加强制执行配

置文件 链接, 创建一个新的强制执行配置文件(为 ubt 用户下发 role)

- ▶ 模板: Aruba RADIUS 强制执行
- ➢ 名称: send-tunnel-mc-role

## 点 Next 按钮进入属性配置页面

1. Radius:Aruba Aruba-User-Role = tunnel-mc

强制执行配置文件			
配置文件 属性 概要	要		
模板:	Aruba RADIUS 强制执行	\$	
名称:	send-tunnel-mc-role		
说明:			
类型:	RADIUS		
操作:	● 接受 ◎ 拒绝 ◎ 删除		
设备组列表:		Remove View Details Modify	
强制执行配置文件 配置文件 属性 概要	Select		
类型	名称	值	_
1. Radius:Aruba	Aruba-User-Ro	e tunnel-m	nc
2. Click to add			

第3步:打开 配置 -> 强制执行 -> 策略,新增 wired-dot1x-enf,在强制 执行策略窗口中点 规则 选项卡,点 "Add Rule"按钮添加一条策略

> 条件: (Tips:Role EQUALS [User Authenticated])

AND (Authentication:Username CONTAINS user6)

●配置文件名: send-tunnel-mc-role

点"保存"按钮,再点"保存"按钮保存配置

E b 面板	配置»强制执行»策略 强制执行策略			
——♀ 此处开始 ——♀ 服务 ■ <del>—</del> ↓ 认证 ■ <b>— —</b> 身份	ClearPass controls networ 过滤器: 名称	k access by evaluating an enforcent	Go Clear Filter	ne service. 显示 20 🗘 记량
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	<ul> <li># 名称▲</li> <li>1. wired-dot1x-e</li> <li>2. wired-mac-au</li> <li>3. wired-portal-e</li> </ul>	类型 nf RADIUS th-enf RADIUS enf WEBAUTH	说明	
业 ➡ 网络 — ➡ Network Scan	显示最后项的前一-后一			复制 导出 删除

则彌梅菇								
		条件						
記以下所有条件:								
类型	名称	运算符	值					
L. Tips	Role	EQUALS	[User Authenticated]					
. Authentication	Username	CONTAINS	user6					
Click to add								
		强制执行配置文件						
2置文件名: [RADIUS	] send-tunnel-mc-role Move Up	1						
	Move Dow	m↓						
	Remove							
Select	to Add							
重 » 强制执行 » 策略 » 编辑 - wirec	-dot1x-enf							
制执行策略 - wired-dot	1x-enf							
医要 强制执行 规则								
则评估算法: ① 选持	肇第一个匹配 ○ 选择所有匹配							
forcement Policy Rules:								
Conditions			Actions					
(Tips:Role EQUALS [User Aut AND (Authentication:Userna	henticated]) me_CONTAINS_user6)		[RADIUS] send-tunnel-m	ic-role				
			Add Rule	Move Up ↑ Move Down ↓				

第4步:打开 配置 -> 服务, 点右上角的 添加服务 链接, 创建一个新的服

▶ 类型: 802.1X 有线

务

- ➢ 名称: wired-dot1x-auth
- 匹配项:以下所有条件

≻ 匹配规则:

- 1. Radius:IETF NAS-Port-Type EQUALS Ethernet (15)
- 2. Radius:IETF Service-Type BELONGS\_TO Login-User (1),

Framed-User (2), Authenticate-Only (8)

3. Radius:IETF NAS-IP-AddressEQUALS 10.X.11.4

a	ruba					ClearPas	s Policy Ma	nager		Menu	Ξ
E	面板	0	配置»	服务							_
	监视	<b>0</b> ⊙	服务						N	<ul> <li>▲ 示</li> <li>▲ 导</li> <li>▲ 导</li> </ul>	加服务 入服务 出服务
-	此处开始 服务 认证		This p autho	age : rizati	shows ion.	the current list and order	of services that	ClearPass fol	llows during authentication and		
±	2 身份		过滤器	: 名和	称	\$ 包含\$			o Clear Filter 显示	20 3	€ 记录
	▶ 安全状况 ■ 22割地 〜		#		顺序	名称		类型	模板	状态	
±-4	网络		1.		1	[Policy Manager Admir Service]	n Network Login	TACACS	TACACS+ Enforcement	0	
-4	Network Scan		2.		2	[AirGroup Authorizatio	n Service]	RADIUS	RADIUS Enforcement ( Generic )	0	
-4	了 東哈10 具		3.		3	[Aruba Device Access	Service]	TACACS	TACACS+ Enforcement		
服务	身份验证 角色	强制 摘要									
类型:		802.1X无线			۲						
名称:		wired-dot1x-auth				]					
描述:		802.1% 无线访问服势	务								
监视核	武:	□ 启用以监视无强制	则的网络访问								
更多设	项:	□ 授权 □ 状况合規	現性 🗏 审核	终端主	机回分	「満点□ 记帐代理					
maa		514.		_			服务规则				
enan	○ 山内助 ○ 以下所有: 类型	JUT:	_	8	称		运算符	_	值		
1.	Radius:IETF			N	AS-Port-T	ype	EQUALS		Wireless-802.11 (19)	Ba	*
2.	Radius:IETF			Se	ervice-Typ	le l	BELONGS_TO		Login-User (1), Framed-User (2), Authenticat Only (8)	e- Ra	맘
з.	Radius:IETF			N	AS-IP-Ad	dress	EQUALS		10.2.11.4	B	Ť
4	Click to add										

第5步:设置认证方法和认证源



配置 » 服务 » 添加
服务
服务 认证 角色 强制执行 概要
认证方法: [EAP PEAP] [EAP MSCHAPv2] Move Up↑ Move Up↑ Move Down↓ Remove View Details Modify
认证源: [Local User Repository] [Local SQL DB] Move Up↑ Move Down↓ Remove View Details Modify Select to Add ◆
剥离用户名规则: □ 启用以指定以逗号分隔的规则列表,用于剥离用户名前缀或后缀
Service Certificate:Select to Add

# 第6步:角色中的角色映射策略保持默认,即未设置角色映射规则

配置》周	服务 » 济	家力口			
服穷					N
服务	认证	角色	强制执行	概要	
角色映射	İ策略:		Select	(	Modify
					角色映射策略详细信息
说明:			-		
默认角色	9:		-		
规则评估	算法:		-		
条	<b>‡</b>	C			角色

# 第7步:在强制策略选择之前创建的 wired-dot1x-enf, 然后保存

服务 - ubt		
概要 服务 认证 角柱	强制执行	
使用缓存的结果:	□ 使用从上一会话中缓存的角色和安全状况属性	
强制执行策略:	wired-dot1x-enf V Modify	
	强制执行策略详细信息	
说明:		
默认配置文件:	[Deny Access Profile]	
规则评估算法:	first-applicable	
条件		强制执行配置文件
1. (Tips:Role EQUALS	5 [User Authenticated])	send-tunnel-mc-role

## 2.4.2 交换机配置 (CLI)

第1步:在 labX-6300-1 上配置 vlan X11, X 74, X 75, 上行接口 1/1/1

放行这些 vlan。接着配置静态路由 ip route 10.X.0.0/16 10.X.11.250,

并测试到 LabX-CX-CPPM(10.X.40.41)是否路由可达。交换默认情况

下会获取到 Vlan 1(对应 native vlan211)IP 地址:10.X.11.YY。

#### *登录到 labX-6300-1 上:*

labX-6300-1# configure terminal

LabX-6300-1(config)# interface 1/1/1

LabX-6300-1 (config-if)# vlan trunk allowed all

LabX-6300-1(config-if)# exitlabX-6300-1(config)# ip route 10.X.0.0/16 10.X.14.11.250

labX-6300-1(config)# exit

labX-6300-1# ping 10.X.43.41 vrf default

PING 10.X.40.41 (10.X.43.41) 100(128) bytes of data.

108 bytes from 10.X.43.41: icmp\_seq=1 ttl=63 time=0.614 ms

### 第2步:配置 Radius 服务器

可以通过 radius-server host 10.X.43.41 key plaintext aruba123 vrf <vrf-name>

#### NOTE

指定通过哪个 vrf 发送 radius 请求,未指定时默认表示 vrf default

#### 登录到 labX-6300-1 上:

labX-6300-1# configure terminal

labX-6300-1(config)# radius-server host 10.X.43.41 key plaintext aruba123

labX-6300-1(config)#ip source-interface radius 10.X.11.4 <-可选配置,先前步骤中应该有设置,如果没有的话,请再次设置好源接口 IP,当设置了 source-interface,交换机将始终使用此 IP 或者接口发起 radius 情况;未设置 source-interface 时,如果 radius server ip 是直连路由,将选择直连接口 ip 作为 source ip 发起 radius 请求,如果非直连路由,交换机将根据路由表选择与下一跳 ip 直连的接口 ip 作为 surce ip 发起 radius 请求</p>

第3步:配置 Radius Tracking (可选配置)。此功能用于检测 Radius 服务器

是否可用,只有 Radius 服务器可用时才向此服务器发起认证。

Radius 测试完毕后, 请通过 radius-server host 10.X.40.41 tracking disable 命令关 NOTE

闭 tracking, 以免 ClearPass 访问跟踪器中全是此用户的 Radius 认证记录。



<-交换机使

#### 第4步:配置 Radius 服务器组

可以通过 server 10.X.43.41 vrf <vrf-name>指定通过哪个 VRF 发送 radius 请求,

#### NOTE

未指定时表示 VRF default

#### 登录到 labX-6300-1 上:

labX-6300-1# configure terminal

labX-6300-1 (config)# aaa group server radius clearpass

labX-6300-1(config-sg)# server 10.X.43.41

labX-6300-1 (config-sg)# exit

#### 第5步:配置 Radius fail-through。

只有开启了 aaa authentication allow-fail-through 功能, 当第一个 Radius 服务器认

NOTE 证失败后才会到第二个 Radius 服务器进行认证,否则认证失败将直接无法接入,默认

配置下未开启该功能。

*登录到 labX-6300-1 上:* 

labX-6300-1# configure terminal

labX-6300-1 (config)# aaa authentication allow-fail-through

第6步:全局配置下开启 radius 动态授权功能,并配置 radius 动态授权客户

端。

只有开启了 dyn-authorization 才可以通过 radius 下发用户角色。

NOTE 只有开启了 dyn-authorization 并配置了 dyn-authorization client 才可以通过 radius

下发 CoA。

#### 登录到 labX-6300-1 上:

labX-6300-1# configure terminal

labX-6300-1(config)# radius dyn-authorization enable

labX-6300-1(config)# radius dyn-authorization client 10.X.43.41 secret-key plaintext aruba12 3

## 第7步:开启 Radius Accounting,设置每10分钟发送一次 Accounting

Interim(计费更新)报文。



labX-6300-1# configure terminal

labX-6300-1(config)# aaa accounting port-access start-stop interim 10 group clearpass

#### 第8步:交换机上配置 ubt-client-vlan,即 tunnel 用户保留 vlan。

登录到 labX-6300-1 上: labX-6300-1# configure terminal labX-6300-1(config)# vlan 1000

labX-6300-1(config-vlan-1000)# exit

labX-6300-1(config)# ubt-client-vlan 1000

labX-6300-1(config)# ip source-interface ubt 10.X.11.YY

#### 第9步:交换机上配置 ubt zone。

在 ubt 实验中, 所有 lab 组使用各自的 2 台 VMC(Cluster), vmc1: 10.X.41.11,

vmc2: 10.X.41.12。

primary-controller ip 和 backup-controller ip 必须为 MD 的物理接口 IP,不能指定

NOTE VRRP IP

MD Cluster 情况下,交换机通过 primary-controller ip 即可获取 cluster 信息,这里 指定 backup-controller 是为了避免 vmc1 宕机后,新上线的交换机因无法访问 vmc1,

而无法获取 cluster 信息

#### 登录到 labX-6300-1 上:

labX-6300-1# configure terminal

labX-6300-1 (config)# ubt zone test vrf default

labX-6300-1(config-ubt-test)# primary-controller ip 10.X.41.11 <-必须指定物理接口 I

Ρ

 labX-6300-1(config-ubt-test)# backup-controller ip 10.X.41.12
 <-设置 backup-cont</td>

 roller ip 可以避免 vmc1 宕机后,新上线的交换机因无法访问 vmc1,而无法获取 cluster 信息

labX-6300-1 (config-ubt-test)# enable

labX-6300-1 (config-ubt-test)# exit

#### 第10步: 交换机上配置 LUR(Local User Role), 名称为 tunnel-mc。

#### 登录到 labX-6300-1 上:

labX-6300-1# configure terminal

labX-6300-1 (config)# port-access role tunnel-mc

labX-6300-1 (config-pa-role)# gateway-zone zone test gateway-role authenticated

#### 第11步: 通过 Lab Management 页面登录 labX-6300-1 的 SSH 界面。

全局配置下开启 Dot1X 认证,并指定 Dot1X 认证的服务器组。

#### 登录到 labX-6300-1 上:

labX-6300-1# configure terminal

labX-6300-1(config)# aaa authentication port-access dot1x authenticator radius server-grou p clearpass

labX-6300-1(config)# aaa authentication port-access dot1x authenticator enable

### 第 12 步: 交换机 1/1/10 接口开启 Dot1X 认证。

#### 登录到 labX-6300-1 上:

labX-6300-1# configure terminal

labX-6300-1(config)# interface 1/1/10

labX-6300-1(config-if)# aaa authentication port-access dot1x authenticator enable

## 2.4.3 控制器配置(CLI)

第1步:针对控制器的配置,在 ubt 配置的 gateway-role(这里为 authenticated)下配置 VLAN X30,用户通过 tunnel 到 VMC 拿到此 role 会通过此 VLAN 获取 IP。本实验所有 lab 组的 VMC-1 和 VMC-2, 学员可以登录到 VMM 上进行管理和查看 VMC 的配置。

(LabX-CX-MM) [mynode] #show switches (查看下当前 mm 管理域下的控制 器状态) All Switches IP Address IPv6 Address Name Location Type Model Version Status Configuration State Config Sync Time (sec) Config ID \_\_\_\_\_ \_\_\_\_ \_\_\_\_\_ \_\_\_\_\_ 10.X.50.21 None LabX-CX-MM Building1.floor1 master ArubaMM-VA 8.6.0. 2\_73853 up UPDATE SUCCESSFUL 0 12 10.X.41.11 None LabX-CX-VMC-1 Building1.floor1 MD ArubaMC-VA 8.6.0. 2\_73853 up UPDATE SUCCESSFUL 6 12 10.X.41.12 None LabX-CX-VMC-2 Building1.floor1 MD ArubaMC-VA 8.6.0. 2\_73853 up UPDATE SUCCESSFUL 8 12 Total Switches:3 (LabX-CX-MM) [mynode] #show configuration node-hierarchy (查看下当前无线控制器的配 置路径) Default-node is not configured. Autopark is disabled. Configuration node hierarchy Config Node Name Туре System /md System /md/ubt Group /md/ubt/00:50:56:ac:60:e1 Device LabX-CX-VMC-2 /md/ubt/00:50:56:ac:bc:49 Device LabX-CX-VMC-1 /mm System /mm/mynode System

(LabX-CX-MM) [mynode] #cd /md/ubt (更改配置路径到 /md/ubt) (LabX-CX-MM) [ubt] #configure terminal Enter Configuration commands, one per line. End with CNTL/Z (LabX-CX-MM) [ubt] (config) #vlan X30 (创建 UBT 用户 VLAN) (LabX-CX-MM) ^ [ubt] (config-submode)#! (LabX-CX-MM) ^ [ubt] (config) #write memory (LabX-CX-MM) [ubt] (config) #user-role authenticated (LabX-CX-MM) [ubt] (config-submode)#vlan X30 (LabX-CX-MM) ^[ubt] (config-submode)#! (LabX-CX-MM) ^[ubt] (config-submode)#!

(LabX-CX-VMC-1) [MDC] #show rights authenticated

Valid = 'Yes'

CleanedUp = 'No'

Derived Role = 'authenticated'

Up BW:No Limit Down BW:No Limit

L2TP Pool = default-l2tp-pool

PPTP Pool = default-pptp-pool

Number of users referencing it = 0

```
Assigned VLAN = X30
```

Periodic reauthentication: Disabled

DPI Classification: Enabled

Youtube education: Disabled

Web Content Classification: Enabled

IP-Classification Enforcement: Enabled

ACL Number = 85/0

Openflow: Enabled

Max Sessions = 65535

## 2.4.4 验证结果

第1步:有线测试终端修改 Dot1X 认证用户名密码, wired-user6/123456

Advanced settings ×	
802.1X settings	
Specify authentication mode	
User authentication V Replace credentials	
Delete credentials for all users	
Enable single sign on for this network	
Perform immediately before user logon	
Perform immediately after user logon	
Maximum delay (seconds):	Windows Security X
Allow additional dialogs to be displayed during single sign on	Replace credentials
☐ This network uses separate virtual LANs for machine and user authentication	Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).
	wired-user6
OK Cancel	OK Cancel

第2步:关闭并再次开启 1/1/10 接口,以触发有线终端 Dot1X 认证

由于虚机问题,可能关闭接口不能触发,可以禁用网卡再启用。如果提示

管理员用户名密码,可以用 lab-admin/aruba123



第3步:查看有线终端 Ethernet1 网口是否正常获取 IP, 可以看到终端获取到

10.X.30.0/24 段的 IP

NOTE 终端通过 tunnel 到 vmc,在 vmc 上获取到 authenticated 角色,该角色下配置了 vlan

Don't touch!!! arubalab.net Intel(R) 82574 VIA Connectio Disabled Aruba Virtual	L Gigabit Net on Adapter	Ethernet 2 Disabled Aruba L2 Virtual Adapter	Ethernet1 Network 5 Intel(R) 82574L Gigabit Net
Network Connection Det	ails	×	
Network Connection Detail:	s:		
Property	Value	~	
Connection-specific DN Description Physical Address DHCP Enabled IPv4 Address IPv4 Subnet Mask Lease Obtained Lease Expires IPv4 Default Gateway IPv4 DHCP Server IPv4 DNS Servers IPv4 WINS Server NetBIOS over Topip En Link-local IPv6 Address IPv6 Default Gateway	arubalab.net http://) 92574_6 Ggabb 00-50-56-AC-C5-4D Yes 10.0.30.100 255.255.255.0 Monday, April 20, 2020 Tuesday, April 20, 2020 Tuesday, April 21, 2020 10.0.50.20 114.114.114.114 10.0.50.20 Yes fe80::951b:671d:b7aa.5	Network Cour 7:26:33 PM 7:31:47 PM 31a%9	
<		Close	

#### X30,终端是通过此 vlan 获取的 ip 地址,网关位于核心交换机。

# 无线控制器上的命令:

第1步:学员可以通过各自 lab 环境中的 LabX-CX-MM, 查看 ubt 用户状态,

由于各 lab 组都采用的 wired-user6 以及获取到 10.X.30.0/24 段的 IP,

请检查本组 lab 终端获取的 ip, 通过此 ip 查询用户, 记录该用户当前所处

的控制器, vmc1: 10.X.41.11, vmc2: 10.X.41.12

(LabX-CX-MM) [mynode] #show global-user-table list ip 10.X.30.100							
Global Users							
IP	MAC	2	Name	Current switch	Role		Auth
	AP name	Roaming	Essid	Bssid	Phy	Profile	
Туре	User Type						



#### 第2步:通过 mdconnect 进入用户所处的 vmc(这里为 vmc-1), 通过 show

tunneled-node-mgr tunneled-nodes 命令查看交换机建立 ubt 隧道的

SAC(主用)和 S-SAC(备用)

(LabX-CX-MM) [mynode] #cd labx-cx-vmc-1

(LabX-CX-MM) [00:50:56:ac:3d:ca] #mdconnect

(LabX-CX-VMC-1) [MDC] #show tunneled-node-mgr tunneled-nodes

Tunneled Node Table Entries

Flags: A - Active Switch Anchor Controller(A-SAC),

- S Standby Switch Anchor Controller(S-SAC),
- U Active User Anchor Controller(A-UAC),
- X Standby User Anchor Controller(S-UAC),
- C Convert BC & MC into Unicast,

NameTunneled Node MacIP AddressAge(d:h:m)KeyTunnel IndexSAC IPAddressS-SAC IP AddressA-UsersS-UsersFlags

labX-6300-1 88:3a:30:a4:0f:00 10.X.14.2 00:02:14 deed tunnel 11 10.X.41.11 10.X.41.12 1 0 AUC 第3步: show tunneled-node-mgr tunneled-users 命令查看 tunnel 用户 信息,注意核对用户 mac,可以看到用户 vlan 显示为 1000 (X30),其 中 1000 为 tunnel 用户保留 vlan (前面配置的 ubt-client-vlan), X30 为用户 vlan,即用户获取到 gateway-role (这里为 authenticated)下配 置的 vlan,可以看到用户是通过 tunnel 10 转发到控制器,可以通过 show datapath tunnel tunnel-id 10 查看该 tunnel 详细信息

(LabX-CX-VMC-1) [MDC] #show tunneled-node-mgr tunneled-users

Tunneled User Table Entries

Flags: U - User Anchor Controller(UAC),

- S Standby User Anchor Controller(S-UAC),
- T Tagged VLAN,
- A Authenticated on Tunneled Node,
- C Convert BC & MC into Unicast,

User Tunneled User Mac Tunneled Node Mac Vlan UAC IP Address Key T unnel Index Flags

wired-user6 00:50:56:ac:c5:4d 88:3a:30:a4:0f:00 1000(X30) 10.X.41.11 a tunnel 10 UAC

(LabX-CX-VMC-1) [MDC] #show datapath tunnel tunnel-id 10

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/Unkno wn 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 t unnel

n - Convert RAs to unicast(VLAN Pooling/L3 Mobility enabled), s - Split tunnel

V - enforce user vlan(open clients only), x - Striping IP, 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

Tunnel's: Session Index, Session route/cache Version Number[TSIDX SRTRCV]

#	Source	Destinatio	n Prt	Туре	MTU	VLA	٨N		Acls			
BSSID	De De	caps End	caps	RxByt	es	TxE	Bytes		Heartl	beats	TSIDX	
SRTRCV	ActvAACIP	StripIP		Flags								
		<u> </u>										
10 1	0.X.41.11	10.X.14.2	47	а	1500	0	0	0	0	0	0	
88:3a:30:a	a4:0f:00	6132	6923	388	36963		274	210	2		0 21	
14	0.0.0	0.0.0.0	E	UPRIY								

第4步:控制器上常用的 debug 命令: show station-table 、show user 、show

tunneled-node-mgr trace-buf count 10

(LabX-CX-VMC-1) [MDC] #show station-table Station Entry \_\_\_\_\_ Name Role MAC Age(d:h:m) Auth AP name Essid Ph y Remote Profile User Type \_\_\_\_\_ 00:50:56:ac:c5:4d wired-user6 authenticated 00:00:25 Yes 10.X.14.2 -1/1/10 No default-tunneled-user TUNNELED USER Station Entries: 1 (LabX-CX-VMC-1) [MDC] #show user This operation can take a while depending on number of users. Please be patient .... Users \_\_\_\_ IP MAC Name Role Age(d:h:m) Auth VPN link AP name Roaming Essid/Bssid/Phy Profile Forward mode Type Host Name User Type \_\_\_\_ 10.X.30.100 00:50:56:ac:c5:4d wired-user6 authenticated 00:00:25 Tunneled-User-80 10.X.14.2 Tunneled tunnel 10/88:3a:30:a4:0f:00/1/1/10 default-tunneled-2.1X TUNNELED USER user tunnel User Entries: 1/1 Curr/Cum Alloc:1/1 Free:0/0 Dyn:1 AllocErr:0 FreeErr:0 (LabX-CX-VMC-1) [MDC] #show tunneled-node-mgr trace-buf count 10 **TNM Trace Buffer** 

Apr 20 17:43:40	SOS	SW hb tun created	10.X.14.2	tunnel 11.
Apr 20 17:43:40	*	SW BS Ack not sent	10.X.14.2	2 bucket map absent.
Apr 20 17:43:40	gsm	Nodelist not sent	10.X.14.2	SW bootstrap ack not yet sent.
Apr 20 17:43:40	*	SW BS Ack not sent	10.X.14.2	2 bucket map absent.
Apr 20 17:43:40	gsm	Bucketmap not sent	10.X.14.2	2 SW bootstrap ack not yet sent.
Apr 20 17:43:40	<	SW Bootstrap Ack	10.X.14.2	SBY=10.X.41.12
Apr 20 19:24:16	>	User bootstrap req	10.X.14.2	00:50:56:ac:c5:4d rsvd-vid=1 vlan=1
000 key=10 role=	authe	enticated flags=6 mtu=	1500 serve	r=0.0.0.0.
Apr 20 19:24:16	SOS	User tunnel created	10.X.14.2	00:50:56:ac:c5:4d dormant=0 tunnel
Apr 20 19:24:16	gsm	Publish tun user	10.X.14.2	00:50:56:ac:c5:4d.
Apr 20 19:24:16	<	User bootstrap ack	10.X.14.2	00:50:56:ac:c5:4d assigned vlan=X3
0 L2=1 S-UAC=	10.X.4	11.12 idx=36 status=1	:Success.	

# 第5步:检查控制器上 license 的消耗: show license-usage ap

(LabX-CX-VMC-1) [MDC] # show license-usage ap				
AP Licenses				
Туре	Number			
C	<b></b>			
AP Licenses	10			
RF Protect Licenses	10			
PEF Licenses	10			
MM Licenses	10			
MC-VA Licenses	10			
MC-VA country	cn			
Controller License	True			
Overall AP License Limit	10			

AP Usage	
Туре	Count
Active CAPs	0
Active RAPs	0
Remote-node Al	Ps 0
Active MUX	0
Active PUTN	1
Total APs	1
Remaining AP C	Capacity
Type Number	
CAPs 9	
RAPs 9	

# 交换机上的命令:

第1步:在 labX-6300-1 上通过 show aaa authentication port-access interface all client-status 查看终端认证状态及用户 role,通过 show port-access role 查看该 role 的参数

*登录到 labX-6300-1 上:* 

labX-6300-1# show aaa authentication port-access interface all client-status

Port Access Client Status Details

Session Details
Port : 1/1/10
Session Time: 1500s
Authentication Details
Status : dot1x Authenticated
Auth Precedence : dot1x - Authenticated, mac-auth - Not attempted
Authorization Details
Status : Applied
labX-6300-1# show port-access role
Role Information:
Name : tunnel-mc
Type : local
Reauthentication Period :
Authentication Mode :
Session Timeout :
Client Inactivity Timeout :
Description :
Gateway Zone : test

UBT Gateway Role	: authenticated	
Access VLAN	:	
Native VLAN	:	
Allowed Trunk VLANs	:	
MTU	:	
QOS Trust Mode	:	
PoE Priority	:	
Captive Portal Profile	:	
Policy	:	

第2步:交换机上常用的 debug 命令: show ubt、show ubt state、show ubt

statistics, show ubt information, show ubt users all, show ubt users

count

登录到 labX-6300-1 上:					
labX-6300-1# show ubt					
Zone Name : test					
Primary Controller : 10.X.41.11					
Backup Controller : 10.X.41.12					
SAC HeartBeat Interval : 1					
UAC KeepAlive Interval : 60					
VLAN Identifier : 1000					
VRF Name : default					
Admin State : Enabled					
PAPI Security Key : Disabled					
labX-6300-1# show ubt state					
Local Master Server (LMS) State:					
LMS Type IP Address State					

Primary	: 10.X.41.11 read	dy_for_bootstrap			
Secondary	Secondary : 10.X.41.12 ready_for_bootstrap				
Switch Ancho	r Controller (SAC)	State:			
	IP Address	MAC Address	State		
Active	: 10.X.41.11	00:50:56:ac:3d:ca	Registered		
Standby :	10.X.41.12	00:0c:29:a3:e0:b6	Registered		
Liser Anchor	Controller/110C): 1	0 X /1 11			
		0.7.41.11			
User	Port Stat	ē	Bucket ID	Gre Kev	
00:50:56:ac:c	5:4d 1/1/10 reg	istered	36	10	
labX-6300-1#	show ubt statisti	cs			
UBT Statistics					
Control Plane	Statistics				
	Gi				
Active : 1	0.X.41.11				
Bootstrap	Tx : 1	Bootstrap	Ack Rx : 1		
Nodelist F	Rx : 0	Nodelist	Ack Tx : 0		
Bucketma	ıpRx :0	Bucketma	p Ack Tx :0		
Failover 1	x : 0	Failove	r Ack Rx : 0		
Unbootstr	ap Tx : 0	Unbootstra	p Ack Rx : 0		
Heartbeat	Tx : 10720	Heartbeat A	ck Rx : 10720		
Standby :	10.X.41.12				
Bootstrap	Tx : 1	Bootstrap	Ack Rx : 1		

```
Nodelist Rx: 0Nodelist Ack Tx: 0Bucketmap Rx: 0Bucketmap Ack Tx: 0Failover Tx: 0Failover Ack Rx: 0Unbootstrap Tx: 0Unbootstrap Ack Rx: 0Heartbeat Tx: 10720Heartbeat Ack Rx: 10720
```

```
UAC : 10.X.41.11
```

Bootstrap Tx	: 2	Bootstrap Ack Rx : 2
Unbootstrap Tx	: 1	Unbootstrap Ack Rx : 1
Keepalive Tx	: 0	Keepalive Ack Rx : 0

UAC : 10.X.41.12

Bootstrap Tx : 0	Bootstrap Ack Rx : 0
Unbootstrap Tx : 0	Unbootstrap Ack Rx : 0
Keepalive Tx : 0	Keepalive Ack Rx : 0

Data Plane Statistics

UAC	Packets Tx Pa	ackets Rx
	<u> </u>	<u></u>
10.0.50.67	: 0	0
10.X.41.11	: 1256	1500
10.X.41.12	: 0	0
labX-6300-1#	show ubt information	n
SAC Informatio	n:	
Active	: 10.X.41.11	
Standby	: 10.X.41.12	

Node List Information :
Cluster Name : selab-ubt
Node List :
10.X.41.11
10.X.41.12
Bucket Map Information :
Bucket Map Active : [0255]
Bucket ID A-UAC S-UAC Connectivity
0 10.X.41.11 10.X.41.12 L2
255 10.X.41.12 10.X.41.11 L2
labX-6300-1# show ubt users all
Displaying All UBT Users for Zone: test
Downloaded user roles are preceded by *
Port Mac-Address Tunnel Status Secondary-UserRole Failure Reason
1/1/10 00:50:56:ac:c5:4d activated authenticated/
labX-6300-1# show ubt users count
Total Number of Users using ubt Zone : test is 1

第3步:在LabX-CX-CPPM上查看访问跟踪器,可以查看到终端 dot1x 认证 成功的记录, Login Status 为 ACCEPT,点击该认证记录进入请求详细信 息界面,打开输出选项卡,强制执行配置文件为 send-tunnel-mc-role, 下发了 Aruba-User-Role 属性。

■■ 面板 图 = 面板				Co. Cloar Filter		
E 监视 □ - → Live Monitoring	⊙ 过滤器: Request ID	₹ 包含Ŧ	+	Go Clear Filter	Login Status	显示 100 → 记录 Request
访问跟踪器	# Server	Source	Osername	Service	Login Status	Timestamp •
₩ 计费	1.	RADIUS	wired-user6	wired-dot1x-auth	ACCEPT	2020/04/20 19:31:52
请求详细信息 概要 输入 输出						
强制执行配置文件:	send-tunnel-mc-role					
系统安全状况状态:	UNKNOWN (100)					
审计安全状况状态:	UNKNOWN (100)					
RADIUS 响应						
Dadius Amuka Amuka I	leas Dele humal me					
Radius:Aruba:Aruba-U	Jser-Role tunnel-mc					
2.5 基于 D	UR 的 UBT 配置					
251 0	learPass 配置(GIII)					
2.0.1 ()						
第1步:打开配	置 -> 身份 -> 本	地用户,点	右上角的 添	加用户 链接	,新	

增一个用户

用户名	密码	说明
wired-user7	123456	dot1x 认证,实现 DUR 下的 ubt

aruba	ClearPass Policy Manager	Menu 🗮
■ 面板 ○ 図 监視 ○ ※ 配置 ○ - ☆ 此处开始 - ☆ 服务	配置 » 身份 » 本地用户 本地用户 ClearPass Policy Manager lists all local users in the Local Users page.	<ul> <li>≱添加用户</li> <li>▲ 导入用户</li> <li>▲ 导出用户</li> <li>▲ 导出用户</li> <li>☑ Account Settings</li> </ul>
<ul> <li>● 认证</li> <li>● 身份</li> <li>● Single Sign-On (SSO)</li> <li>● 本地用户</li> <li>● 端点</li> <li>● 静态主机列表</li> <li>● 角色</li> <li>● 角色映射</li> </ul>	过滤器: 用户 ID ◆ 包含◆	显示 20 ◆ 记录 <del>状态</del> 导出 删除
编辑本地用户		
用户 ID:	wired-user7	
名称:	wired-user7	
密码:		
认证密码:		
启用用户:	☑ (选中可启用本地用户)	
更改密码:	Check to force change password on	
角色:	[Other]	
	属性	
属性	值 值	
1. Click to add		

#	用户 ID ▲	名称	角色	状态
1.	wired-user1	wired-user1	[Other]	Enabled
2.	wired-user2	wired-user2	[Other]	Enabled
3.	wired-user3	wired-user3	[Other]	Enabled
4.	wired-user4	wired-user4	[Other]	Enabled
5.	wired-user5	wired-user5	[Other]	Enabled
6.	wired-user6	wired-user6	[Other]	Enabled
7.	wired-user7	wired-user7	[Other]	Enabled

第 2 步:打开 配置 -> 强制执行-> 配置文件,点右上角的 添加强制执行配 置文件 链接,创建一个新的强制执行配置文件(为 ubt 用户下发 DUR)

➢ 模板: Aruba RADIUS 强制执行

➢ 名称: send-DUR-tunnel-mc2-role

## 点 Next 按钮进入属性配置页面

# 1. Radius:Aruba Aruba-CPPM-Role = <下面命令>

port-access role tunnel-mc2					
gateway-zone zone tes	st gateway-role authentica	ted			
exit					
强制执行配置文件					
配置文件 属性 概要			- $Q$		
模板:	Aruba RADIUS 强制执行	\$			
名称:	send-DUR-tunnel-mc2-role				
说明:					
类型:	RADIUS		$\overline{\mathbf{C}}$		
操作:	● 接受 ◎ 拒绝 ◎ 删除	6			
设备组列表:		Remove View Details Modify			
	Select	<b>\$</b>			
强制执行配置文件					
配置文件 属性 概要					
类型	名称		值		
1. Radius:Aruba	Aruba-CPPM-Role	-	port-access role tunnel-mc2 gateway-zone zone test gateway-role authenticated exit		
2. Click to add.					

# 第3步:打开 配置 -> 强制执行 -> 策略,在右边的窗口中点击

wired-dot1x-enf,在强制执行策略窗口中点 规则 选项卡,点 "Add Rule"

### 按钮添加一条策略

> 条件: (Tips:Role EQUALS [User Authenticated])

AND (Authentication:Username CONTAINS user7)

▶ 配置文件名: send-DUR-tunnel-mc2-role

# 点"保存"按钮,再点"保存"按钮保存配置

	面板	<ul> <li>配置 » 强制执行 » 策略</li> <li>强制执行策略</li> <li>ClearPass controls network acces</li> </ul>	ss by evaluating a	an enforcement po	olicy associated	with the service.	🍦 添加强制 🔔 导入强制 🙎 导出强制	执行策略 执行策略 执行策略
	认证	计读器, 夕玫 ▲			Go Clear Fil	ter	显示 20	▲ 记录
+-2	身份		包含 wired	**************************************	Go Clear I II		亚尔 20	• шж
±- 🖶	安全状况	# ■ 1 wired-dot1x-enf		RADIUS				
	:强制执行	2. wired-mac-auth-enf		RADIUS				
	□ 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	3. wired-portal-enf		WEBAUTH				
	网络	显示最后项的前一-后一				复	制导出	删除
强行	Network Scan 制执行策略 - wirec 褒 强制执行 规则	d-dot1x-enf				<u>, , , , , , , , , , , , , , , , , , , </u>		
ŧ0 01	山平估質法・	● 洗择第一个匹配 ◎ 洗择所有D	<b>広型</b>					
Enfo	proment Policy Pules:		_ HU					
	Conditions			Actions				
1.	(Tips:Role EQUALS [[	Jser Authenticated])		[Allow Access	Profile]			
2.	(Tips:Role EQUALS [L	Jser Authenticated])		send-vlan				
2	(Tips:Role EQUALS [l	User Authenticated])		cond omploye				
5.	AND (Authentication	1:Username CONTAINS user3	3)	send-employe	e-role			
4.	AND (Authentication	Jser Authenticated]) n:Username CONTAINS user4	4)	send-DUR-rol	e			
5.	(Tips:Role EQUALS [l	Jser Authenticated])	5)	send-tunnel-n	nc-role			
	AND (Automation	Add Rule Con	y Rule Mov	ve Up ↑ Mo	ve Down ↓			
±0 M	偏相器							
75692	Januarahulu							
			条件					
匹酉	记以下所有条件:					**		
4	类型 Trace	名称	50	运算符		值		
1.	Tips	Role	EQ			[User Authenticated]		
2.	Click to add	Userhame		INTAINS		user /	J	
			强制执行配	置文件			_	
西己的	置文件名:	ADIUS] send-DUR-tunnel-mc2-role						
			Move Up ↑ Move Down ↓ Remove					
		Select to Add		\$)				

	概要	强制执行	规则						
规	则评估	算法:	• 选持	择第一个匹	匹配 💿 选择	释所有匹配			
Er	forcer	ment Policy	Rules:						
	Con	ditions					Actions	5	
1.	(Tips AND	Role EQU (Authen	ALS [User A tication:User	Authentica rname C	ated])	user1)	[Allow Ac	ccess Profile]	
2.	(Tips AND	Role EQU (Authen	ALS [User A tication:User	Authentica rname C	ated])	user2)	send-vla	n	
3.	(Tips AND	Role EQU (Authen	ALS [User A tication:User	Authentica rname <i>C</i>	ated])	user3)	send-em	ployee-role	
4.	(Tips	Role EQU (Authen	ALS [User A tication:User	Authentica	ated])	user4)	send-DU	R-role	
5.	(Tips AND	Role EQU (Authen	ALS [User A tication:User	Authentica rname C	ated])	user6)	send-tun	nel-mc-role	
6.	(Tips AND	Role EQU (Authen	ALS [User A tication:User	Authentica rname C	ated])	user7)	[RADIUS	] send-DUR-tunnel-m	nc2-role
				A	dd Rule	Copy Rule	Move Up ↑	Move Down J E	dit Rule

## 2.5.2 交换机配置 (CLI)

本章节规划用户采用 wired-user7/123456 完成 Dot1X 认证后, ClearPass 下发 DUR

(tunnel-mc2) 到交换机,并下发此 role 的 gateway-role 为 authenticated。

基于 DUR 的 UBT, 交换机上不需要配置本地的 role(即 port-access role

NOTE tunnel-mc2),由 ClearPass 下发此 role 及 role 下的配置。

要实现 DUR, 交换机上需要安装 ClearPass HTTPS 服务器证书的根证书 (Root CA),

ClearPass 上需要创建具有下载 user role 权限的账户,这部分的内容在上一章的"通

过 Dot1X 认证实现 DUR"中已完成,这里不再介绍。

第1步:交换机上配置 ubt-client-vlan,即 tunnel 用户保留 vlan 1000,这

部分配置在"基于 LUR 的 UBT 配置"章节中已完成,此处不需要再配置。

#### 登录到 labX-6300-1 上:

labX-6300-1# configure terminal

labX-6300-1(config)# vlan 1000

labX-6300-1(config-vlan-1000)# exit

labX-6300-1(config)# ubt-client-vlan 1000

labX-6300-1(config)# ip source-interface ubt 10.X.11.4

### 第2步:交换机上配置 ubt zone, 这部分配置在"基于 LUR 的 UBT 配置"章

## 节中已完成,此处不需要再配置。

#### *登录到 labX-6300-1 上:*

labX-6300-1# configure terminal

labX-6300-1(config)# ubt zone test vrf default

labX-6300-1(config-ubt-test)# primary-controller ip 10.X.41.11

labX-6300-1(config-ubt-test)# backup-controller ip 10.X.41.12

labX-6300-1 (config-ubt-test)# enable

labX-6300-1 (config-ubt-test)# exit

## 第3步:交换机 1/1/10 接口开启 Dot1X 认证,这部分配置在"基于 LUR 的

## UBT 配置"章节中已完成,此处不需要再配置。

#### 登录到 labX-6300-1 上:

labX-6300-1# configure terminal

labX-6300-1(config)# interface 1/1/10

labX-6300-1(config-if)# aaa authentication port-access dot1x authenticator enable

# 2.5.3 控制器配置(CLI)

第1步:针对控制器的配置,在 ubt 配置的 gateway-role(这里为 authenticated)下配置 VLAN X30,用户通过 tunnel 到 VMC 拿到此 role 会通过此 VLAN 获取 IP。本实验所有 lab 组的 VMC-1 和 VMC-2,



## 2.5.4 验证结果

## 第1步:有线测试终端修改 Dot1X 认证用户名密码, wired-user7/123456

] Specify authentication mode	
User authentication $\checkmark$ Replace credentials	
Delete credentials for all users	
Enable single sign on for this network	
Perform immediately before user logon	
O Perform immediately after user logon	
Maximum delay (seconds): 10	Windows Security ×
Allow additional dialogs to be displayed during single sign on	Replace credentials
$\square$ This network uses separate virtual LANs for machine and user authentication	Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).
	wired-user7
	•••••

# 第2步:关闭并再次开启1/1/10接口,以触发有线终端 Dot1X 认证

登录到 labX-6300-1 上: labX-6300-1# configure terminal labX-6300-1(config)# interface 1/1/10 labX-6300-1(config-if)# shutdown labX-6300-1(config-if)# no shutdown

第3步:查看有线终端 Ethernet1 网口是否正常获取 IP, 可以看到终端获取到

10.X.30.0/24 段的 IP

NOTE 终端通过 tunnel 到 vmc,在 vmc 上获取到 authenticated 角色,该角色下配置了 vlan

#### Don't touch!!! Ethernet 2 Ethernet1 Network 5 Intel(R) 82574L Gigabit Net. arubalab.net Disabled all a Intel(R) 82574L Gigabit Net... and the Aruba L2 Virtual Adapter VIA Connection Disabled Aruba Virtual Adapter Network Connection Details × Network Connection Details: Property Value Connection-specific DN... arubalab.net Description Intel(B) 82574L Gigabit Network Con Physical Address 00-50-56-AC-C5-4D DHCP Enabled Yes IPv4 Address 10.0.30.100 IPv4 Subnet Mask 255.255.255.0 Lease Obtained Monday, April 20, 2020 9:55:37 PM Lease Expires Tuesday, April 21, 2020 9:55:37 PM IPv4 Default Gateway 10.0.30.250 114 114 114 114 IPv4 DNS Servers 10.0.50.20 IPv4 WINS Server NetBIOS over Topip En... Yes Link-local IPv6 Address fe80::951b:671d:b7aa:531a%9 IPv6 Default Gateway IPv6 DNS Server < Close

X30,终端是通过此 vlan 获取的 ip 地址,网关位于核心交换机。

# <mark>无线控制器上的命令:</mark>

第1步:学员可以通过各自 lab 环境中的 LabX-CX-MM, 查看 ubt 用户状态, 由于各 lab 组都采用的 wired-user7 以及获取到 10.0.30.0/24 段的 IP, 请检查本组 labX 终端获取的 IP,通过此 IP 查询用户,记录该用户当前所

处的控制器, VMC-1: 10.X.41.11, VMC-2: 10.X.41.12

(LabX-CX-MM) [mynode] #show global-user-table list ip 10.X.30.100							
Global Users							
IP	MAC	2	Name	Current switch	Role		Auth
	AP name	Roaming	Essid	Bssid	Phy	Profile	
Туре	User Type						



### 第2步:通过 mdconnect 进入用户所处的 VMC(这里为 VMC-1),通过 show

tunneled-node-mgr tunneled-nodes 命令查看交换机建立 ubt 隧道的

SAC(主用)和 S-SAC(备用)

(LabX-CX-MM) [mynode] # cd labx-cx-vmc-1

(LabX-CX-MM) [00:50:56:ac:3d:ca] #mdconnect

(LabX-CX-VMC-1) [MDC] #show tunneled-node-mgr tunneled-nodes

Tunneled Node Table Entries

Flags: A - Active Switch Anchor Controller(A-SAC),

- S Standby Switch Anchor Controller(S-SAC),
- U Active User Anchor Controller(A-UAC),
- X Standby User Anchor Controller(S-UAC),
- C Convert BC & MC into Unicast,

Name Tunneled Node Mac IP Address Age(d:h:m) Key Tunnel Index SAC IP Address S-SAC IP Address A-Users S-Users Flags

labX-6300-1 88:3a:30:a4:0f:00 10.X.14.2 00:04:13 deed tunnel 11 10.X.41.11 10.X.41.12 1 0 AUC 第3步: show tunneled-node-mgr tunneled-users 命令查看 tunnel 用户 信息,注意核对用户 mac,可以看到用户 vlan 显示为 1000 (X30),其 中 1000 为 tunnel 用户保留 vlan (前面配置的 ubt-client-vlan), X30 为用户 vlan,即用户获取到 gateway-role (这里为 authenticated)下配 置的 vlan,可以看到用户是通过 tunnel 10 转发到控制器,可以通过 show datapath tunnel tunnel-id 10 查看该 tunnel 详细信息

(LabX-CX-VMC-1) [MDC] #show tunneled-node-mgr tunneled-users

Tunneled User Table Entries

Flags: U - User Anchor Controller(UAC),

- S Standby User Anchor Controller(S-UAC),
- T Tagged VLAN,
- A Authenticated on Tunneled Node,
- C Convert BC & MC into Unicast,

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/Unkno wn 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 t unnel n - Convert RAs to unicast(VLAN Pooling/L3 Mobility enabled), s - Split tunnel V - enforce user vlan(open clients only), x - Striping IP, 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 Tunnel's: Session Index, Session route/cache Version Number[TSIDX SRTRCV] Prt Type MTU VLAN # Destination Acls Source BSSID Decaps Encaps **RxBytes** TxBytes Heartbeats TSIDX StripIP SRTRCV ActvAACIP Flags 10 10.X.41.11 10.X.14.2 1500 0 47 a 0 0 0 0 0 32 88:3a:30:a4:0f:00 0 21 81 5055 7119 14 0.0.0.0 0.0.0.0 EUPRIY

第4步:控制器上常用的 debug 命令: show station-table show user show

tunneled-node-mgr trace-buf count 10

(LabX-CX-VMC-1) [MDC] #show station-table

Station Entry

MAC Name Role Age(d:h:m) Auth AP name Essid Ph y Remote Profile User Type
00:50:56:ac:c5:4d wired-user7 authenticated 00:00:04 Yes 10.X.14.2 - 1/1/10 No default-tunneled-user TUNNELED USER
Station Entries: 1
(LabX-CX-VMC-1) [MDC] #show user
This operation can take a while depending on number of users. Please be patient
Users
IP MAC Name Role Age(d:h:m) Auth VPN link AP name Roaming Essid/Bssid/Phy Profile Forward mode Type Host Name User Type
10.X.30.10000:50:56:ac:c5:4dwired-user7authenticated00:00:05Tunneled-User-802.1X10.X.14.2Tunneledtunnel10/88:3a:30:a4:0f:00/1/1/10default-tunneled-user tunnelTUNNELEDUSER
User Entries: 1/1
Curr/Cum Alloc:1/1 Free:0/0 Dyn:1 AllocErr:0 FreeErr:0
(LabX-CX-VMC-1) [MDC] #show tunneled-node-mgr trace-buf count 10
TNM Trace Buffer
Apr 20 21:52:19 gsm Publish tun user 10.X.14.2 00:50:56:ac:c5:4d.

 Apr 20 21:52:19 <--- User bootstrap ack</td>
 10.X.14.2
 00:50:56:ac:c5:4d assignedvlan=30

 L2=1 S-UAC=10.X.41.12 idx=36 status=1:Success.

 Apr 20 21:54:46 ---> User Unbootstrap Req
 10.X.14.2
 00:50:56:ac:c5:4d reason=5, key=

 10.

 Apr 20 21:54:46 sos
 User tunnel removed
 10.X.14.2
 00:50:56:ac:c5:4d tunnel 10.

 Apr 20 21:54:46 gsm
 Delete tun user
 10.X.14.2
 00:50:56:ac:c5:4d.

 Apr 20 21:54:46 gsm
 Delete tun user
 10.X.14.2
 00:50:56:ac:c5:4d.

 Apr 20 21:54:46 sos
 User Unbootstrap Ack
 10.X.14.2
 00:50:56:ac:c5:4d key=10 status=

 1:Success.
 Apr 20 21:54:52 --->
 User bootstrap req
 10.X.14.2
 00:50:56:ac:c5:4d rsvd-vid=1 vlan=

 1000 key=10 role=authenticated flags=6 mtu=1500 server=0.0.0.0.
 Apr 20 21:54:52 sos
 User tunnel created
 10.X.14.2
 00:50:56:ac:c5:4d dormant=0 tunn

 el 10.
 Apr 20 21:54:52 gsm
 Publish tun user
 10.X.14.2
 00:50:56:ac:c5:4d.

 Apr 20 21:54:52 sos
 User bootstrap ack
 10.X.14.2
 00:50:56:ac:c5:4d.

 Apr 20 21:54:52 sos
 User bootstrap ack
 10.X.14.2
 00:50:56:ac:c5:4d.

 Apr 20 21:54:52 <---</td>
 User bootstrap ack
 10.X.14.2
 00:

# 第5步:检查控制器上 license 的消耗: show license-usage ap

(LabX-CX-VMC-1) [MDC	] # show license-usage ap
AP Licenses	
Туре	Number
6	·····
AP Licenses	10
RF Protect Licenses	10
PEF Licenses	10
MM Licenses	10
MC-VA Licenses	10
MC-VA country	cn
Controller License	True
Overall AP License Limit	10

AP Usage		
Туре	Count	
Active CAPs	0	
Active RAPs	0	
Remote-node Al	Ps 0	
Active MUX	0	
Active PUTN	1	
Total APs	1	
Remaining AP C	Capacity	
Type Number		
CAPs 9		
RAPs 9		

# 交换机上的命令:

第1步:在 labX-6300-1 上通过 show aaa authentication port-access

interface all client-status 查看终端认证状态及用户 role, 通过 show

port-access role 查看该 role 的参数

#### 登录到 labX-6300-1 上:

labX-6300-1# show aaa authentication port-access interface all client-status

Port Access Client Status Details

Client 00:50:56:ac:c5:4d, wired-user7

#### Session Details

Port : 1/1/10

Session Time : 105s

#### Authentication Details

-----

Status : dot1x Authenticated

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

Authorization Details

-----

Role : send\_DUR\_tunnel\_mc2\_role-3012-1

Status : Applied

labX-6300-1# show port-access role

Role Information:

#### Name : send\_DUR\_tunnel\_mc2\_role-3012-1

Type : clearpass

Status: Completed

Reauthentication Period	:
Authentication Mode	:
Session Timeout	:
Client Inactivity Timeout	:
Description	:
Gateway Zone	: test
UBT Gateway Role	: authenticated
Access VLAN	:
Native VLAN	:

Allowed Trunk VLANs	:	
MTU	:	
QOS Trust Mode	:	
PoE Priority	:	
Captive Portal Profile	:	
Policy	:	

# 第2步:交换机上常用的 debug 命令: show ubt、show ubt state、show ubt

statistics, show ubt information, show ubt users all, show ubt users

count

登录到 labX-6300-1 上:
labX-6300-1# show ubt
Zone Name : test
Primary Controller : 10.X.41.11
Backup Controller : 10.X.41.12
SAC HeartBeat Interval : 1
UAC KeepAlive Interval : 60
VLAN Identifier : 1000
VRF Name : default
Admin State : Enabled
PAPI Security Key : Disabled
labX-6300-1# show ubt state
Local Master Server (LMS) State:
LMS Type IP Address State
Primary : 10.X.41.11 ready_for_bootstrap
Secondary : 10.X.41.12 ready_for_bootstrap

Switch Anchor Controller (SAC) State:					
IP Address MAC Ad	ldress State				
Active : 10.X.41.11 00:50:56:	ac:3d:ca Registered				
Standby : 10.X.41.12 00:0c:29	a3:e0:b6 Registered				
User Anchor Controller(UAC): 10.X.41.11					
User Port State	Bucket ID Gre Key				
00:50:56:ac:c5:4d 1/1/10 registered	36 10				
labX-6300-1# show ubt statistics					
UBT Statistics					
Control Plane Statistics					
Active : 10.X.41.11					
Bootstrap Tx : 1	Bootstrap Ack Rx : 1				
Nodelist Rx : 0	Nodelist Ack Tx : 0				
Bucketmap Rx : 0	Bucketmap Ack Tx : 0				
Failover Tx : 0	Failover Ack Rx : 0				
Unbootstrap Tx : 0	Unbootstrap Ack Rx : 0				
Heartbeat Tx : 15655	Heartbeat Ack Rx : 15655				
Standby : 10.X.41.12					
Bootstrap Tx : 1	Bootstrap Ack Rx : 1				
Nodelist Rx : 0	Nodelist Ack Tx : 0				
Bucketmap Rx : 0	Bucketmap Ack Tx : 0				
Failover Tx : 0	Failover Ack Rx : 0				

Unbootstrap T	x : 0	Unbootstrap Ack Rx : 0
Heartbeat Tx	: 15655	Heartbeat Ack Rx : 15655
UAC : 10.X.41	.11	
Bootstrap Tx	: 7	Bootstrap Ack Rx : 7
Unbootstrap T	x :6	Unbootstrap Ack Rx : 6
Keepalive Tx	: 0	Keepalive Ack Rx : 0
UAC : 10.X.41	.12	
Bootstrap Tx	: 0	Bootstrap Ack Rx : 0
Unbootstrap T	x : 0	Unbootstrap Ack Rx : 0
Keepalive Tx	: 0	Keepalive Ack Rx : 0
Data Plane Stat	stics	
UAC	Packets Tx Packets	s Rx
UAC	Packets Tx Packets	s Rx
UAC	Packets Tx Packets	s Rx
UAC  10.0.50.67 :	Packets Tx Packets	s Rx O
UAC  10.0.50.67 :	Packets Tx Packets	o Rx
UAC  10.0.50.67 : 10.X.41.11 :	Packets Tx Packets	s Rx 0 0
UAC  10.0.50.67 : 10.X.41.11 :	Packets Tx Packets	s Rx 0 0
UAC 	Packets Tx Packets	s Rx 0 0
UAC 	Packets Tx Packets	s Rx 0 0
UAC 10.0.50.67 : 10.X.41.11 : 10.X.41.12 : labX-6300-1# sho	Packets Tx Packets	s Rx 0 0
UAC 10.0.50.67 : 10.X.41.11 : 10.X.41.12 : labX-6300-1# shc	Packets Tx Packets	s Rx 0 0
UAC 10.0.50.67 : 10.X.41.11 : 10.X.41.12 : labX-6300-1# sho SAC Information :	Packets Tx Packets	s Rx 0 0 0
UAC 10.0.50.67 : 10.X.41.11 : 10.X.41.12 : labX-6300-1# sho SAC Information :	Packets Tx Packets	s Rx 0 0
UAC 10.0.50.67 : 10.X.41.11 : 10.X.41.12 : labX-6300-1# sho SAC Information : Active :	Packets Tx Packets	s Rx 0 0

Node List Information :
Cluster Name : selab-ubt
Node List :
10.X.41.11
10.X.41.12
Bucket Map Information :
Bucket Map Active : [0255]
Bucket ID A-UAC S-UAC Connectivity
0 10.X.41.11 10.X.41.12 L2
255 10.X.41.12 10.X.41.11 L2
JabX-6300-1# show ubt users all
Displaying All LIBT Lisers for Zone: test
Downloaded user roles are preceded by *
Port Mac-Address Tunnel Status Secondary-UserRole Failure Reason
1/1/10 00:50:56:ac:c5:4d activated authenticated/
labX-6300-1# show ubt users count
TOTAL MULTIPEL OF OSEIS USING UPL 2011E . LEST IS I

第3步:在LabX-CX-CPPM上查看访问跟踪器,可以查看到终端 dot1x 认证

成功的记录, Login Status 为 ACCEPT, 点击该认证记录进入请求详细信

息界面,打开输出选项卡,强制执行配置文件为

send-DUR-tunnel-mc2-role,下发了 Aruba-CPPM-Role 属性。

画板	过滤器: Request ID	◆ 包含◆		🛨 🛛 Go 🛛 Clear Fil	ter	显示 [100 \$] 记述
Elive Monitoring	# Server	Source	Username	Service	Login Status	Request Timestamp +
	1.	RADIUS	wired-user7	wired-dot1x-aut	ACCEPT	2020/04/20 22:02:50
m						
概要 输入 输出			$\mathcal{O}$			
强制执行配置文件:	send-DUR-tunnel-mc2	2-role		2		
系统安全状况状态:	UNKNOWN (100)		~~~~			
审计安全状况状态:	UNKNOWN (100)		$\sim$			
RADIUS 响应						
Radius:Aruba:Aruba-CPPM-F	<pre>tole send_DUR_tunnel_ port-access role tu</pre>	_mc2_role-3012- nnel-mc2	1			
	gateway-zone zone	e test gateway-ro	ole authenticated			
	exit					
2.6 配置备份						
登录到 labX-6300-1 上:						
laby 6200 14 write r						
tabx-0300-1# write n	lenory					
Configuration change	es will take ti	me to proc	ess, please b	e patient.		
labX–6300–1# copy ru	unning-config c	heckpoint	task3-done-la	abX	(配置保存	
到交换机本地 flash 上)						
Configuration change	es will take ti	me to proc	ess, please b	e patient.		
labX-6300-1# show ch	neckpoint list					
CPC20200408031408						

CPC20200408032505

task2-done-labX

task3-done-labX

startup-config

CPC20200408035054

AUT020200408035118

CPC20200408100133

ZER0-labX

依次针对其他交换机 (labX-8400-1、labX-8400-2 和 labX-8400-core) 设备重复上面的配置备份 操作。