# 在无线局域网控制器中配置验证和排除有线访客 故障

# 目录

# 简介

本文档介绍如何在9800和IRCM中使用外部Web身份验证配置、验证和排除有线访客接入故障。

# 先决条件

### 要求

Cisco 建议您了解以下主题:

9800 WLC

AireOS WLC

移动隧道

ISE

假设在配置有线访客接入之前,已在两个WLC之间建立移动隧道。

这方面的内容不在本配置示例的范围之内。有关详细说明,请参阅附件标题为<u>在9800上配置移动拓</u> <u>扑</u>的文档

使用的组件

9800 WLC版本17.12.1

5520 WLC版本8.10.185.0

ISE版本3.1.0.518

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

# 在锚定到另一个catalyst 9800的catalyst 9800上配置有线访客

#### 网络图



网络拓扑

# 外部9800 WLC上的配置

# 配置Web参数映射

第1步:导航到配置>安全> Web身份验证,选择全局,验证控制器的虚拟IP地址和信任点映射,并 确保将类型设置为webauth。





注意:Web Auth intercept HTTPs是一个可选设置。如果需要HTTPS重定向,则必须启用 Web Auth intercept HTTPS选项。但是,不建议使用此配置,因为它会增加CPU使用率。

第2步:在高级选项卡下,配置客户端重定向的外部网页URL。设置"Redirect URL for Login"和 "Redirect On-Failure";"Redirect On-Success"是可选的。配置后,重定向URL的预览显示在网络身 份验证配置文件中。 O Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch\_url=https://192.0.2.1/login.html&redirect=<website-name>

#### Redirect to external server

Redirect URL for login	http://10.127.196.171/w
Redirect On-Success	http://10.127.196.171/w
Redirect On-Failure	http://10.127.196.171/w
Redirect Append for AP MAC Address	
Redirect Append for Client MAC Address	
Redirect Append for WLAN SSID	
Portal IPV4 Address	10.127.196.171
Portal IPV6 Address	X:X:X:X:X

Advanced选项卡

#### CLI 配置

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
intercept-https-enable
trustpoint TP-self-signed-3915430211
webauth-http-enable
```

注意:在此方案中,使用全局参数映射。根据要求,通过选择Add配置自定义Web参数映射 ,并在Advanced选项卡下设置重定向URL。信任点和虚拟IP设置从全局配置文件继承。

AAA设置:

第1步:创建Radius服务器:

导航到Configuration > Security > AAA,单击"Server/Group"部分下的"Add",然后在"Create AAA Radius Server"页上输入服务器名称、IP地址和共享密钥。

Configuration • > Security • >	AAA Show Me How		
+ AAA Wizard			
Servers / Groups AAA Metho	d List AAA Advanced		
+ Add X Delete			
RADIUS	Server Groups		
Create AAA Radius Server			×
Name*		Support for CoA (i)	ENABLED
Server Address*	IPv4/IPv6/Hostname	CoA Server Key Type	Clear Text
PAC Key	0	CoA Server Key (i)	
Кеу Туре	Clear Text 🔻	Confirm CoA Server Key	
Key* (i)		Automate Tester	0
Confirm Key*			
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		
Cancel			Apply to Device

RADIUS 服务器配置

#### CLI 配置

radius server ISE-Auth
 address ipv4 10.197.224.122 auth-port 1812 acct-port 1813
 key \*\*\*\*\*
 server name ISE-Auth

第2步:创建RADIUS服务器组:

在Server Groups部分下选择Add以定义服务器组,并切换要包含在组配置中的服务器。

Configurati	on - > Security - > AAA Show	w Me How
+ AAA W	fizard	
Servers / G	AAA Method List	AAA Advanced
+ Add	d × Delete	
RADIUS	Servers	Server Groups
TACAC	Create AAA Radius Server	Group
LDAP	Name*	ISE-Group
	Group Type	RADIUS
	MAC-Delimiter	none 🔻
	MAC-Filtering	none 🔻
	Dead-Time (mins)	5
	Load Balance	DISABLED
	Source Interface VLAN ID	2074 🗸 🔽
	Available Servers	Assigned Servers
		> ISE-Auth <

Radius服务器组

CLI 配置

aaa group server radius ISE-Group server name ISE-Auth ip radius source-interface Vlan2074 deadtime 5

第3步:配置AAA方法列表:

导航到AAA Method List选项卡,选择Authentication下的Add,定义Type为"login"且Group type为

"Group"的方法列表名称,并在Assigned Server Group部分下映射配置的身份验证服务器组。



身份验证方法列表

#### CLI 配置

aaa authentication login ISE-List group ISE-Group

## 配置策略配置文件

第1步:导航到配置>标签和配置文件>策略,在常规选项卡中命名您的新配置文件,并使用状态切 换功能启用它。

Configuration -> Tags & Profiles -> Policy					
	+ Add X Delete				
Ac	dd Policy Profile				
	Disabling a Policy	y or configuring it in 'Enabled' state, will	result in loss of conn	ectivity for clients assoc	iated with this Policy profile
G	eneral Access Policies	QOS and AVC Mobility	Advanced		
	Name*	GuestLANPolicy	WLAN	Switching Policy	
	Description	Enter Description	Central	I Switching	ENABLED
	Status	ENABLED	Central	I Authentication	ENABLED
	Passive Client	DISABLED	Central	I DHCP	ENABLED
	IP MAC Binding	ENABLED	Flex NA	AT/PAT	DISABLED
	Encrypted Traffic Analytics	DISABLED			
	CTS Policy				
	Inline Tagging	O			
	SGACL Enforcement	D			
	Default SGT	2-65519			

策略配置文件

第2步:在访问策略选项卡下,在锚点控制器上完成vlan映射时分配随机vlan。在本例中,配置了 vlan 1

General	Access Policies	QOS and AVC	Mobility	Advanced				
RADIUS I	Profiling	D			WLAN ACL			
HTTP TL	/ Caching				IPv4 ACL	Search or Select	•	
DHCP TL	V Caching	D			IPv6 ACL	Search or Select	•	
WLAN L	ocal Profiling				URL Filters		i	
Global St Classifica	ate of Device	Disablec	i					
Local Sul	oscriber Policy Name	Search	or Select	▼ 2	Pre Auth	Search or Select	•	
VLAN					Post Auth	Search or Select	•	
VLAN/VL	AN Group	1		<b>▼</b> (i				
Multicast	VLAN	Enter M	Multicast VLAN					

Access Policy选项卡

## 第3步:在移动选项卡下,将锚点控制器切换到主(1),并根据冗余要求选择配置辅助和第三移动隧 道

General	Access Policies	QOS and AVC	Mobility	Advanced
Mobility	Anchors			
Export An	chor			
Static IP N	Nobility	DISABLED		

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

#### Available (3)

10.106.40.11

10.76.118.75

10.76.118.74

Anchor IP

#### Selected (1)



移动映射

# CLI 配置

wireless profile policy GuestLANPolicy mobility anchor 10.76.118.70 priority 1 no shutdown

## 配置访客LAN配置文件

第1步:导航到配置>无线>访客LAN,选择添加,配置唯一的配置文件名称,启用有线VLAN,输入 有线访客用户的VLAN ID,并将配置文件状态切换到启用。

General	Security			
Profile	Name*	Guest-Profile	Client Association Limit	2000
Guest	LAN ID*	1	Wired VLAN Status	ENABLE
mDNS	Mode	Bridging •	Wired VLAN ID*	2024
Status	[	ENABLE		

访客LAN配置文件

第2步:在"安全"(Security)选项卡下,启用网络身份验证,映射网络身份验证参数映射,然后从"身 份验证"(Authentication)下拉列表中选择RADIUS服务器。

# dit Guest LAN Profile

General	Security

Layer3



访客LAN安全选项卡

CLI 配置

guest-lan profile-name Guest-Profile 1 wired-vlan 2024 security web-auth authentication-list ISE-List security web-auth parameter-map global

访客LAN映射

导航到Configuration > Wireless > Guest LAN。

在访客LAN映射配置部分下,选择添加并映射策略配置文件和访客LAN配置文件

#### Guest LAN Map Configuration

+ Add Map	
Guest LAN Map : GuestMap + Add × Delete	
Guest LAN Profile Name Y Policy Name Y	
No records available.	Profile Name Guest-Profile
Image: Image         Image: Image         0 - 0 of 0 items	Policy Name GuestLANPolicy 2
	✓ Save

访客LAN映射

#### CLI 配置

```
wireless guest-lan map GuestMap
guest-lan Guest-Profile policy GuestLANPolicy
```

# 锚点9800 WLC上的配置

# 配置Web参数映射

第1步:导航到配置>安全> Web身份验证,选择全局,验证控制器的虚拟IP地址和信任点映射,并 确保将类型设置为webauth。

Conf	iguration	Edit Web Auth Parameter				
+	Add × Delete	General Advanced	General Advanced			
	Descenter Marchlere	Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1	
	global	Maximum HTTP connections	100	Trustpoint	TP-self-signed-3 🔻	
	Web-Filter	Init-State Timeout(secs)	120	Virtual IPv4 Hostname		
⊨		Туре	webauth 👻	Virtual IPv6 Address	XIXIXIX	
		Captive Bypass Portal	0	Web Auth intercept HTTPs		
		Disable Success Window	0	Enable HTTP server for Web Auth		
		Disable Logout Window	O	Disable HTTP secure server	0	
		Disable Cisco Logo	0	for Web Auth		
		Sleeping Client Status	0	Banner Configuration		
		Sleeping Client Timeout (minutes)	720	Banner Title		
				Banner Type   None	O Banner Text	

第2步:在高级选项卡下,配置客户端重定向的外部网页URL。设置"Redirect URL for Login"和 "Redirect On-Failure";"Redirect On-Success"是可选的。

#### 配置后,重定向URL的预览显示在网络身份验证配置文件中。



#### Redirect to external server

Redirect URL for login	http://10.127.196.171/w
Redirect On-Success	http://10.127.196.171/w
Redirect On-Failure	http://10.127.196.171/w
Redirect Append for AP MAC Address	
Redirect Append for Client MAC Address	
Redirect Append for WLAN SSID	
Portal IPV4 Address	10.127.196.171
Portal IPV6 Address	X:X:X:X:X

Advanced选项卡

#### CLI 配置

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
intercept-https-enable.
trustpoint TP-self-signed-3915430211
webauth-http-enable
```

AAA设置:

第1步:创建Radius服务器:

导航到Configuration > Security > AAA,单击"Server/Group"部分下的Add,在"Create AAA Radius Server"页上,输入服务器名称、IP地址和共享密钥。

Configuration * > Security * >	AAA Show Me How		
+ AAA Wizard			
Servers / Groups AAA Metho	d List AAA Advanced		
+ Add × Delete			
RADIUS	ervers Server Groups		
Create AAA Radius Server			×
Name*		Support for CoA (i)	ENABLED
Server Address*	IPv4/IPv6/Hostname	CoA Server Key Type	Clear Text 🔻
PAC Key	0	CoA Server Key (i)	
Кеу Туре	Clear Text 🔻	Confirm CoA Server Key	
Key*		Automate Tester	0
Confirm Key*			
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		
Cancel			Apply to Device

RADIUS 服务器配置

#### CLI 配置

radius server ISE-Auth
 address ipv4 10.197.224.122 auth-port 1812 acct-port 1813
 key \*\*\*\*\*
 server name ISE-Auth

# 第2步:创建RADIUS服务器组:

在"Server Groups"部分下,选择Add以定义服务器组,并切换要包含在组配置中的服务器。

Name*	ISE-Group
Group Type	RADIUS
MAC-Delimiter	none 🔻
MAC-Filtering	none 🔻
Dead-Time (mins)	5
Load Balance	DISABLED
Source Interface VLAN ID	2081 🔻 🕄
Available Servers	Assigned Servers
	> ISE-Auth
锚点RADIUS组	
CLI 配置	
aaa group server radius ISE-Group server name ISE-Auth ip radius source-interface Vlan2081 deadtime 5	

第3步:配置AAA方法列表:

导航到AAA Method List选项卡,在Authentication下选择Add,定义Type为"login"和Group type为 "Group"的方法列表名称,并在Assigned Server Group部分下映射配置的身份验证服务器组。

Configuration • >	Security • >	AAA Show Me How			
+ AAA Wizard					
Servers / Groups	AAA Met	hod List AAA Advanced			
Authentication		+ Add × Delete			
Authorization					
Accounting		Quick Setup: AAA Authentic	cation		
		Method List Name*	ISE-List		
		Туре*	login	<b>▼</b> (i)	
		Group Туре	group	<b>▼</b> (i)	
		Fallback to local	0		
		Available Server Groups		Assigned Server Group	s
		undefined Radius-Group Test-group test-group undefined tacacs1	> < >> (	ISE-Group	

身份验证方法列表

CLI 配置

aaa authentication login ISE-List group ISE-Group

# 配置策略配置文件

第1步:导航到配置>标签和配置文件>策略,使用与外部控制器上的名称相同的名称配置策略配置 文件并启用配置文件。

Gene	ral Access Policies	QOS and AVC M	Iobility Advance	ced	
Ν	lame*	GuestLANPolicy		WLAN Switching Policy	
C	Description	Enter Description		Central Switching	ENABLED
S	Status	ENABLED		Central Authentication	ENABLED
F	Passive Client	DISABLED		Central DHCP	ENABLED
I	P MAC Binding	ENABLED		Flex NAT/PAT	DISABLED
E	ncrypted Traffic Analytics	DISABLED			
(	CTS Policy				
li	nline Tagging	O			
S	GACL Enforcement	D			
C	Default SGT	2-65519			

锚点策略配置文件

第2步:在访问策略下,从下拉列表中映射有线客户端VLAN

General	Access Policies	QOS and AVC	Mobility	Advance
RADIUS F	Profiling			
HTTP TLV	/ Caching			
DHCP TL	V Caching			
WLAN L	ocal Profiling			
Global Sta Classifica	ate of Device tion	Disabled	i	
Local Sub	oscriber Policy Name	Search	n or Select	▼ 2
VLAN				
VLAN/VL	AN Group	VLAN2	2024	• i

"访问策略"选项卡



注意:除VLAN外,策略配置文件的配置必须在外部和锚点控制器上匹配。

第3步:在移动选项卡下,选中导出锚点复选框。

General	Access Policies	QOS and AVC	Mobility	Advanced
Mobility	/ Anchors			
Export A	nchor			
Static IP	Mobility	DISABLEI	D	

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (2)	Selected (0)	
Anchor IP	Anchor IP	And

导出锚点



注意:此配置指定9800无线局域网控制器(WLC)作为与指定策略配置文件关联的任何 WLAN的锚点WLC。当外部9800 WLC将客户端重定向到锚点WLC时,它会提供有关 WLAN和分配给客户端的策略配置文件的详细信息。这使锚点WLC能够根据收到的信息应 用适当的本地策略配置文件。

CLI 配置

wireless profile policy GuestLANPolicy mobility anchor vlan VLAN2024 no shutdown

配置访客LAN配置文件

第1步:导航到配置>无线>访客LAN,然后选择添加创建并配置访客LAN配置文件。确保配置文件

# 名称与外部控制器的配置文件名称匹配。请注意,必须在锚点控制器上禁用有线VLAN。

Current LAN Configuration							
+ Add		011					
Ado	d Guest LAN Prof	ile					
Ge	eneral Security						
	Profile Name*	Guest-Profile		Client Association Limit	2000		
> Gi	Guest LAN ID*	1		Wired VLAN Status	DISABLE		
	mDNS Mode	Bridging •					
· + /	Status						

访客LAN配置文件

第2步:在安全设置中,启用Web Auth,然后配置Web Auth参数映射和身份验证列表。

# General Security Layer3 Web Auth Web Auth Parameter Map global

Authentication List

global <br/>
<br/>
ISE-List <br/>
<br/>



注意:除有线VLAN状态外,外部控制器和锚点控制器之间的访客LAN配置文件配置必须相 同

#### CLI 配置

guest-lan profile-name Guest-Profile 1
security web-auth authentication-list ISE-List
security web-auth parameter-map global

## 访客LAN映射

第1步:导航到配置>无线>访客LAN。在Guest LAN MAP configuration部分中,选择Add并将策略 配置文件映射到访客LAN配置文件。

#### Guest LAN Map Configuration

+	Add Map X Delete Map					
Guest	Add Classical Contents of Cont					
	Guest LAN Profile Name	Policy Name	<b>T</b>	Profile Name	Guest-Profile	
<b>I</b>	<ul> <li>In tems per p</li> </ul>	age 0 - 0 of 0 items	5	Policy Name	GuestLANPolicy	
				✓ Save		<b>່ວ</b> Cancel

访客LAN映射

wireless guest-lan map GuestMap guest-lan Guest-Profile policy GuestLANPolicy

# 在锚定到AireOS 5520控制器的Catalyst 9800上配置有线访客



网络拓扑

# 外部9800 WLC上的配置

## 第1步:导航到配置>安全> Web身份验证,然后选择全局。验证控制器的虚拟IP地址和信任点是否 正确映射到配置文件(类型设置为webauth)。

General Advanced			
Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-3 🔻
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Туре	webauth 🔻	Virtual IPv6 Address	X:X:X:X:X
Captive Bypass Portal	0	Web Auth intercept HTTPs	0
Disable Success Window	D	Enable HTTP server for Web Auth	
Disable Logout Window	D	Disable HTTP secure server	0
Disable Cisco Logo	0	for Web Auth	
Sleeping Client Status	0	Banner Configuration	
Sleeping Client Timeout (minutes)	720	Banner Title	
		Banner Type   None  Read	e O Banner Text I From File

Web参数映射

第2步:在高级选项卡下,指定客户端必须重定向到的外部网页URL。配置Redirect URL for Login和Redirect On-Failure。Redirect On-Success设置是可选配置。

Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch\_url=https://192.0.2.1/login.html&redirect=<website-name>

#### Redirect to external server

Redirect URL for login	http://10.127.196.171/w
Redirect On-Success	http://10.127.196.171/w
Redirect On-Failure	http://10.127.196.171/w
Redirect Append for AP MAC Address	
Redirect Append for Client MAC Address	
Redirect Append for WLAN SSID	
Portal IPV4 Address	10.127.196.171
Portal IPV6 Address	X:X:X:X:X

Advanced选项卡

## CLI 配置

parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
trustpoint TP-self-signed-3010594951
webauth-http-enable



注意:有关AAA配置,请参阅外部9800 WLC的""部分中提供的配置详细信息。

配置策略配置文件

第1步:导航到配置>标签和配置文件>策略。选择Add,然后在General选项卡中为配置文件提供名 称并启用状态切换。

General	Access Policies	QOS and AVC	Mobility	Advand	ced		
Name*	ĸ	Guest			WLAN Switching Policy		
Descri	ption	Enter Description	on		Central Switching	ENABL	.ED
Status		ENABLED	)		Central Authentication	ENABL	ED
Passiv	e Client	DISABLED	)		Central DHCP	ENABL	.ED
IP MAG	C Binding	ENABLED	)		Flex NAT/PAT		ISABLED
Encryp	oted Traffic Analytics	DISABLED	)				
CTS F	Policy						
Inline 7	Tagging	D					
SGACI	L Enforcement						
Defaul	t SGT	2-65519					

策略配置文件

第2步:在访问策略(Access Policies)选项卡中,分配随机VLAN。

General	Access Policies	QOS and AVC	Mobility	Advanced
RADIUS Pr	ofiling			
HTTP TLV	Caching	O		
DHCP TLV Caching		Ο		
WLAN Lo	cal Profiling			
Global Stat Classificati	e of Device on	Disab	led (i)	
Local Subscriber Policy Name		Sea	rch or Select	▼ 2
VLAN				
VLAN/VLA	N Group	1		• (i)
Multicast V	'LAN	Ente	er Multicast VLAN	I

访问策略

第3步:在Mobility选项卡中,切换锚点控制器并将其优先级设置为Primary (1)

General	Access Policies	QOS and AVC	Mobility	Advanced
Mobility A	Anchors			
Export And	chor			
Static IP M	lobility	DISABLE	ED	

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (1)	Selected (1)	Selected (1)		
Anchor IP	Anchor IP	Anchor Priority		
✓ 10.76.6.156 →	10.76.118.74	Primary (1)		

Mobility选项卡



注意:9800外部WLC的策略配置文件必须与5520锚点WLC的访客LAN配置文件匹配,但 vlan配置除外

#### CLI 配置

wireless profile policy Guest no accounting-interim exclusionlist timeout 180 no flex umbrella dhcp-dns-option mobility anchor 10.76.118.74 priority 1 no shutdown

## 配置访客LAN配置文件

第1步:导航到配置>无线>访客LAN,选择添加。配置唯一的配置文件名称并启用有线VLAN,指定

# 专用于有线访客用户的VLAN ID。最后,将配置文件状态切换为Enabled。

Ge	neral Security					
	Profile Name*	Guest		Client Association Limit	2000	
	Guest LAN ID*	2		Wired VLAN Status	ENABLE	
	mDNS Mode	Bridging	•	Wired VLAN ID*	11	
	Status					

访客LAN策略

第2步:在安全选项卡下,启用网络身份验证,映射Web身份验证参数映射,然后从身份验证下拉 列表中选择RADIUS服务器。

General	Security		
Layer3			
Web Auth		ENABLE	
Web Auth F	Parameter Map	global	▼
Authenticat	ion List	ISE-List	•

"安全"选项卡



注意:对于9800外部和5520锚点控制器,访客LAN配置文件名称必须相同

CLI 配置

guest-lan profile-name Guest 2 wired-vlan 11 security web-auth authentication-list ISE-List security web-auth parameter-map global

## 访客LAN映射

第1步:导航到配置>无线>访客LAN。在访客LAN映射配置部分中,选择添加,并将策略配置文件 映射到访客LAN配置文件。

Suest LAN Map Configuration					
+ Add Map X Delete Map					
Guest LAN Map : GuestMap + Add × Delete					
Guest LAN Profile Name	Policy Name				
No records av	ailable.	Profile Name Guest			
I ≤ ≤ ► ► 10 ▼ items per p	age 0 - 0 of 0 items	Policy Name Guest			
		Save Cancel			

访客LAN映射

#### CLI 配置

wireless guest-lan map GuestMap guest-lan Guest policy Guest

# 锚点5520 WLC上的配置

## 配置Web身份验证

第1步:导航到安全>网络身份验证>网络登录页面。将Web身份验证类型设置为External (Redirect to external server),并配置外部Web身份验证URL。登录后重定向URL是可选的,并且可以在客户端需要在身份验证成功之后重定向到专用页时进行配置。

ահանո			Save Configuration Ping Logout Refresh
cisco	MONITOR WLANS CONTROLLER WIRE	ELESS SECURITY MANAGEMENT COMMANDS HE	LP User:admin(ReadWrite) 🔒 Home
Security	Web Login Page		Preview Apply
AAA     General     General     Authentication     Accounting     Auth Cached Users     Fallback     DNS     Downloaded AVP     TCACC5+     LDAP     Local Net Users     MAC Filtering     Disabled Clients     User Login Policies     Ap Policies     Password Policies	Web Authentication Type Redirect URL after login Login Success Page Type External Webauth URL QrCode Scanning Bypass Timer QrCode Scanning Bypass Count	External (Redirect to external server) >>         http://10.127.196.171/webauth/logout.html         None >>         http://10.127.196.171/webauth/login.html	
Local EAP			
Advanced EAP			
Priority Order			
Certificate			
Access Control Lists			
Wireless Protection     Policies			
Web Auth     Web Login Page     Contificate			

Web身份验证设置

# AAA设置:

#### 第1步:配置RADIUS服务器

导航到Security > Radius > Authentication > New。

սիսիս		Save Configuration Ping Logout Befre
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	User:admin(ReadWrite) 🔒 🖽 or
Security	RADIUS Authentication Servers	Apply New
AAA     General     RADIUS	Auth Called Station ID Type AP MAC Address:SSID V	
Authentication	Use AES Key Wrap  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)	
Auth Cached Users	MAC Delimiter Hyphen ~	
Fallback DNS	Framed MTU 1300	
Downloaded AVP		

RADIUS 服务器

第2步:在控制器上配置RADIUS服务器IP和共享密钥。将服务器状态切换到已启用并选中网络用户 复选框。
# **RADIUS Authentication Servers > New**

Server Index (Priority)	4 ~
Server IP Address(Ipv4/Ipv6)	
Shared Secret Format	ASCII ~
Shared Secret	
Confirm Shared Secret	
Apply Cisco ISE Default settings	
Apply Cisco ACA Default settings	
Key Wrap	(Designed for FIPS customers)
Port Number	1812
Server Status	Enabled ~
Support for CoA	Disabled ~
Server Timeout	5 seconds
Network User	Enable
Management	Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	Enable
PAC Provisioning	Enable
IPSec	Enable
Cisco ACA	Enable

服务器配置

配置访问控制列表

第1步:导航到安全>访问控制列表,然后选择新建。创建预身份验证ACL,允许流量流向DNS和外

## 部Web服务器。

،،ا،،،ا،، cısco	MON	itor <u>w</u>	LANs <u>C</u> ONTR	OLLEF	R W <u>I</u> RELESS	<u>s</u>	ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HEL	P			
Security	Acc	ess Con	trol Lists > I	dit	L									
AAA     General     RADIUS	Gen	eral						_						
Authentication Accounting Auth Cached Users Fallback	Acces Deny	s List Nam Counters	e Pre-A O	uth_A	CL									
DNS Downloaded AVP	Seq	Action	Source IP/Ma	isk	Destination IP/Mask		Protocol	Source Port	Dest Port		SCP	Direction	Number of Hits	
TACACS+ LDAP Local Net Users	1	Permit	0.0.0.0 0.0.0.0	/	0.0.0.0 0.0.0.0	/	UDP	Any	DNS		Any	Any	0	•
MAC Filtering Disabled Clients	2	Permit	0.0.0.0 0.0.0.0	/	0.0.0.0 0.0.0.0	/	UDP	DNS	Any		Any	Any	0	
User Login Policies AP Policies	3	Permit	0.0.0.0 0.0.0.0	/	10.127.196.171 255.255.255.255	/	тср	Any	HTTP		Any	Any	0	
Local EAP	4	Permit	10.127.196.17 255.255.255.2	1 / 55	0.0.0.0 0.0.0.0	/	тср	HTTP	Any		Any	Any	0	
Advanced EAP	5	Permit	0.0.0.0 0.0.0.0	/	10.127.196.171 255.255.255.255	/	тср	Any	HTTPS		Any	Any	0	•
Certificate	6	Permit	10.127.196.17 255.255.255.2	1 / 55	0.0.0.0 0.0.0.0	/	ТСР	HTTPS	Any		Any	Any	0	
Access Control Lists Access Control Lists CPU Access Control Lists														

允许流量流向Web服务器的访问列表

## 配置访客LAN配置文件

第1步:导航到WLAN >选择Create New。

选择Type作为Guest LAN,并配置与9800外部控制器的策略配置文件相同的名称。

<u>M</u> ONITOR <u>W</u> LANS	ONTROLLER WIRE	ESS <u>S</u> ECURITY N	M <u>A</u> NAGEMENT	C <u>o</u> mmands	HELP
WLANS	J				
Current Filter: Non	e [ <u>Change F</u>	iter] [Clear Filter]			Create New V Go
UWLAN ID Type	Profile Name	WL	AN SSID		Admin Status Security Policies
创建访客LAN					
MONITOR WLANS CONTROLLER	WIRELESS SECURITY M	ANAGEMENT COMMANDS	HELP		User:admin(ReadWrite) n Home
WLANs > New					< Back Apply
Type Gu	est LAN 🗸				
Profile Name Gu	est				
ID 2	~				

访客LAN配置文件

第2步:在访客LAN配置文件上映射入口和出口接口。

在本例中,Ingress接口为none,因为入口接口是来自外部控制器的EoIP隧道。

出口接口是有线客户端物理连接的VLAN。

General	Security	QoS Advanced
Profile Na	ame	Guest
Туре		Guest LAN
Status		Enabled
Security	Policies	Web-Auth (Modifications done under security tab will appear after applying the changes.)
Ingress I	nterface	None ~
Egress In	terface	wired-vlan-11 V
NAS-ID		none

访客LAN配置文件

## 第3步:在"安全"选项卡下,选择第3层安全作为Web身份验证,并映射预身份验证ACL。

W	LANs > E	dit 'Guest'	1			
	General	Security	QoS Advan	ced		
(	Layer 2	Layer 3	AAA Servers			
	Layer 3 Preauthe Override	Security entication ACL e Global Config <sup>2</sup>	IPv4 Pre-Auth	h_ACL ∽ IPv6	Web Authent	ication ∨

访客LAN安全选项卡

第4步:导航到安全> AAA服务器。

选择下拉菜单并将RADIUS服务器映射到访客LAN配置文件。

General	Security	QoS	Advan	ced	
Layer 2	Layer 3		Servers		
	corvers below	w to ove	rrido uso d	f dof	ault corvers on thi
RADIUS Se	rvers	w to ove	inde use c	n uen	aut servers on th
				-	
	Authenticat	ion Serv	ers	Acco	ounting Servers
	🗹 Enabled			<u></u> П в	nabled
Server 1	IP:10.197.2	24.122,	ort:1812 >	Nor	ne
Server 2	None		~	Nor	ne
Server 3	None		~	Nor	ne
Server 4	None		~	Nor	ne

将RADIUS服务器映射到访客LAN配置文件

## 第5步:导航到WLAN。将鼠标悬停在访客LAN配置文件的下拉图标上并选择Mobility Anchors。

□ <u>2</u>	Guest LAN	Guest	 Disabled	Web-Auth	<b>P</b>
					Remove
					Mobility Anchors

## 第6步:选择Mobility Anchor Create将控制器配置为此访客LAN配置文件的导出锚点。

WLAN SSID Guest		
Switch IP Address (Anchor)	Data Path	Control Path
local	up	up
Mobility Anchor Create		

创建移动锚点

# 在锚定到catalyst 9800的AireOS 5520上配置有线访客



网络拓扑

## 外部5520 WLC上的配置

## 控制器接口配置

第1步:导航到控制器>接口>新建。配置接口名称、VLAN ID并启用访客LAN。

有线访客需要两个动态接口。

首先,创建一个第2层动态接口并将其指定为访客LAN。此接口用作访客LAN的入口接口,其中有线 客户端以物理方式连接。

،،ا،،،ا،، cısco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NA
Controller	Interface	s > Edit				
General Icons	General I	nformati	ion			
Inventory Interfaces Interface Groups	Interface MAC Addi	Name ress	wired-g a0:e0:a	uest f:32:d9:ba		
Multicast <ul> <li>Network Routes</li> </ul>	Configura	tion				
<ul> <li>Fabric Configuration</li> <li>Redundancy</li> </ul>	NAS-ID	I	none			
Ports	Physical 1	Informat	ion			
▶ NTP	Backup Po	ort				
<ul><li>CDP</li><li>PMIPv6</li></ul>	Active Por	t	1			
Tunneling	Interface	Address	_			
IPv6	VLAN Ide	ntifier		2020		
P MUNS	Enable DF	ACP Ontion	82			

Ingress 接口

第2步:导航到控制器>接口>新建。配置接口名称、VLAN ID。

第二个动态接口必须是控制器上的第3层接口,有线客户端从此vlan子网接收IP地址。此接口用作访客LAN配置文件的出口接口。

cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLEF	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAC		
Controller	Interface	s > Edit						
General Icons Inventory Interfaces Interface Groups Multicast Network Routes Fabric Configuration Redundancy Mobility Management	General I Interface MAC Add Configura Guest Lat Quarantir Quarantir	n Name ress ntion n ne ne Vlan Id	ion vlan2 a0:e0	024 9:af:32:d9:ba				
Ports	NAS-ID		Inone		]			
NTP	Physical 3	Informat	ion					
> PMIPv6	Port Num Backup P	ber ort		0				
IPv6	Active Po Enable D	Active Port1Enable Dynamic AP Management						
Advanced	Interface	Address	;					
Lawful Interception	VLAN Ide	ntifier ss		2024				
	Gateway			10.105.211.1	28			

Egress 接口

## 交换机端口配置

有线访客用户连接到接入层交换机,这些指定端口必须配置为具有在控制器上启用访客LAN的VLAN

接入层交换机端口配置

interface gigabitEthernet <x/x/x>

有线访客接入说明

switchport access vlan 2020

switchport mode access

## 结束

外部控制器上行链路端口配置

interface TenGigabitEthernet<x/x/x>

描述连接到外部WLC的中继端口

switchport mode trunk

switchport trunk native vlan 2081

switchport trunk allowed vlan 2081,2020

结束

锚点控制器上行链路端口配置

interface TenGigabitEthernet<x/x/x>

描述连接到锚点WLC的中继端口

switchport mode trunk

switchport trunk native vlan 2081

switchport trunk allowed vlan 2081,2024

结束

## 配置Web身份验证

第1步:导航到安全>网络身份验证>网络登录页面。将Web身份验证类型设置为External (Redirect to external server),并配置外部Web身份验证URL。登录后重定向URL是可选的,并且可以在客户端需要在身份验证成功之后重定向到专用页时进行配置。

			Save Configuration Ping Logout Befresh
CISCO	MONITOR WLANS CONTROLLER W	IRELESS SECURITY MANAGEMENT COMMANDS HEL	P User:admin(ReadWrite)
Security	Web Login Page	,	Preview Apply
AAA     General     FROIUS     Authentication     Accounting     Auth Cached Users     Failback     DNS     Downloaded AVP     TACACS+     LDAP     Local Net Users     MAC Filtering     Disabled Clients     User Login Policies     AP Policies     Password Policies	Web Authentication Type Redirect URL after login Login Success Page Type External Webauth URL QrCode Scanning Bypass Timer QrCode Scanning Bypass Count	External (Redirect to external server)  http://10.127.196.171/webauth/logout.html http://10.127.196.171/webauth/login.html	
Local EAP			
Advanced EAP			
Priority Order			
Certificate			
Access Control Lists			
Wireless Protection     Policies			
Web Auth Web Login Page Certificate			

Web身份验证设置

## AAA设置:

#### 第1步:配置RADIUS服务器

导航到Security > Radius > Authentication > New。

ahaha		Save Configuration Ping Logout Refre
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	User:admin(ReadWrite) 🔒 Hon
Security	RADIUS Authentication Servers	Apply New
AAA     General	Auth Called Station ID Type 🛛 AP MAC Address:SSID 🗸	
	Use AES Key Wrap  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)	
Auth Cached Users	MAC Delimiter Hyphen V	
Fallback DNS	Framed MTU 1300	
Downloaded AVP		

RADIUS 服务器

第2步:在控制器上配置RADIUS服务器IP和共享密钥。将服务器状态切换到已启用并选中网络用户 复选框。

# **RADIUS Authentication Servers > New**

Server Index (Priority)	4 ~
Server IP Address(Ipv4/Ipv6)	
Shared Secret Format	ASCII ~
Shared Secret	
Confirm Shared Secret	
Apply Cisco ISE Default settings	
Apply Cisco ACA Default settings	
Key Wrap	(Designed for FIPS customers)
Port Number	1812
Server Status	Enabled ~
Support for CoA	Disabled ~
Server Timeout	5 seconds
Network User	Enable
Management	Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	Enable
PAC Provisioning	Enable
IPSec	Enable
Cisco ACA	Enable

服务器配置

配置访问控制列表

第1步:导航到安全>访问控制列表,然后选择新建。创建预身份验证ACL,允许流量流向DNS和外

## 部Web服务器。

،،ا،،،ا،، cısco	MON	TOR <u>w</u>	LANs <u>C</u> ON	NTROLLER	WIRELESS	<u>s</u>	ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP			
Security	Acc	ess Con	trol Lists	> Edit	Ľ								
▼ AAA General ▼ RADIUS	Gene	eral											
Authentication Accounting	Acces	s List Nam	e P	re-Auth_A	CL								
Auth Cached Users Fallback	Deny	Counters	0										
DNS Downloaded AVP	Seq	Action	Source IP	/Mask	Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
TACACS+ LDAP Local Net Users	1	Permit	0.0.0.0 0.0.0.0	/	0.0.0.0 0.0.0.0	/	UDP	Any	DNS	Any	Any	0	•
MAC Filtering Jisabled Clients	2	Permit	0.0.0.0 0.0.0.0	/	0.0.0.0 0.0.0.0	/	UDP	DNS	Any	Any	Any	0	
User Login Policies AP Policies	3	Permit	0.0.0.0 0.0.0.0	/	10.127.196.171 255.255.255.255	/	тср	Any	HTTP	Any	Any	0	
Password Policies     Local EAP	4	Permit	10.127.196	5.171 / 55.255	0.0.0.0 0.0.0.0	/	ТСР	НТТР	Any	Any	Any	0	•
Advanced EAP	5	Permit	0.0.0.0 0.0.0.0	/	10.127.196.171 255.255.255.255	1	тср	Any	HTTPS	Any	Any	0	•
Priority Order     Certificate	6	Permit	10.127.196 255.255.25	5.171 / 55.255	0.0.0.0 0.0.0.0	/	ТСР	HTTPS	Any	Any	Any	0	
Access Control Lists Access Control Lists													

允许流量流向Web服务器的访问列表

## 配置访客LAN配置文件

## 第1步:导航到WLAN >新建>转到。

<u>M</u> ONITOR <u>W</u> LANS <u>2</u> 0	NTROLLER W <u>I</u> RELESS <u>S</u> ECURIT	Y M <u>A</u> NAGEMENT C <u>O</u> MMANDS	HELP				
WLANS							
Current Filter: None [Change Filter] [Clear Filter] Create New V Go							
WLAN ID Type	Profile Name	WLAN SSID	Admin Status Security Policies				

访客LAN配置文件

选择Type as Guest LAN并配置配置文件名称。必须在9800锚点控制器的策略配置文件和访客 LAN配置文件上配置相同的名称。

# Type Guest LAN Profile Name Guest-Profile ID 3

访客LAN配置文件

第2步:在常规(General)选项卡下,在访客LAN配置文件中映射入口和出口接口。

入口接口是有线客户端物理连接到的vlan。

出口接口是客户端请求IP地址的VLAN子网。

General	Security	QoS	Adva	anced			
Profile Na	ame	Guest-F	Profile				
Туре		Guest L	AN				
Status		🗹 Enat	bled				
				•			
Security	Policies	Web-A	uth				
		(Modifica	ations do	ne under	security tab will	appear a	fter applying th
Ingress I	nterface	wired-g	juest 🗸				
Egress Ir	terface	vlan202	24	$\checkmark$			
NAS-ID		none					

访客LAN配置文件

第3步:导航到安全>第3层。

选择Layer 3 Security作为Web Authentication,并映射预身份验证ACL。

General	Security	QoS	Advan	ced			
Layer 2	Layer 3	AAA S	Servers				
Layer 3 Preauthe Override	Security entication ACL e Global Config <sup>2</sup>		Pre-Auth	n_ACL ∽]	IPv6	None 🗸	Web Authentication ~

Layer 3 Security选项卡

## 步骤4:

在AAA servers选项卡下,映射RADIUS服务器并选中Enabled复选框。

Ge	neral	Security	QoS	Advan	ced	
L	ayer 2	Layer 3	<b>AAA</b> :	Servers		
Se	elect AAA	servers belo	w to ove	erride use o	of defa	ault servers on th
R/	ADIUS Se	rvers				
		Authenticat	tion Serv	vers	Acco	ounting Servers
		Authenticat	tion Serv	vers	Acco	ounting Servers
	Server 1	Authenticat C Enabled IP:10.197.2	t <b>ion Serv</b> 224.122,	v <b>ers</b> Port:1812 \	Acco E Nor	nabled
	Server 1 Server 2	Authenticat Enabled IP:10.197.2	t <b>ion Serv</b> 224.122,	Port:1812 \	Acco E Nor	nabled ne
	Server 1 Server 2 Server 3	Authenticat Enabled IP:10.197.2 None None	t <b>ion Serv</b> 224.122,	Port:1812 \	Acco Nor Nor	nabled ne ne
	Server 1 Server 2 Server 3 Server 4	Authenticat Enabled IP:10.197.2 None None	224.122,	Port:1812 \	Acco Nor Nor	nabled ne ne ne

将RADIUS服务器映射到访客LAN配置文件

第5步:导航到WLAN页面并将鼠标悬停在访客LAN配置文件的下拉图标上,然后选择移动锚点。

<u>30</u>	WLAN	guest-1665	guest-1665	Disabled	[WPA + WPA2][Auth(PSK)]	
	Guest LAN	Guest-Profile		Enabled	Web-Auth	
□ <u>2</u>	Guest LAN	Guest		Disabled	Web-Auth	Mobility Anchors

移动锚点

## 第6步:将移动锚点从下拉列表映射到访客LAN配置文件。

**Mobility Anchors** 

WLAN SSID Guest-	Profile		
Switch IP Address (And	chor) local	Data Path	Co
Mobility Anchor Create	10.106.39.41		
Hobinty Anchor create	10.76.6.156		
Switch IP Address (/	Anchor)		
Foot Notes			

将移动锚点映射到访客LAN

# 锚点9800 WLC上的配置

## 配置Web参数映射

第1步:导航到配置>安全> Web身份验证,然后选择全局。验证控制器的虚拟IP地址和信任点是否 正确映射到配置文件(类型设置为webauth)。

General Advanced			
Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-3
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Туре	webauth 🔻	Virtual IPv6 Address	X:X:X:X:X
Captive Bypass Portal	0	Web Auth intercept HTTPs	0
Disable Success Window	D	Enable HTTP server for Web Auth	
Disable Logout Window	D	Disable HTTP secure server	0
Disable Cisco Logo	0	for Web Auth	
Sleeping Client Status	0	Banner Configuration	
Sleeping Client Timeout (minutes)	720	Banner Title	
		Banner Type   None  Reac	e O Banner Text I From File

Web参数映射

第2步:在高级选项卡下,指定客户端必须重定向到的外部网页URL。配置Redirect URL for

## Login和Redirect On-Failure。Redirect On-Success设置是可选配置。

Dravious of the Dedirect LIDL:
/login.html?switch_url=https://192.0.2.1/login.html&redirect= <website-name></website-name>
1

#### Redirect to external server

Redirect URL for login	http://10.127.196.171/w
Redirect On-Success	http://10.127.196.171/w
Redirect On-Failure	http://10.127.196.171/w
Redirect Append for AP MAC Address	
Redirect Append for Client MAC Address	
Redirect Append for WLAN SSID	
Portal IPV4 Address	10.127.196.171
Portal IPV6 Address	X:X:X:X:X

Advanced选项卡

## CLI 配置

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
trustpoint TP-self-signed-3010594951
webauth-http-enable
```



注:有关AAA配置,请参阅外部9800 WLC的"在Catalyst 9800上配置锚定到其他Catalyst 9800的有线访客"部分中提供的配置详细信息。

配置策略配置文件

第1步:导航到配置>标签和配置文件>策略。使用与外部控制器的访客LAN配置文件相同的名称配 置策略配置文件。

General	Access Policies	QOS and AVC	Mobility	Advanc	ed	
Name'	*	Guest-Profile			WLAN Switching Policy	
Descri	ption	Enter Description			Central Switching	ENABLED
Status					Central Authentication	ENABLED
Passiv	e Client	DISABLED			Central DHCP	ENABLED
IP MAG	C Binding	ENABLED			Flex NAT/PAT	DISABLED
Encryp	oted Traffic Analytics	DISABLED				
CTS F	Policy					
Inline 7	Tagging	O				
SGAC	L Enforcement					
Defaul	t SGT	2-65519				

策略配置文件

第2步:在访问策略(Access Policies)选项卡下,从下拉列表中映射有线客户端VLAN

General	Access Policies	QOS and AVC	Mobility	Advanced
RADIUS	Profiling			
HTTP TL	V Caching			
DHCP TL	V Caching			
WLAN L	ocal Profiling			
Global St Classifica	tate of Device ation	Disablec	i	
Local Su	bscriber Policy Name	Search	n or Select	▼ 2
VLAN				
VLAN/VL	AN Group	VLAN2	2024	• i
Multicast	VLAN	Enter N	Aulticast VLAN	

访问策略

第3步:在移动选项卡下,选中导出锚点复选框。

G	General	Access Policies	QOS and AVC	Mobility	Advanced
	Mobility	Anchors			
	Export An	chor			
	Static IP N	Mobility	DISABLE	D	

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Mobility选项卡

## CLI 配置

```
wireless profile policy Guest-Profile
no accounting-interim
exclusionlist timeout 180
no flex umbrella dhcp-dns-option
mobility anchor
vlan VLAN2024
no shutdown
```

## 配置访客LAN配置文件

第1步:导航到配置>无线>访客LAN,选择添加配置访客LAN配置文件并禁用有线VLAN状态。

锚点上的访客LAN配置文件名称必须与外部WLC上的访客LAN配置文件相同。

Ge	eneral Security				
	Profile Name*	Guest-Profile		Client Association Limit	2000
	Guest LAN ID*	1		Wired VLAN Status	DISABLE
	mDNS Mode	Bridging	•		
	Status	ENABLE			

访客LAN配置文件

第2步:在安全选项卡下,启用网络身份验证。 从下拉列表中选择Web Auth参数映射和 Authentication List

dit Guest L	AN Profile		
General	Security		
Layer3			
Web Auth		ENABLE	
Web Auth P	arameter Map	global	•
Authenticati	on List	ISE-List	•

访客LAN安全选项卡

CLI 配置

```
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

## 访客LAN映射

第1步:导航到配置>无线>访客LAN。在访客LAN映射配置部分中,选择添加,并将策略配置文件 映射到访客LAN配置文件。

#### Guest LAN Map Configuration

+ Add Map X Delete Map	
Guest LAN Map : GuestMap + Add × Delete	
Guest LAN Profile Name Y Policy Name Y	
No records available.	Profile Name Guest-Profile
Image: Image         Image: Image         0 - 0 of 0 items	Policy Name Guest-Profile 2
	✓ Save

访客LAN映射

# 验证

## 验证控制器配置

#show guest-lan summary

GLAN	GLAN Profile Name	Status
1	Guest-Profile	UP
2	Guest	UP

## #show guest-lan id 1

#### <#root>

Guest-LAN Profile	Name :	Guest	
Guest-LAN ID Wired-Vlan		:	2
11			

Status

#### Enabled

Number of Active Clients Max Associated Clients Security	: 0 : 2000
WebAuth	:
Enabled	
Webauth Parameter Map Webauth Authentication List	: global :
ISE-List	
Webauth Authorization List mDNS Gateway Status	: Not configured : Bridge

## #show parameter-map type webauth global

#### <#root>

Parameter Map Name Type	: global :
webauth	
Redirect: For Login	:
http://10.127.196.171/webauth	n/login.html
On Success	:
http://10.127.196.171/webauth	n/logout.html
On Failure	:
http://10.127.196.171/webauth	n/failed.html
Portal ipv4	:
10.127.196.171	
Virtual-ipv4	:
192.0.2.1	

#show parameter-map type webauth name <profile name> (如果使用自定义web参数配置文件)

#show wireless guest-lan-map summary

GLAN Profile Name	Policy Name
Guest	Guest

Guest

#### #show无线移动性摘要

IP	Public Ip	MAC Address
10.76.118.70	10.76.118.70	f4bd.9e59.314b

#show ip http server status

HTTP server status: Enabled HTTP server port: 80 HTTP server active supplementary listener ports: 21111 HTTP server authentication method: local HTTP secure server capability: Present HTTP secure server status: Enabled

HTTP secure server port: 443 HTTP secure server trustpoint: TP-self-signed-3010594951

>show guest-lan summary

Number of Guest LANs 1			
GLAN ID	GLAN Profile Name	Status	Interface Name
2	Guest	Enabled	wired-vlan-11

>show guest-lan 2

Guest LAN Identifier..... 2 Profile Name..... Guest Status..... Enabled Interface..... wired-vlan-11 Radius Servers Authentication..... 10.197.224.122 1812 \* Web Based Authentication..... Enabled Web Authentication Timeout...... 300 IPv4 ACL..... Pre-Auth\_ACL Mobility Anchor List IP Address GLAN ID Status \_\_\_\_\_ \_\_\_\_\_ \_\_\_\_\_ 2 10.76.118.74 Up

Radius Authentication Method	PAP
Cisco Logo	Enabled
CustomLogo	None
Custom Title	None
Custom Message	None
Custom Redirect URL	<pre>http://10.127.196.171/webauth/logout.html</pre>
Web Authentication Login Success Page Mode	None
Web Authentication Type	External
Logout-popup	Enabled
External Web Authentication URL	http://10.127.196.171/webauth/login.html
QR Code Scanning Bypass Timer	0
QR Code Scanning Bypass Count	0

>show custom-web guest-lan 2

Guest LAN Status	Enabled
Web Security Policy	Web Based Authentication
WebAuth Type	External
Global Status	Enabled

验证客户端策略状态

外国、

#show无线客户端摘要

客户端成功关联后,外部控制器上的客户端策略管理器状态为RUN。

<#root>

MAC Address	AP Name	Type ID	State	Protocol	Meth
a0ce.c8c3.a9b	5 N/A				
GLAN 1					
Run					
802.3					
Web Auth					
Export Foreign	1				

>show client detail a0ce.c8c3.a9b5

#### <#root>

Client MAC Address Client Username Client Webauth Username Client State User Authenticated by	a0:ce:c8:c3:a9:b5 N/A N/A Associated None
Client User Group Client NAC OOB State guest-lan Wireless LAN Profile Name Mobility State	Access 1 Guest-Profile
Export Foreign	
Mobility Anchor IP Address	
10.76.118.70	
Security Policy Completed	
Yes	
Policy Manager State	
RUN	
Pre-auth IPv4 ACL Name EAP Type Interface	Pre-Auth_ACL Unknown
wired-guest-egress	
VLANQuarantine VLAN	2024 0

## 在锚点上,

必须在锚点控制器上监控客户端状态转换。

客户端策略管理器状态为Web Auth pending(网络身份验证挂起)。

#### <#root>

MAC Address	AP Name	Type ID	State	Protocol Meth
a0ce.c8c3.a9b	5 10.76.6.156			
GLAN 1				
Webauth P	ending			
802.3				
Web Auth				
Export Anchor				

客户端进行身份验证后,策略管理器状态会转换为RUN状态。

MAC Address	AP Name	Type ID	State	Protocol	Meth
a0ce.c8c3.a9b5	10.76.6.156	GLAN 1	Run	802.3	Web

#show无线客户端mac-address a0ce.c8c3.a9b5 detail

#### <#root>

```
Client MAC Address : a0ce.c8c3.a9b5
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :
10.105.211.69
Client State : Associated
Policy Profile : Guest-Profile
Flex Profile : N/A
Guest Lan:
 GLAN Id: 1
 GLAN Name: Guest-Profile
Mobility:
 Foreign IP Address
                           :
10.76.118.74
 Point of Attachment
                          : 0xA000003
 Point of Presence
                             : 0
                             : 1
 Move Count
 Mobility Role
                             :
Export Anchor
 Mobility Roam Type
                        :
L3 Requested
Policy Manager State:
Webauth Pending
Last Policy Manager State :
IP Learn Complete
Client Entry Create Time : 35 seconds
VLAN : VLAN2024
Session Manager:
 Point of Attachment : mobility_a0000003
              : 0xA0000003
 IIF ID
                   : FALSE
 Authorized
 Session timeout : 28800
 Common Session ID: 4a764c0a000008ea0285466
 Acct Session ID : 0x0000000
 Auth Method Status List
       Method : Web Auth
```

Webauth State :

Login

Webauth Method :

#### Webauth

```
Server Policies:
Resultant Policies:
URL Redirect ACL :
```

WA-v4-int-10.127.196.171

Preauth ACL :

WA-sec-10.127.196.171

VLAN Name : VLAN2024 VLAN :

#### 2024

Absolute-Timer : 28800

#### 客户端在成功进行Web身份验证后进入RUN状态。

show wireless client mac-address a0ce.c8c3.a9b5 detail

#### <#root>

```
Client MAC Address : a0ce.c8c3.a9b5
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :
10.105.211.69
Client Username :
testuser
Client State : Associated
Policy Profile : Guest-Profile
Flex Profile : N/A
Guest Lan:
 GLAN Id: 1
 GLAN Name: Guest-Profile
Wireless LAN Network Name (SSID) : N/A
BSSID : N/A
Connected For : 81 seconds
Protocol : 802.3
```

Policy Manager State:

#### Run

Last Policy Manager State :

```
Webauth Pending
Client Entry Create Time : 81 seconds
VLAN : VLAN2024
Last Tried Aaa Server Details:
       Server IP :
10.197.224.122
 Auth Method Status List
       Method : Web Auth
               Webauth State : Authz
               Webauth Method : Webauth
 Resultant Policies:
               URL Redirect ACL :
IP-Adm-V4-LOGOUT-ACL
                                : VLAN2024
               VLAN Name
               VLAN
                                1
2024
               Absolute-Timer : 28800
```

>show client detail a0 : ce : c8 : c3 : a9 : b5

#### <#root>

Client MAC Address	a0:ce:c8:c3:a9:b5
Client Username	N/A
Client Webauth Username	N/A
Client State	Associated
Wireless LAN Profile Name	Guest
WLAN Profile check for roaming	Disabled
Hotspot (802.11u)	Not Supported
Connected For	90 secs
IP Address	10.105.211.75
Gateway Address	10.105.211.1
Netmask	255.255.255.128
Mobility State	

#### Export Anchor

Mobility Foreign IP Address.....

#### 10.76.118.70

Security Policy Completed..... No Policy Manager State.....

#### WEBAUTH\_REQD

Pre-auth IPv4 ACL Name.....

Pre-Auth\_ACLPre-auth

IPv4 ACL Applied Status..... Yes Pre-auth IPv4 ACL Applied Status..... 身份验证客户端转换到RUN状态后。

<#root>

<pre>show client detail a0:ce:c8:c3:a9:b5 Client MAC Address Client Username</pre>	a0:ce:c8:c3:a9:b5
testuser	
Client Webauth Username	
testuser	
Client State	
Associated	
User Authenticated by	
RADIUS Server	
Client User Group	testuser Access
Connected For	37 secs
IP Address	
10.105.211.75	
Gateway Address Netmask	10.105.211.1 255.255.255.128
Mobility State	
Export Anchor	
Mobility Foreign IP Address	10.76.118.70
Policy Manager State	res
RUN	
Pre-auth IPv4 ACL Name	Pre-Auth_ACL
Pre-auth IPv4 ACL Applied Status	Yes Unknown
Interface	
wired-vlan-11	
VLAN	
11	
Quarantine VLAN	0

# 故障排除

## AireOS控制器调试

启用客户端调试

>debug client <H.H.H>

验证是否启用了调试

>show debugging

要禁用调试

debug disable-all

## 9800放射性痕迹

激活Radio Active Tracing以在CLI中为指定的MAC地址生成客户端调试跟踪。

启用放射性跟踪的步骤:

确保禁用所有条件调试。

clear platform condition all

## 启用对指定mac地址的调试。

debug wireless mac <H.H.H> monitor-time <Time is seconds>

## 重现问题后,请禁用调试以停止RA跟踪收集。

no debug wireless mac <H.H.H>

一旦RA跟踪停止,将在控制器的bootflash中生成调试文件。

show bootflash: | include ra\_trace 2728 179 Jul 17 2024 15:13:54.000000000 +00:00 ra\_trace\_MAC\_aaaabbbbcccc\_HHMMSS.XXX\_timezone\_Day

## 将文件复制到外部服务器。

copy bootflash:ra\_trace\_MAC\_aaaabbbbcccc\_HHMMSS.XXX\_timezone\_DayWeek\_Month\_Day\_year.log tftp://<IP addr

## 显示调试日志:

more bootflash:ra\_trace\_MAC\_aaaabbbbcccc\_HHMMSS.XXX\_timezone\_DayWeek\_Month\_Day\_year.log

## 在GUI中启用RA跟踪,

Troubleshooting - > Radioactive Trace	
Conditional Debug Global State: Started	d 🙆 Wireless Deb
+ Add × Delete <	Stop Last Run
Add MAC/IP Address	×
MAC/IP Address*	C/IP Address every newline
	Apply to Device

嵌入式数据包捕获

导航到故障排除>数据包捕获。输入捕获名称并指定客户端的MAC地址作为内部过滤器MAC。将缓 冲区大小设置为100并选择上行链路接口来监控传入和传出数据包。

Troubleshooting	
+ Add × Delete	
Create Packet Capture	×
Capture Name* TestPCap	
Filter* any	
Monitor Control Plane 🚯 🛛 🔲	
Inner Filter Protocol DHCP	
Inner Filter MAC	
Buffer Size (MB)* 100	
Limit by* Duration	
Available (12) Search Q Selected (1)	
▼ Tw0/0/1	÷
▼ Tw0/0/2	
Ţw0/0/3 →	
Te0/1/0 →	

嵌入式数据包捕获



注意:选择"监控控制流量"选项以查看重定向到系统CPU并重新注入数据平面的流量。

导航到故障排除>数据包捕获,选择开始捕获数据包。

	Capture Name	Interface	T	Monitor Control Plane	Ŧ	Buffer Size	Ŧ	Filter by	Limit	Status	Ţ	Action
	TestPCap	TwoGigabitEthernet0/0/0		No		0%		any	@ 3600 secs	Inactive		► Start
												4
开始	数据包捕获											

CLI 配置

monitor capture TestPCap inner mac <H.H.H>
monitor capture TestPCap buffer size 100
monitor capture TestPCap interface twoGigabitEthernet 0/0/0 both
monitor capture TestPCap start

<Reporduce the issue>

monitor capture TestPCap stop

show monitor capture TestPCap

Status Information for Capture TestPCap Target Type: Interface: TwoGigabitEthernet0/0/0, Direction: BOTH Status : Inactive Filter Details: Capture all packets Inner Filter Details: Mac: 6c7e.67e3.6db9 Continuous capture: disabled Buffer Details: Buffer Type: LINEAR (default) Buffer Size (in MB): 100 Limit Details: Number of Packets to capture: 0 (no limit) Packet Capture duration: 3600 Packet Size to capture: 0 (no limit) Maximum number of packets to capture per second: 1000 Packet sampling rate: 0 (no sampling)

#### 将数据包捕获导出到外部TFTP服务器。

monitor capture TestPCap export tftp://<IP address>/ TestPCap.pcap

#### 导航到故障排除>数据包捕获,然后选择导出将捕获文件下载到本地计算机上。

+	Add X Delete	e												
	Capture Name 🍸	Interface	Ŧ	Monitor Control Plane	Ŧ	Buffer Size	Ŧ	Filter by	Ŧ	Limit	Status	Ŧ	Action	
	TestPCap	TwoGigabitEthernet0/0/0		No		0%	)	any		@ 3600 secs	Inactive		► Start	Export
[4	4 1 ⊨ ⊨	10 🔻							E	xport Capture	- TestP	Cap	c	<b>x</b> 1
										Export to*	des	ktop		•
										Cancel			E	xport

下载EPC

工作日志片段

AireOS外部控制器客户端调试日志

从有线客户端接收的有线数据包

\*apfReceiveTask: May 27 12:00:55.127: a0:ce:c8:c3:a9:b5 Wired Guest packet from 10.105.211.69 on mobile

#### 外部控制器构建导出锚点请求

\*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 Attempting anchor export for mobile a0:ce:c8:c3 \*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 mmAnchorExportSend: Building ExportForeignLradM \*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 SGT Payload built in Export Anchor Req 0

外部控制器向锚点控制器发送导出锚点请求。

\*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 Export Anchor request sent to 10.76.118.70

锚点控制器为客户端的锚点请求发送确认

\*Dot1x\_NW\_MsgTask\_5: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Recvd Exp Anchor Ack for mobile a0:ce:c8:c

#### 外部控制器上的客户端的移动角色更新为导出外部。

\*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP\_REQD (7) mobility role update requ
Peer = 10.76.118.70, Old Anchor = 10.76.118.70, New Anchor = 10.76.118.70

#### 客户端转换到RUN状态。

\*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP\_REQD (7) State Update from Mobilit \*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Stopping deletion of Mobile Station: (callerId: \*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Moving client to run state

#### 9800放射性追踪仪

#### 客户端与控制器关联。

2024/07/15 04:10:29.087608331 {wncd\_x\_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b

#### 关联后正在进行移动性发现。

2024/07/15 04:10:29.091585813 {wncd\_x\_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b 2024/07/15 04:10:29.091605761 {wncd\_x\_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b

#### 处理移动性发现后,客户端漫游类型即更新为请求的第3层。

2024/07/15 04:10:29.091664605 {wncd\_x\_R0-0}{1}: [mm-transition] [17765]: (info): MAC: a0ce.c8c3.a9b5 MM 2024/07/15 04:10:29.091693445 {wncd\_x\_R0-0}{1}: [mm-client] [17765]: (info): MAC: a0ce.c8c3.a9b5 Roam t

#### 外部控制器正在向锚点WLC发送导出锚点请求。

2024/07/15 04:10:32.093245394 {mobilityd\_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Ex 2024/07/15 04:10:32.093253788 {mobilityd\_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Fo 2024/07/15 04:10:32.093274405 {mobilityd\_R0-0}{1}: [mm-client] [18316]: (info): MAC: a0ce.c8c3.a9b5 For

#### 从锚点控制器接收导出锚点响应,并从用户配置文件应用vlan。

2024/07/15 04:10:32.106775213 {mobilityd\_R0-0}{1}: [mm-transition] [18316]: (info): MAC: a0ce.c8c3.a9b5 2024/07/15 04:10:32.106811183 {mobilityd\_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Ex 2024/07/15 04:10:32.107183692 {wncd\_x\_R0-0}{1}: [epm-misc] [17765]: (info): [a0ce.c8c3.a9b5:Tw0/0/0] An 2024/07/15 04:10:32.107247304 {wncd\_x\_R0-0}{1}: [svm] [17765]: (info): [a0ce.c8c3.a9b5] Applied User Pr 2024/07/15 04:10:32.107250258 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [17765]: (info): Applied User Profile:

#### 处理导出锚点请求后,客户端移动角色将更新为导出外部。

2024/07/15 04:10:32.107490972 {wncd\_x\_R0-0}{1}: [mm-client] [17765]: (debug): MAC: a0ce.c8c3.a9b5 Proce 2024/07/15 04:10:32.107502336 {wncd\_x\_R0-0}{1}: [mm-client] [17765]: (info): MAC: a0ce.c8c3.a9b5 Mobili 2024/07/15 04:10:32.107533732 {wncd\_x\_R0-0}{1}: [sanet-shim-translate] [17765]: (info): Anchor Vlan: 20 2024/07/15 04:10:32.107592251 {wncd\_x\_R0-0}{1}: [mm-client] [17765]: (note): MAC: a0ce.c8c3.a9b5 Mobili

客户端转换为IP learn状态。

2024/07/15 04:10:32.108210365 {wncd\_x\_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b 2024/07/15 04:10:32.108293096 {wncd\_x\_R0-0}{1}: [client-orch-sm] [17765]: (debug): MAC: a0ce.c8c3.a9b5
2024/07/15 04:10:32.108521618 {wncd\_x\_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b

#### AireOS锚点控制器客户端调试日志

#### 从外部控制器检索导出锚点请求。

\*Dot1x\_NW\_MsgTask\_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Anchor Export Request Recvd for mobile a0:co \*Dot1x\_NW\_MsgTask\_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv: Extracting mmPayloadExpo \*Dot1x\_NW\_MsgTask\_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv Ssid=Guest useProfileName

#### 为客户端应用本地桥接vlan。

\*Dot1x\_NW\_MsgTask\_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Updated local bridging VLAN to 11 while app \*Dot1x\_NW\_MsgTask\_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Applying Interface(wired-vlan-11) policy on \*Dot1x\_NW\_MsgTask\_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 After applying Interface(wired-vlan-11) pol

# 移动角色更新为"导出锚点"(Export Anchor)和"已转换关联的客户端状态"(client state translated Associated)。

移动性完成,客户端状态关联,移动角色为导出锚点。

\*Dot1x\_NW\_MsgTask\_5: May 28 10:46:27.832: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP\_REQD (7) State Update from Mob

### 客户端IP地址在控制器上获知,并且状态从所需的DHCP转换为所需的网络身份验证。

\*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 Static IP client associated to interface wired-vlan

\*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 dtlArpSetType: Changing ARP Type from 0 ---> 1 for \*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 10.105.211.75 DHCP\_REQD (7) Change state to WEBAUTH

#### 正在通过添加外部重定向URL和控制器虚拟IP地址来制定Web身份验证URL。

\*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Preparing redirect URL according to configure \*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Web-auth type External, using URL:http://10.1 \*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added switch\_url, redirect URL is now http://

#### 已将客户端MAC地址和WLAN添加到URL。

\*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added client\_mac , redirect URL is now http:/ \*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added wlan, redirect URL is now \*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added wlan, redirect URL is now http://10.127

#### 对主机10.105.211.1的HTTP GET进行解析后的最终URL

\*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- parser host is 10.105.211.1 \*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- parser path is /auth/discovery \*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5-added redirect=, URL is now http://10.127.196.

#### 重定向URL发送到200 OK响应数据包中的客户端。

\*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- 200 send\_data =HTTP/1.1 200 OK Location:http://10.127.196.171/webauth/login.html?switch\_url=https://192.0.2.1/login.html&client\_mac=a0

客户端与重定向url主机建立TCP连接。客户端在门户上提交登录用户名和密码后,控制器会向 radius服务器发送radius请求

控制器收到Access-Accept后,客户端关闭TCP会话并进入RUN状态。

\*aaaQueueReader: May 28 10:46:59:077: a0:ce:c8:c3:a9:b5 Sending the packet to v4 host 10.197.224.122:18 \*aaaQueueReader: May 28 10:46:59:077: a0:ce:c8:c3:a9:b5 Successful transmission of Authentication Packe

May	28	10:46:59:077:	AVP[01]	User-Name	testuser
May	28	10:46:59:077:	AVP[03]	Calling-Station-Id	a0-ce-c8
May	28	10:46:59:077:	AVP[04]	Nas-Port	0x00000
May	28	10:46:59:077:	AVP[05]	Nas-Ip-Address	0x0a4c76
May	28	10:46:59:077:	AVP[06]	NAS-Identifier	POD1586-
	May May May May May	May 28 May 28 May 28 May 28 May 28	May 28 10:46:59:077: May 28 10:46:59:077: May 28 10:46:59:077: May 28 10:46:59:077: May 28 10:46:59:077:	May 28 10:46:59:077:AVP[01]May 28 10:46:59:077:AVP[03]May 28 10:46:59:077:AVP[04]May 28 10:46:59:077:AVP[05]May 28 10:46:59:077:AVP[06]	May 28 10:46:59:077:       AVP[01] User-Name         May 28 10:46:59:077:       AVP[03] Calling-Station-Id         May 28 10:46:59:077:       AVP[04] Nas-Port         May 28 10:46:59:077:       AVP[05] Nas-Ip-Address         May 28 10:46:59:077:       AVP[06] NAS-Identifier

\*aaaQueueReader: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 radiusServerFallbackPassiveStateUpdate: RADIUS
\*radiusTransportThread: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Access-Accept received from RADIUS serv
\*Dot1x\_NW\_MsgTask\_5: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Processing Access-Accept for mobile a0:ce:c
\*apfReceiveTask: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Moving client to run state

#### 9800锚控制器放射性跟踪

从外部控制器向客户端发送移动通告消息。

2024/07/15 15:10:20.614677358 {mobilityd\_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Re

## 当客户端正在关联时从外部控制器接收的导出锚点请求,该请求的导出锚点响应由锚点控制器发送 ,可在外部控制器RA跟踪上进行验证。

2024/07/15 15:10:22.615246594 {mobilityd\_R0-0}{1}: [mm-transition] [15259]: (info): MAC: a0ce.c8c3.a9b5

客户端已移至关联状态,并且移动角色已转换为导出锚点。

2024/07/15 15:10:22.616156811 {wncd\_x\_R0-0}{1}: [client-orch-state] [14709]: (note): MAC: a0ce.c8c3.a9b 2024/07/15 15:10:22.627358367 {wncd\_x\_R0-0}{1}: [mm-client] [14709]: (note): MAC: a0ce.c8c3.a9b5 Mobili

2024/07/15 15:10:22.627462963 {wncd\_x\_R0-0}{1}: [dot11] [14709]: (note): MAC: a0ce.c8c3.a9b5 Client da 2024/07/15 15:10:22.627490485 {mobilityd\_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Ex 2024/07/15 15:10:22.627494963 {mobilityd\_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Fo

IP学习完成,客户端IP通过ARP学习。

2024/07/15 15:10:22.628124206 {wncd\_x\_R0-0}{1}: [client-iplearn] [14709]: (info): MAC: a0ce.c8c3.a9b5 2024/07/15 15:10:23.627064171 {wncd\_x\_R0-0}{1}: [sisf-packet] [14709]: (info): RX: ARP from interface m 2024/07/15 15:10:24.469704913 {wncd\_x\_R0-0}{1}: [client-iplearn] [14709]: (note): MAC: a0ce.c8c3.a9b5 2024/07/15 15:10:24.470527056 {wncd\_x\_R0-0}{1}: [client-iplearn] [14709]: (info): MAC: a0ce.c8c3.a9b5 2024/07/15 15:10:24.470587596 {wncd\_x\_R0-0}{1}: [client-orch-sm] [14709]: (debug): MAC: a0ce.c8c3.a9b5 2024/07/15 15:10:24.470613094 {wncd\_x\_R0-0}{1}: [client-orch-sm] [14709]: (debug): MAC: a0ce.c8c3.a9b5 客户端策略状态为Web身份验证挂起。

```
2024/07/15 15:10:24.470748350 {wncd_x_R0-0}{1}: [client-auth] [14709]: (info): MAC: a0ce.c8c3.a9b5 Cli
```

TCP握手被控制器欺骗。当客户端发送HTTP GET时,会发送200 OK响应帧,其中包含重定向 URL。

客户端必须与重定向URL建立TCP握手并加载页面。

```
2024/07/15 15:11:37.579177010 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579190912 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579226658 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579230650 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:47.123072893 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:47.123072893 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:47.123082753 {wnc2024/07/15 15:12:04.280574375 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]
```

当客户端在Web门户页面提交登录凭证时,Access-Request数据包将发送到RADIUS服务器进行身 份验证。

2024/07/15 15:12:04.281076844 {wncd\_x\_R0-0}{1}: [radius] [14709]: (info): RADIUS: Send Access-Request t 2024/07/15 15:12:04.281087672 {wncd\_x\_R0-0}{1}: [radius] [14709]: (info): RADIUS: authenticator e3 01 2024/07/15 15:12:04.281093278 {wncd\_x\_R0-0}{1}: [radius] [14709]: (info): RADIUS: Calling-Station-Id 2024/07/15 15:12:04.281097034 {wncd\_x\_R0-0}{1}: [radius] [14709]: (info): RADIUS: User-Name 2024/07/15 15:12:04.281148298 {wncd\_x\_R0-0}{1}: [radius] [14709]: (info): RADIUS: Cisco AVpair

从radius服务器收到Access-Accept,webauth成功。

2024/07/15 15:12:04.683597101 {wncd\_x\_R0-0}{1}: [radius] [14709]: (info): RADIUS: Received from id 1812 2024/07/15 15:12:04.683607762 {wncd\_x\_R0-0}{1}: [radius] [14709]: (info): RADIUS: authenticator 52 3e 2024/07/15 15:12:04.683614780 {wncd\_x\_R0-0}{1}: [radius] [14709]: (info): RADIUS: User-Name

身份验证成功,客户端策略状态为RUN。

2024/07/15 15:12:04.683901842 {wncd\_x\_R0-0}{1}: [webauth-state] [14709]: (info): mobility\_a0000001[a0ce 2024/07/15 15:12:04.690643388 {wncd\_x\_R0-0}{1}: [errmsg] [14709]: (info): %CLIENT\_ORCH\_LOG-6-CLIENT\_ADD 2024/07/15 15:12:04.690726966 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [14709]: (info): [ Applied attribute :bs 2024/07/15 15:12:04.691064276 {wncd\_x\_R0-0}{1}: [client-orch-state] [14709]: (note): MAC: a0ce.c8c3.a9b

## 嵌入式数据包捕获分析

No.		Time	Source	Destination	Length	Protocol	Info				
+	804	15:10:24.826953	10.105.211.69	10.105.211.1		HTTP	GET /auth/disco	overy?architecture=9 HTTP/1.1			
-	806	15:10:24.826953	10.105.211.1	10.105.211.69		HTTP	HTTP/1.1 200 OK	K (text/html)			
	Eromo 00	6. 962 hutes on	uire (6004 bits)	962 hutos conturs	d (6004 bi	tc)	0				
1	Ethornot	TT Srci Cicco	50.21.4b (f4.bd.0	obs bytes capture	Cicco 24:0	Arch (6crEer	2h.24.00.ch)				
1	Internet	Internet 11, STC: L15C0_39731140 (14:00:90:39731:40), USC: L15C0_34:90:CD (00:30:34:90:CD)									
1	llcor Dat	Internet Protocol Version 4, SrC: 10./0.110./0, USC: 10./0.0.130									
1	user Datagram Protocol, STC POTT: 1000/ USE POTT: 1000/										
1	Ethernet	TI Src: Cisco	34.00.d4 (6c.5e.3)	b:34:00:d4) Det:	Celink c3:	a0.65 (a0.ce	c8:c3:a0:b5)				
1	802 10 V	irtual LAN PRT.	0 DET: 0 TD: 4	0.54.50.047, 030.	CELINA_CO.	as.bs (ac.ee.	.co.co.ao.bo/				
5	Internet	Protocol Versio	n 4 Src 10 105	211.1. Dst+ 10.105	211.69						
ŝ	Transmis	sion Control Pro	tocol. Src Port: 1	RØ. Dst Port: 5435	1. Seg: 1.	Ack: 108. 14	en: 743				
Ú	Hypertex	t Transfer Proto	col	00, 030 10101 0400	, seq. 1,	Henti 100, Et					
	> HTTP/	1.1 200 OK\r\n									
	Locat	ion: http://10.1	27.196.171/webauth	/login.html?switc	h url=https	5://192.0.2.1	/login.html&redi	<pre>irect=http://10.105.211.1/auth/discovery?architecture=9\r\n</pre>			
	Conte	nt-Type: text/ht	ml\r\n	, ,	_		, ,				
	> Conte	nt-Length: 527\r	\n								
	\r\n	-									
	(HTTP response 1/1)										
	[Time since request: 0.000000000 seconds]										
	[Request in frame: 804]										
	<pre>[Request URI: http://10.105.211.1/auth/discovery?architecture=9]</pre>										
	File	Data: 527 bvtes									

客户端被重定向到门户页面

## 收到重定向URL后,会话关闭。

	804	15:10:24.826953	10.105.211.69	10.105.211.1	HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
	805	15:10:24.826953	10.105.211.1	10.105.211.69	TCP	80 → 54351 [ACK] Seq=1 Ack=108 Win=65152 Len=0 TSval=2124108437 TSecr=2231352500
-	806	15:10:24.826953	10.105.211.1	10.105.211.69	НТТР	HTTP/1.1 200 OK (text/html)
	807	15:10:24.826953	10.105.211.69	10.105.211.1	TCP	54351 → 80 [ACK] Seq=108 Ack=744 Win=131008 Len=0 TSval=2231352500 TSecr=2124108437
	812	15:10:24.835955	10.105.211.69	10.105.211.1	TCP	54351 → 80 [FIN, ACK] Seq=108 Ack=744 Win=131072 Len=0 TSval=2231352510 TSecr=2124108437
	813	15:10:24.836947	10.105.211.1	10.105.211.69	TCP	80 → 54351 [FIN, ACK] Seq=744 Ack=109 Win=65152 Len=0 TSval=2124108447 TSecr=2231352510
L	814	15:10:24.836947	10.105.211.69	10.105.211.1	TCP	54351 → 80 [ACK] Seq=109 Ack=745 Win=131072 Len=0 TSval=2231352510 TSecr=2124108447

收到重定向URL后,TCP会话关闭

客户端向重定向URL主机发起TCP三次握手,并发送HTTP GET请求。

页面加载后,登录凭证在门户上提交,控制器向radius服务器发送访问请求以对客户端进行身份验 证。

身份验证成功后,与Web服务器的TCP会话关闭,并且在控制器上,客户端策略管理器状态转换为 RUN。

	111110	000100	D C C C C C C C C C C C C C C C C C C C	Longer I rotooor	
2348	15:11:38.598968	10.105.211.69	10.127.196.171	TCP	54381 → 80 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2678067533 TSecr=0
2349	15:11:38.599959	10.127.196.171	10.105.211.69	TCP	80 → 54381 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 WS=256 SACK_PERM
2350	15:11:38.599959	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2351	15:11:38.600966	10.105.211.69	10.127.196.171	HTTP	GET /webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=http://3.3.3.3/
2352	15:11:38.602965	10.127.196.171	10.105.211.69	HTTP	[TCP Previous segment not captured] Continuation
2354	15:11:38.602965	10.127.196.171	10.105.211.69	тср	[TCP Out-Of-Order] 80 - 54381 [ACK] Seg=1 Ack=485 Win=2097408 Len=1380
2355	15:11:38.603957	10.105.211.69	10.127.196.171	тср	[TCP Dup ACK 2350#1] 54381 → 80 [ACK] Seq=485 Ack=1 Win=262144 Len=0 SLE=1381 SRE=1737
2356	15:11:38.603957	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=485 Ack=1737 Win=260352 Len=0
2358	15:11:38.615965	10.105.211.69	10.127.196.171	HTTP	GET /webauth/yourlogo.jpg HTTP/1.1
2359	15:11:38.616957	10.127.196.171	10.105.211.69	HTTP	HTTP/1.1 304 Not Modified
2360	15:11:38.616957	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=1113 Ack=1880 Win=261952 Len=0
2362	15:11:38.621961	10.105.211.69	10.127.196.171	HTTP	GET /webauth/aup.html HTTP/1.1
2363	15:11:38.623960	10.127.196.171	10.105.211.69	HTTP	HTTP/1.1 304 Not Modified
2364	15:11:38.623960	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=1706 Ack=2023 Win=261952 Len=0
2747	15:12:04.280976	10.76.118.70	10.197.224.122	RADIUS	Access-Request id=0
2751	15:12:04.682963	10.197.224.122	10.76.118.70	RADIUS	Access-Accept id=0
2836	15:12:09.729957	10.105.211.69	10.127.196.171	HTTP	GET /webauth/logout.html HTTP/1.1
2837	15:12:09.731956	10.127.196.171	10.105.211.69	HTTP	HTTP/1.1 304 Not Modified
2838	15:12:09.731956	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=2186 Ack=2166 Win=261952 Len=0
4496	15:13:07.964946	10.105.211.69	10.127.196.171	TCP	54381 → 80 [FIN, ACK] Seq=2186 Ack=2166 Win=262144 Len=0
4497	15:13:07.964946	10.127.196.171	10.105.211.69	TCP	80 → 54381 [FIN, ACK] Seq=2166 Ack=2187 Win=2097408 Len=0
4498	15:13:07.965938	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=2187 Ack=2167 Win=262144 Len=0

客户端向门户页面发送HTTP GET请求并成功完成身份验证

## Radius访问请求数据包

2747 15:12:04.280976 10.76.118.70 10.197.224.122

RADIUS Access-Request id=0

- Frame 2747: 405 bytes on wire (3240 bits), 405 bytes captured (3240 bits)
- Ethernet II, Src: Cisco\_59:31:4b (f4:bd:9e:59:31:4b), Dst: Cisco\_34:90:cb (6c:5e:3b:34:90:cb)
- Internet Protocol Version 4, Src: 10.76.118.70, Dst: 10.197.224.122
- > User Datagram Protocol, Src Port: 60222, Dst Port: 1812
- RADIUS Protocol Code: Access-Request (1) Packet identifier: 0x0 (0) Length: 363 Authenticator: e3018f5d8e52fccbe0d703dac1a209e6 [The response to this request is in frame 2751] Attribute Value Pairs AVP: t=Calling-Station-Id(31) l=19 val=a0-ce-c8-c3-a9-b5 AVP: t=User-Name(1) l=10 val=testuser AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9) > AVP: t=Framed-IP-Address(8) l=6 val=10.105.211.6 AVP: t=Message-Authenticator(80) l=18 val=6f469fa30834350d2aed4e4b226cddf7 AVP: t=Service-Type(6) l=6 val=Dialout-Framed-User(5) AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9) AVP: t=Vendor-Specific(26) l=22 vnd=ciscoSystems(9) > AVP: t=User-Password(2) l=18 val=Encrypted > AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9) > AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9) AVP: t=NAS-IP-Address(4) l=6 val=10.76.118.70 > AVP: t=NAS-Port-Type(61) l=6 val=Virtual(5)

访问请求数据包

#### Radius访问接受数据包

	2751 15:12:04.682963	10.197.224.122	10.76.118.70	RADIUS	Access-Accept id=0	
Fr Et 80 In	ame 2751: 151 bytes or hernet II, Src: Cisco 2.1Q Virtual LAN, PRI: ternet Protocol Versic	<pre>wire (1208 bits) _34:90:cb (6c:5e:3) 0, DEI: 0, ID: 20 0n 4, Src: 10.197. </pre>	, 151 bytes captured ( b:34:90:cb), Dst: Cisc 081 224.122, Dst: 10.76.11	1208 bits) o_59:31:4b (f4:bd: 8.70	9e:59:31:4b)	
RA	DIUS Protocol	SIC POIL: 1012, D	St POIL: 00222			
	Code: Access-Accept ( Packet identifier: 0x Length: 105 Authenticator: 523eb0 [This is a response t	2) 0 (0) 1399aba715577647a1 <u>o a request in fra</u>	fbe3b899 me 2747]			
	[Time from request: 0	.401987000 seconds	.]			
×	<pre>&gt; AVP: t=User-Name(1) &gt; AVP: t=Class(25) l= &gt; AVP: t=Message-Auth</pre>	) l=10 val=testuse =57 val=434143533a henticator(80) l=1	r 3030303030303030303030303030 8 val=223df8645f1387d7	303030373342354243 137428b20df9e0c1	3343437423a69736533316	57

访问接受数据包

## 相关文章

在Catalyst 9800上配置WLAN锚点移动功能

使用AireOS控制器的有线访客接入配置示例

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。