为动态VLAN分配配置RADIUS服务器和WLC

目录

简介 先决条件 要求 使用的组件 规则 使用 RADIUS 服务器执行动态 VLAN 分配 配置 网络图 配置 配置步骤 RADIUS 服务器配置 利用 Cisco Airespace VSA 属性配置 ACS 以执行动态 VLAN 分配 为多个 VLAN 配置交换机 WLC 配置 无线客户端实用程序配置 验证 故障排除 相关信息

<u>简介</u>

本文档介绍了动态 VLAN 分配的概念。本文档描述了如何配置无线 LAN 控制器 (WLC) 和 RADIUS 服务器来动态地将无线 LAN (WLAN) 客户端分配到特定 VLAN 中。

<u>先决条件</u>

<u>要求</u>

尝试进行此配置之前,请确保满足以下要求:

- •基本了解 WLC 和轻量接入点 (LAP)
- 了解 AAA 服务器的功能
- 全面了解无线网络和无线安全问题
- •基本了解轻量接入点协议 (LWAPP)

<u>使用的组件</u>

本文档中的信息基于以下软件和硬件版本:

- 运行固件 5.2 版的 Cisco 4400 WLC
- Cisco 1130 系列 LAP
- •运行固件 4.4 版的 Cisco 802.11a/b/g 无线客户端适配器
- 运行 4.4 版的 Cisco Aironet Desktop Utility (ADU)
- •运行 4.1 版的 Cisco 安全访问控制服务器 (ACS)
- Cisco 2950 系列交换机

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。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息,请参阅 Cisco 技术提示规则。

使用 RADIUS 服务器执行动态 VLAN 分配

在大多数 WLAN 系统中,每个 WLAN 都有适用于与服务集标识符 (SSID) 关联的所有客户端的静态 策略,即以控制器术语表示 WLAN。虽然此方法功能强大,但也具有局限性,这是因为,它要求客 户端与不同的 SSID 相关联以便继承不同的 QoS 和安全策略。

然而,Cisco WLAN 解决方案支持网络标识。这使得网络可以通告一个 SSID,但允许特定用户根据 用户凭证继承不同的 QoS 或安全策略。

动态 VLAN 分配便是一项这样的功能,它根据无线用户提供的凭证将该用户置于特定 VLAN 中。这 项将用户分配到特定 VLAN 的任务由 RADIUS 身份验证服务器(如 CiscoSecure ACS)处理。例 如,利用此任务可使无线主机能够在园区网络中移动时保持位于同一 VLAN 中。

因此,当客户端尝试关联到在控制器中注册的 LAP 时,LAP 会将用户的凭证传递到 RADIUS 服务 器以进行验证。成功执行身份验证后,RADIUS 服务器便会将某些 Internet 工程任务组 (IETF) 属性 传递给用户。这些 RADIUS 属性确定应该分配给无线客户端的 VLAN ID。客户端的 SSID(WLAN,从 WLC 的角度而言)并不重要,这是因为,会始终为用户分配此预先确定的 VLAN ID。

用于 VLAN ID 分配的 RADIUS 用户属性包括:

- IETF 64(隧道类型)— 将此项设置为 VLAN。
- IETF 65(隧道介质类型)— 将此项设置为 802。
- IETF 81 (隧道专用组 ID) 将此项设置为 VLAN ID。

VLAN ID 为 12 位,并且其值介于 1 和 4094 之间(包含 1 和 4094)。由于Tunnel-Private-Group-ID是字符串类型(如<u>RFC2868</u> 中定义,用于IEEE 802.1X),因此VLAN ID整数值将编码为字符串。 当发送这些隧道属性时,需要填写 Tag 字段。

如RFC2868<u>第3.</u>1节所述:**Tag 字段在长度上是一个八位组,它旨在提供一种方法将同一数据包中** 表示同一隧道的属性进行分组。此字段的有效值是 0x01 到 0x1F(包含 0x01 和 0x1F)。如果未使 用 Tag 字段,则它一定为零 (0x00)。 有关所有 RADIUS 属性的详细信息,请参阅 <u>RFC 2868。</u>

配置

本部分提供有关如何配置本文档所述功能的信息。

本文档使用以下网络设置:



下面是此图中使用的组件的配置详细信息:

- ACS (RADIUS) 服务器的 IP 地址为 172.16.1.1。
- WLC 的管理接口地址为 172.16.1.30。
- WLC 的接入点管理器接口地址为 172.16.1.31。
- DHCP服务器地址172.16.1.1用于为LWAPP分配IP地址。**控制器上的内部 DHCP 服务器用于将** IP 地址分配给无线客户端。
- 在此配置的整个过程中都将用到 VLAN10 和 VLAN11。RADIUS 服务器配置 user1 将其置于 VLAN10 中,配置 user2 将其置于 VLAN11 中。**注:本**文档仅显示与user1相关的所有配置信 息。请为user2完成本文档中介绍的相同步骤。
- 本文档使用带有 LEAP 的 802.1x 作为安全机制。注意:Cisco建议您使用高级身份验证方法

,如EAP-FAST和EAP-TLS身份验证,以保护WLAN。本文档之所以使用 LEAP,仅仅是为了 简单起见。

<u>配置</u>

本文档假设在配置之前已经在 WLC 中注册了 LAP。有关详细信息,请参阅<u>无线 LAN 控制器和轻量</u> <u>接入点基本配置示例。</u>有关涉及的注册过程的信息,请参阅<u>轻量接入点 (LAP) 注册到无线 LAN 控</u> <u>制器 (WLC) 。</u>

配置步骤

此配置分为三类:

- 1. RADIUS 服务器配置
- 2. <u>为多个 VLAN 配置交换机</u>
- 3. <u>WLC 配置</u>
- 4. 无线客户端实用程序配置

RADIUS 服务器配置

此配置要求执行下列步骤:

- <u>将WLC配置为RADIUS服务器上的AAA客户端</u>
- 在 RADIUS 服务器上配置用于动态 VLAN 分配的用户和 RADIUS (IETF) 属性

在 RADIUS 服务器上将 WLC 配置为 AAA 客户端

此过程说明如何在 RADIUS 服务器上将 WLC 添加为 AAA 客户端,以便 WLC 可以将用户凭证传递 到 RADIUS 服务器。

请完成以下步骤:

- 1. 从 ACS GUI 中,单击 Network Configuration。
- 2. 在 AAA Clients 字段下单击 Add Entry 部分。
- 3. 输入 AAA 客户端的 IP 地址和密钥。该 IP 地址应该是 WLC 的管理接口 IP 地址。确保您输入 的密钥与在 WLC 上的 Security 窗口下配置的密钥相同。此密钥是 AAA 客户端 (WLC) 和 RADIUS 服务器之间进行通信时使用的密钥。
- 4. 从 Authenticate Using 字段中选择 RADIUS (Cisco Airespace) 作为身份验证类型。

CISCO SYSTEMS	Network Configuration
addina dillor -	Edit
User Setup	
Group Setup	Add AAA Client
Shared Profile Components	
Netvork Configuration	AAA Client Hostname WLC4400
System Configuration	AAA Client IP Address
Configuration	Shared Secret cisco
Administration Control	RADIUS Key Wrap
Databases	Key Encryption Key
noon Posture	Message Authenticator Code
Network Access Profiles	Key Input Format O ASCII O Hexadecimal
Reports and Activity	Authenticate Using RADIUS (Cisco Airespace)
Documentation	□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure)
	Log Update/Watchdog Packets from this AAA Client
	Log RADIUS Tunneling Packets from this AAA Client
	Replace RADIUS Port info with Username from this AAA Client
	Match Framed-IP-Address with user IP address for accounting packets from this AAA Client
	Submit Submit + Apply Cancel

在 RADIUS 服务器上配置用于动态 VLAN 分配的用户和 RADIUS (IETF) 属性

此过程说明如何配置 RADIUS 服务器上的用户和用于将 VLAN ID 分配给这些用户的 RADIUS (IETF) 属性。

请完成以下步骤:

- 1. 从 ACS GUI 中,单击 User Setup。
- 2. 在 User Setup 窗口的 User 字段中输入用户名,然后单击 Add/Edit。



3. 在 Edit 页上,输入下面所示的必需用户信息

:

CISCO SYSTEMS	User Setup
antilliterentillitere -	Edit
User Setup	User: User1
Setup Shared Profile Components	Account Disabled
Network Configuration	Supplementary User Info 🤶
System Configuration	Real Name User1
Interface Configuration	Description User1
Administration Control	
External User Databases	User Setup 🤶
BBBB Posture Validation	Password Authentication:
Network Access Profiles	CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.)
Activity	Password •••••
Online Documentation	Confirm Password
	Separate (CHAP/MS-CHAP/ARAP)
	Password •••••••••
	Confirm Password
	When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

在此图中,请注意您在 User Setup 部分下提供的口令应该与用户身份验证期间在客户端提供 的口令相同。

4. 向下滚动 Edit 页并找到 IETF RADIUS Attributes 字段。

:

5. 在 IETF RADIUS Attributes 字段中,选中 3 个隧道属性旁边的复选框并配置属性值,如下所示

CISCO SYSTEMS	User Setup	
	Failed attempts since login: 0	last successful
User Setup	Reset current faile	d attempts count
Group Setup	on submit	
Shared Profile Components		
Network Configuration	Download	lable ACLs 🤶
System Configuration	Assign IP ACL:	VPN_Access
Configuration		<u></u>
Administration Control	IETF RADIU	S Attributes
- Content Letternal User	☑ [064] Tunnel-Type	
90 Databases	Tag 1 🗾 Value	VLAN 💽
BBBB Posture Validation	Tag 2 🗾 Value	
Network Access	🗹 [065] Tunnel-Medium-1	Туре
Profiles	Tag 1	▼ Value 802 ▼
Reports and Activity	Tag 2	▼ Value
	🗹 (081) Tunnel-Private-0	Group-ID
	Tag 1 💌 Va	lue 10
	Tag 2 💌 Va	lue
la de la companya de		

注意:在ACS服务器的初始配置中,可能不显示IETF RADIUS属性。选择 **Interface Configuration > RADIUS (IETF) 以在用户配置窗口中启用 IETF 属性。**然后,在 User 和 Group 列中选中属性 **64、65 和 81 对应的复选框。**



注:为了使RADIUS服务器将客户端动态分配给特定VLAN,WLC上需要在RADIUS服务器的 IETF 81(Tunnel-Private-Group-ID)字段下配置的VLAN-ID。选中 Interface Configuration > Advanced Options 下的 Per User TACACS+/RADIUS 属性对应的复选框,以针对每项用户配 置启用 RADIUS 服务器。此外,因为 LEAP 用作身份验证协议,所以,请确保在 RADIUS 服 务器的 System Configuration 窗口中启用 LEAP,如下所示

2



System Configuration

******************	Cisco client initial message:
User Setup	PEAP session timeout (minutes): 120
Group Setup	Enable Fast Reconnect: 🔽
Shared Profile Components	EAP-FAST EAP-EAST Configuration
Network Configuration	
System Configuration	Allow EAP-TLS
Configuration	Select one or more of the following options: Certificate SAN comparison
Administration	🖾 Certificate CN comparison
Databases	EAP-TLS session timeout (minutes): 120
Donal Posture Validation	
Network Access Profiles	LEAP ■ Allow LEAP (For Aironet only)
Reports and Activity	EAP-MD5
Documentation	Allow EAP-MD5
	AP EAP request timeout (seconds): 20

利用 Cisco Airespace VSA 属性配置 ACS 以执行动态 VLAN 分配

在最新ACS版本中,您还可以配置Cisco Airespace [VSA(供应商特定)]属性,以根据ACS上的用 户配置为使用VLAN接口名称(而非VLAN ID)分配已成功通过身份验证的用户。要实现此目的,请 执行本部分中的步骤。

注意:本部分使用ACS 4.1版本配置Cisco Airespace VSA属性。

<u>用 Cisco Airespace VSA 属性选项配置 ACS 组</u>

请完成以下步骤:

- 1. 在 ACS 4.1 GUI 中,单击导航栏中的 **Interface Configuration。**然后,从 Interface Configuration 页中选择 **RADIUS (Cisco Airespace) 以配置 Cisco Airespace 属性选项。**
- 2. 在 RADIUS (Cisco Airespace) 窗口中,选中 Aire-Interface-Name 旁边的 User 复选框(若需

要,可选中 Group 复选框)以使其显示在 User Edit 页上。然后,单击 Submit。



- 3. 转至 user1 的 Edit 页。
- 4. 从 User Edit 页中,向下滚动到 Cisco Airespace RADIUS Attributes 部分。选中 Aire-Interface-Name 属性旁边的复选框并指定要在成功执行用户身份验证后分配的动态接口的名称 。此示例将用户分配到 admin VLAN。

Cisco Systems	User Setup	
	L Date exceeds.	May 🔽 24 2000
User Setup Setup Setup Shared Profile Components Network Configuration	☐ Failed attempts excee 5 Failed attempts since login: 0 ☐ Reset current failed on submit	ad: last successful d attempts count
Configuration		
Configuration	Download	lable ACLs 🤶
Control	Assign IP ACL:	VPN_Access
Databases		
Validation	Cisco Airespace R	
Profiles	☑ [14179\005] Aire-Interfa	ice-Name
	l Indmin	
Reports and Activity	laumin	

5. 单击"Submit"。

为多个 VLAN 配置交换机

为了允许通过交换机的多个 VLAN,您需要发出以下命令以配置连接到控制器的交换机端口:

- 1. Switch(config-if)#switchport mode trunk
- 2. Switch(config-if)#switchport trunk encapsulation dot1q

注意:默认情况下,大多数交换机都允许通过中继端口在该交换机上创建的所有VLAN。

对于 Catalyst 操作系统 (CatOS) 交换机,这些命令会有所不同。

如果有线网络连接到交换机,则可以将此相同配置应用于连接到有线网络的交换机端口。这样将在 位于有线网络和无线网络中的相同 VLAN 之间实现通信。

注意:本文档不讨论VLAN间通信。此内容超出了本文档的范围。您必须了解,对于 VLAN 间路由 ,需要第 3 层交换机或具有适当的 VLAN 和中继配置的外部路由器。有几篇文档介绍了 VLAN 间路 由配置。

<u>WLC 配置</u>

此配置要求执行下列步骤:

- <u>用身份验证服务器的详细信息配置 WLC</u>
- <u>配置动态接口 (VLAN)</u>
- 配置 WLAN (SSID)

用身份验证服务器的详细信息配置 WLC

必须配置 WLC,它才能够与 RADIUS 服务器进行通信以对客户端进行身份验证;另外,对于任何 其他事务,也必须配置 WLC。

请完成以下步骤:

:

- 1. 从控制器 GUI 中,单击 Security。
- 2. 输入 RADIUS 服务器的 IP 地址以及在 RADIUS 服务器和 WLC 之间使用的共享密钥。此共享 密钥应该与在 RADIUS 服务器中的 Network Configuration > AAA Clients > Add Entry 下配置 的密钥相同。下面是 WLC 中的示例窗口

ahaha		and the second				Carlo Saye Co	nfiguration Eng	Logout Befresh
CISCO	MONITOR MLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	RADIUS Authentics	ation Server	s > New	-			< Back	Apply
Security AAA General RADIUS Authentication Accounting Follback TACACS= UDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Local EAP Priority Order Certificate Access Control Lists Wireless Protection	RADIUS Authentics Server Index (Priority Server IP Address Shared Secret Format Shared Secret Confirm Shared Secre Key Wrap Port Number Server Status Support for RPC 3576 Server Timeout Network User Management	ation Serven	s > New 1 = 172.16.1.1 ASCII = •••••• (Designed f 1812 Enabled = 2 second Enabled = 2 second Enabled = 2 second	for FIPS custon	ners and requires	a key wrap comp	< Back	Apply :
Policies	IPSec		Enable	,				
> Advanced	L							

<u>配置动态接口 (VLAN)</u>

此过程说明如何在 WLC 上配置动态接口。如本文档中上文所述,WLC 中也必须具有在 RADIUS 服务器的 Tunnel-Private-Group ID 属性下指定的 VLAN ID。

在此示例中,在 RADIUS 服务器上使用 **Tunnel-Private-Group ID 10 (VLAN =10) 指定了 user1。**请 参阅 user1 的 User Setup 窗口的 <u>IETF RADIUS Attributes 部分。</u>

在此示例中,您会看到在 WLC 中配置的同一动态接口 (VLAN=10)。从控制器 GUI 的 Controller > Interfaces 窗口下,将配置动态接口。

uhuhu cisco		LANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Saya Co C <u>O</u> MMANDS	nfiguration <u>P</u> ing HELP	Logout Befresh
Controller	Interfaces >	New					< Back	Apply
General Inventory Interfaces	Interface Nan VLAN Id	vian10						
Multicast Network Routes								
Internal DHCP Server Mobility Management Douts								
NTP								
Advanced								

- 1. 单击此窗口中的 Apply。这会将您带到此动态接口(这里为 VLAN 10)的 Edit 窗口中。
- 2. 输入此动态接口的 IP 地址和默认网关。

cisco	MONITOR WLANS CO	ONTROLLER WIRELESS	SECURITY	MONAGEMENT	COMMANDS		Contrast Person
Controller	Interfaces > Edit					< Back	Apply
General Inventory Interfaces	General Information						
Multicast	Interface Name	vlan10					
Network Routes	MAC Address	00:0b:85:48:53:c0					
 Internal DHCP Server Mobility Management 	Configuration						
Ports	Guest Lan						
NTP	Quarantine						
▶ CDP	Quarantine Vlan Id	0					
Advanced	Physical Information						
	Port Number	1					
	Backup Port	0					
	Active Port	0					
	Enable Dynamic AP Man	agement 🔲					
	Interface Address						
	VLAN Identifier	10					
	IP Address	172.18.1.10					
	Netmask	255.255.0.0	_				
	Gateway	172.18.1.30					
	DHCP Information						
	Primary DHCP Server	172.16.1.30					
	Secondary DHCP Server						

注意:由于本文档在控制器上使用内部DHCP服务器,因此此窗口的主DHCP服务器字段指向WLC本身的管理接口。您也可以使用外部 DHCP 服务器、路由器或 RADIUS 服务器本身作为无线客户端的 DHCP 服务器。在这种情况下,主 DHCP 服务器字段指向用作 DHCP 服务器的 ip 地址。有关详细信息,请参阅 DHCP 服务器文档。

3. 单击 Apply。现在,您已在 WLC 中配置了一个动态接口。同样,您可以在 WLC 中配置多个 动态接口。不过,请记住,RADIUS 服务器上也必须存在相同 VLAN ID,才能将该特定 VLAN 分配给客户端。

配置 WLAN (SSID)

请完成以下步骤:

- 1. 从控制器 GUI 中,选择 WLAN >New 以创建一个新 WLAN。此时会显示 New WLANs 窗口。
- 2. 输入 WLAN ID 和 WLAN SSID 信息。您可以输入任意名称作为 WLAN SSID。此示例使用

VLAN10 作为 V	VLAN SSID。							
cisco			WIRELESS	SECURITY	Management	Save C C <u>O</u> MMANDS	enfiguration Eing HELP	Logout Befresh
WLANs	WLANs > New						< Back	Apply
 ₩LANs WLANs Advanced 	Type Profile Name SSID ID	VLAN: VLAN: 3						

3. 单击 Apply 以转至 WLAN SSID10 的 Edit 窗口。

WLANs General Security QoS Advanced Profile Name YLANI0 Type WLAN SSID YLANI0 Status Fenabled Security Policies [WPA2][Auth(002.1X)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All Interface management = Broadcast SSID Enabled	
Advanced Profile Name VLANI0 Type WLAN SSID VLANI0 Status IF Enabled Security Policies [WPA2][Auth(882.1X)] (Nodifications done under security tab will appear after applying the changes.) Radio Policy All Interface Imanagement Broadcast SSID IF Enabled	
Type WLAN SSID YLANIO Status F Enabled Security Policies [WPA2][Auth(002.1X)] (Nodifications done under security tab will appear after applying the changes.) Radio Policy All Interface management = Broadcast SSID Enabled	
SSID VLANIO Status Image: Enabled Security Policies [WPA2][Auth(002.1X)] (Nodifications done under security tab will appear after applying the changes.) Radio Policy All Image: Interface Interface Imanagement Image: Enabled	
Status Enabled Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All Interface management = Broadcast SSID Enabled	
Security Policies [WPA2][Auth(002.1X)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All III Interface management IIII Broadcast SSID If Enabled	
Radio Policy All . Interface management . Broadcast SSID I Enabled	
Interface management . Broadcast SSID IF Enabled	
Broadcast SSID 🗭 Enabled	
an a	

WLANS WLANS > Edit <estack< td=""> WLANS WLANS General Security QoS Advanced I ayer 2 Layer 3 AAA Servers Layer 2 Security 2 802.1X I ayer 2 Security 2 802.1X</estack<>	Logout Befi
WLANS WLANS General Security QoS Advanced I ayer 2 Layer 3 AAA Servers Layer 2 Security 802.1X I ayer 2 Security 802.1X I mAC Filtering 802.11 Data Encryption Type Rey Size Rey Size I Data Encryption Type Key Size	Apply
Advanced Layer 2 Layer 3 AAA Servers Layer 2 Security 2 802.1X MAC Filtering 802.11 Data Encryption Type Key Size @ WEP 104 bits	
Layer 2 Security Z 802.1X x MAC Filtering 802.11 Data Encryption Type Key Size @ WEP 104 bits x	
802.11 Data Encryption Type Key Size	
802.11 Data Encryption Type Key Size	
🚱 WEP 104 bits 🖃	

通常,在无线 LAN 控制器中,每个 WLAN 都会映射到一个特定 VLAN (SSID),以便将属于该 WLAN 的特定用户置于所映射的特定 VLAN 中。此映射通常是在 WLAN SSID 窗口的 Interface Name 字段下完成的。

cisco	MONITOR WLAN: CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP						
/LANs	WLANs > Edit < Back	Apply					
WLANS WLANS	General Security QoS Advanced						
Advanced	Layer 2 Layer 3 AAA Servers						
		-					
	Select AAA servers below to override use of default servers on this WLAN						
	Radius Servers LDAP Servers						
	Authentication Servers Accounting Servers Server 1 None -						
	F Enabled Server 2 None -						
	Server 1 1P:172.16.1.1, Port:1012 None Server 3 None -						
	Server 2 None None						
	Server 3 None X None X						
	Local EAP Authentication						
	Local EAP Authentication Enabled						
	Authentication priority order for web-auth user	4					
	LOCAL Up	_					

在所提供的示例中,RADIUS 服务器负责在成功执行身份验证后将无线客户端分配到特定 VLAN。因此,WLAN 不需要映射到 WLC 上的特定动态接口。否则,即使 WLAN 到动态接口 的映射是在 WLC 上完成的,RADIUS 服务器也会覆盖此映射,并将来自该 WLAN 的用户分 配到在 RADIUS 服务器的用户 **Tunnel-Group-Private-ID 字段下指定的 VLAN。**

4. 选中 Allow AAA Override 复选框以便由 RADIUS 服务器覆盖 WLC 配置。

5. 在控制器中为所配置的每个 WLAN (SSID) 启用 Allow AAA Override。

cisco	MONITOR WUANS CONTROLLER WIRELESS SECURITY	MANAGEMENT COMMANDS HELP
CISCO /LANs WLANs WLANs Advanced	MONITOR MULANS CONTROLLER WIRELESS SECURITY WLANS > Edit General Security QoS Advanced Allow AAA Override Imabled Enabled Coverage Hole Detection Imable Enabled Coverage Hole Detection Imable Enabled Enable Imable Session Timeout (secs) Aironet IE Imabled Enabled Diagnostic Channel Enabled Enabled JPv6 Enable Imabled Imabled Override Interface ACL None Imabled Imabled P2P Blocking Action Imabled Imabled Client Exclusion I Imabled Imabled HREAP Imabled Imabled HREAP Enabled Imabled HREAP Imabled Imabled Client IP Address I Imabled Enabled	MANAGEMENT COMMANDS HELP C Back A DHCP Override DHCP Server Override DHCP Addr. Assignment Required Management Frame Protection (MFP) Infrestructure MFP Infrestructure MFP If (Global MFP Disabled) MPP Client Optional ■ Protection # Optional ■ DTIM Period (In beacon intervals)) 602.11a/n (1 - 255) Image: Image:

如果"AAA 覆盖"处于启用状态,并且客户端拥有冲突的 AAA 和控制器 WLAN 身份验证参数 ,则由 AAA (RADIUS) 服务器执行客户端身份验证。在此身份验证期间,操作系统将客户端 移至由 AAA 服务器返回的 VLAN。这是在控制器接口配置中预定义的。例如,如果公司 WLAN 主要使用分配给 VLAN 2 的管理接口,并且"AAA 覆盖"返回指向 VLAN 100 的重定向 ,则操作系统会将所有客户端传输重定向到 VLAN 100,即使将 VLAN 100 分配到了物理端口 也是如此。如果"AAA 覆盖"处于禁用状态,则所有客户端身份验证均默认为控制器身份验证参 数设置,并且当控制器 WLAN 不包含任何特定于客户端的身份验证参数时,身份验证仅由 AAA 服务器执行。

<u>无线客户端实用程序配置</u>

本文档使用 ADU 作为用户配置文件配置的客户端实用程序。此配置也使用 LEAP 作为身份验证协议。按照本部分中的示例所示配置 ADU。

从 ADU 菜单栏中,选择 Profile Management > New 以创建一个新配置文件。

示例客户端配置为SSID VLAN10的一部分。以下图表显示如何在客户端上配置用户配置文件:

Cisco Aironet Desktop Utility - Current Profile:	Default 🛛 💽
Current Status Profile Management Diagnostics	
Default LAP	<u>N</u> ew
Ext.Web	Modily
	Remove
	Activate
Details	
Network Type: Security Mode:	Import
Network Name 1 (SSID1):	Export
Network Name 2 (SSID2):	Scan.
Network Name 3 (SSID3):	
Auto Select Profiles	Order Profiles

Profile N	anagemer	nt		? 🛛
General	Security 4	Advance	a]	
~ Profil	e Settings			
	Profile	Name:	vlan10	
	Client	Name:	wcs	
Netw	ork Names		·····	
		SSID1:	vlan10	
		SSID2:		
		SSID3:		
	* * * *			
				Cancel

WPA/WPA2/CCKM WPA/WPA2/CCKM EAP WPA/WPA2 Passphrase 802.1x 802.1x B02.1x EaP None Configure Allow Association to Mixed Cells Locked Prolie Group Policy Delay:	et Security Options		
802.1x EAP Type: LEAP 802.1x EAP Type: LEAP Pre-Shared Key (Static WEP) None Allow Association to Mixed Cells Locked Profile Group Policy Delay: 60 \$ sec	○ WPA/WPA2/CCKM WPA ○ WPA/WPA2 Passphrase	/WPA2/CCKM EAP Type: LEAP	×
Configure Allow Association to Mixed Cells Locked Profile Group Policy Delay: 60 \$ sec	802.1x Pre-Shared Key (Static WEP) None	802.1× EAP Type: LEAP	~
	Configure Group Policy Delay:	Allow Association to Mixed Cells	
		[] 김 김 남아? 김 김 김 김 남아? 김 김 희 김 남아? 김 희 희	

<u>验证</u>

激活您在 ADU 中配置的用户配置文件。根据配置,系统会提示您输入用户名和口令。您也可以指 示 ADU 使用 Windows 用户名和口令进行身份验证。客户端可以利用一些选项接收身份验证。您可 以在所创建的用户配置文件的 Security > Configure 选项卡下配置这些选项。

在上一示例中,请注意, user1 被分配到在 RADIUS 服务器上指定的 VLAN10。

此示例从客户端使用以下用户名和口令接收身份验证,并且此用户名和口令将由 RADIUS 服务器分 配到 VLAN :

• 用户名 = user1

• 口令 = user1

此示例说明如何提示 SSID VLAN10 输入用户名和口令。在此示例中输入用户名和口令:

Cisco Aironet Action Options H	Desktop Utility - Current Profile: vlan10 ep	? 🗙
Current Status Pr	ofile Management Diagnostics	
Default		New
LAP Ext.Web	Modify	
Vian10		Remove
Enter Wireless N	etwork Password 🗙	Activate
Please enter your Li network	EAP username and password to log on to the wireless	Import
User Name :	user1	Export
		Scan
Password :		Order Profiles
Log on to :		
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter	
Profile Name :	vlan10	
	OK Cancel	

成功执行身份验证和相应验证后,您便会收到成功状态消息。

然后,您需要按照所发送的 RADIUS 属性验证是否已将您的客户端分配到适当的 VLAN。要实现此 目的,请完成下列步骤:

1. 从控制器 GUI 中,选择 Wireless > AP。

:

2. <u>单击 Clients(它显示在接入点 (AP) 窗口的左角上)。此时会显示客户端统计信息。</u>

cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Elud 1	rudon	e i Rieu	e a n
Monitor	Clients								Entrie	s 1 - 4	of 4	
Summary	Current Fi	lter	None	Change Filte	r] (Show All)							
Access Points												
Statistics	Client MA	C Addr	AP Name		WLAN	Profile	Protocol	Status	Auth	Port	WGB	
♦ CDP	00:21:5c:0	9:08:dd	AP1130		Unknow	MD	802.11a	Probing	No	2	No	
Rogues	00:21:50:5	0:3a:1f	AP1130		VLAN1	0	802.11g	Associated	Yes	2	No	
Clients												
Multicast												

3. 单击 Details 以识别客户端的完整详细信息,如 IP 地址、它被分配到的 VLAN 等等。此示例 显示客户端 user1 的以下详细信息

cisco	MONITOR WLANS CONT	ROLLER WIRELESS SECURI	ITY MANAGEMENT COM	Saye Configuration <u>P</u> ing Logout <u>B</u> efre AAND'S HELP
Monitor	Clients > Detail		< Back	Apply Link Test Remove
Summary Access Points	Client Properties		AP Properties	
Statistics	MAC Address	00:21:50:50:3a:1f	AP Address	00:15:c7:ab:55:90
➤ CDP	IP Address	17.18.1.35	AP Name	AP1130
Rogues	Client Type	Regular	AP Type	802.11g
Clients	User Name	User1	WLAN Profile	VLAN10
Multicast	Port Number	2	Status	Associated
	Interface	vlan10	Association ID	1
	VLAN ID	10	802.11 Authentication	Open System
	CCX Version	CCXv4	Reason Code	0
	E2E Version	E2Ev1	Status Code	0
	Mobility Role	Local	CF Pollable	Not Implemented
	Mobility Peer IP Address	N/A	CF Poll Request	Not Implemented
	Policy Manager State	RUN	Short Preamble	Implemented
	Mirror Mode	Disable 💌	PBCC	Not Implemented
	Management Frame Protection	No	Channel Agility	Not Implemented
			Timeout	1800
	Security Information		WEP State	WEP Disable
	Security Policy Completed	Yes		
	Policy Type	802.1X		
	Encryption Cipher	WEP (104 bits)		
	EAP Type	LEAP		
	NAC State	Access		

从此窗口中,您会观察到,已按照在 RADIUS 服务器上配置的 RADIUS 属性将此客户端分配 到 VLAN10。**注:如**果动态VLAN分配基于**Cisco Airespace VSA属性**设置,**接口名称将显示为** 管理员,如本例所示,在客户端详细信息页。

使用本部分可确认配置能否正常运行。

```
• debug aaa events enable — 此命令可用于确保通过控制器成功将 RADIUS 属性传输到客户端
 。调试输出的此部分可确保成功地传输 RADIUS 属性:
 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[0]:
 attribute 64, vendorId 0, valueLen 4
 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[1]:
 attribute 65, vendorId 0, valueLen 4
 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[2]:
 attribute 81, vendorId 0, valueLen 3
 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[3]:
 attribute 79, vendorId 0, valueLen 32
 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Received EAP Attribute
 (code=2, length=32,id=0) for mobile 00:40:96:ac:e6:57
 Fri Jan 20 02:25:08 2006: 00000000: 02 00 00 20 11 01 00 18
 4a 27 65 69 6d e4 05 f5
 .....J'eim...00000010: d0 98 0c cb 1a 0c 8a 3c
 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[4]:
 attribute 1, vendorId 9, valueLen 16
 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[5]:
 attribute 25, vendorId 0, valueLen 28
 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[6]:
 attribute 80, vendorId 0, valueLen 16
 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Type 16777229
 should be 13 for STA 00:40:96:ac:e6:57
 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Medium-Type 16777222
 should be 6 for STA 00:40:96:ac:e6:57
 Fri Jan 20 02:30:00 2006: 00:40:96:ac:e6:57 Station 00:40:96:ac:e6:57
 setting dot1x reauth timeout = 1800
```

• 下列命令也十分有用: debug dot1x aaa enabledebug aaa packets enable

<u>故障排除</u>

目前没有针对此配置的故障排除信息。

注意:动态VLAN分配不适用于WLC的Web身份验证。

相关信息

- 使用 RADIUS 服务器执行 EAP 身份验证
- <u>Cisco LEAP</u>
- Cisco 无线 LAN 控制器配置指南 4.0 版
- <u>技术支持和文档 Cisco Systems</u>