# 在交换机上配置基于MAC的身份验证

### 目标

802.1X是允许列出设备的管理工具,可确保不未经授权访问您的网络。本文档介绍如何使用图形用 户界面(GUI)在交换机上配置基于MAC的身份验证。 要了解如何使用命令行界面(CLI)配置基于 MAC的身份验证,请单击<u>此处</u>。

**注意:**本指南分9节和1节冗长,用于验证主机是否已通过身份验证。喝上咖啡、茶或水,确保您有 充足的时间审核并执行相关步骤。

<u>有关其他信息,请参阅词汇表。</u>

### RADIUS 如何工作?

802.1X身份验证有三个主要组件:请求方(客户端)、身份验证器(网络设备(如交换机)和身份验证服务器(RADIUS)。 远程身份验证拨入用户服务(RADIUS)是使用身份验证、授权和记帐(AAA)协议的接入服务器,可帮助管理网络访问。RADIUS使用客户端 — 服务器模型,在该模型中

,RADIUS服务器和一个或多个RADIUS客户端之间交换安全身份验证信息。它验证客户端的身份 ,并通知交换机客户端是否获得访问LAN的授权。

身份验证器在客户端和身份验证服务器之间工作。首先,它会向客户端请求身份信息。作为响应 ,身份验证器会向身份验证服务器验证信息。最后,它会向客户端中继响应。在本文中,身份验证 器将是包含RADIUS客户端的交换机。交换机将能够封装并解封可扩展身份验证协议(EAP)帧,以与 身份验证服务器交互。

### 基于MAC的身份验证如何?

在基于MAC的身份验证中,当请求方不了解如何与身份验证器通信或无法通信时,它使用主机的 MAC地址进行身份验证。基于MAC的请求方使用纯RADIUS(不使用EAP)进行身份验证。 RADIUS服务器具有仅包含允许的MAC地址的专用主机数据库。服务器不将基于MAC的身份验证请 求视为密码身份验证协议(PAP)身份验证,而是通过属性6 [服务类型] = 10识别此请求。服务器将将 呼叫站ID属性中的MAC地址与主机数据库中存储的MAC地址进行比较。

版本2.4增加了配置为基于MAC的请求方发送的用户名格式并定义EAP身份验证方法或纯RADIUS的 功能。在此版本中,您还可以配置用户名的格式以及为基于MAC的请求方配置不同于用户名的特定 密码。

拓扑:



**注意:**在本文中,我们将使用SG550X-24同时用于RADIUS服务器和身份验证器。RADIUS服务器的静态IP地址为192.168.1.100,身份验证器的静态IP地址为192.168.1.101。

本文档中的步骤在高级显示模**式下**执行。要将模式更改为高级,请转到右上角并在"显示模式"下**拉** 列表中选*择"高*级"。

Language:	English	▼.	Display Mode:	Advanced	•	Logout	SNA	About	Help
									Q

目录

- 1. RADIUS服务器全局设置
- 2. RADIUS服务器密钥
- 3. RADIUS服务器组
- 4. RADIUS服务器用户
- 5. RADIUS客户端
- 6. 802.1X身份验证属性
- 7. 802.1X身份验证基于MAC的身份验证设置
- 8.802.1X身份验证主机和会话身份验证
- 9. 802.1X身份验证端口身份验证
- 10. <u>结论</u>

### 适用设备

- •SX350X系列
- SG350XG系列
- Sx550X 系列
- SG550XG系列

## 软件版本

• 2.4.0.94

## RADIUS服务器全局设置

步骤1.登录到将配置为RADIUS服务器的交换机的基于Web的实用程序,然后导航到**Security >** RADIUS Server > RADIUS Server Global Settings。



步骤2.要启用RADIUS服务器功能状态,请选中RADIUS服务器状态字段中的启用复选框。

RADIUS Server Global Settings		
RADIUS Server Status:	Enable	
Authentication Port:	1812	sec (Range: 1 - 65535, Default: 1812)
Accounting Port:	1813	sec (Range: 1 - 65535, Default: 1813)
Trap Settings		
RADIUS Accounting Traps:	Enable	
RADIUS Authentication Failure Traps:	Enable	
RADIUS Authentication Success Traps:	Enable	
Apply Cancel		

步骤3.要为RADIUS记帐事件、失败的登录或成功的登录生成陷阱,请选中所需的**启用**复选框以生 成陷阱。陷阱是通过简单网络管理协议(SNMP)生成的系统事件消息。发生违规时,陷阱会发送到交 换机的SNMP管理器。以下陷阱设置为:

- RADIUS记帐陷阱 选中以生成RADIUS记帐事件的陷阱。
- RADIUS Authentication Failure Traps 选中以为失败的登录生成陷阱。
- RADIUS Authentication Success Traps 选中以生成成功登录的陷阱。

RADIUS Server Global Settings				
RADIUS Server Status:	Enable			
Authentication Port:	1812	sec (Range: 1 - 65535, Default: 1812)		
C Accounting Port:	1813	sec (Range: 1 - 65535, Default: 1813)		
Trap Settings				
RADIUS Accounting Traps:				
RADIUS Authentication Failure Traps: 🕑 Enable				
RADIUS Authentication Success Traps: C Enable				
Apply Cancel				

步骤4.单击"**应用**"保存设置。

## RADIUS服务器密钥

步骤1.导航至**Security > RADIUS Server > RADIUS Server Keys**。"RADIUS服*务器密钥"*页面打开 。

cisco SG550X-24	cisco RADIUS Language English • Display Mode: Advanced • Logout SNA About Help 24-Port Gigabit Stackable Managed Switch
MAC Address Tables     Multicast	RADIUS Server Keys
Multicast     IP Configuration     Configur	Default Key:       Keep existing default key         Encrypted       Plaintext         Plaintext       (0/128 characters used)         MD5 Digest:       Secret Key Table         NAS Address       Secret Key's MD5         0 results found.       Add         Edit.       Delete
Secure Sensitive Data Man     SSL Server     SSH Server     SSH Client     CCP/UDP Services     O     2011-2018 Cisco Systems, Inc. A	I Rights Reserved.

步骤2.在"密钥*表"部分*,单击**添加……** 添加密钥。

RADIUS Server	RADIUS Server Keys				
Default Key: <ul> <li>Keep existing default key</li> <li>Encrypted</li> <li>Plaintext</li> </ul> (0/128 characters used)					
MD5 Digest:					
Apply Can	Apply Cancel				
Secret Key Table	Secret Key Table				
NAS Address	Secret Key's MD5				
0 results found.					
Add E	dit Delete				

步骤3.将打*开Add Secret Key*窗口页。在*NAS Address*字段中,输入包含RADIUS客户端的交换机的 地址。在本例中,我们将使用IP地址192.168.1.101作为RADIUS客户端。

NAS Address:	192.168.1.101	(IPv4 or IPv6 Address)
Secret Key:	Use default key     Encrypted     Plaintext	(0/128 characters used)
Apply	Close	

步骤4.选择一个用作密钥的单选按钮。以下选项为:

- 使用默认密钥 对于指定的服务器,设备尝试使用现有的默认密钥字符串对RADIUS客户端进 行身份验证。
- 加密 要使用消息摘要算法5(MD5)加密通信,请以加密形式输入密钥。
- •明文 在明文模式下输入密钥字符串。

在本示例中,我们将选择*Plaintext*,并使用单词example**作为**我们的*Secret Key*。按"应用"后,您的 密钥将以加密形式显示。

**注意:**我们不建议使用单词**example**作为密钥。请使用更强的密钥。最多可使用128个字符。如果密码太复杂,记不住,则密码是个好密码,但更好的是,如果你能将密码转换成易于记忆的密码,用特殊字符和数字代替元音——"P@55w0rds@reH@rdT0Remember"。最好不要使用字典中可以找到的任何单词。最好选择一个短语,将一些字母替换为特殊字符和数字。有关详细信息,<u>请参</u>阅此思科博文。

S NAS Address:	192.168.1.101	(IPv4 or IPv6 Address)
Secret Key:	Use default key Encrypted	
1	Plaintext example     2/128 cha	aracters used)
Apply	Close	

步骤5.单击"**应用**"保存配置。密钥现在使用MD5加密。MD5是加密哈希函数,它获取一段数据并创 建唯一的十六进制输出,通常不可复制。MD5使用128位哈希值。

RADIUS Server Keys	
Default Key: <ul> <li>Keep existing default key</li> <li>Encrypted</li> <li>Plaintext</li> </ul>	(0/128 characters used)
MD5 Digest:	
Apply Cancel	
Secret Key Table	
NAS Address Secret Key's MD5	
192.168.1.101 (1a79a4d60de6718e8e5b326e338a	e533
Add Edit Delete	

### RADIUS服务器组

步骤1.导航至Security > RADIUS Server > RADIUS Server Groups。



步骤2.单击Add... 添加新的RADIUS服务器组。

RADIUS Server Groups					
RADIUS Server Group table					
Group Name	Privilege Level	Time Range		VLAN ID	VLAN Name
		Name	State		
0 results found.					
Add Edit Delete					
	DIUS Server DIUS Server Gro Group Name sults found.	DIUS Server Groups DIUS Server Group table Group Name Privilege Level sults found. Add Edit	DIUS Server Groups DIUS Server Group table Group Name Privilege Level Time Ra Name sults found. Edit Delete	DIUS Server Groups DIUS Server Group table Group Name Privilege Level Time Range Name State sults found. Add Edit Delete	DIUS Server Groups         DIUS Server Group table         Group Name       Privilege Level       Time Range       VLAN ID         Name       State         sults found.       Edit       Delete

步骤3.将打开"添加RADIUS服务器组"页。输入组的名称。在本例中,我们将使用MAC802作为组名

Group Name:	MAC802	(6/32 characters	used)
Servilege Level:	1	(Range: 1 - 15, Default: 1)	
Time Range:	Enable		
Time Range Name:	The Edit		
VLAN:	None		
	VLAN ID		(Range: 1 - 4094)
	VLAN Name		(0/32 characters used)
Apply Clos	e		

步骤4.在"权限级别"字段中输入组的管理访*问权限*级别。范围为1 - 15, 15是最特权值,默认值为1。 在本例中,我们将将特权级别保留为1。

#### **注意**:本文不会配*置时*间范*围*或VLAN。

0

🗳 Group Name:	MAC802	(6/32 characters	used)
Privilege Level:	1	(Range: 1 - 15, I	Default: 1)
Time Range:	Enable		
Time Range Name:	The Edit		
VLAN:	None     VLAN ID     VLAN Name		(Range: 1 - 4094) (0/32 characters used)
Apply Clo	se		
步骤5.单击"应 <b>用"</b> (	呆存设置。		

## RADIUS服务器用户

步骤1.导航至Security > RADIUS Server > RADIUS Server Users以配置RADIUS用户。

cisco SG550X-24	Save cisco RADIUS Language: English Visplay Mode: Advanced Visplay Mode: Q
Spanning Tree	PADIUS Server Licere
MAC Address Tables	
Multicast	RADIUS User Table
IP Configuration	
<ul> <li>Security</li> </ul>	Finter: Group ware equals to MACSO2 GO Clear Finter
TACACS+ Client	User Name Group Name Password's MD5
RADIUS Client	0 results found.
RADIUS Server 2	Add Edit Delete
RADIUS Server Global Se	
RADIUS Server Groups	
RADIUS Server Users 3	
RADIUS Server Accountil	
RADIUS Server Rejected	
RADIUS Server Unknowr	
RADIUS Server Statistics	
Password Strength	
Key Management	
Mgmt Access Method	
Secure Sensitive Data Man	
<ul> <li>SSL Server</li> </ul>	
SSH Server	
SSH Client	
TODI IDD Sonifor	
© 2011-2018 Cisco Systems, Inc. Al	II Rights Reserved.



RADIUS Server Users						
RADIUS U	RADIUS User Table					
Filter:	Filter: Group Name equals to MAC802 Go Clear Filter					
	User Name	Group Name	Password's MD5			
0 results fo	ound.					
Add	Edit Dele	te				

步骤3.将打*开"添加RADIUS服务器*用户"页。在*用户名*字段中,输入用户的MAC地址。在本例中,我 们将在计算机上使用以太网MAC地址。

注意:部分MAC地址已模糊。

Ser Name:	54:EE:75:	(17/32 charac	ters used)
Group Name:	MAC802 V		
Password:	Encrypted		
	Plaintext		(0/32 characters used)
Apply	Close		

步骤4.在Group Name下拉列*表中*选择组。如RADIUS服务器<u>组</u>部<u>分的第3步中</u>突出显示的,我们将 选择**MAC802作为此**用户的组名称。

Subser Name:	54:EE:75:	7/32 characters used)
Group Name:	MAC802 V	
Password:	Encrypted	
	Plaintext	(0/32 characters used)
Apply	Close	

步骤5.选择以下单选按钮之一:

- •加密 密钥用于使用MD5加密通信。要使用加密,请以加密形式输入密钥。
- 明文 如果没有加密的密钥字符串(来自其他设备),请在明文模式下输入密钥字符串。生成并显示加密密钥字符串。

我们将选择明文*作为*此用户的密码,并在示例中键入**明文**作为我们的明文密码。

注意:建议不要将示例用作明文密码。我们建议使用更强的密码。

S4:EE:75: (17/32 char	acters used)
Group Name: MAC802 ▼	
Password: Encrypted	
1 Plaintext example	2/32 characters used)
Apply Close	

步骤6.完成配置后单击"应用"。

现在,您已完成RADIUS服务器的配置。在下一节中,我们将配置第二台交换机作为身份验证器。

### RADIUS客户端

步骤1.登录到将配置为身份验证器的交换机的基于Web的实用程序,然后导航至**Security > RADIUS** Client。

cisco SG550X-24	cisco Authenticator Language: English • Display Mode: Advanced • Logout 24-Port Gigabit Stackable Managed Switch	SNA About Help
Getting Started  Dashboard Configuration Wizards	RADIUS Client RADIUS Accounting for Management Access can only be enabled when TACACS+ Accounting is disabled. TACACS+ Accounting is currently Disabled.	ŕ
Search   Status and Statistics  Administration  Port Management  Smartport	RADIUS Accounting: Port Based Access Control (802.1X, MAC Based, Web Authentication) Management Access Both Port Based Access Control and Management Access None	
VLAN Management     Spanning Tree	Use Default Parameters	
MAC Address Tables     Multicast     IP Configuration	© Retries:         3         (Range: 1 - 15, Default: 3)           © Timeout for Repty:         3         sec (Range: 1 - 30, Default: 3)	
Security     TACACS+ Client	Dead Time:     0 min (Range: 0 - 2000, Default: 0)     Key String:     Ecconded	
RADIUS Client) 2  RADIUS Server  Password Strength	Plaintext     (0/128 characters used)	
Key Management     Mgmt Access Method	Source IPv6 Interface: Auto V Source IPv6 Interface: Auto V	
Secure Sensitive Data Man     SSI Senver	Apply Cancel	
© 2011-2018 Cisco Systems, Inc. A	ights Reserved.	

步骤2.向下滚动到*RADIUS表*部分,然后单**击添加……**添加RADIUS服务器。

Use Default Parameters											
C Retries:		3		(Range: 1 - 15, D	efault: 3)						
Timeout for	r Reply:	3		sec (Range: 1 - 3	0, Default: 3)						
🗢 Dead Time	¢	0		min (Range: 0 - 2	000, Default: (	))					
Key String:		Encrypted     Identified (0/128 characters used)									
Source IPv	4 Interfac	e: Auto 🔻									
Source IPv	6 Interfac	e: Auto 🔻									
Apply	Canc	el									
RADIUS Table	е										
Server	Priority	Key String (Encrypted)	Timeout for Reply	Authentication Port	Accounting Port	Retries	Dead Time	Usage Type			
0 results found	0 results found.										
Add	Ed	it Delete									

An \* indicates that the parameter is using the default global value.

第3步。(可选)在"服务器定义"字段中,选择是按IP地址还是名称指*定RADIUS服*务器。在本例中 ,我们将保留默认选择的"按**IP地址"**。

Server Definition:	( By IP address) By name
IP Version:	Version 6  Version 4
IPv6 Address Type:	Iink Local Global
Link Local Interface:	VLAN 1 *
Server IP Address/Name	:
OPriority:	(Range: 0 - 65535)
Key String:	Use Default     User Defined (Encrypted)
	User Defined (Plaintext) (0/128 characters used)
Timeout for Reply:	Use Default     User Defined Default sec (Range: 1 - 30, Default: 3)
Authentication Port:	1812 (Range: 0 - 65535, Default: 1812)
Accounting Port:	<b>1813</b> (Range: 0 - 65535, Default: 1813)
Retries:	Use Default     User Defined Default (Range: 1 - 15, Default: 3)
🗢 Dead Time:	Use Default     User Defined Default min (Range: 0 - 2000, Default: 0)
Usage Type:	Login     802.1x     All

步骤4.(可选)在IP Version字段中选择RADIUS服务器IP地址*的版*本。我们将保留本示例的默**认版** 本4选择。

Server Definition:	🖲 By IP address 🔵 By name	
IP Version:	Version 6 Version 4	
IPv6 Address Type:	Link Local      Global	
Link Local Interface:	VLAN 1 *	
Server IP Address/Name	2:	
Priority:	(Range: 0 - 65535)	
Key String:	Use Default	
	User Defined (Encrypted)	
	User Defined (Plaintext) (0/128 characters used)	
Timeout for Reply:	Use Default	
	User Defined Default sec (Range: 1 - 30, Default: 3)	
Authentication Port:	<b>1812</b> (Range: 0 - 65535, Default: 1812)	
Accounting Port:	<b>1813</b> (Range: 0 - 65535, Default: 1813)	
Setries:	Use Default	
	User Defined Default (Range: 1 - 15, Default: 3)	
Dead Time:	Use Default	
	User Defined Default min (Range: 0 - 2000, Default: 0)	
Usage Type:	Cogin	
	02.1x	
	All	
		-
Apply Close		Ţ

步骤5.按IP地址或名称输入RADIUS服务器。我们将在Server IP Address/Name字**段中输入IP地**址 192.168.1.100。

Server Definition:	💿 By IP address 🔵 By name
IP Version:	Version 6  Version 4
IPv6 Address Type:	Iink Local Global
Link Local Interface:	VLAN 1 *
Server IP Address/Name	н <b>(192.168.1.100</b>
Priority:	(Range: 0 - 65535)
Key String:	Use Default     User Defined (Encrypted)
Timeout for Reply:	User Defnuet (Plaintext) (0/128 characters used) Use Default User Defined Default sec (Range: 1 - 30, Default: 3)
Authentication Port:	1812 (Range: 0 - 65535, Default: 1812)
Accounting Port:	1813 (Range: 0 - 65535, Default: 1813)
CRETIES:	Use Default     User Defined Default     (Range: 1 - 15, Default: 3)
Ö Dead Time:	Use Default     User Defined Default min (Range: 0 - 2000, Default: 0)
Usage Type:	Login 802.1x All

步骤6.输入服务器的优先级。优先级确定设备尝试联系服务器以验证用户的顺序。设备首先从优先 级最高的RADIUS服务器启动。零是最高优先级。

[	
Server Definition:	By IP address By name
IP Version:	Version 6      Version 4
IPv6 Address Type:	Iink Local Global
Link Local Interface:	VLAN 1 ¥
Server IP Address/Name	: 192.168.1.100
Priority:	(Range: 0 - 65535)
Key String:	Use Default     User Defined (Encrypted)
	User Defined (Plaintext) (0/128 characters used)
Timeout for Reply:	Use Default     User Defined Default sec (Range: 1 - 30, Default: 3)
Authentication Port:	<b>1812</b> (Range: 0 - 65535, Default: 1812)
Accounting Port:	1813 (Range: 0 - 65535, Default: 1813)
Retries:	Use Default     User Defined Default (Range: 1 - 15, Default: 3)
Contemporary Dead Time:	Use Default     User Defined Default min (Range: 0 - 2000, Default: 0)
Usage Type:	Login     802.1x     All
Apply Close	

步骤7.输入用于验证和加密设备与RADIUS服务器之间通信的密钥字符串。此密钥必须与RADIUS服 务器上配置的密钥匹配。可以以加密或明**文格**式**输入**它。如果**选择Use Default**,设备将尝试使用默 认密钥字符串向RADIUS服务器进行身份验证。我们将使用"用户定**义(明文)"**并在关键示例中**输入** 。

**注意:**我们将保留其余配置为默认配置。如果需要,可以配置它们。

Server Definition:	By IP address      By name	
IP Version:	Version 6      Version 4	
IPv6 Address Type:	Eink Local      Global     Global	
Link Local Interface:	VLAN 1 ¥	
Server IP Address/Name	: 192.168.1.100	
Priority:	0 (Range: 0 - 65535)	
Key String:	Use Default User Defined (Encrypted)	
	User Defined (Plaintext) example (7/128 characters used)	
Timeout for Reply:	Use Default     User Defined Default sec (Range: 1 - 30, Default: 3)	
Authentication Port:	1812 (Range: 0 - 65535, Default: 1812)	
Accounting Port:	1813 (Range: 0 - 65535, Default: 1813)	
· Retries:	Use Default     User Defined Default (Range: 1 - 15, Default: 3)	
Dead Time:	Use Default     User Defined Default min (Range: 0 - 2000, Default: 0)	
Usage Type:	<ul> <li>Login</li> <li>802.1x</li> <li>All</li> </ul>	
Apply Close	)	Ŧ

步骤8.单击Apply保存配置。

### 802.1X身份验证属性

属性页用于全局启用端口/设备身份验证。要使身份验证正常运行,必须在每个端口上全局和单独激 活它。

步骤1.导航至Security > 802.1X Authentication > Properties。

cisco SG550X-24	24-Port Gigabit Stackable	© <sup>Save</sup> elsee Authenticator Language English ▼ Display Mode: Advanced ▼ Logout SNA A le Managed Switch	About Help
IP Configuration     Security	Properties		^
TACACS+ Client RADIUS Client RADIUS Server Password Strength Key Management	Port-Based Authentication: Authentication Method:	Enable     RADIUS, None     RADIUS     RADIUS     None	
<ul> <li>Mgmt Access Method Management Access Authe</li> <li>Secure Sensitive Data Man</li> <li>SSL Server</li> </ul>	Guest VLAN: Guest VLAN ID: Guest VLAN Timeout:	Enable      Iv     Investate     Ives Defined	
SSH Server     SSH Server     SSH Glent     TCP/UDP Services     Storm Control     Port Security     002-1X Authentication     Port Authentication     Host and Session Authen     Authenticated Hosts     Locked Clents     Web Authenticated     Marb.Based Authenticate     A	Trap Settings 802.1x Authentication Failure Traps: 802.1x Authentication Success Traps: MAC Authentication Failure Traps: MAC Authentication Success Traps: Supplicant Authentication Sulfure Traps: Web Authentication Failure Traps: Web Authentication Success Traps: Web Authentication Success Traps:	User Defined     sec (Range: 30 - 180)       Enable     Enable       Enable     Enable       Stable     sec (Range: 30 - 180)	Ţ
© 2011-2018 Cisco Systems, Inc. Al	Rights Reserved.		

步骤2.选中Enable复选框以启用基于端口的身份验证。

Properties			
Port-Based Authentica	ation:	Enable	
Authentication Method	d:	RADIUS, None RADIUS None	
Guest VLAN:		Enable	
Guest VLAN ID:	1	<b>v</b>	
Guest VLAN Timeout:	•	Immediate	Range: 30 - 180)
Trap Settings			(ange: 00 - 100)
802.1x Authentication	Failure Traps:	Enable	
802.1x Authentication	Success Traps:	Enable	
MAC Authentication F	ailure Traps:	Enable	
MAC Authentication S	Success Traps:	Enable	
Supplicant Authentica	tion Failure Traps:	Enable	
Supplicant Authentica	tion Success Traps: 📃	Enable	
Web Authentication F	ailure Traps:	Enable	
Web Authentication S	uccess Traps:	Enable	
Web Authentication Q	uiet Traps:	Enable	

步骤3.选择用户身份验证方法。我们将选择RADIUS作为身份验证方法。以下选项为:

- RADIUS, None 首先使用RADIUS服务器执行端口身份验证。如果没有从RADIUS收到响应 (例如,如果服务器关闭),则不执行身份验证,并允许会话。如果服务器可用,但用户凭证 不正确,则访问被拒绝,会话终止。
- RADIUS 在RADIUS服务器上对用户进行身份验证。如果未执行身份验证,则不允许会话。
- •无 不对用户进行身份验证。允许会话。

Pro	operties			
	Port-Based Authentication:		Enable	
	Authentication Method:		RADIUS, None RADIUS None	
	Guest VLAN:		Enable	
	Guest VLAN ID:	1	V	
ø	Guest VLAN Timeout:	•	Immediate User Defined	sec (Range: 30 - 180)
	Trap Settings		,	
	802.1x Authentication Failure Traps:		Enable	
	802.1x Authentication Success Traps:		Enable	
	MAC Authentication Failure Traps:		Enable	
	MAC Authentication Success Traps:		Enable	
	Supplicant Authentication Failure Traps:		Enable	
	Supplicant Authentication Success Traps:		Enable	
	Web Authentication Failure Traps:		Enable	
	Web Authentication Success Traps:		Enable	
	Web Authentication Quiet Traps:		Enable	

步骤4.(可选)选中MAC Authentication Failure Traps和MAC Authentication Success Traps的

**Enable复选框。**如果MAC身份验证失败或成功,这将生成陷阱。在本示例中,我们将同时启*用 MAC身份验证失败陷*阱和*MAC身份验证成功陷阱*。

Properties			
Port-Based Authentication:		Enable	
Authentication Method:	•	RADIUS, None RADIUS None	
Guest VLAN:		Enable	
Guest VLAN ID:	1	<b>V</b>	
Guest VLAN Timeout:	•	Immediate User Defined	sec (Range: 30 - 180)
Trap Settings		,	
802.1x Authentication Failure Traps:		Enable	
802.1x Authentication Success Traps:		Enable	
MAC Authentication Failure Traps:		Enable	
MAC Authentication Success Traps:		Enable	
Supplicant Authentication Failure Traps:		Enable	
Supplicant Authentication Success Traps:		Enable	
Web Authentication Failure Traps:		Enable	
Web Authentication Success Traps:		Enable	
Web Authentication Quiet Traps:		Enable	

步骤5.单击"**应用"**。

## 802.1X身份验证基于MAC的身份验证设置

此页面允许您配置适用于基于MAC的身份验证的各种设置。

步骤1.导航至Security > 802.1X Authentication > MAC-Based Authentication Settings。

cisco SG550X-24	24-Port Gigabit S	elsco Authenticator Language: English 🔹 Display Mode: Advanced V Logout SNA About Help Stackable Managed Switch
Security TACACS+ Client	MAC-Based Auther	tication Settings
RADIUS Client RADIUS Server Password Strength	MAC Authentication Typ	e: • EAP RADIUS
<ul> <li>Key Management</li> <li>Mgmt Access Method Management Access Auther</li> </ul>	Username Format Group Size:	01
Secure Sensitive Data Man     SSL Server     SSH Server		○ 2 4 • 12
<ul> <li>SSH Client TCP/UDP Services</li> </ul>	Group Separator:	0: •
Port Security  802.1X Authentication 2	Case:	Lowercase     Uppercase
Properties Port Authentication	MAC Authentication Pa	issword
Authenticated Hosts Locked Clients	Password:	Use default (Username)     Encrypted
Web Authentication Custo Supplicant Credentials	Password MD5 Digest:	Plaintext (0/32 characters used)
Denial of Service Preventio	Apply Cancel	Display Sensitive Data as Plaintext
© 2011-2018 Cisco Systems, Inc. All	Rights Reserved.	

步骤2.在MAC身份验证类型中,选择以下选项之一:

- EAP 对交换机(RADIUS客户端)和RADIUS服务器(对基于MAC的请求方进行身份验证 )之间的流量使用RADIUS和EAP封装。
- RADIUS 对交换机(RADIUS客户端)和RADIUS服务器(对基于MAC的请求方进行身份验证)之间的流量使用不带EAP封装的RADIUS。

Username Format Group Size: Group Separator:	<ul> <li>1</li> <li>2</li> <li>4</li> <li>12</li> </ul>	
Group Size: Group Separator:	<ul> <li>1</li> <li>2</li> <li>4</li> <li>12</li> </ul>	
Group Separator:		
	<ul> <li>○ :</li> <li>● -</li> <li>○ .</li> </ul>	
Case:	<ul><li>Lowercase</li><li>Uppercase</li></ul>	
MAC Authentication Pa	ssword	
Password:	Use default (Username)     Encrypted	
Password MD5 Digest:	Plaintext	(0/32 characters used)

步骤3.在Username Format*中*,选择作为用户名发送的MAC地址的分隔符之间的ASCII字符数。在 本例中,我们将选择2作为组大小。

**注意:**确保用户名格式与在"Radius服务器用户"部分输入MAC地址<u>的方式</u>相同。

MAC-Based Auther	ntication Settings
MAC Authentication Typ	e: EAP • RADIUS
Username Format	
Group Size:	
	0 4 0 12
Group Separator:	<ul> <li>○ :</li> <li>○ -</li> <li>○ .</li> </ul>
Case:	<ul> <li>Lowercase</li> <li>Uppercase</li> </ul>
MAC Authentication P	assword
Password:	Use default (Username)     Encrypted
Password MD5 Digest:	
Apply Cancel	Display Sensitive Data as Plaintext

步骤4.选择用作MAC地址中已定义字符组之间分隔符的字符。在本例中,我们将选择:作为组分隔符

o

MAC-Based Auther	ntication Settings
MAC Authentication Typ	e: EAP • RADIUS
Username Format	
Group Size:	<ul> <li>1</li> <li>2</li> <li>4</li> <li>12</li> </ul>
Group Separator:	
Case:	<ul> <li>Lowercase</li> <li>Uppercase</li> </ul>
MAC Authentication Pa	assword
Password:	<ul> <li>Use default (Username)</li> <li>Encrypted</li> <li>Plaintext</li> <li>(0/32 characters used)</li> </ul>
Password MD5 Digest:	
Apply Cancel	Display Sensitive Data as Plaintext
步骤5.在"大小 <i>写"</i> 字段中	,选择 <b>小写</b> 或 <b>大写</b> ,以便以小写或大写形式发送用户名。

MAC-Based Auther	ntication Settings
MAC Authentication Type	e: EAP • RADIUS
Username Format	
Group Size:	<ul> <li>1</li> <li>2</li> <li>4</li> <li>12</li> </ul>
Group Separator:	● : ● - ● .
Case:	Lowercase Uppercase
MAC Authentication Pa	assword
Password:	<ul> <li>Use default (Username)</li> <li>Encrypted</li> <li>Plaintext</li> <li>(0/32 characters used)</li> </ul>
Password MD5 Digest:	
Apply Cancel	Display Sensitive Data as Plaintext

步骤6.密码定义交换机如何通过RADIUS服务器进行身份验证。选择以下选项之一:

- •使用默认(用户名)—选择此项以使用定义的用户名作为密码。
- Encrypted 以加密格式定义密码。
- •明文(Plaintext)—以明文格式定义密码。

MAC-Based Authenti	cation Settings
MAC Authentication Type:	<ul><li>EAP</li><li>RADIUS</li></ul>
Username Format	
Group Size:	<ul> <li>1</li> <li>2</li> <li>4</li> <li>12</li> </ul>
Group Separator:	● : ○ - ○ .
Case:	<ul><li>Lowercase</li><li>Uppercase</li></ul>
MAC Authentication Pass	sword
Password:	<ul> <li>Use default (Username)</li> <li>Encrypted</li> <li>Plaintext example (7/32 characters used)</li> </ul>
Password MD5 Digest:	
Apply Cancel	Display Sensitive Data as Plaintext

**注意:**密码消息摘要算法5(MD5)摘要显示MD5摘要密码。MD5是加密哈希函数,它获取一段数据并 创建一个通常不可复制的唯一十六进制输出。MD5使用128位哈希值。

步骤7.单击"应用",将设置保存到"运行配置"文件。

### 802.1X身份验证主机和会话身份验证

"主机和会话身份验证"页可以定义802.1X在端口上运行的模式以及检测到违规时要执行的操作。

步骤1.导航至Security > 802.1X Authentication > Host and Session Authentication。

cisco SG550X-24	24-	Port Gi	gabit	Stackable Ma	<sup>save cisco</sup> inaged Swit	o Auth	enticator Languag	e: English	۲	Display Mode	Advanced •	Logout	SNA A	About	Help <b>Q</b>
Security TACACS+ Client	Hos	st and Se	ssion	Authentication											*
RADIUS Client	Ho	st and Sessi	on Auth	entication Table							Showing 1-28	of 28 Al	l▼ per i	page	
<ul> <li>RADIUS Server</li> <li>Password Strength</li> </ul>	Filt	er: Interface	<i>Type</i> eq	uals to Port of Unit 1 🔻	Go				1						
Key Management		Entry No.	Port	Host Authentication	Single Host										
Management Access Authe					Action on Violation	Traps	Trap Frequency	Number of Violations							
<ul> <li>Secure Sensitive Data Man</li> </ul>		1	GE1	Multiple Host (802.1X)											
<ul> <li>SSL Server</li> </ul>		2	GE2	Multiple Host (802.1X)											
▶ SSH Server		3	GE3	Multiple Host (802.1X)											
SSH Client		4	GE4	Multiple Host (802.1X)											
Storm Control		5	GE5	Multiple Host (802.1X)											
Port Security		6	GE6	Multiple Host (802.1X)											
( 802.1X Authentication) (2)		7	GE7	Multiple Host (802.1X)											
Properties		8	GE8	Multiple Host (802.1X)											
Port Authentication		9	GE9	Multiple Host (802.1X)											
Host and Session Authen 3		10	GE10	Multiple Host (802.1X)											
Locked Clients		11	GE11	Multiple Host (802.1X)											
Web Authentication Custo		12	GE12	Multiple Host (802.1X)											
Supplicant Credentials		13	GE13	Multiple Host (802.1X)											
MAC-Based Authenticatic		14	GE14	Multiple Host (802 1X)											
Denial of Service Preventio		15	GE15	Multiple Host (802.1X)											-
© 2011-2018 Cisco Systems, Inc. All	Rights	Reserved.	5210	(002.1X)											

步骤2.选择要配置主机身份验证的端口。在本例中,我们将在GE1连接到终端主机时对其进行配置

	lost	t and Se	ssion	Authentica	ation										
Г	Llead	and Secol		ntiection Tobl											
ŀ	Host	and Sessie	on Authe	ntication labi	e										
	Filter	: Interface	<i>Type</i> equ	als to Port of	f Unit 1 ▼	Go									
		Entry No.	Port	Host Authenti	cation	Single Ho	ost	-					6 X C		
ŀ		1	CE1	Multiple Hest	(802.1V)	Action or	n Violation	n Ir	aps	Trap F	requency	Numb	er of Vio	lations	
ŀ		2	GE2	Multiple Host	(802.1X)										
ł		3	GE3	Multiple Host	(802.1X)										
ľ		4	GE4	Multiple Host	(802.1X)										
		5	GE5	Multiple Host	(802.1X)										
		6	GE6	Multiple Host	(802.1X)										
ŀ		7	GE7	Multiple Host	(802.1X)										
ŀ		9	GE9	Multiple Host	(802.1X)										
ľ		10	GE10	Multiple Host	(802.1X)										
l		11	GE11	Multiple Host	(802.1X)										
		12	GE12	Multiple Host	(802.1X)										
l		13	GE13	Multiple Host	(802.1X)										
ļ		14 • ¥ + -	GE14		(802.1X)										
Ż	ケ滎	3.単击∟	:dit ∦	<b>笔直</b> ज日。											
	0		10	GE10	Multiple	Host	(802.1	1X)							
			11	GE11	Multiple	Host	(802.1	1X)							
			12	GE12	Multiple	Host	(802.1	IX)							
			13	GE13	Multiple	Host	(802.1	1X)							
I			14	GE14	Multiple	Host	(802.1	IX)							
l			15	GE15	Multiple	Host	(802.1	1X)							
I	0		16	GE16	Multiple	Host	(802.1	1X)							
l			17	GE17	Multiple	Host	(802.1	IX)							
I	0		18	GE18	Multiple	Host	(802.1	1X)							
			19	GE19	Multiple	Host	(802.1	IX)							
I	0		20	GE20	Multiple	Host	(802.1	IX)							
l			21	GE21	Multiple	Host	(802.1	IX)							
	0		22	GE22	Multiple	Host	(802.1	1X)							
			23	GE23	Multiple	Host	(802.1	IX)							
			24	GE24	Multiple	Host	(802.1	1X)							
	•		25	XG1	Multiple	Host	(802.1	1X)							
			26	XG2	Multiple	Host	(802.1	1X)							
			27	XG3	Multiple	Host	(802.1	IX)							
			28	XG4	Multiple	Host	(802.1	IX)							

步骤4.在Host Authentication*字段*中,选择以下选项之一:

Edit...

Copy Settings...

- 如果有授权的客户端,则端口被授权。一个端口上只能有一台主机获得授权。
- 当端口未授权且启用访客VLAN时,无标记流量将重新映射到访客VLAN。除非标记流量属于 访客VLAN或未经身份验证的VLAN,否则将丢弃该流量。如果端口上未启用访客VLAN,则 只桥接属于未经身份验证的VLAN的标记流量。
- 当端口被授权时,来自授权主机的未标记和已标记流量会根据静态VLAN成员端口配置进行 桥接。来自其他主机的流量将被丢弃。
- 用户可以指定在身份验证过程中,来自授权主机的无标记流量将重新映射到由RADIUS服务 器分配的VLAN。除非标记流量属于RADIUS分配的VLAN或未经身份验证的VLAN,否则将 丢弃该流量。端口上的Radius VLAN分配在端口身份验证页中设置。
- 2. 多主机模式
  - 如果至少有一个授权客户端,则端口会被授权。
  - 当端口未授权且启用访客VLAN时,无标记流量将重新映射到访客VLAN。除非标记流量属于 访客VLAN或未经身份验证的VLAN,否则将丢弃该流量。如果端口上未启用访客VLAN,则 只桥接属于未经身份验证的VLAN的标记流量。
  - 当端口被授权时,会根据静态VLAN成员端口配置桥接来自连接到端口的所有主机的无标记和有标记流量。
  - 您可以指定来自授权端口的无标记流量将重新映射到身份验证过程中由RADIUS服务器分配 的VLAN。除非标记流量属于RADIUS分配的VLAN或未经身份验证的VLAN,否则将丢弃该 流量。端口上的Radius VLAN分配在端口身份验证页中设置。
- 3. 多会话模式
  - 与单主机和多主机模式不同,多会话模式中的端口没有身份验证状态。此状态分配给连接到端口的每个客户端。
  - •无论主机是否已授权,属于未经身份验证的VLAN的标记流量都始终会桥接。
  - 来自非未经身份验证的VLAN的未授权主机的已标记和未标记流量在VLAN上定义和启用时重 新映射到访客VLAN,或在端口上未启用访客VLAN时丢弃。
  - 您可以指定来自授权端口的无标记流量将重新映射到身份验证过程中由RADIUS服务器分配的VLAN。除非标记流量属于RADIUS分配的VLAN或未经身份验证的VLAN,否则将丢弃该流量。端口上的Radius VLAN分配在端口身份验证页中设置。

Host Authentication:		
(	Single Host Multiple Host (802.1X) Multiple Sessions	
Single Host Violation Settings		
Action on Violation:	<ul> <li>Protect (Discard)</li> <li>Restrict (Forward)</li> <li>Shutdown</li> </ul>	
Traps:	Enable	
Trap Frequency:	10	sec (Range: 1 - 1000000, Default: 10)

步骤5.单击"**应用**"保存配置。

**注意:**使用*复制设置……* 将GE1的相同配置应用到多个端口。将连接到RADIUS服务器的端口保留 *为多主机(802.1X)*。

### 802.1X身份验证端口身份验证

"端*口身份验*证"页启用每个端口的参数配置。由于某些配置更改仅在端口处于强制授权状态(例如 主机身份验证)时才可能发生,因此建议在进行更改之前将端口控制更改为强制授权。配置完成后 ,将端口控制恢复到其先前状态。

注意:我们将仅配置基于MAC的身份验证所需的设置。其余配置将保留为默认值。

步骤1.导航至Security > 802.1X Authentication > Port Authentication。

cisco SG550X-24	24-	Port G	igabi	t Stackat	ole Manage	<sub>cisco Auther</sub> d Switch	nticator La	anguage: Englis	sh	<ul> <li>Display Mode</li> </ul>	Advanced •	Logout SNA	About Help
Multicast     IP Configuration	Po	rt Authe	nticati	on									^
TACACS+ Client RADIUS Client	Po Filt	ter: Interfac	cation Ta se Type e	ble quals to Port o	f Unit 1 🔻 Go								
<ul> <li>RADIUS Server</li> <li>Password Strength</li> </ul>		Entry No	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access	802.1x Based Authentication	MAC Based Authentication	Web Based Authentication	Periodic Reauthentication	Reauth
Mgmt Access Method     Management Access Auther			GE1 GE2	Authorized Port Down	Force Authorized	Disabled Disabled	Disabled Disabled	Disabled Disabled	Enabled Enabled	Disabled Disabled	Disabled Disabled	Disabled Disabled	
<ul> <li>Secure Sensitive Data Man</li> <li>SSL Server</li> </ul>		:	GE3	Port Down	Force Authorized	Disabled Disabled	Disabled Disabled	Disabled	Enabled Enabled	Disabled	Disabled Disabled	Disabled	
<ul> <li>SSH Server</li> <li>SSH Client</li> </ul>		ŧ	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
TCP/UDP Services Storm Control			6 GE6 7 GE7	Port Down Port Down	Force Authorized Force Authorized	Disabled Disabled	Disabled Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
Port Security 802.1X Authentication 2		8	3 GE8 9 GE9	Port Down Port Down	Force Authorized Force Authorized	Disabled Disabled	Disabled Disabled	Disabled Disabled	Enabled Enabled	Disabled Disabled	Disabled Disabled	Disabled Disabled	
Properties Port Authentication 3		10	GE10	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
Host and Session Authen Authenticated Hosts	0	12	GE12	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
Locked Clients Web Authentication Custo		10	6E13 GE14	Port Down Port Down	Force Authorized Force Authorized	Disabled Disabled	Disabled Disabled	Disabled Disabled	Enabled Enabled	Disabled Disabled	Disabled Disabled	Disabled Disabled	•
A	Right	Reconved											Þ

步骤2.选择要配置端口授权的端口。

注意:请勿配置交换机所连接的端口。交换机是受信任设备,因此将该端口保留为"强制授权"。

Por	Port Authentication											
Por	Port Authentication Table											
Filte	er: Interface	<i>Type</i> eq	uals to Port of	f Unit 1 🔻 Go								
	Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access	802.1x Based Authentication	MAC Based Authentication	Web Based Authentication	Periodic Reauthentication	Reauth
0					Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
0	2	GE2	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
	3	GE3	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
0	4	GE4	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
	6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
	7	GE7	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
0	8	GE8	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
	9	GE9	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
0	10	GE10	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
	11	GE11	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
	12	GE12	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
	13	GE13	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
0	14	GE14	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	

步骤3.然后向下滚动并单击"编辑……"配置端口。

0	11	GE11	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0	12	GE12	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
•	13	GE13	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0	14	GE14	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
•	15	GE15	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
$\odot$	16	GE16	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
•	17	GE17	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0	18	GE18	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
•	19	GE19	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0	20	GE20	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
•	21	GE21	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0	22	GE22	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
•	23	GE23	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
$\odot$	24	GE24	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
•	25	XG1	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
$\odot$	26	XG2	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
•	27	XG3	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
0	28	XG4	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled
С	opy Sett	ings	Edit.								

在"编辑*端口身份验证*"页中,"当前端口控制"字段显示当前端口授权状态。如果状态为"*授权*",则端 口将通过身份验证或"管理端口控制"为"强制授权"。相反,如果状态为"未授权",则端口要么未通过 身份验证,要么"管理端口控制"为"强制未授权"。如果接口上启用了Supplicant客户端,则当前端口 控制将是Supplicant客户端。

步骤4.选择管理端口授权状态。将端口配置为Auto。可用选项包括:

- 强制未授权 通过将接口移至未授权状态来拒绝接口访问。设备不通过接口向客户端提供身份 验证服务。
- •自动 在设备上启用基于端口的身份验证和授权。接口根据设备和客户端之间的身份验证交换 在授权或未授权状态之间移动。
- •强制授权—授权接口,不进行身份验证。

**注意:** 强制授权是默认值。

Interface:	Unit 1 V Port GE1 V	
Current Port Control:	Authorized	
Administrative Port Control:	Force Unauthorized	
RADIUS VLAN Assignment:	<ul> <li>Disable</li> <li>Reject</li> <li>Static</li> </ul>	
Guest VLAN:	Enable	
Open Access:	Enable	
802.1x Based Authentication:	Enable	
MAC Based Authentication:	Enable	
Web Based Authentication:	Enable	
Periodic Reauthentication:	Enable	
Reauthentication Period:	3600	sec (Range: 300 - 4294967295, Default: 3600)
Reauthenticate Now:		
Authenticator State:	Force Authorized	
Time Range:	Enable	
Time Range Name:	▼ Edit	
Maximum WBA Login Attempts	:  Infinite User Defined	(Range: 3 - 10)
The second secon	<ul> <li>Infalls</li> </ul>	

步骤5.在"基于*802.1X的身份验证"字*段中,取消选中**启用**复选框,因为我们不会使用802.1X作为身 份验证。默认值为*802.1x Based Authentication*已启用。

	Interface:	Unit 1 V Port GE1 V	
	Current Port Control:	Authorized	
	Administrative Port Control:	Force Unauthorized     Auto     Force Authorized	
	RADIUS VLAN Assignment:	<ul> <li>Disable</li> <li>Reject</li> <li>Static</li> </ul>	
	Guest VLAN:	Enable	
	Open Access:	Enable	
	802.1x Based Authentication:	Enable	
	MAC Based Authentication:	Enable	
	Web Based Authentication:	Enable	
	Periodic Reauthentication:	Enable	
0	Reauthentication Period:	3600 sec	(Range: 300 - 4294967295, Default: 3600)
	Reauthenticate Now:		
	Authenticator State:	Force Authorized	
	Time Range:	Enable	
	Time Range Name:	▼ Edit	
0	Maximum WBA Login Attempts:	Infinite     User Defined	(Range: 3 - 10)
	Maximum WBA Silence Period	Infinite	

步骤6.选中*基于MAC的身份验证*的**启用**复选框,因为我们要根据请求方MAC地址启用端口身份验证 。端口上只能使用8个基于MAC的身份验证。

_			
	Interface:	Unit 1 V Port GE1 V	Î
	Current Port Control:	Authorized	
	Administrative Port Control:	Force Unauthorized     Auto     Force Authorized	
	RADIUS VLAN Assignment:	Disable     Reject     Static	
	Guest VLAN:	Enable	
	Open Access:	Enable	
	802.1x Based Authentication:	Enable	
	MAC Based Authentication:	e Enable	
	Web Based Authentication:	Enable I	
	Periodic Reauthentication:	Enable	
	Reauthentication Period:	3600 sec (Range: 300 - 4294967295, Default: 3600)	
	Reauthenticate Now:		
	Authenticator State:	Force Authorized	
	Time Range:	Enable	
	Time Range Name:	v Edit	
	Maximum WBA Login Attempts:	Infinite     User Defined     (Range: 3 - 10)	
	Maximum WBA Silence Period:	Infinite	•

步骤7.单击"**应用**"保存更改。

如果要保存配置,请按屏幕顶部的Save按钮。



## 结论

您现在已成功在交换机上配置基于MAC的身份验证。要验证基于MAC的身份验证是否正常工作,请 执行以下步骤。

步骤1.导航至Security > 802.1X Authentication > Authenticated Hosts,**查看有关已**验证用户的详细 信息。



步骤2.在本例中,您可以看到我们的以太网MAC地址已在已验证的主*机表中进行身份验证*。以下字 段定义为:

- 用户名 在每个端口上进行身份验证的请求方名称。
- 端口 端口的编号。
- •会话时间(DD:HH:MM:SS) 请求方在端口进行身份验证和授权访问的时间。
- Authentication Method 对上次会话进行身份验证的方法。
- Authenticated Server RADIUS服务器。
- MAC地址 显示请求方MAC地址。
- VLAN ID 端口的VLAN。

Authenticated Hosts							
Authenticated Host Table							
User Name	Port	Session Time (DD:HH:MM:SS)	Authentication Method	Authentication Server	MAC Address	VLAN ID	
54:EE:75:	GE1/1	00:00:06:56	MAC	Remote	54:ee:75:		

步骤3.(可选)导航至Status and Statistics > View Log > RAM Memory。"RAM*内存"*页面将按时间 顺序显示保存在RAM(缓存)中的所有消息。条目根据"日志设置"(Log Settings)页面中的配置存储 *在RAM日*志中。

cisco SG550X-24	cisco Authenticator Language: English	elp <b>2</b>
Getting Started  Dashboard	RAM Memory	^
Configuration Wizards	Alert Icon Blinking: Enabled Disable Alert Icon Blinking	
Search  Status and Statistics	Pop-Up Syslog Notifications: Enabled Disable Pop-Up Syslog Notifications	
System Summary	Current Logging Threshold: Informational Edit	
CPU Utilization Port Utilization	RAM Memory Log Table Showing 1-50 of 75 50 V per page	
Interface	Log Index Log Time Severity Description	
Etherlike	2147483573 2018-May-31 04:33:00 Warning %AAAEAP-W-RADIUSREPLY: Invalid attribute 26 ignored - vendor id is not Microsoft	
GVRP	2147483574 2018-May-31 04:33:00 Warning %STP-W-PORTSTATUS: gi1/0/1: STP status Forwarding	
802.1x EAP	2147483575 2018-May-31 04:32:56 Informational %LINK-I-Up: gi1/0/1	
Hardware Resource Utiliza	2147483576 2018-May-31 04:32:53 Warning %LINK-W-Down: gi1/0/1	
Health and Power	2147483577 2018-May-31 04:31:56 Informational %SEC-I-SUPPLICANTAUTHORIZED: MAC 54:ee:75: a sauthorized on port gi1/0/1	
SPAN & RSPAN	2147483578 2018-May-31 04:31:56 Warning %AAAEAP-W-RADIUSREPLY: Invalid attribute 26 ignored - vendor id is not Microsoft	
<ul> <li>Diagnostics</li> </ul>	2147483579 2018-May-31 04:31:56 Warning %STP-W-PORTSTATUS: gl1/0/1: STP status Forwarding	
RMON	2147483580 2018-May-31 04:31:51 Informational %LINK-I-Up: gi1/0/1	
View Log 2	2147483581 2018-May-31 04:31:48 Warning %LINK-W-Down: gi1/0/1	
RAM Memory 3	2147483582 2018-May-31 04:30:55 Notice %COPY-N-TRAP: The copy operation was completed successfully	
Flash Memory	2147483583 2018-May-31 04:30:53 Informational %COPY-I-FILECPY: Files Copy - source URL running-config destination URL flash://system/configuration/startup-config	
<ul> <li>Administration</li> </ul>	2147483584 2018-May-31 04:13:26 Informational %SEC-I-SUPPLICANTAUTHORIZED: MAC 54:ee:75: is authorized on port gi1/0/1	
System Settings	2147483585 2018-May-31 04:13:26 Warning %AAAEAP-W-RADIUSREPLY: Invalid attribute 26 ignored - vendor id is not Microsoft	-
@ 2011-2018 Cisco Systems Inc. A	Right's Reserved	

步骤4.在RAM内存日志表中,您应看到一条信息性日志消息,指出您的MAC地址已在端口gi1/0/1上获得授权。

注意:部分MAC地址已模糊。



单击此处查看思科提供的其他技术讲座