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，请单击此处。

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。

有关其他信息，请参阅词汇表。

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。

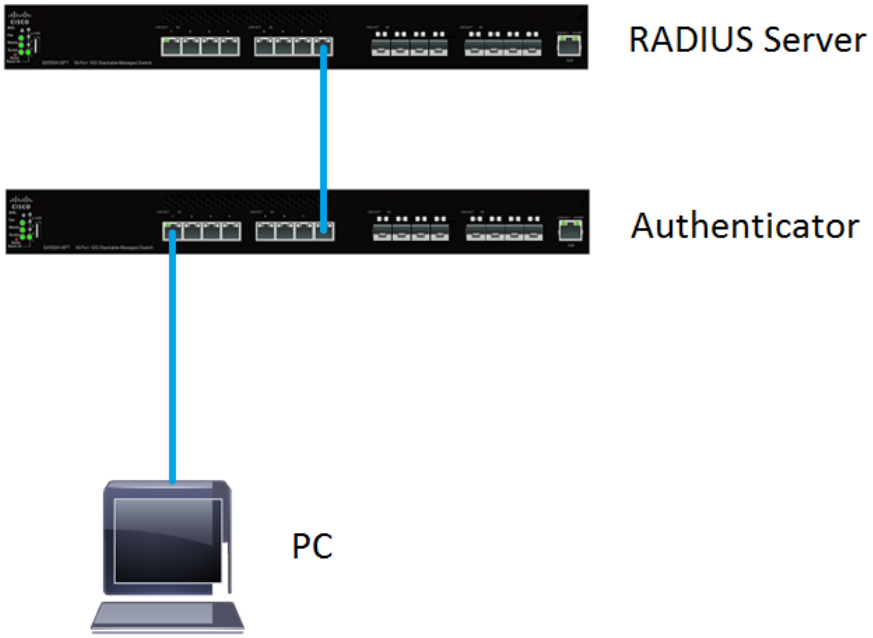
身份验证器在客户端和身份验证服务器之间工作。首先，它会向客户端请求身份信息。作为响应，身份验证器会向身份验证服务器验证信息。最后，它会向客户端中继响应。在本文中，身份验证器将是包含RADIUS客户端的交换机。交换机将能够封装并解封可扩展身份验证协议(EAP)帧，以与身份验证服务器交互。

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。

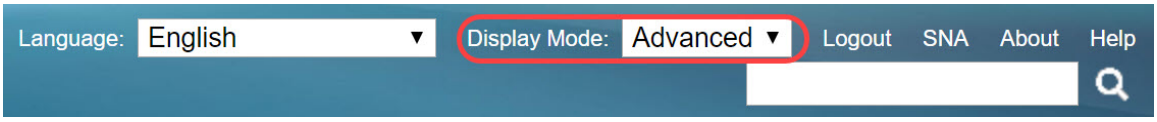
版本2.4增加了配置为基于MAC的请求方发送的用户名格式并定义EAP身份验证方法或纯RADIUS的功能。在此版本中，您还可以配置用户名的格式以及为基于MAC的请求方配置不同于用户名的特定密码。

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”*。



目录

适用设备

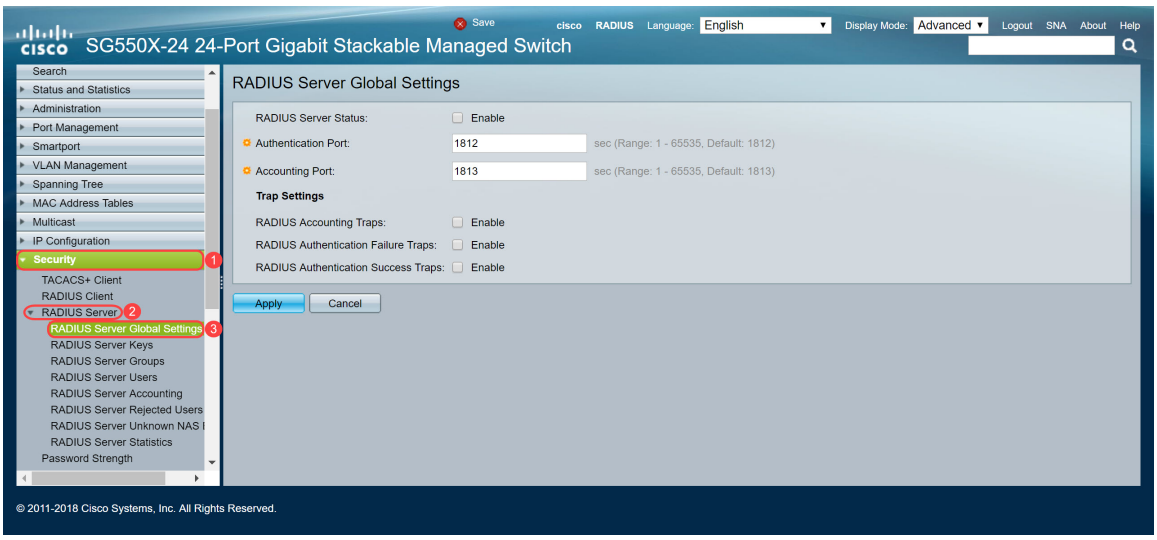
- SX350X系列
- SG350XG系列
- Sx550X 系列
- SG550XG系列

软件版本

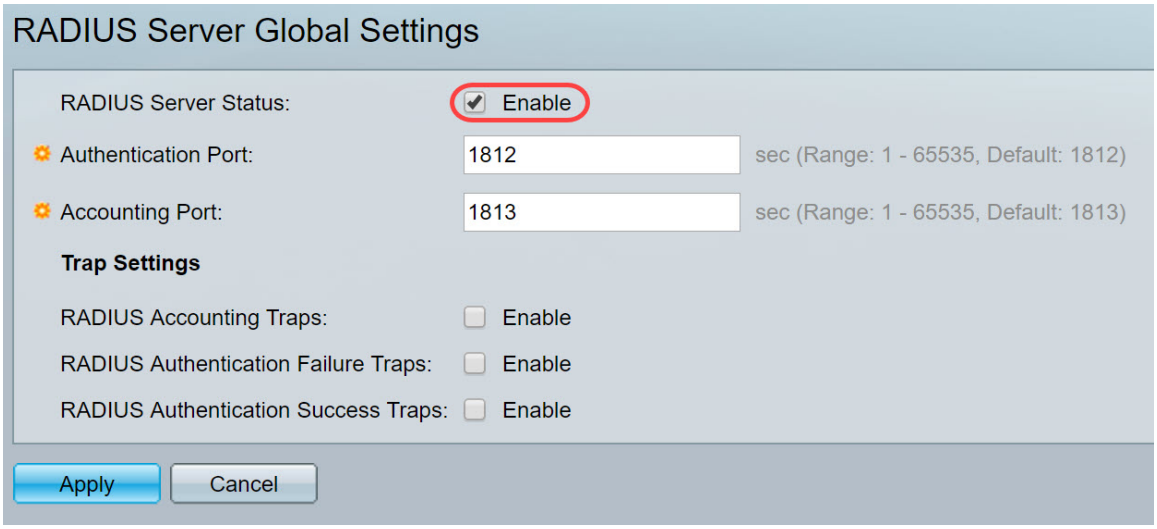
- 2.4.0.94

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**。

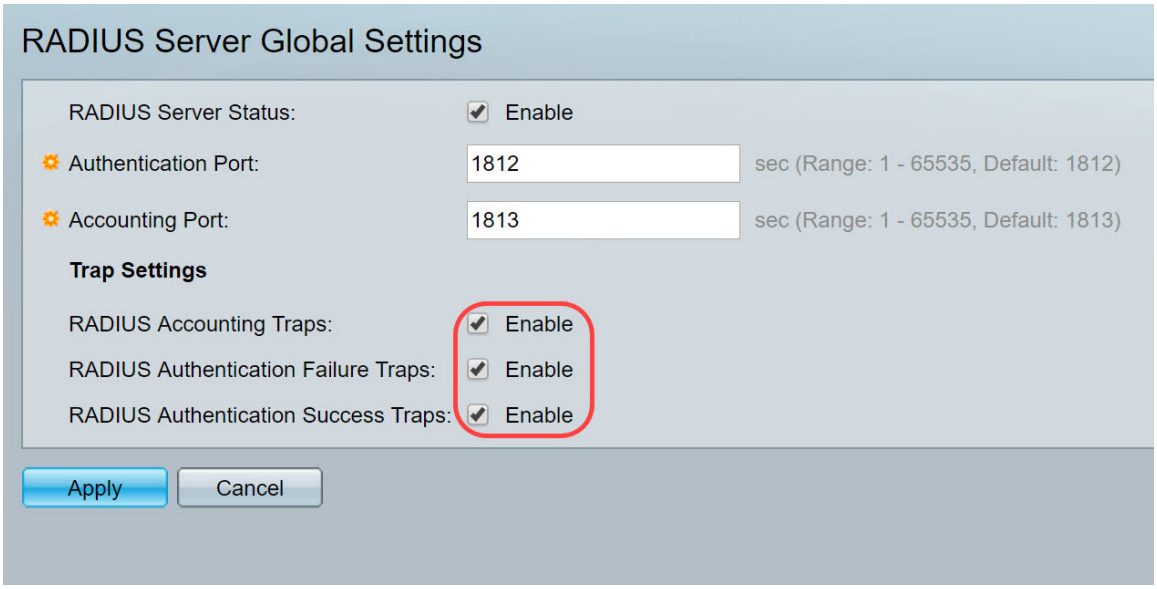


步骤2.要启用RADIUS服务器功能状态，请选中RADIUS服务器状**态字**段中的启*用复选框*。



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：

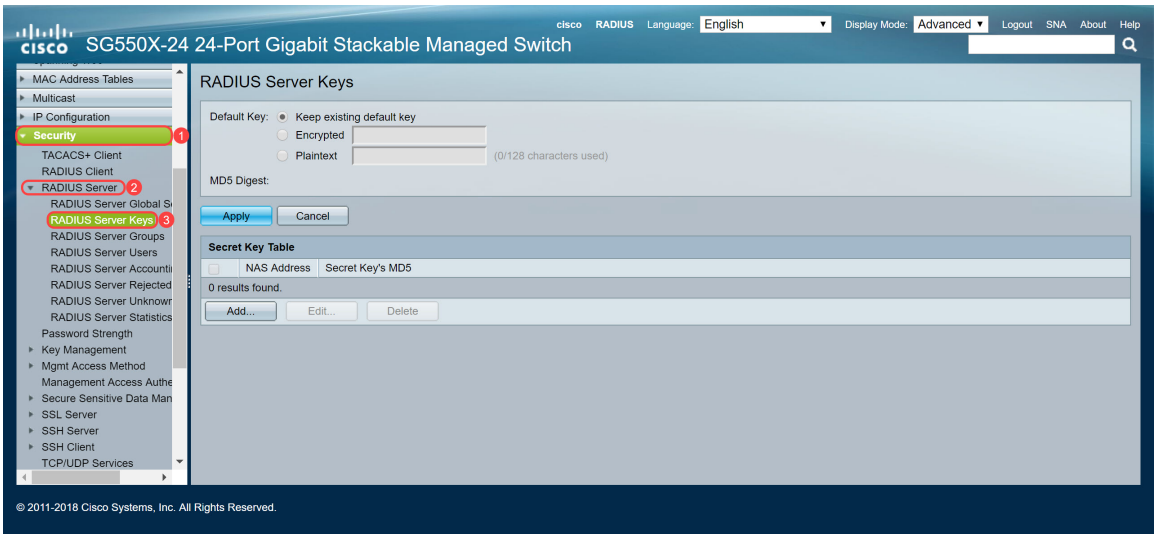
- RADIUS记帐陷阱 — 选中以生成RADIUS记帐事件的陷阱。
- RADIUS Authentication Failure Traps — 选中以为失败的登录生成陷阱。
- RADIUS Authentication Success Traps — 选中以生成成功登录的陷阱。



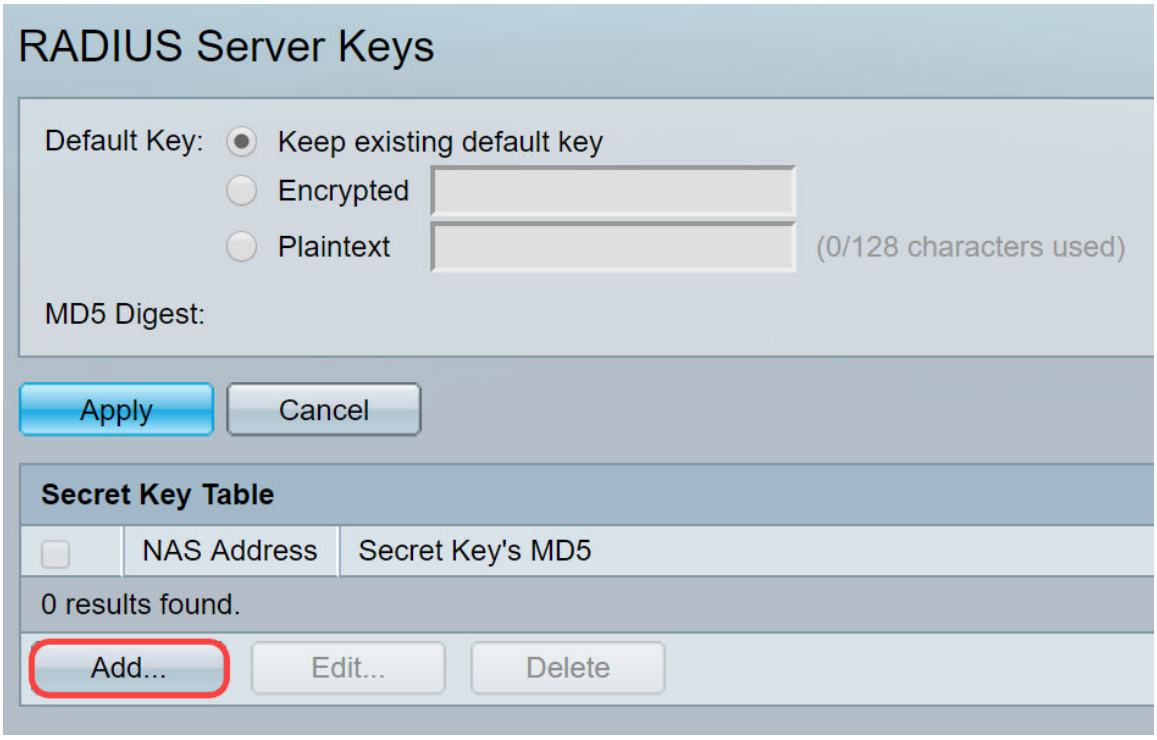
步骤4.单击“**应用**”保存设置。

RADIUS服务器密钥

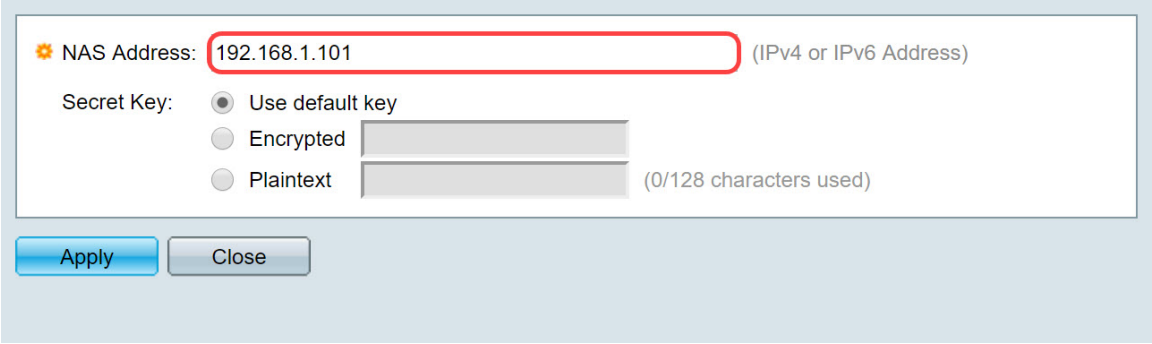
步骤1.导航至**Security > RADIUS Server > RADIUS Server Keys**。“RADIUS服务*器密钥*”页面打开。



步骤2.在“密钥*表”部分*，单击**添加.....** 添加密钥。



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。

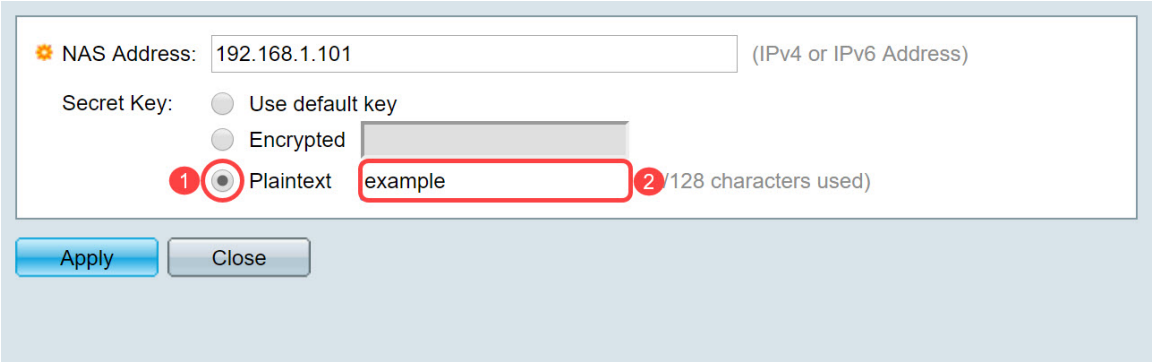


步骤4.选择一个用作密钥的单选*按钮*。以下选项为：

- 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。

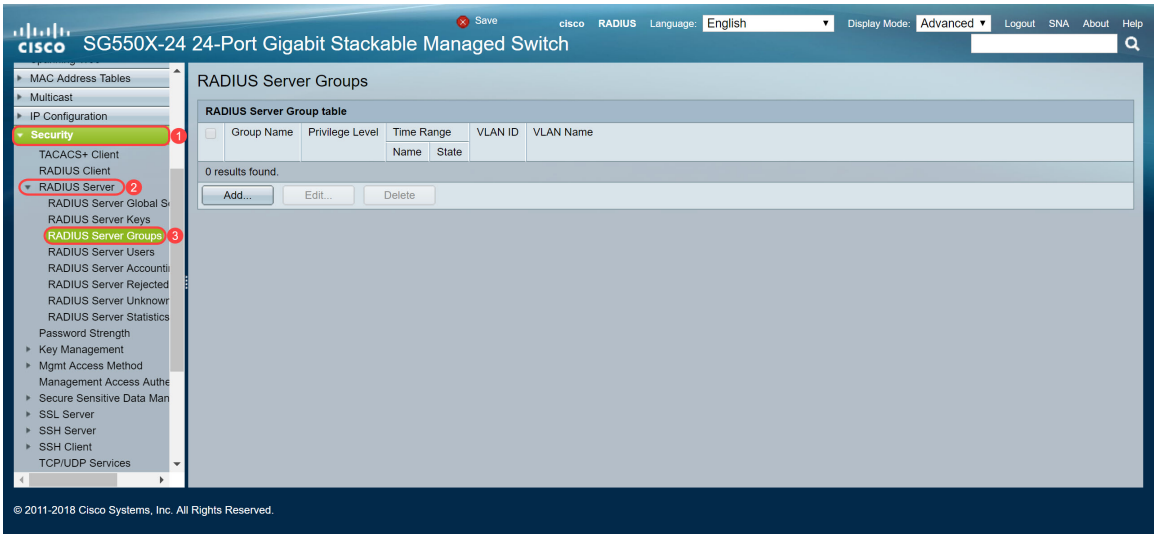
注意：我们不建议使用单词**example**作为密钥。请使用更强的密钥。最多可使用128个字符。如果密码太复杂，记不住，则密码是个好密码，但更好的是，如果你能将密码转换成易于记忆的密码，用特殊字符和数字代替元音 — “P@55w0rds@reH@rdT0Remember”。 最好不要使用字典中可以找到的任何单词。最好选择一个短语，将一些字母替换为特殊字符和数字。有关详细信息，请参阅此思科博文。



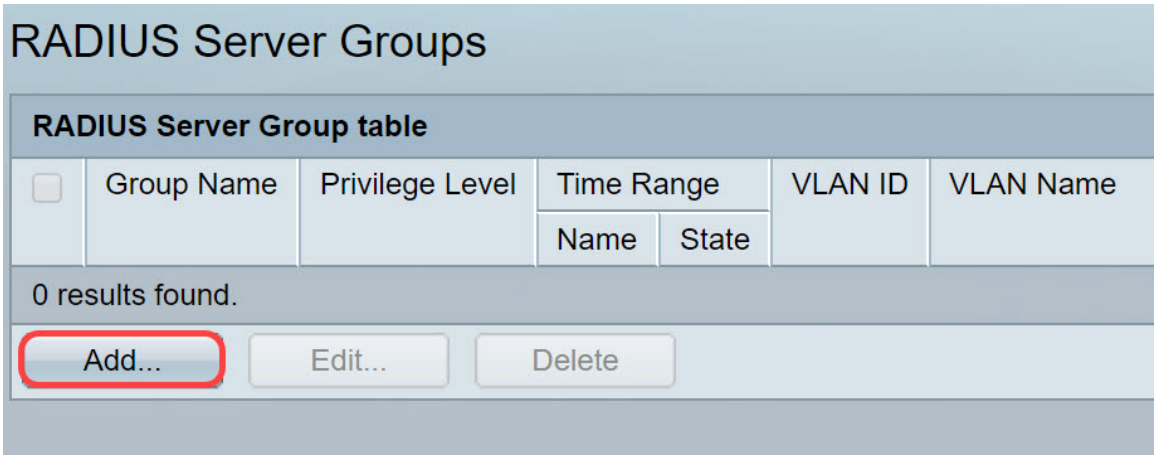
步骤5.单击“**应用**”保存配置。密钥现在使用MD5加密。MD5是加密哈希函数，它获取一段数据并创建唯一的十六进制输出，通常不可复制。MD5使用128位哈希值。

RADIUS服务器组

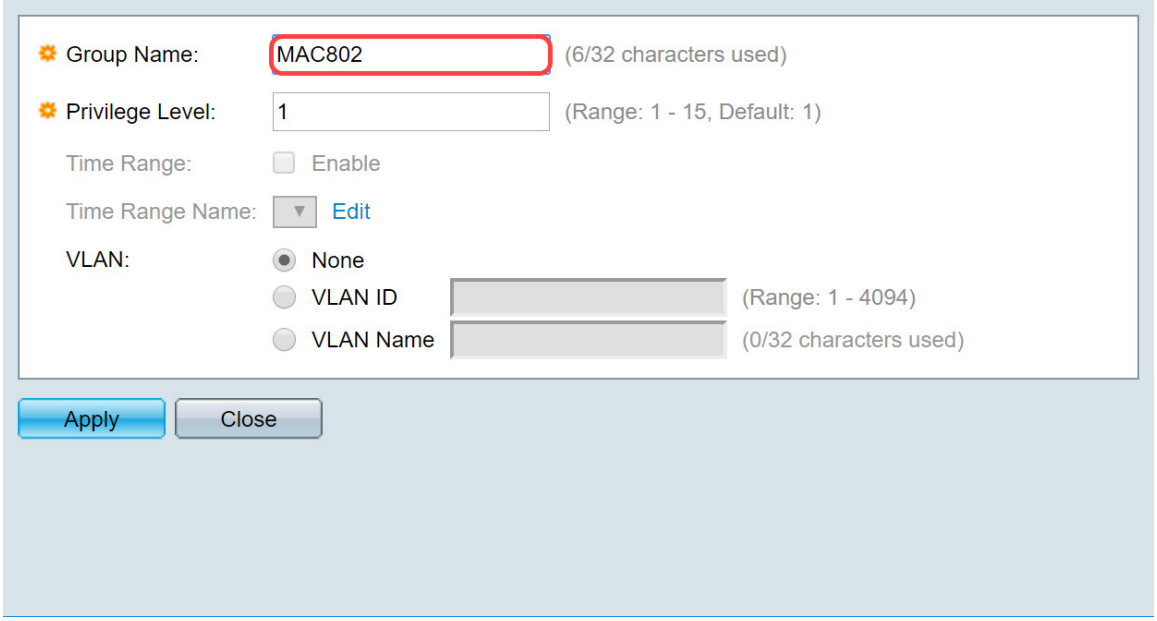
步骤1.导航至**Security > RADIUS Server > RADIUS Server Groups**。



步骤2.单击**Add...** 添加新的RADIUS服务器组。

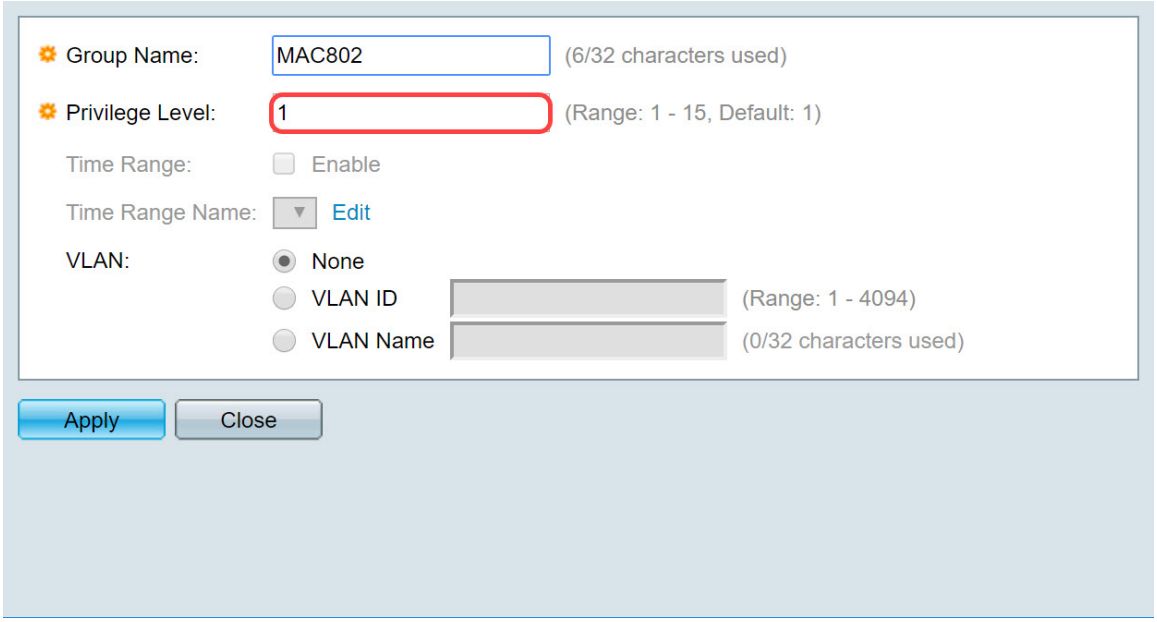


步骤3.将打*开"添加RADIUS服*务器组"页。输入组的名称。在本例中，我们将使用**MAC802**作为组名。



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。

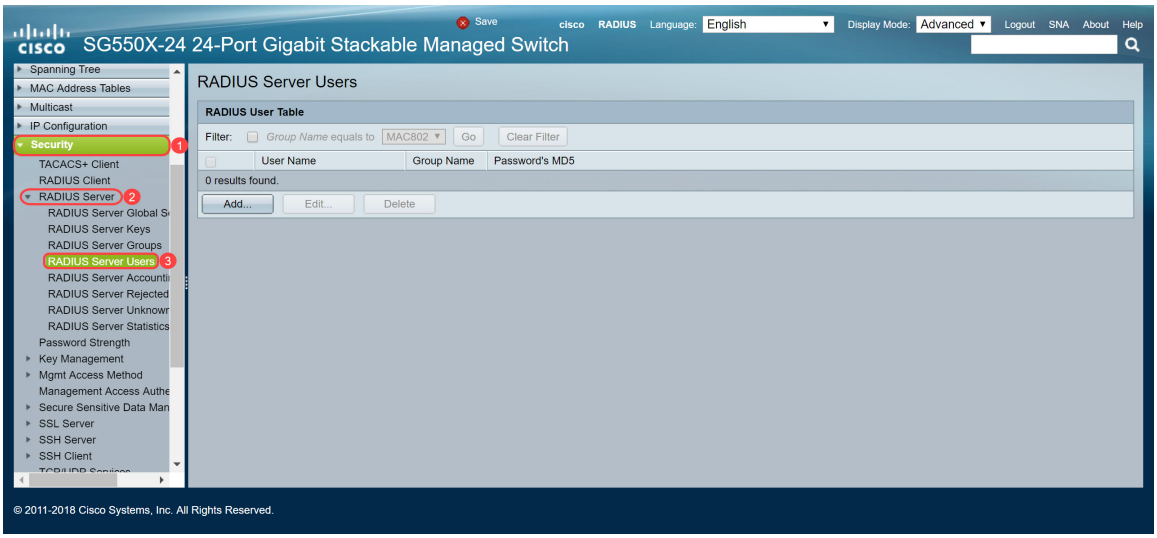
注意：本文不会配*置时*间范*围*或VLAN。



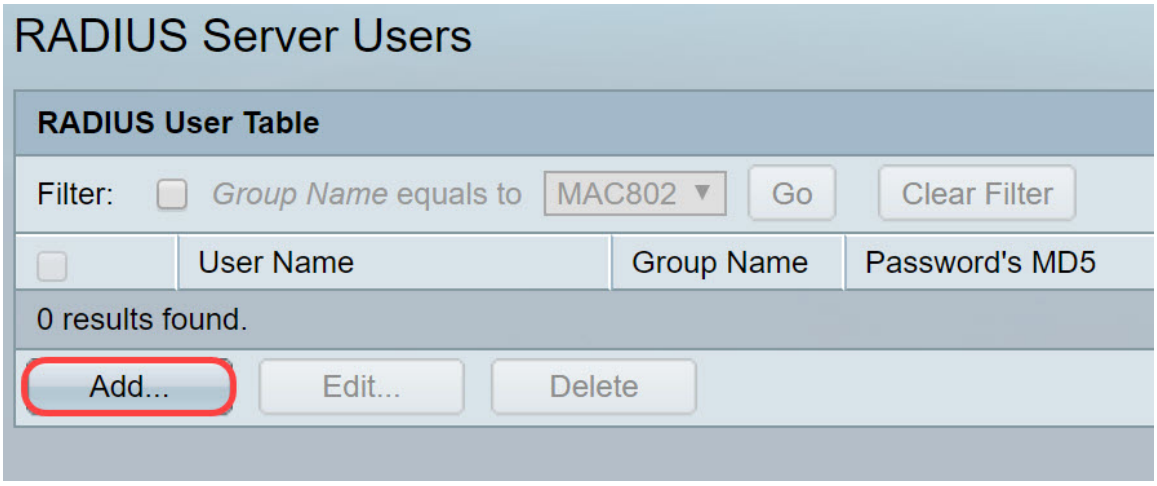
步骤5.单击"应**用**"保存设置。

RADIUS服务器用户

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

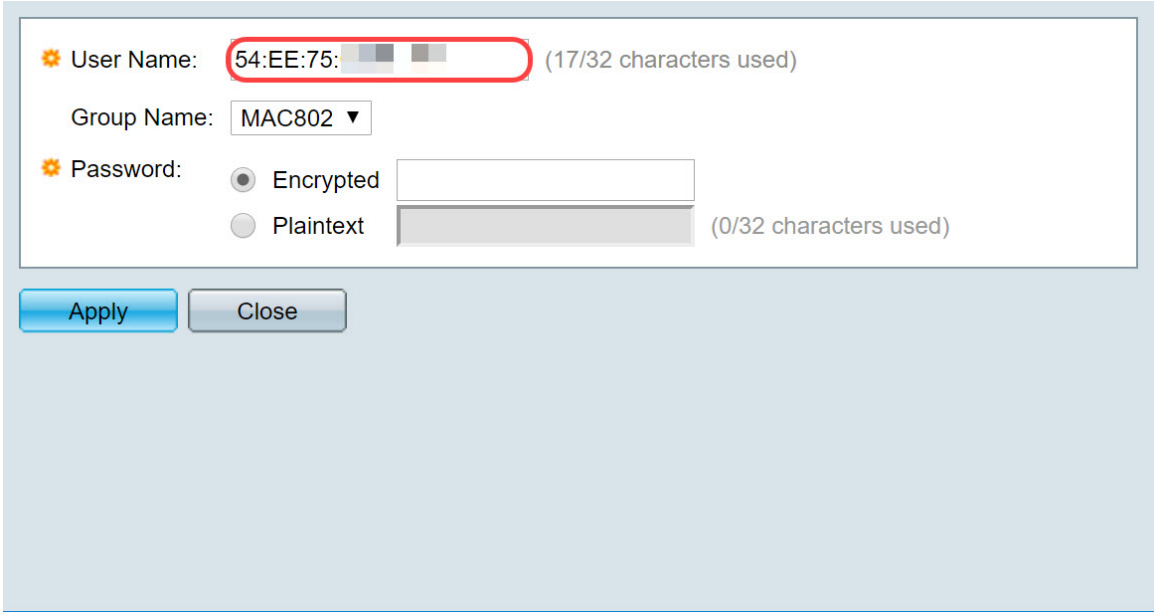


步骤2.单击**Add...** 的子菜单。

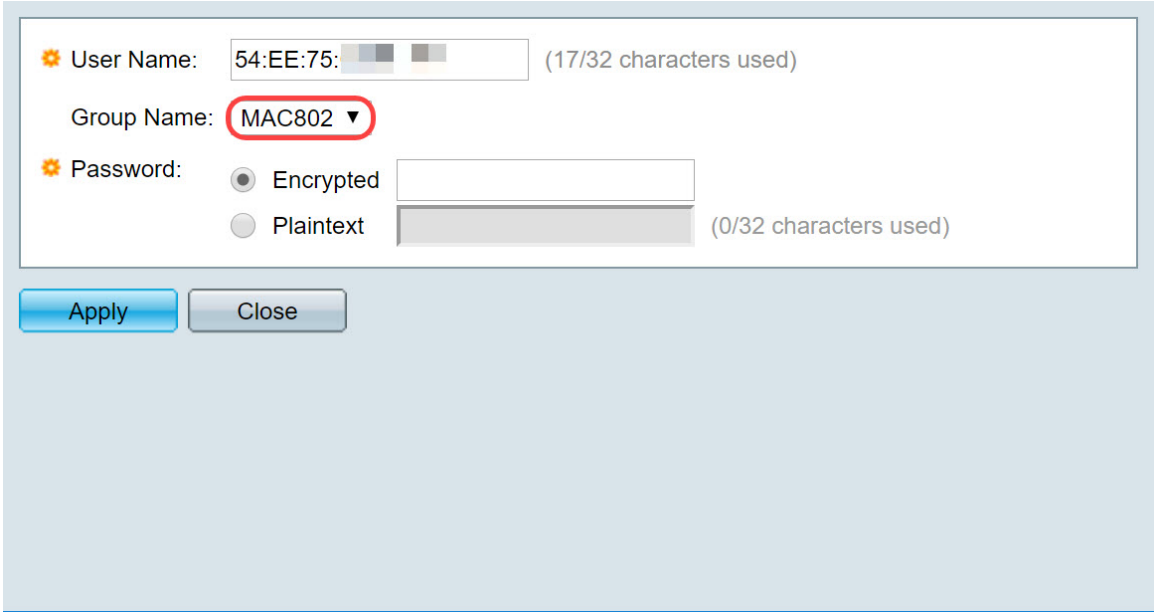


步骤3.将打*开"添加RADIUS服务器*用户"页。在*用户名*字段中，输入用户的MAC地址。在本例中，我们将在计算机上使用以太网MAC地址。

注意：部分MAC地址已模糊。



步骤4.在Group Name下拉列表中选择组。如RADIUS服务器组部分的第3步中突出显示的，我们将选择**MAC802作为此**用户的组名称。

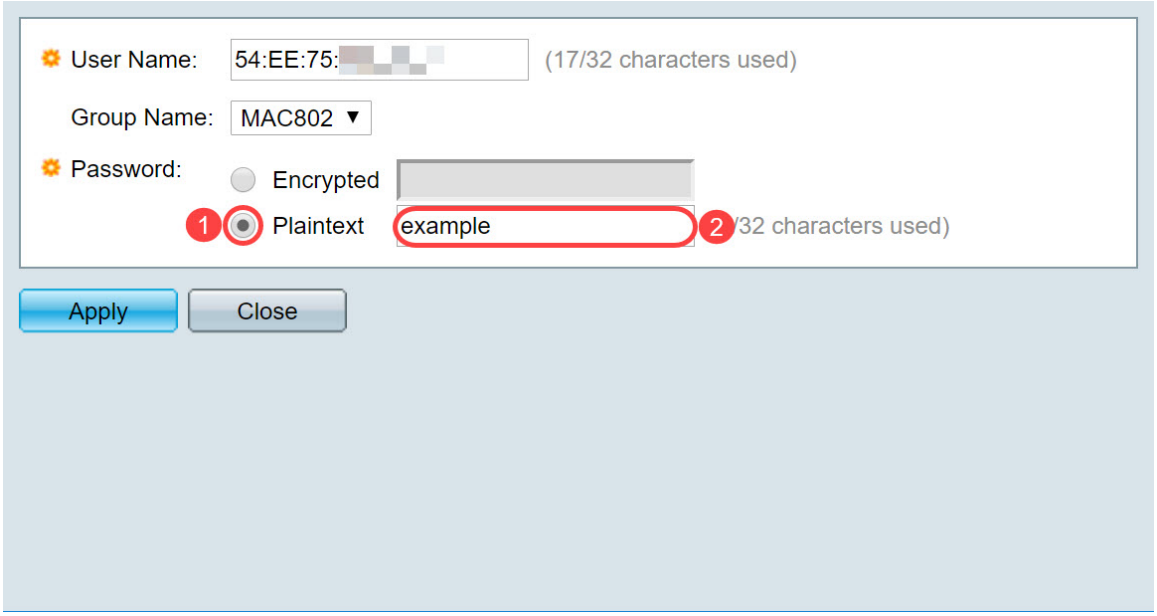


步骤5.选择以下单选按钮之一：

- 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。

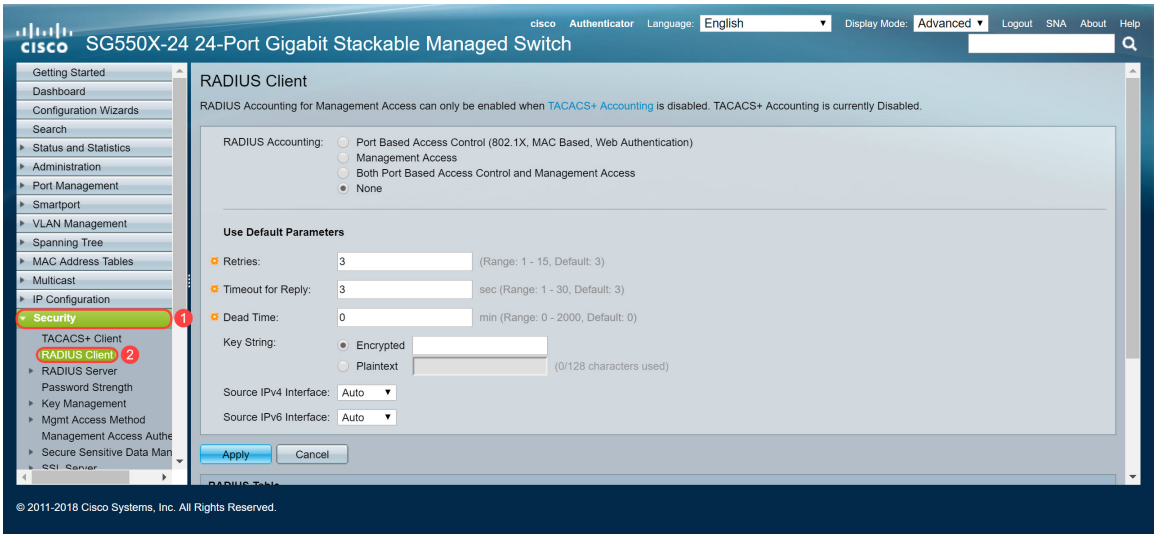


步骤6.完成配**置后**单击“应用”。

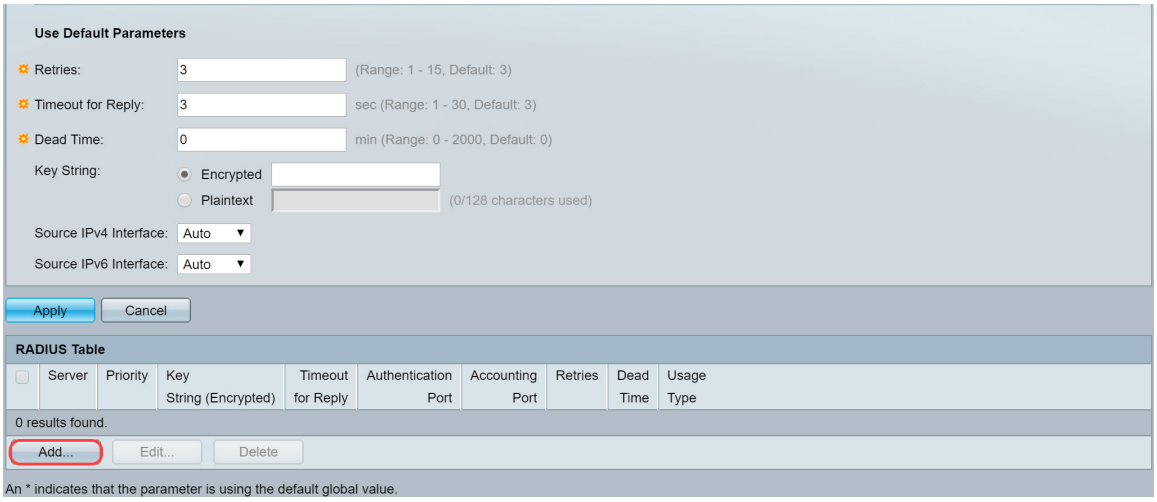
现在，您已完成RADIUS服务器的配置。在下一节中，我们将配置第二台交换机作为身份验证器。

RADIUS客户端

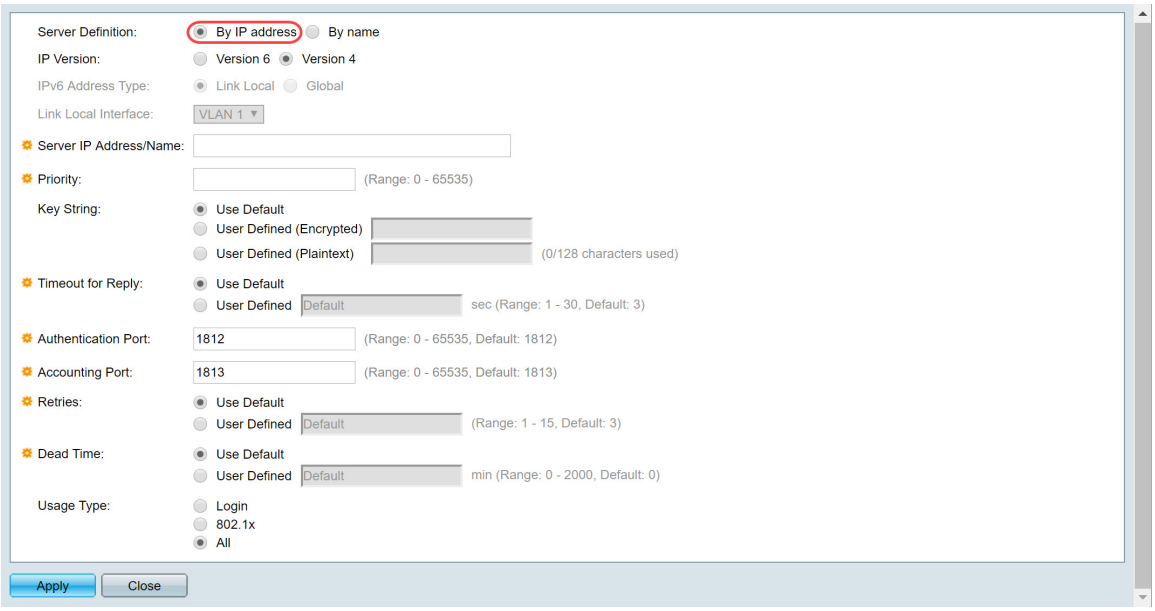
步骤1.登录到将配置为身份验证器的交换机的基于Web的实用程序，然后导航至**Security > RADIUS Client**。



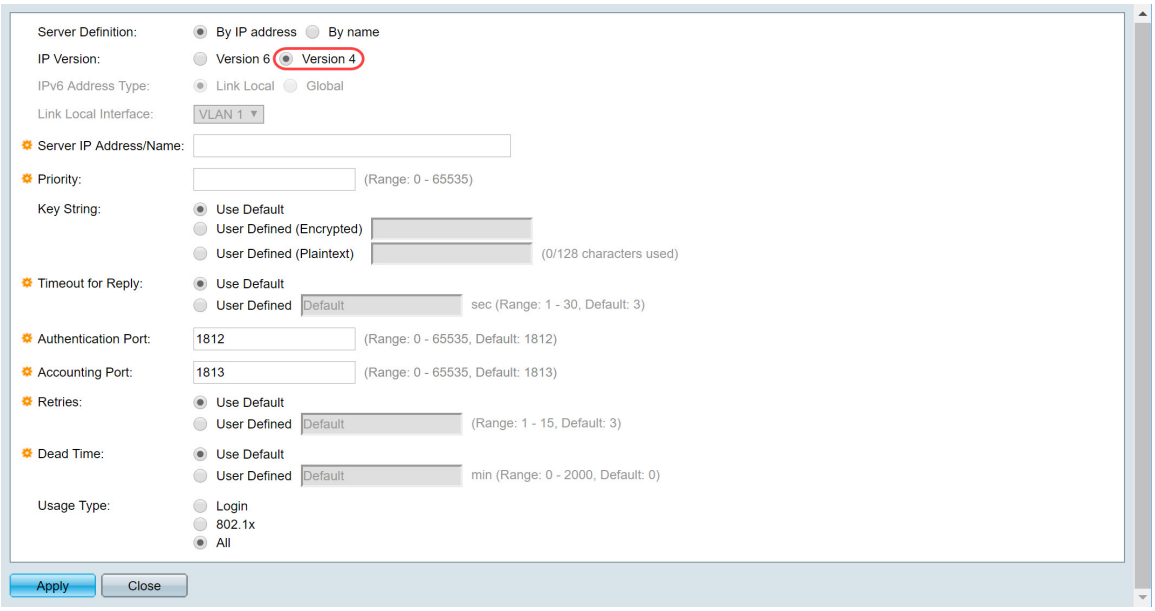
步骤2.向下滚动到*RADIUS表*部分，然后单**击添加……** 添加RADIUS服务器。



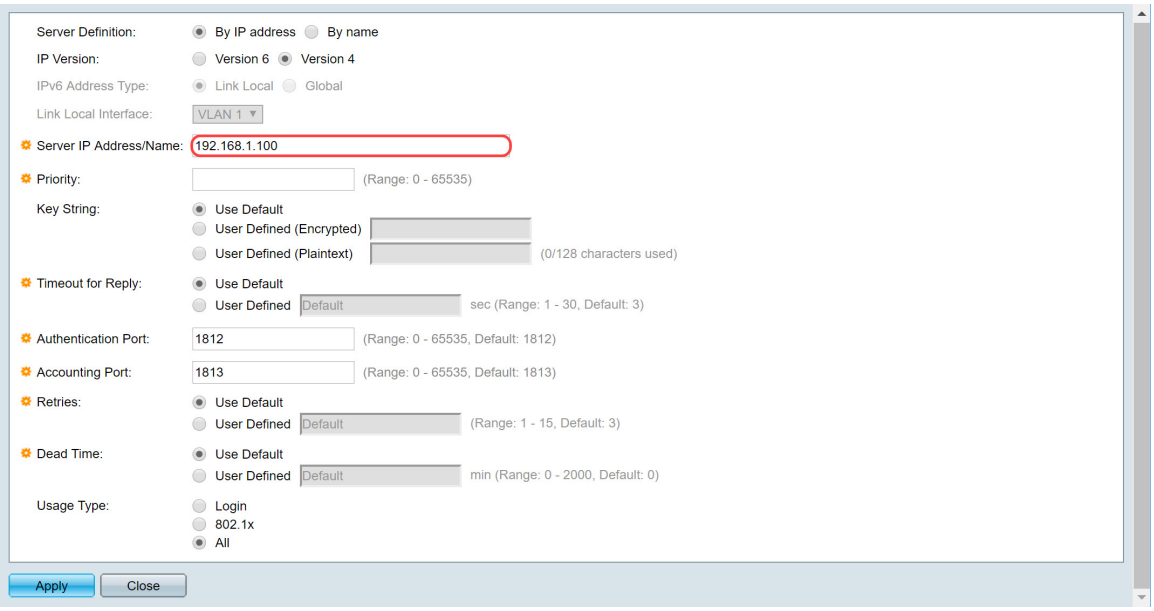
第3步。（可选）在“服务器定义”字段中，选择是按IP地址还是名称指*定RADIUS服*务器。在本例中，我们将保留默认选择的“按**IP地址**”。



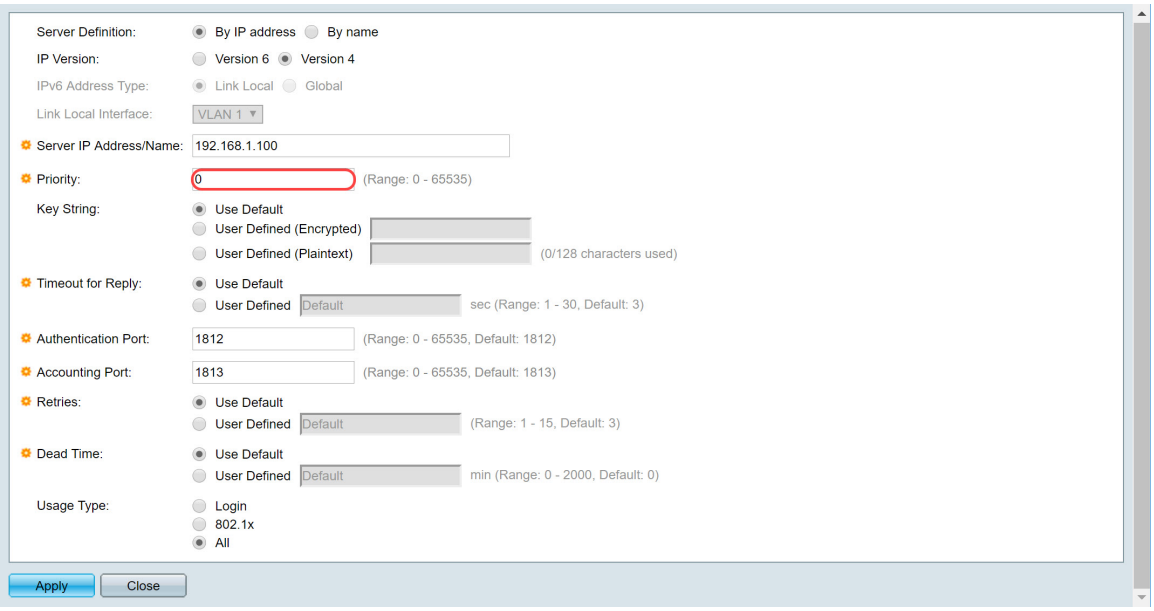
步骤4.（可选）在IP Version字段中选择RADIUS服务器IP地址*的版*本。我们将保留本示例的默**认版**本4选择。



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*。

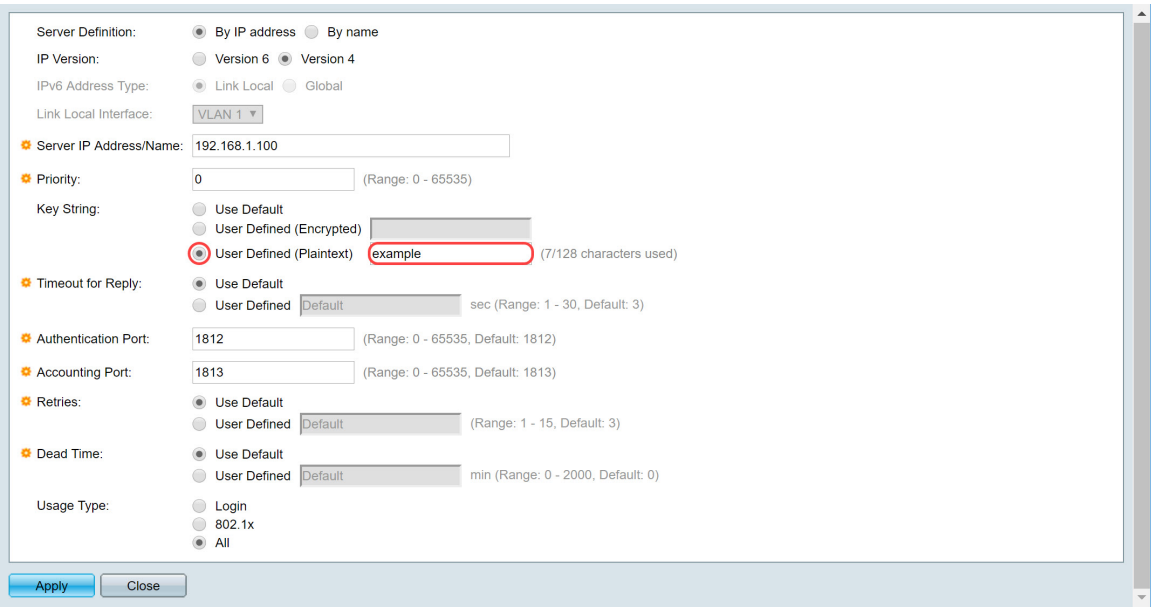


步骤6.输入服务器的优先级。优先级确定设备尝试联系服务器以验证用户的顺序。设备首先从优先级最高的RADIUS服务器启动。零是最高优先级。



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。

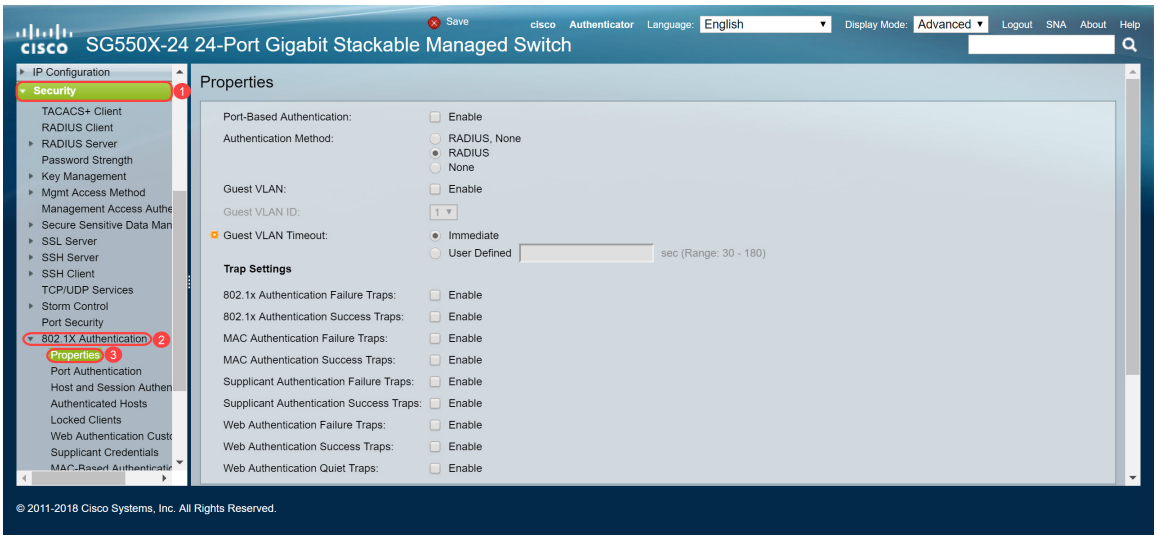


步骤8.单击Apply保存配置。

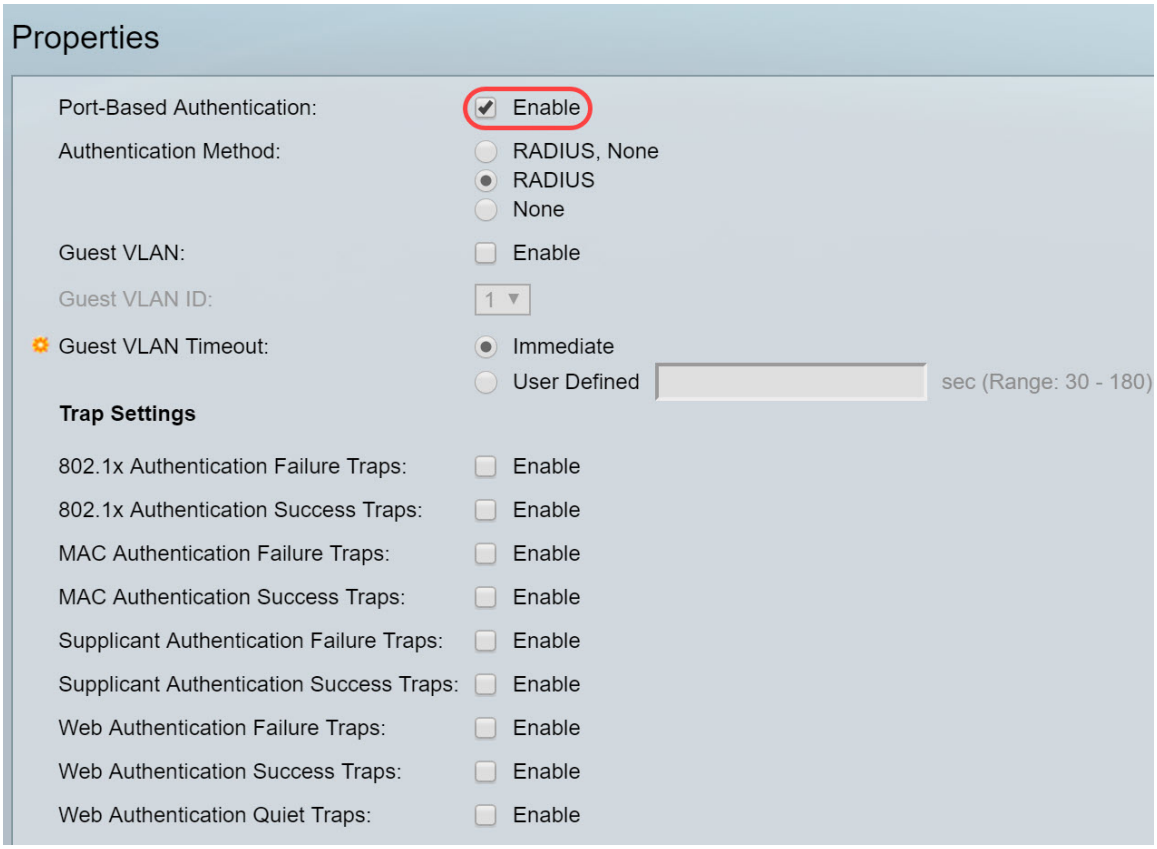
802.1X身份验证属性

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。

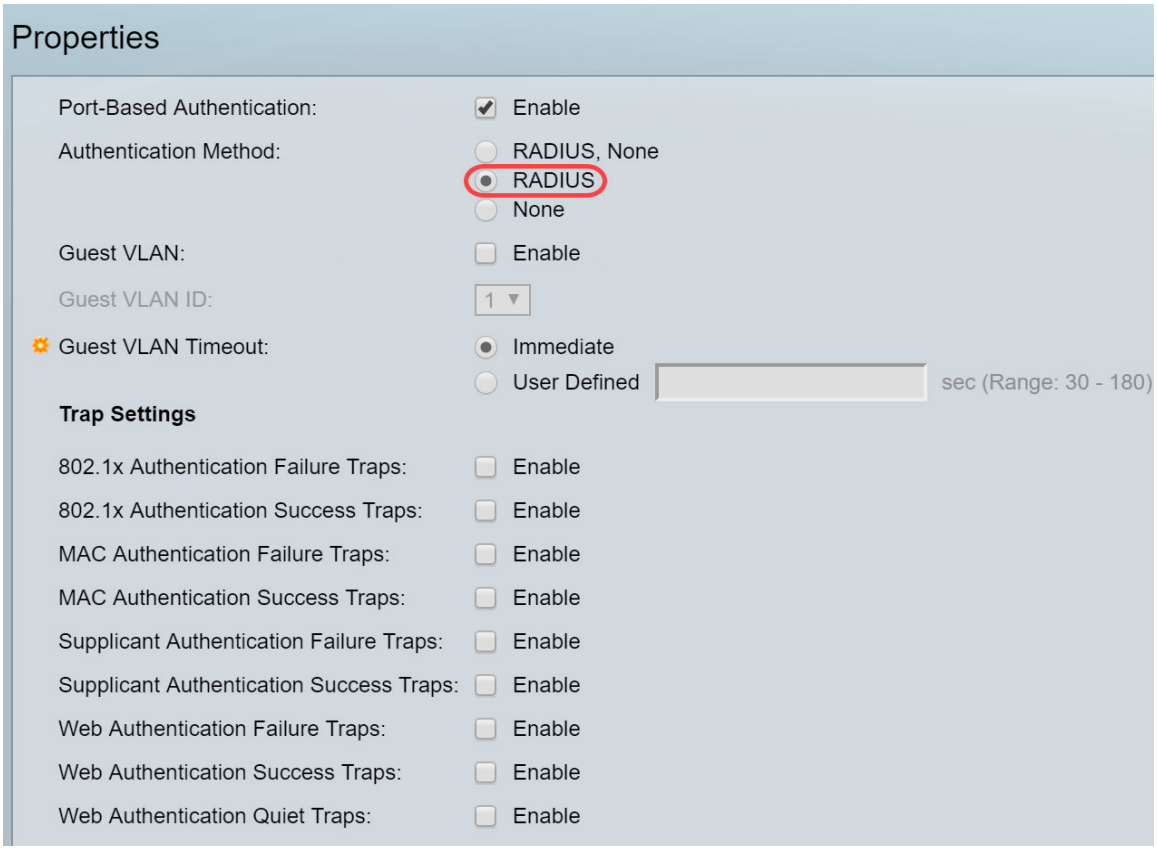


步骤2.选中Enable复选框以启用基于端口的身份验证。



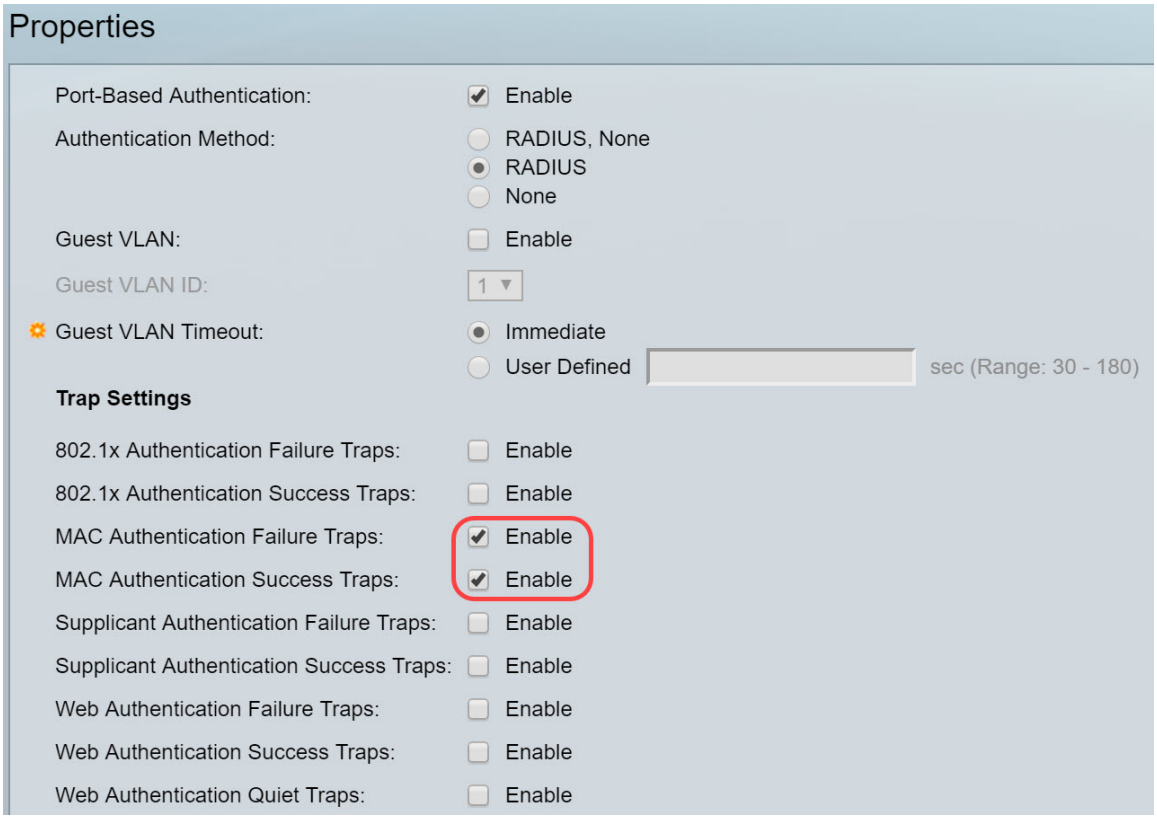
步骤3.选择用户身份验证方法。我们将选择RADIUS作为身份验证方法。以下选项为：

- 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。



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*。

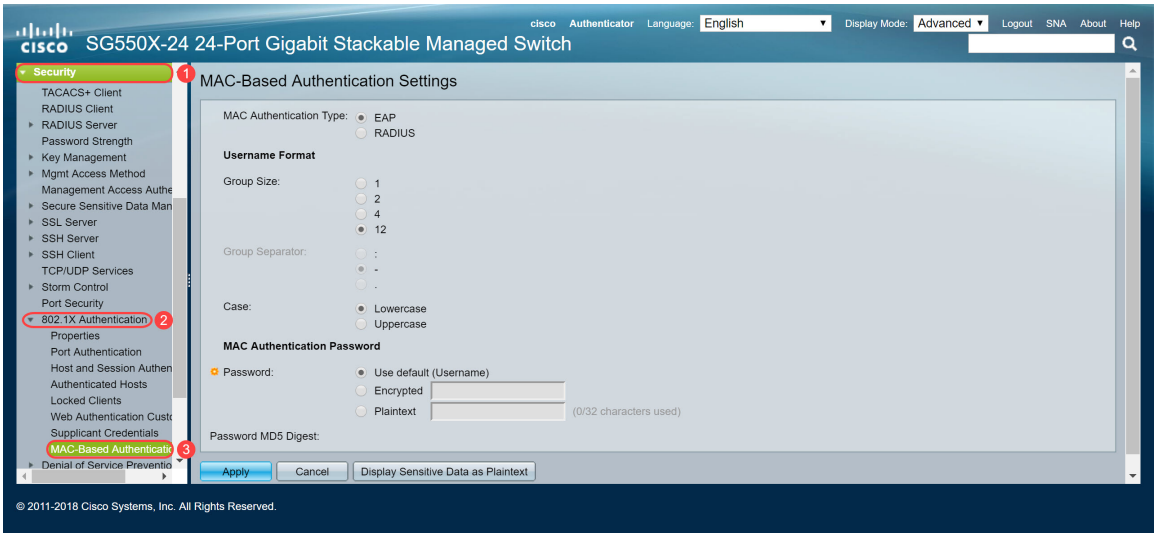


步骤5.单击“**应用**”。

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。

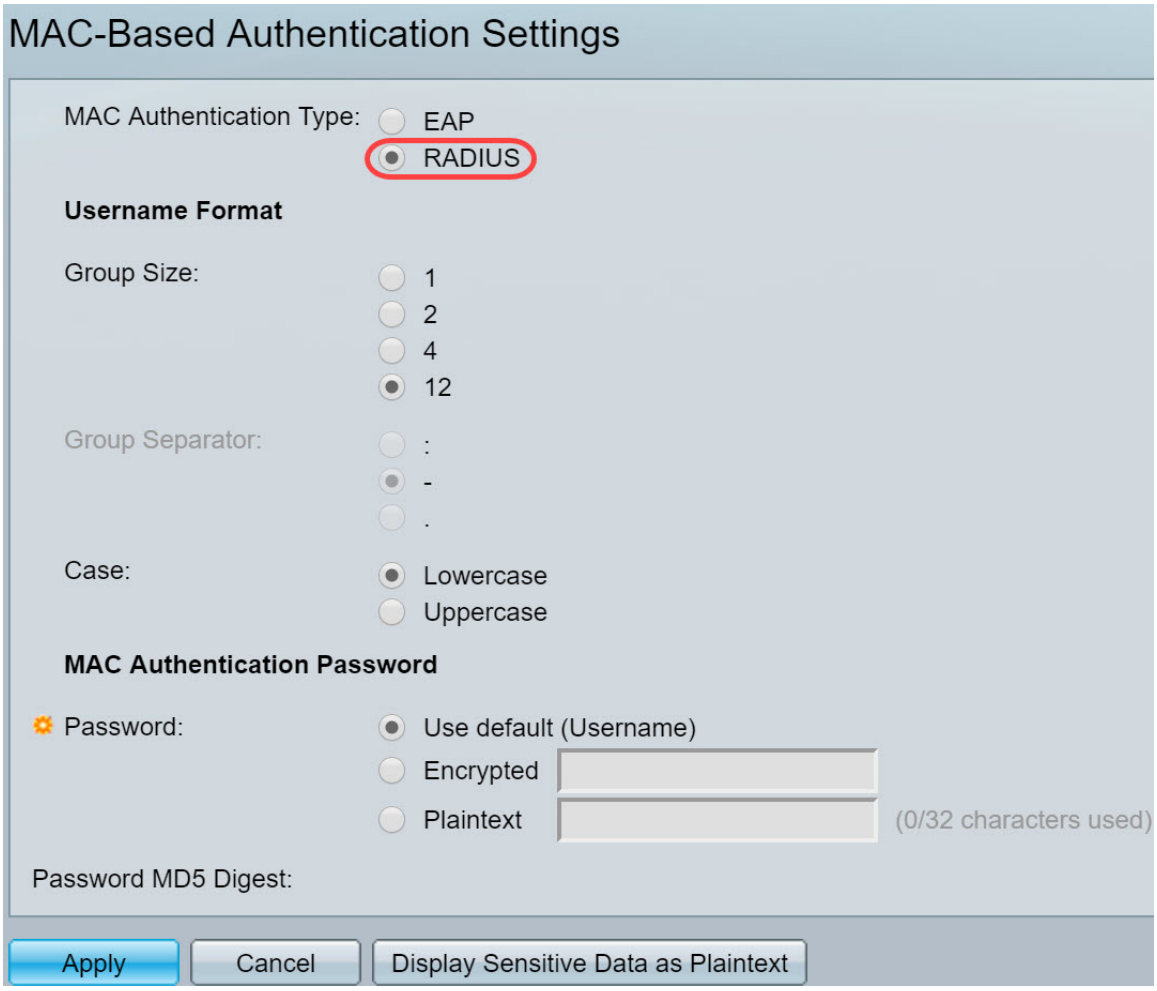
步骤1.导航至**Security > 802.1X Authentication > MAC-Based Authentication Settings**。



步骤2.在MAC身*份验证类*型中，选择以下选项之一：

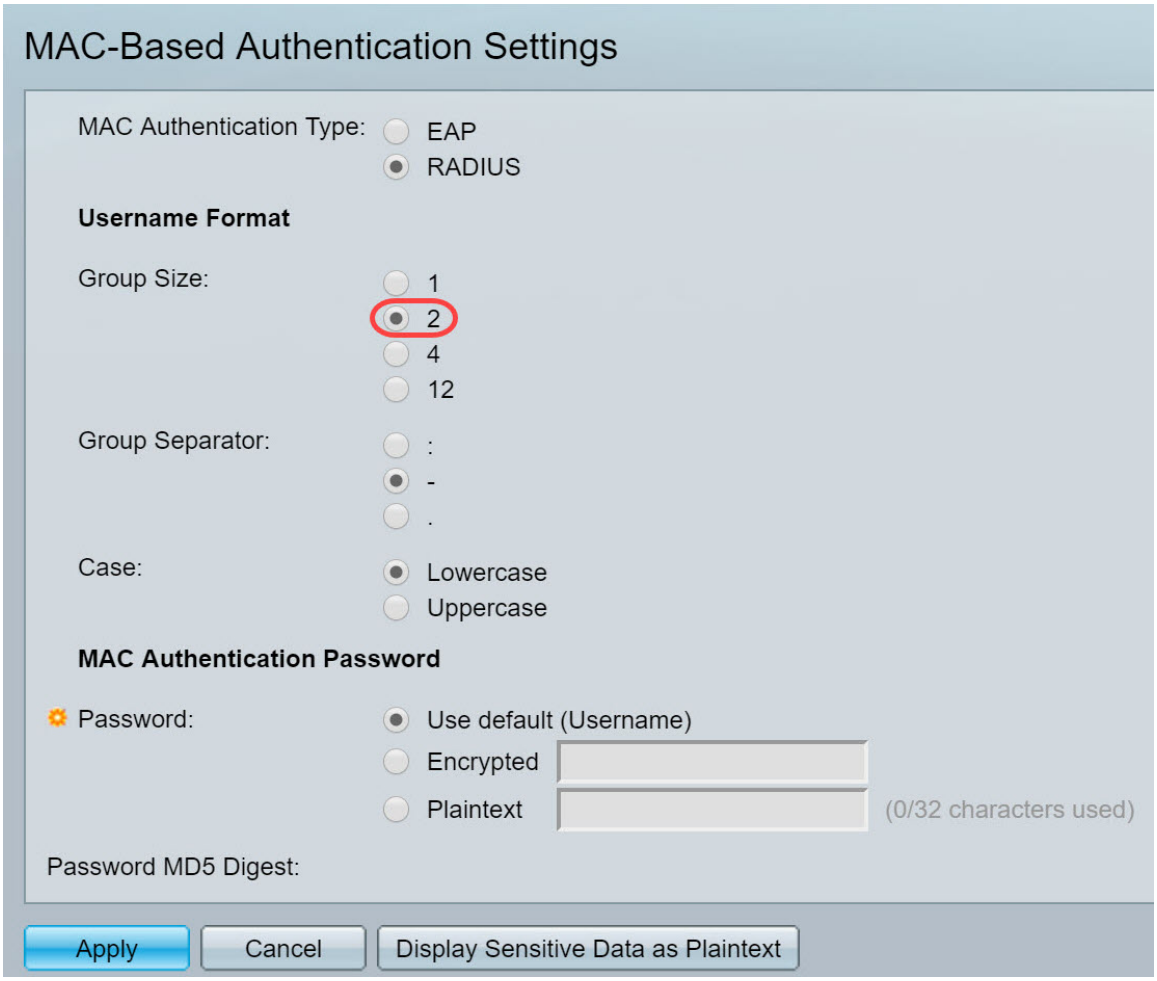
- EAP — 对交换机（RADIUS客户端）和RADIUS服务器（对基于MAC的请求方进行身份验证）之间的流量使用RADIUS和EAP封装。
- RADIUS — 对交换机（RADIUS客户端）和RADIUS服务器（对基于MAC的请求方进行身份验证）之间的流量使用不带EAP封装的RADIUS。

在本例中，我们将选择RADIUS作为MAC身份验证类型。

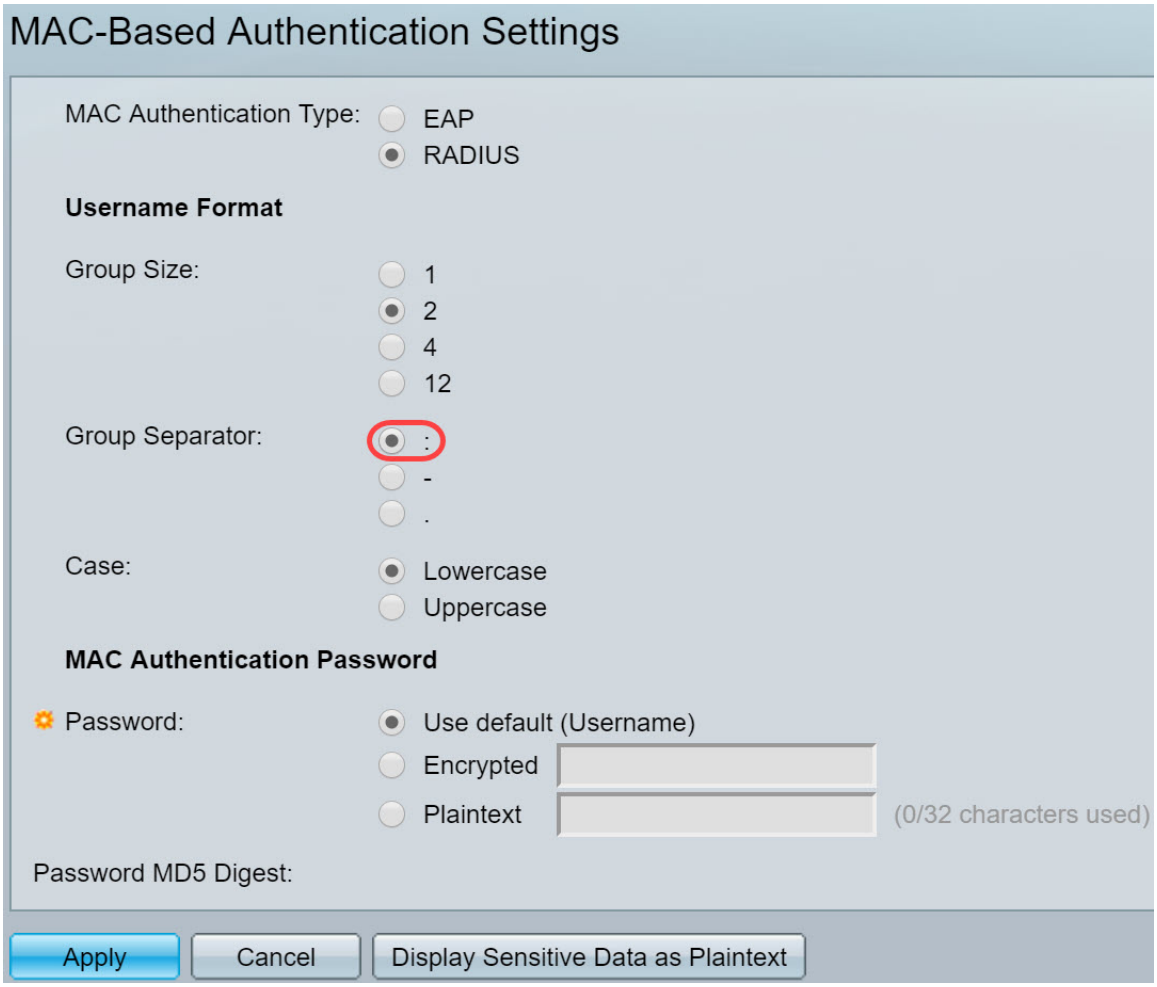


步骤3.在Username Format中，选择作为用户名发送的MAC地址的分隔符之间的ASCII字符数。在本例中，我们将选择2作为组大小。

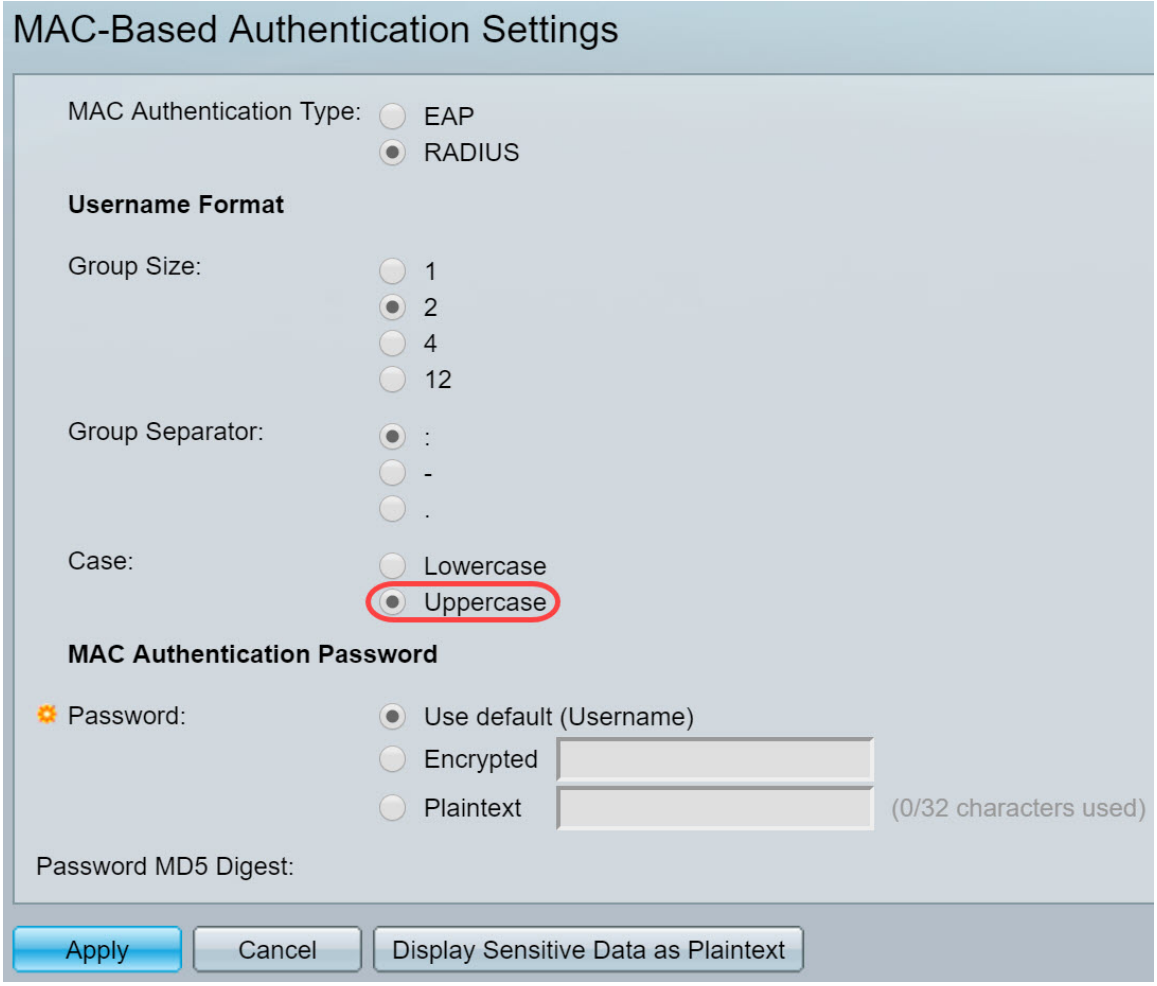
注意：确保用户名格式与在“Radius服务器用户”部分输入MAC地址*的方式*相同。



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。

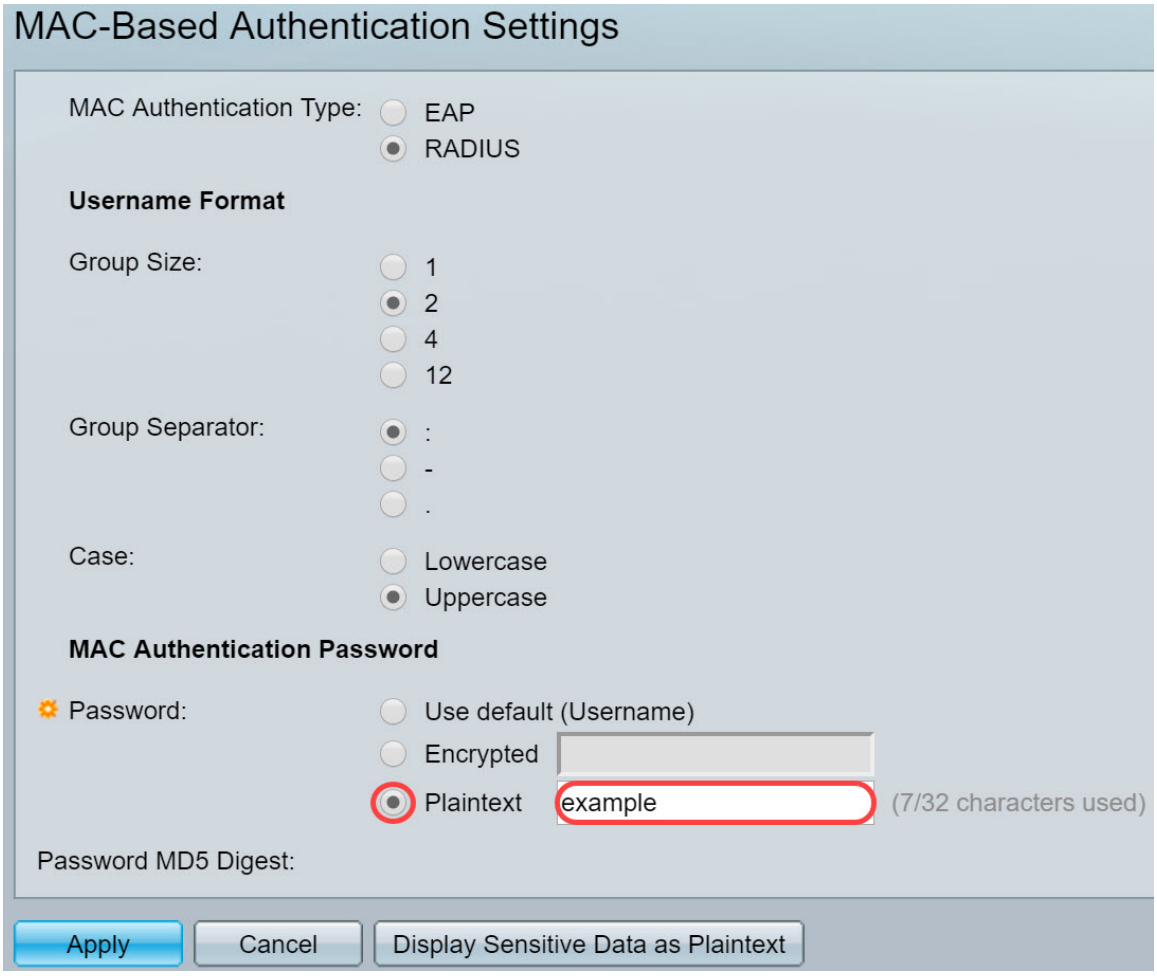


步骤5.在“大小写”字段中，选择**小写**或**大写**，以便以小写或大写形式发送用户名。



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。



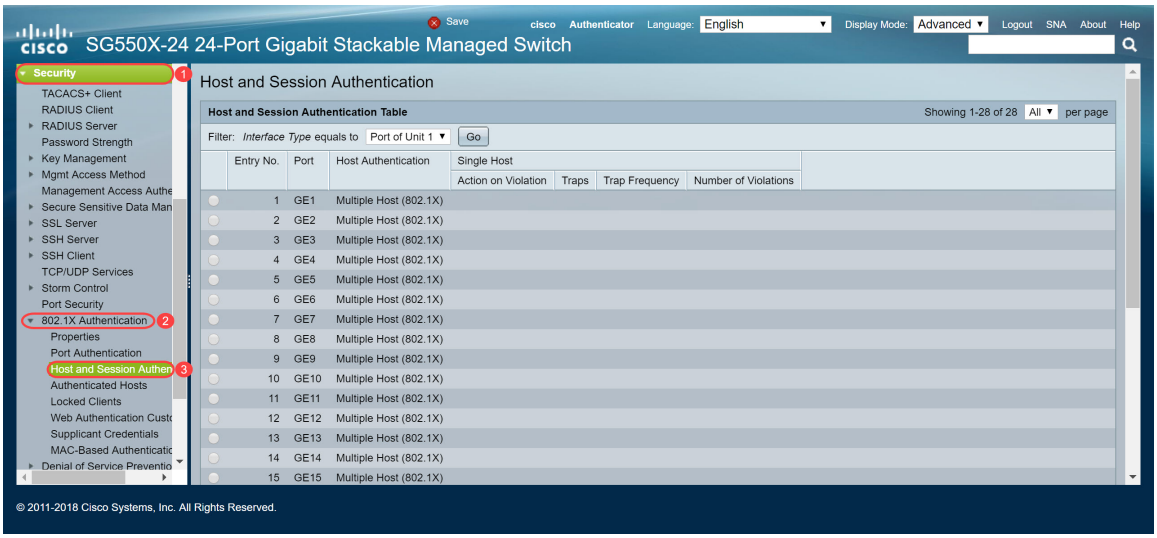
注意：*密码消息摘要算法5(MD5)摘要显*示MD5摘要密码。MD5是加密哈希函数，它获取一段数据并创建一个通常不可复制的唯一十六进制输出。MD5使用128位哈希值。

步骤7.单击“**应用**”，将设置保存到“运行配置”文件。

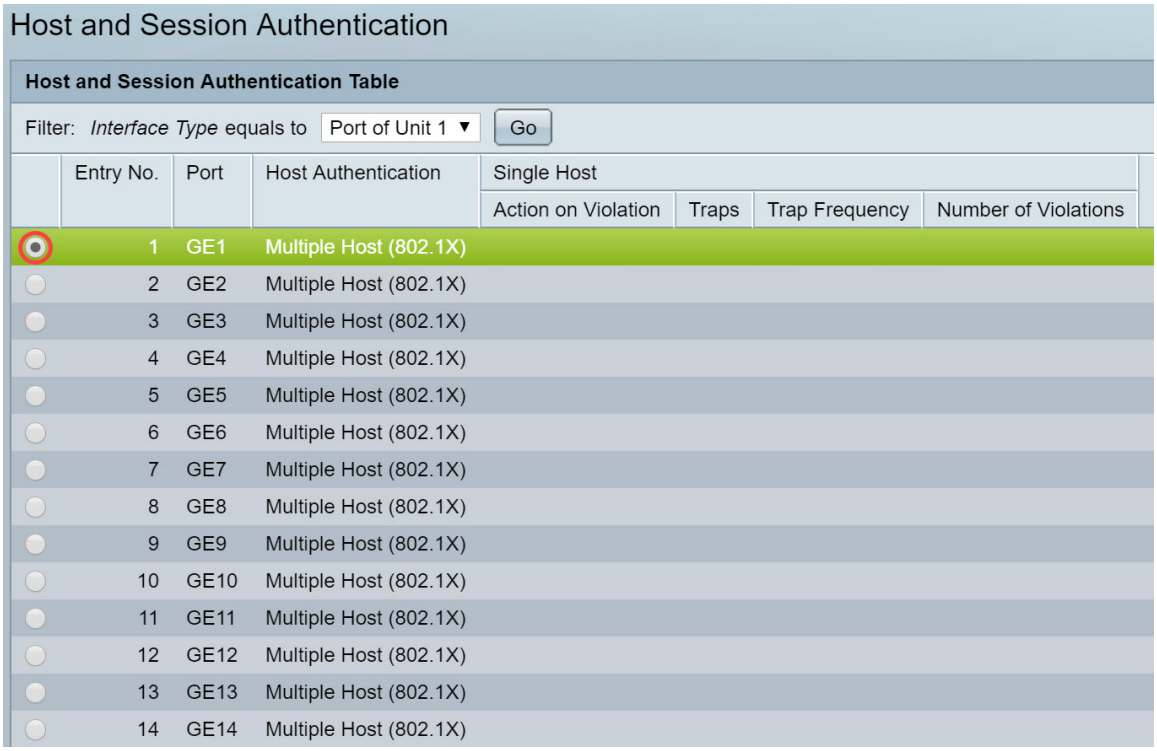
802.1X身份验证主机和会话身份验证

“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。

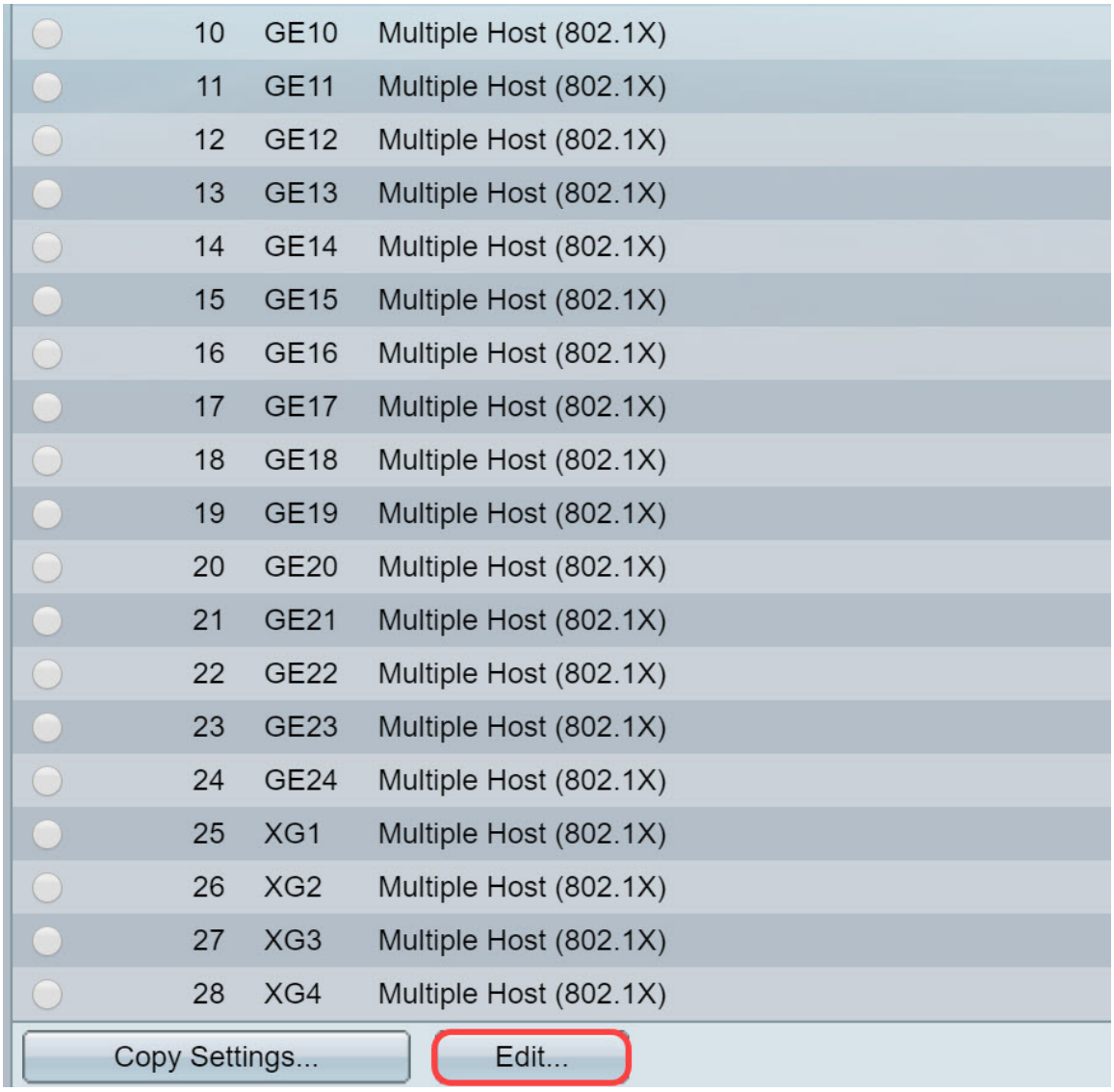
步骤1.导航至**Security > 802.1X Authentication > Host and Session Authentication**。



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。



步骤3.单击**Edit...** 配置端口。

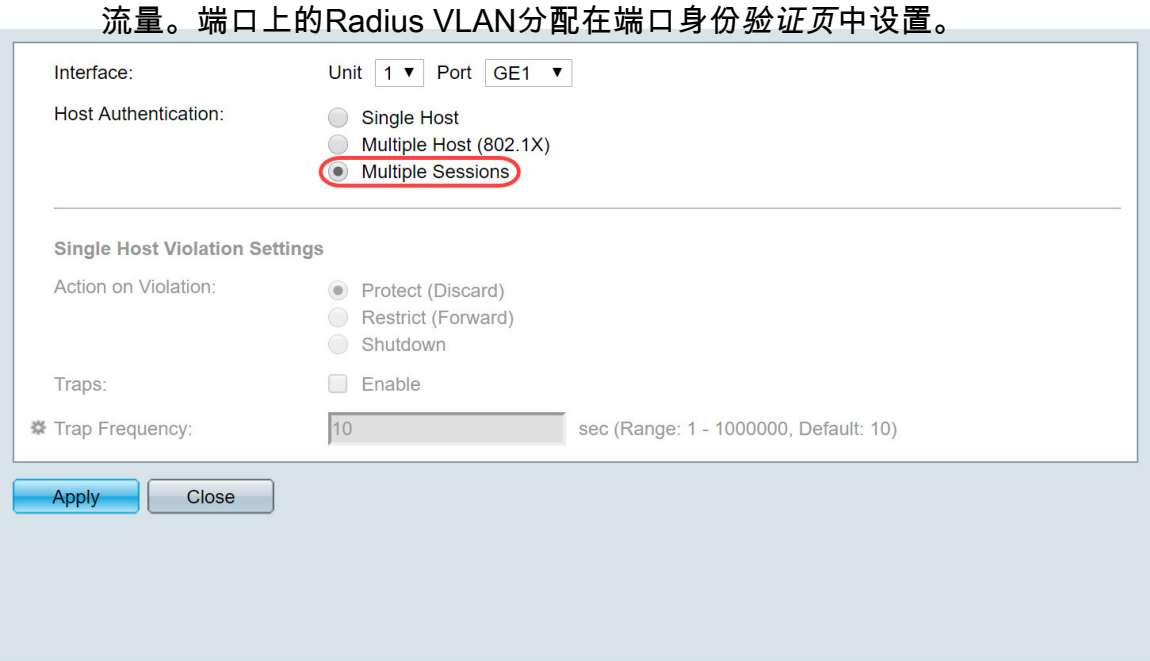


步骤4.在Host Authentication*字段*中，选择以下选项之一：

1. 单主机模式

- 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。



步骤5.单击“**应用**”保存配置。

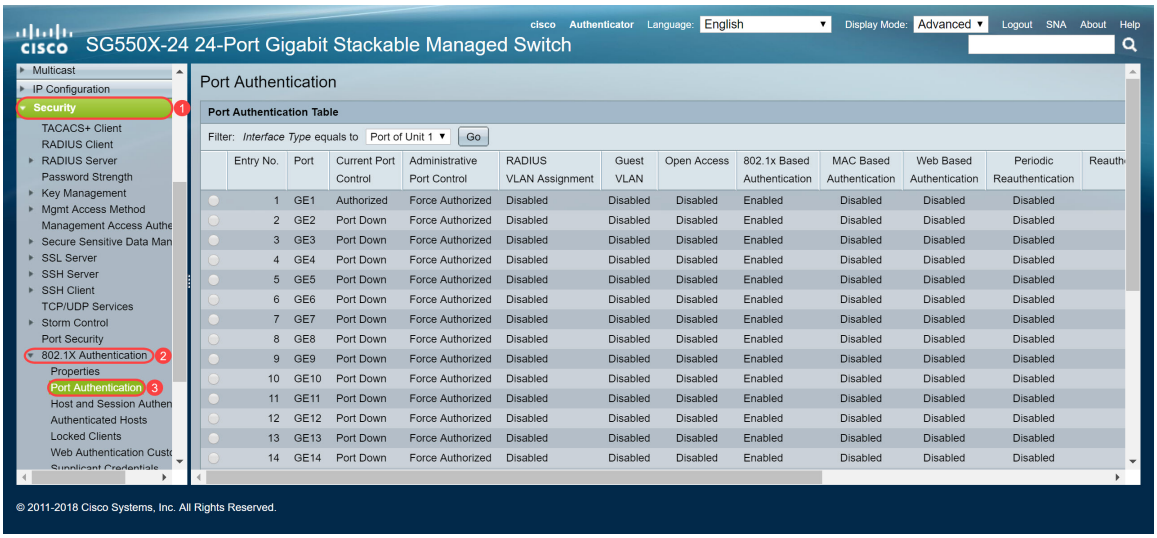
注意：使用*复制设置……* 将GE1的相同配置应用到多个端口。将连接到RADIUS服务器的端口保留*为多主机(802.1X)*。

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。

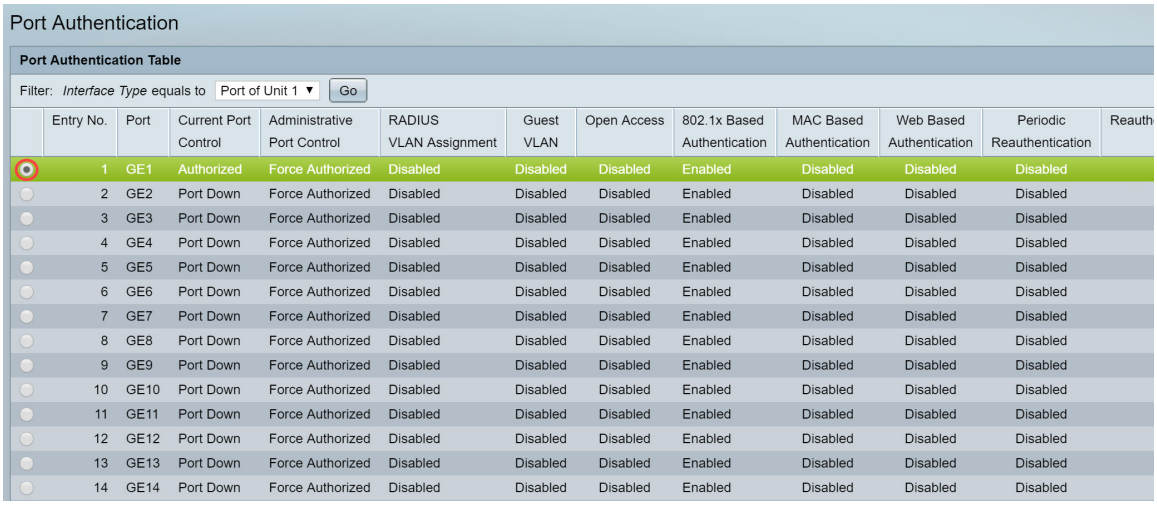
注意：我们将仅配置基于MAC的身份验证所需的设置。其余配置将保留为默认值。

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



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*”。



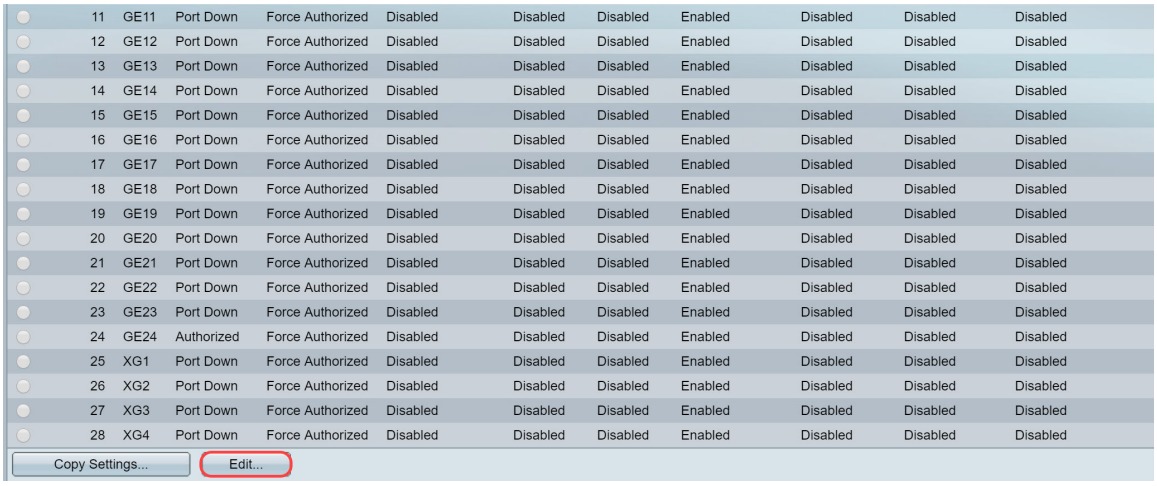
Port Authentication

Port Authentication Table

Filter: *Interface Type* equals to Port of 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
1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	
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	
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	
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	
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	
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。



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
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
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
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
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
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
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
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
28	XG4	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled

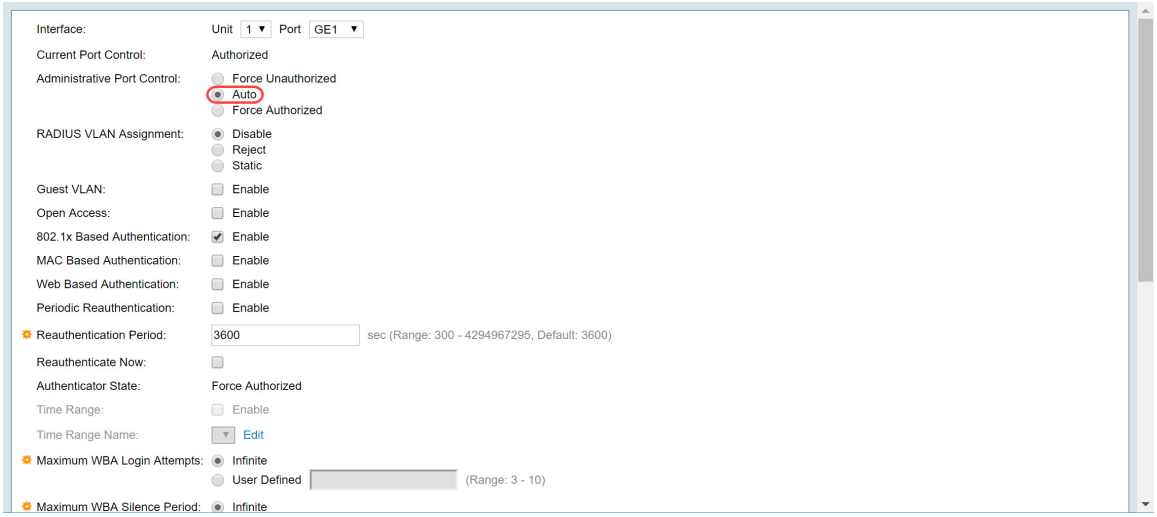
Copy Settings... Edit...

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。

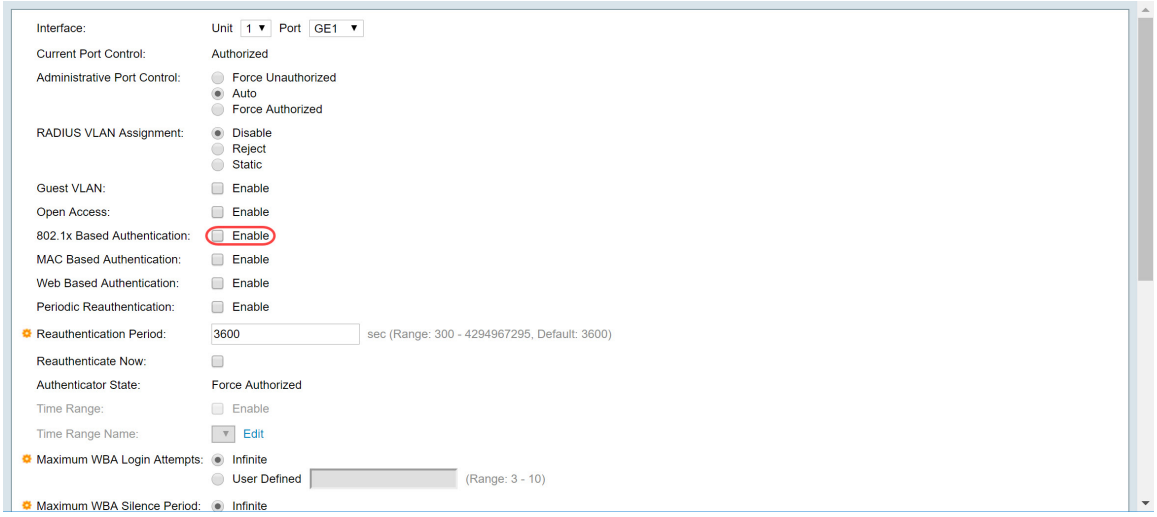
步骤4.选择管理端口授权状态。将端口配置为**Auto**。可用选项包括：

- 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。

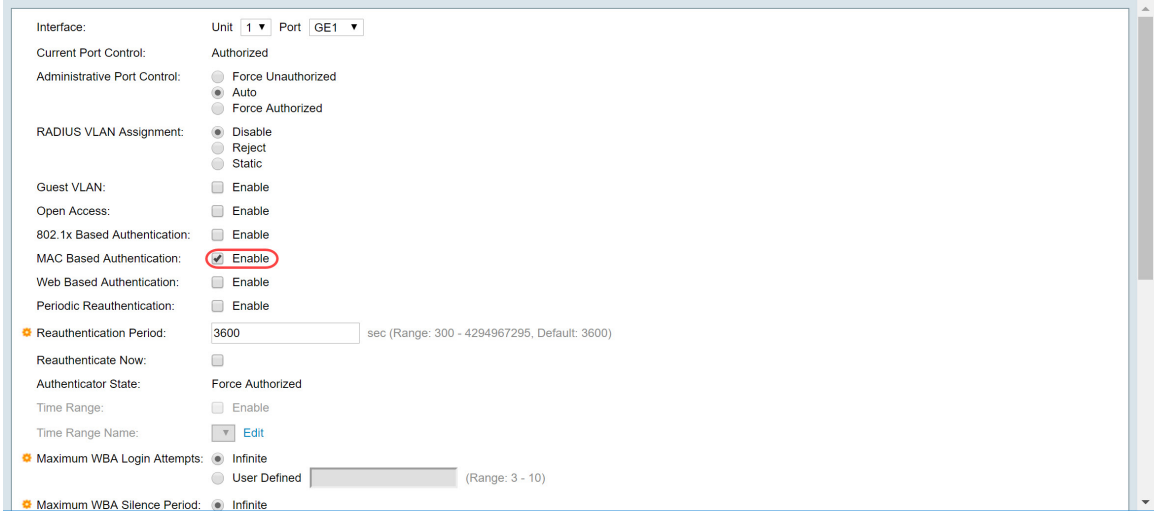
注意：*强制授*权是默认值。



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。



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。



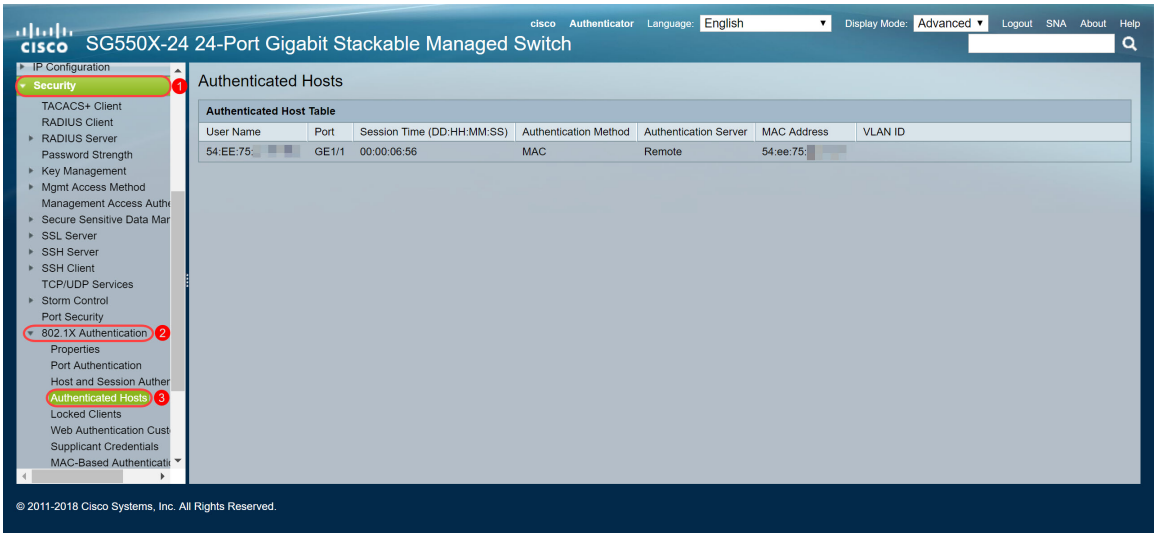
步骤7.单击“**应用**”保存更改。

如果要保存配置，请按屏幕顶部的**Save**按钮。

结论

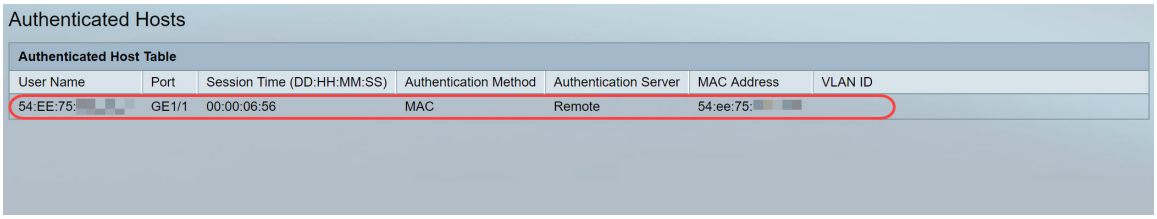
您现在已成功在交换机上配置基于MAC的身份验证。要验证基于MAC的身份验证是否正常工作，请执行以下步骤。

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。

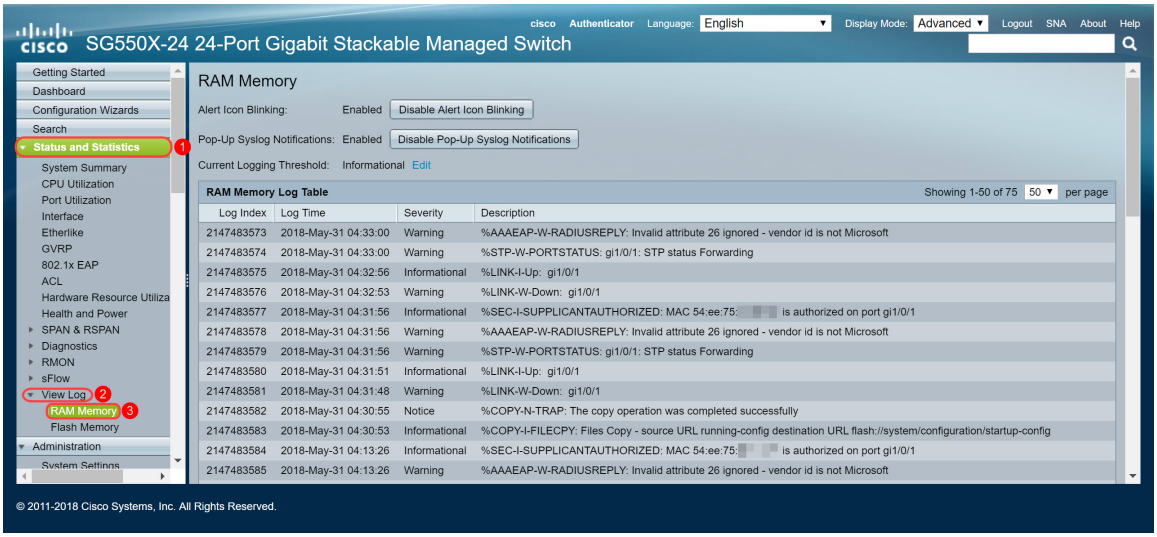


步骤2.在本例中，您可以看到我们的以太网MAC地址已在已验证的主*机表中进行身份验证*。以下字段定义为：

- 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。



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。



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。

2147483584 2018-May-31 04:13:26 Informational %SEC-I-SUPPLICANTAUTHORIZED: MAC 54:ee:75: is authorized on port gi1/0/1

查看本文的视频版本……

单击此处查看思科提供的其他技术讲座