

# 在交换机上配置802.1x端口身份验证设置

## 目标

IEEE 802.1x是一种标准，可促进客户端和服务端之间的访问控制。在通过局域网(LAN)或交换机向客户端提供服务之前，连接到交换机端口的客户端必须由运行远程身份验证拨入用户服务(RADIUS)的身份验证服务器进行身份验证。

802.1x身份验证限制未授权客户端通过可公开访问的端口连接到LAN。802.1x身份验证是客户端 — 服务器模型。在此模型中，网络设备具有以下特定角色：

**客户端或请求方** — 客户端或请求方是请求访问LAN的网络设备。客户端已连接到身份验证器。

**身份验证器** — 身份验证器是提供网络服务并连接了请求方端口的网络设备。支持以下身份验证方法：

**基于802.1x** — 在所有身份验证模式中均受支持。在基于802.1x的身份验证中，身份验证器从802.1x消息或LAN上EAP(EAPoL)数据包中提取可扩展身份验证协议(EAP)消息，然后使用RADIUS协议将其传递到身份验证服务器。

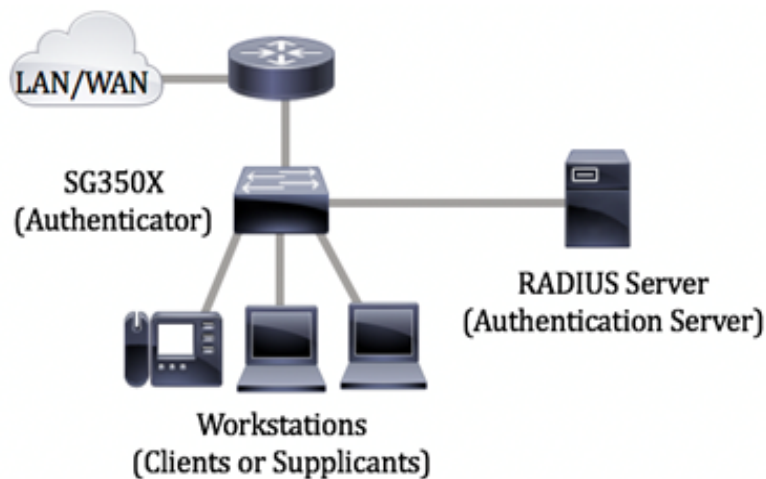
**基于MAC** — 在所有身份验证模式中均受支持。使用基于媒体访问控制(MAC)的身份验证器，身份验证器本身代表寻求网络访问的客户端执行软件的EAP客户端部分。

**基于Web** — 仅在多会话模式下受支持。使用基于Web的身份验证，身份验证器本身代表寻求网络访问的客户端执行软件的EAP客户端部分。

**身份验证服务器** — 身份验证服务器执行客户端的实际身份验证。设备的身份验证服务器是具有EAP扩展的RADIUS身份验证服务器。

**注意：**网络设备可以是客户端或请求方、身份验证器，也可以是每个端口的两者。

下图显示根据特定角色配置设备的网络。在本例中，使用SG350X交换机。



### 配置802.1x的准则：

创建虚拟接入网络(VLAN)。要使用交换机的基于Web的实用程序创建VLAN，请单击[此处](#)。有关基于CLI的说明，请单击[此处](#)。

在交换机上配置端口到VLAN设置。要使用基于Web的实用程序进行配置，请单击[此处](#)。要使用CLI，请单击[此处](#)。

在交换机上配置802.1x属性。802.1x应在交换机上全局启用，以启用基于802.1x端口的身份验证。如需指导，请点击[这里](#)。

(可选) 在交换机上配置时间范围。要了解如何在交换机上配置时间范围设置，请单击[此处](#)。

配置802.1x端口身份验证。本文提供有关如何在交换机上配置802.1x端口身份验证设置的说明。

要了解如何在交换机上配置基于mac的身份验证，请单击[此处](#)。

## 适用设备

Sx300系列

Sx350 系列

SG350X 系列

Sx500系列

Sx550X 系列

# 软件版本

1.4.7.06 - Sx300、Sx500

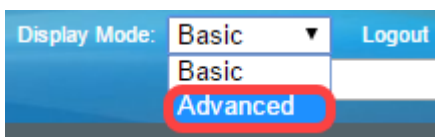
2.2.8.04 — Sx350、SG350X、Sx550X

## 在交换机上配置802.1x端口身份验证设置

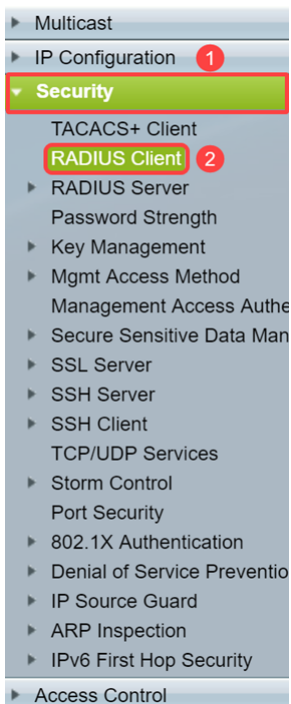
### 配置RADIUS客户端设置

步骤1.登录到交换机的基于Web的实用程序，然后在“显示模式”下拉列表中选择**高级**。

**注意：**可用菜单选项可能因设备型号而异。在本例中，使用SG550X-24。



步骤2.导航至**Security > RADIUS Client**。



步骤3.向下滚动到RADIUS表部分，然后单击**添加.....**以添加RADIUS服务器。

Retries: 3 (Range: 1 - 15, Default: 3)

Timeout for Reply: 3 sec (Range: 1 - 30, Default: 3)

Dead Time: 0 min (Range: 0 - 2000, Default: 0)

Key String:
 

- Encrypted
- Plaintext (0/128 characters used)

Source IPv4 Interface: Auto

Source IPv6 Interface: Auto

Apply Cancel

Server	Priority	Key String (Encrypted)	Timeout for Reply	Authentication Port	Accounting Port	Retries	Dead Time	Usage Type
0 results found.								

Add... Edit... Delete

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

Display Sensitive Data as Plaintext

步骤4.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“IP版本”字段中选择RADIUS服务器的IP地址的版本。

注意：在本例中，我们将使用By IP地址和版本4。

Add RADIUS Server - Google Chrome

Not secure | https://192.168.1.125/cs30a6baef/mts/mgmtauthen/security\_authen\_radius\_a\_jq.htm

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:

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: 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:
 

- Login
- 802.1x
- All

步骤5.按IP地址或名称输入RADIUS服务器。

注意：我们将在Server IP Address/Name字段中输入IP地址192.168.1.146。

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: 192.168.1.146

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: 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:  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。0是最高优先级。

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: 192.168.1.146

Priority: 0 (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: 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:  Login  802.1x  All

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，则设备会尝试使用默认密钥字符串向RADIUS服务器进行身份验证。

**注意：**我们将使用“用户定义（明文）”并在关键示例中输入。

要了解如何在交换机上配置RADIUS服务器设置，请单击[此处](#)。

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: 192.168.1.146

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:  Login  802.1x  All

步骤8.在“回复超时”字段中，选择“使用默认值”或“用户定义”。如果选择了User Defined，请输入设备在重试查询之前等待RADIUS服务器回答的秒数，或者如果重试的次数达到最大值则切换到下一台服务器。如果选择“使用默认值”，则设备使用默认超时值。

注意：在本示例中，选择了“使用默认值”。

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

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:  Login  802.1x  All

Apply Close

步骤9.在Authentication Port字段中输入身份验证请求的RADIUS服务器端口的UDP端口号。在Accounting Port字段中输入记帐请求的RADIUS服务器端口的UDP端口号。

注意：在本例中，我们将同时使用身份验证端口和记帐端口的默认值。

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

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: 1 1812 (Range: 0 - 65535, Default: 1812)

Accounting Port: 2 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:  Login  802.1x  All

Apply Close

步骤10.如果为重试字段选择了“用户定义”，请输入在认为发生故障之前发送到RADIUS服务器的请求数。如果选择“使用默认值”，则设备将使用默认值作为重试次数。

如果为Dead Time选择了User Defined，请输入在为服务请求绕过无响应RADIUS服务器之前必须经过的分钟数。如果选择“使用默认值”，则设备使用失效时间的默认值。如果输入0分钟，则没有停机时间。

注意：在本例中，我们将为这两个字段选择使用默认值。

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface: VLAN 1

Server IP Address/Name: 192.168.1.146

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: 1  Use Default  User Defined Default (Range: 1 - 15, Default: 3)

Dead Time: 2  Use Default  User Defined Default min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  802.1x  All

Apply Close

步骤11.在Usage Type字段中，输入RADIUS服务器身份验证类型。选项有：

登录 - RADIUS服务器用于验证要求管理设备的用户。

802.1x - RADIUS服务器用于802.1x身份验证。

**全部** - RADIUS服务器用于对要求管理设备的用户进行身份验证，以及对802.1x进行身份验证。

The screenshot shows a web browser window titled "Add RADIUS Server - Google Chrome". The address bar shows a URL starting with "https://192.168.1.125/cs30a6baef/mts/mgmtauthen/security\_authen\_radius\_a\_jq.htm". The page contains a configuration form with the following visible settings:

- IP Version:  Version 6  Version 4
- IPv6 Address Type:  Link Local  Global
- Link Local Interface: VLAN 1
- Server IP Address/Name: 192.168.1.146
- 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:  Login  802.1x  All

At the bottom of the form, there are two buttons: "Apply" and "Close". The "Apply" button is highlighted with a red box in the subsequent image.

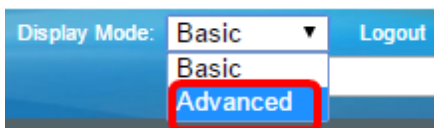
步骤12. 单击“应用”。

This screenshot is identical to the one above, showing the same configuration form. The only difference is that the "Apply" button at the bottom left is now highlighted with a red rectangular box.

## 配置802.1x端口身份验证设置

步骤1. 登录到交换机的基于Web的实用程序，然后在“显示模式”下拉列表中选择高级。

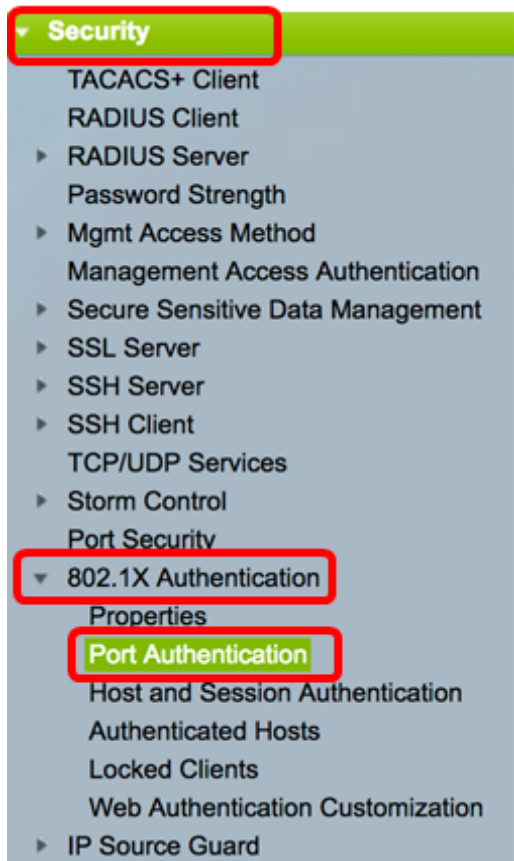
**注意：**可用菜单选项可能因设备型号而异。在本例中，使用SG350X-48MP。



**注意：**如果您有Sx300或Sx500系列交换机，请跳至[步骤2](#)。

步骤2. 选择Security > 802.1X Authentication > Port Authentication。



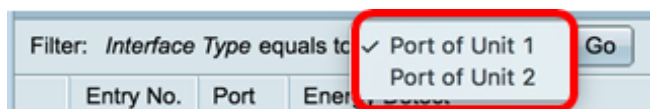


步骤3.从Interface Type下拉列表中选择接口。

端口 — 从接口类型下拉列表中，如果只需要选择一个端口，请选择端口。

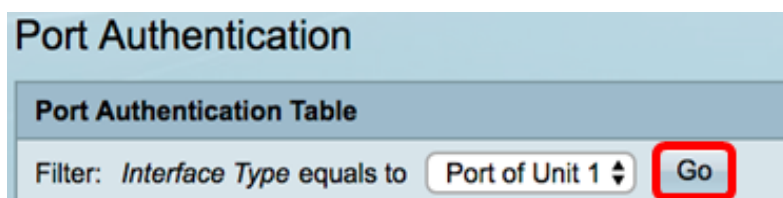
LAG — 从Interface Type下拉列表中，选择要配置的LAG。这会影响在LAG配置中定义的端口组。

**注意：**在本例中，选择单元1的端口。



**注意：**如果您有非堆叠式交换机（如Sx300系列交换机），请跳至[步骤5](#)。

步骤4.单击Go，打开接口上的端口或LAG列表。



步骤5.点击要配置的端口。

Port Authentication Table										
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	
1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	
2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	
3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	
4	GE4	Authorized	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	
5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	
6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled	Enabled	Disabled	Disabled	

**注意：**在本例中，选择GE4。

步骤6. 向下滚动页面，然后单击“编辑”。

46	GE46	Port Down	Force Authorized	Disabled	Disabled
47	GE47	Port Down	Force Authorized	Disabled	Disabled
48	GE48	Port Down	Force Authorized	Disabled	Disabled
49	XG1	Authorized	Force Authorized	Disabled	Disabled
50	XG2	Port Down	Force Authorized	Disabled	Disabled
51	XG3	Port Down	Force Authorized	Disabled	Disabled
52	XG4	Authorized	Force Authorized	Disabled	Disabled

Copy Settings... Edit...

步骤7. ( 可选 ) 如果要编辑其他接口，请从Unit and Port下拉列表中选择。

Interface: Unit 1 Port GE4  
 Current Port Control: Authorized

**注意：**在本例中，选择单元1的端口GE4。

步骤8. 在Administrative Port Control区域中，点击与所需端口控制对应的单选按钮。选项有：

强制未授权 — 通过将端口移至未授权状态来拒绝接口访问。端口将丢弃流量。

自动 — 端口根据请求方的身份验证在授权或未授权状态之间移动。

强制授权 — 授权端口，不进行身份验证。端口将转发流量。

Administrative Port Control:  Force Unauthorized  Auto  Force Authorized

**注意：**在本例中，选择了Auto。

步骤9. 点击RADIUS VLAN Assignment单选按钮，以在所选端口上配置动态VLAN分配。选项有：

禁用 — 功能未启用。

拒绝 — 如果RADIUS服务器授权请求方，但未提供请求方VLAN，则请求方被拒绝。

静态 — 如果RADIUS服务器授权请求方，但未提供请求方VLAN，则接受请求方。

RADIUS VLAN Assignment:  Disable  
 Reject  
 Static

**注意：**在本例中，选择Static。

步骤10.选中Guest VLAN中的**Enable**复选框，为未授权端口启用Guest VLAN。访客VLAN使未授权端口自动加入在802.1属性的访客VLAN ID区域中选择的VLAN。

Guest VLAN:  Enable

步骤11. ( 可选 ) 选中Enable Open Access复选框以启用开放访问。开放式访问可帮助您了解连接到网络的主机的配置问题，监控不良情况，并使这些问题得以解决。

**注意：**在接口上启用开放访问时，交换机将从RADIUS服务器收到的所有故障视为成功，并允许连接到接口的工作站访问网络，而不考虑身份验证结果。在本例中，禁用开放访问。

Guest VLAN:  Enable  
Open Access:  Enable

步骤12.选中**Enable 802.1x Based Authentication**复选框以在端口上启用802.1X身份验证。

Guest VLAN:  Enable  
Open Access:  Enable  
802.1x Based Authentication:  Enable

步骤13.选中**Enable MAC Based Authentication**复选框以根据请求方MAC地址启用端口身份验证。端口上只能使用八个基于MAC的身份验证。

**注意：**要使MAC身份验证成功，RADIUS服务器请求方用户名和密码必须是请求方MAC地址。MAC地址必须以小写字母形式输入，且不带。或 — 分隔符（例如0020aa00bbcc）。

802.1x Based Authentication:  Enable  
MAC Based Authentication:  Enable

**注意：**在本示例中，禁用基于MAC的身份验证。

步骤14.选中**Enable Web Based Authentication**复选框以在交换机上启用基于Web的身份验证。在本示例中，禁用基于Web的身份验证。

802.1x Based Authentication:  Enable  
MAC Based Authentication:  Enable  
Web Based Authentication:  Enable

**注意：**在本示例中，禁用基于Web的身份验证。

第15步。( 可选 ) 选中**Enable Periodic Reauthentication**复选框，强制端口在给定时间后重新进行身份验证。此时间在Reauthentication Period字段中定义。

Web Based Authentication:  Enable  
Periodic Reauthentication:  Enable

**注意：**在本例中，启用了期间重新身份验证。

步骤16. ( 可选 ) 在Reauthentication Period字段中输入值。此值表示接口重新验证端口之前的秒数。默认值为3600秒，范围为300至4294967295秒。

Periodic Reauthentication:  Enable  
Reauthentication Period:  sec

**注意：**在本例中，配置了6000秒。

第17步。( 可选 ) 选中**Enable Reauthenticate Now** ( 立即启用重新身份验证 ) 复选框，强制立即进行端口重新身份验证。在本例中，立即重新身份验证被禁用。

Periodic Reauthentication:  Enable  
Reauthentication Period:  sec  
Reauthenticate Now:   
Authenticator State: Force Authorized

身份验证器状态区域显示端口的授权状态。

第18步。( 可选 ) 选中**Enable Time Range**复选框以启用对端口授权时间的限制。

Time Range:  Enable  
Time Range Name:  Edit

**注意：**在本例中，启用了时间范围。如果您希望跳过此功能，请继续[步骤20](#)。

步骤19. ( 可选 ) 从Time Range Name下拉列表中，选择要使用的时间范围。

Time Range:  Enable  
Time Range Name:  iii  
Maximum WBA Login Attempts:

**注意：**在本例中，选择Dayshift。

步骤20.在Maximum WBA Login Attempts区域，点击Infinite for no limit或User Defined以设置限制。如果选择“用户定义”(User Defined)，请输入允许进行基于Web的身份验证的最大登录尝试次数。

Maximum WBA Login Attempts:  Infinite  
 User Defined

**注意：**在本例中，选择Infinite。

步骤21.在Maximum WBA Silence Period区域，点击Infinite for no limit或User Defined以设置限制。如果选择“用户定义”，请输入接口上允许的基于Web的身份验证的静默期的最大长度。

Maximum WBA Silence Period:  Infinite  User Defined  sec

注意：在本例中，选择Infinite。

步骤22.在Max Hosts区域中，点击Infinite for no limit或User Defined以设置限制。如果选择“用户定义”，请输入接口上允许的最大授权主机数。

Max Hosts:  Infinite  User Defined

注意：将此值设置为1，以在多会话模式下模拟单主机模式进行基于Web的身份验证。在本例中，选择Infinite。

步骤23.在Quiet Period字段中，输入身份验证交换失败后交换机保持静默状态的时间。当交换机处于静默状态时，这意味着交换机未侦听来自客户端的新身份验证请求。默认值为60秒，范围为1到65535秒。

Quiet Period:

注意：在本例中，静音周期设置为120秒。

步骤24.在Resending EAP字段中，输入交换机在重新发送请求之前等待请求方发出响应消息的时间。默认值为30秒，范围为1到65535秒。

Quiet Period:   
Resending EAP:

注意：在本例中，重发EAP设置为60秒。

步骤25.在“最大EAP请求数”字段中，输入可发送的最大EAP请求数。EAP是802.1X中使用的一种身份验证方法，用于在交换机和客户端之间交换身份验证信息。在这种情况下，EAP请求将发送到客户端进行身份验证。然后，客户端必须响应并匹配身份验证信息。如果客户端未响应，则根据Resending EAP值设置另一个EAP请求，然后重新启动身份验证过程。默认值为2，范围为1到10。

Quiet Period:   
Resending EAP:   
Max EAP Requests:

注意：在本例中，使用默认值2。

步骤26.在Supplicant客户端超时(Supplicant Timeout)字段中，输入EAP请求重新发送给请求方之前的时间。默认值为30秒，范围为1到65535秒。

☛ Max EAP Requests:  (Rar

☛ Supplicant Timeout:  sec |

**注意：**在本例中，请求方超时设置为60秒。

步骤27.在 *Server Timeout* 字段中，输入交换机再次向RADIUS服务器发送请求之前经过的时间。默认值为30秒，范围为1到65535秒。

☛ Max EAP Requests:  (Ran

☛ Supplicant Timeout:  sec |

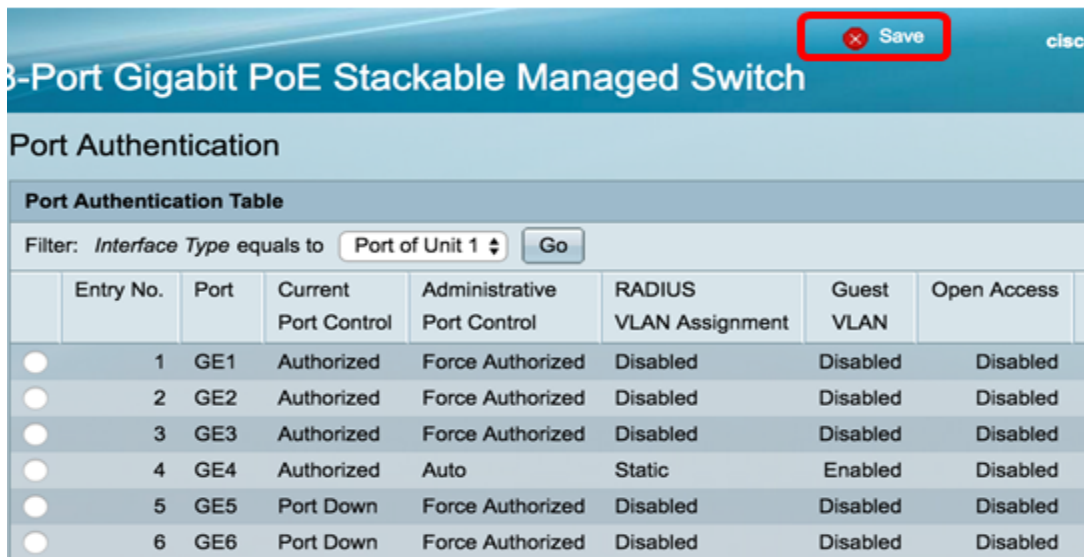
☛ Server Timeout:  sec |

**注意：**在本例中，服务器超时设置为60秒。

步骤28.单击“应用”，然后单击“关闭”。

Interface:	Unit	1	Port	GE4
Current Port Control:	Unauthorized			
Administrative Port Control:	<input type="radio"/> Force Unauthorized <input checked="" type="radio"/> Auto <input type="radio"/> Force Authorized			
RADIUS VLAN Assignment:	<input type="radio"/> Disable <input type="radio"/> Reject <input checked="" type="radio"/> Static			
Guest VLAN:	<input checked="" type="checkbox"/> Enable			
Open Access:	<input type="checkbox"/> Enable			
802.1x Based Authentication:	<input checked="" type="checkbox"/> Enable			
MAC Based Authentication:	<input type="checkbox"/> Enable			
Web Based Authentication:	<input type="checkbox"/> Enable			
Periodic Reauthentication:	<input checked="" type="checkbox"/> Enable			
Reauthentication Period:	6000	sec (Range: 300 - 4294967295, Default: 3600)		
Reauthenticate Now:	<input type="checkbox"/>			
Authenticator State:	Connecting			
Time Range:	<input type="checkbox"/> Enable			
Time Range Name:	Dayshift <a href="#">Edit</a>			
Maximum WBA Login Attempts:	<input checked="" type="radio"/> Infinite <input type="radio"/> User Defined <input type="text"/> (Range: 3 - 10)			
Maximum WBA Silence Period:	<input checked="" type="radio"/> Infinite <input type="radio"/> User Defined <input type="text"/> sec (Range: 60 - 65535)			
Max Hosts:	<input checked="" type="radio"/> Infinite <input type="radio"/> User Defined <input type="text"/> sec (Range: 1 - 4294967295)			
Quiet Period:	120	sec (Range: 10 - 65535, Default: 60)		
Resending EAP:	60	sec (Range: 30 - 65535, Default: 30)		
Max EAP Requests:	2	(Range: 1 - 10, Default: 2)		
Supplicant Timeout:	60	sec (Range: 1 - 65535, Default: 30)		
Server Timeout:	60	sec (Range: 1 - 65535, Default: 30)		
<input checked="" type="button" value="Apply"/> <input type="button" value="Close"/>				

步骤29. ( 可选 ) 单击“保存”将设置保存到启动配置文件。



3-Port Gigabit PoE Stackable Managed Switch

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
<input type="radio"/>	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	4	GE4	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled

现在，您应该已成功配置交换机上的802.1x端口身份验证设置。

## 将接口配置设置应用到多个接口

步骤1. 点击要将身份验证配置应用到多个接口的接口的单选按钮。

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
<input type="radio"/>	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input checked="" type="radio"/>	4	GE4	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled

**注意：**在本例中，选择GE4。

步骤2. 向下滚动，然后单击“复制设置”。

<input type="radio"/>	43	GE43	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	44	GE44	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	45	GE45	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	46	GE46	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	47	GE47	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	48	GE48	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	49	XG1	Authorized	Force Authorized	Disabled	Disabled
<input type="radio"/>	50	XG2	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	51	XG3	Port Down	Force Authorized	Disabled	Disabled
<input type="radio"/>	52	XG4	Authorized	Force Authorized	Disabled	Disabled

Copy Settings... Edit...

步骤3. 在to字段中，输入要应用所选接口配置的接口范围。可以使用接口编号或接口名称作为输入。您可以输入以逗号分隔的每个接口（如1、3、5或GE1、GE3、GE5），也可以输入接口范围（如1-5或GE1-GE5）。



Copy configuration from entry 4 (GE4)

to:  (Example: 1,3,5-10 or: GE1,GE3-XG4)

注意：在本例中，配置设置将应用于端口47到48。

步骤4.单击“应用”，然后单击“关闭”。

Copy configuration from entry 4 (GE4)

to:  (Example: 1,3,5-10 or: GE1,GE3-XG4)

下图描述了配置后的更改。

Port Authentication Table							
Filter: <i>Interface Type</i> equals to <input type="text" value="Port of Unit 1"/> <input type="button" value="Go"/>							
	Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access
<input type="radio"/>	1	GE1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	2	GE2	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	3	GE3	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	4	GE4	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	5	GE5	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	6	GE6	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	45	GE45	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	46	GE46	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	47	GE47	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	48	GE48	Authorized	Auto	Static	Enabled	Disabled
<input type="radio"/>	49	XG1	Authorized	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	50	XG2	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	51	XG3	Port Down	Force Authorized	Disabled	Disabled	Disabled
<input type="radio"/>	52	XG4	Authorized	Force Authorized	Disabled	Disabled	Disabled

现在，您应该已成功复制一个端口的802.1x身份验证设置，并应用到交换机上的其他端口。