

# 802.1X在Cisco 200/300系列被管理的交换机的端口身份验证配置

## 客观

本文目标将解释802.1X在200/300系列被管理的交换机的端口认证。802.1X端口认证enable (event) 802.1X参数的配置每个端口的。端口请求的认证称为请求方。证明人是交换机或作为网络卫兵给恳求者的接入点。证明人寄认证消息给RADIUS服务器，以便端口验证并且能发送和获得信息。

## 可适用的设备

- SF/SG 200和SF/SG 300系列被管理的交换机

## 软件版本

- 1.3.0.62

## 端口身份验证配置

步骤1.登陆到Web配置工具并且选择安全> 802.1x >端口认证。端口认证页打开：

Entry No.	Port	User Name	Current	RADIUS	Guest	Authentication	Periodic	Reauthentication	Authenticator	Time Range	Quiet	
			Port Control	VLAN Assignment	VLAN	Method	Reauthentication	Period	State	Name	State	Period
<input checked="" type="radio"/>	1	FE1	Authorized	Disabled	Disabled	802.1x Only	Disabled	3600	Force Authorized		Inactive	60
<input type="radio"/>	2	FE2	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
<input type="radio"/>	3	FE3	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
<input type="radio"/>	4	FE4	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
<input type="radio"/>	5	FE5	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
<input type="radio"/>	6	FE6	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
<input type="radio"/>	7	FE7	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
<input type="radio"/>	8	FE8	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
<input type="radio"/>	9	FE9	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60
<input type="radio"/>	10	FE1	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize		Inactive	60

步骤2.点击对应于端口您希望编辑的单选按钮。

步骤3.点击编辑。编辑端口认证窗口出现。

Interface:	Port	FE1	
User Name:			
Current Port Control:		Authorized	
Administrative Port Control:		<input type="radio"/> Force Unauthorized <input type="radio"/> Auto <input checked="" type="radio"/> Force Authorized	
RADIUS VLAN Assignment:		<input type="checkbox"/> Enable	
Guest VLAN:		<input type="checkbox"/> Enable	
Authentication Method:		<input checked="" type="radio"/> 802.1x Only <input type="radio"/> MAC Only <input type="radio"/> 802.1x and MAC	
Periodic Reauthentication:		<input checked="" type="checkbox"/> Enable	
Reauthentication Period:		3000	sec. (Range: 300 - 4294967295, Default: 3600)
Reauthenticate Now:		<input type="checkbox"/>	
Authenticator State:		Force Authorized	
Time Range:		<input type="checkbox"/> Enable	
Time Range Name:		<input type="text"/> Edit	
Quiet Period:		100	sec. (Range: 0 - 65535, Default: 60)
Resending EAP:		200	sec. (Range: 30 - 65535, Default: 30)
Max EAP Requests:		5	(Range: 1 - 10, Default: 2)
Supplicant Timeout:		50	sec. (Range: 1 - 65535, Default: 30)
Server Timeout:		15	sec. (Range: 1 - 65535, Default: 30)
Termination Cause:		Not terminated yet	

Apply Close

用户名名称字段显示端口的用户名。

**Note:**当前的端口控制字段显示当前的端口状态。如果端口在未授权的状态意味着端口或者没有验证或设置管理端口控制强制未授权的。另一方面，如果端口在Authorized State，意味着端口或者验证或设置管理端口控制强制核准。

第 4 步：在管理端口控制字段，请点击其中一个可用的单选按钮确定端口认证状态：

- 未授权的强制—此选项迁移选择的接口向未授权的状态。在此状态下，交换机不提供认证给客户端被联络到接口。
- 自动—在选择接口的此选项enable (event)认证和授权。在此状态下，交换机提供802.1X认证给客户端被联络到接口并且根据与客户端的认证信息交换决定，如果客户端验证或没有，并且迁移接口向授权或未授权的国。
- 被核准的强制—此选项设置接口对核准，不用客户端验证。

在客户VLAN字段的第5步(可选)，检查**Enable复选框**使用客户VLAN未授权的端口。

第6步。在认证方法字段，请点击其中一个可用的单选按钮验证端口。选项是：

- 仅802.1X —仅802.1X认证在端口进行。

- 仅MAC —仅基于MAC验证来在端口执行。仅8个基于MAC的认证在单个端口可以进行。
- 802.1X和MAC —两个认证方法在端口执行。

第 7 步：在定期再验证字段，请检查**Enable复选框**对根据再验证周期值的端口的enable (event)定期认证。

第8.步。在再验证周期字段，请以秒钟进入时候重新鉴别端口。

第9.步。当前检查**重新鉴别复选框**立即重新鉴别端口。

**Note:**证明人State字段显示认证当前状态。

第10.步(可选)，如果端口基于认证在交换机，然后时间范围和时间范围名称字段允许是启用的。在时间范围字段，请输入时期(以秒钟)端口被核准为使用的地方，如果802.1X授权是启用的。在时间范围名字下拉列表中，请选择识别时间范围的配置文件。

第11.步。在安静周期字段，请输入交换机在状态相当依然是，在失败的认证交换后的时间。当交换机在平静的状态时，意味着交换机不细听自客户端的新证书请求。

步骤12。在再发出的EAP (可扩展的认证协议)字段，请输入交换机在再发出请求前等待从请求方的一个响应消息的时间。

第13步。在最大EAP请求字段，请输入的EAP请求的最大数量可以发送。EAP是提供在交换机和客户端之间的认证信息交换用于802.1X的认证方法。在这种情况下，EAP请求被发送到认证的客户端。客户端必须然后回应和匹配认证信息。如果客户端不回应，则根据再发出的EAP值集合的另一个EAP请求，并且认证过程被重新启动。

步骤14。在请求方超时字段，在EAP请求被再发出对请求方前，请输入时间。

第15步。在服务器超时字段，请输入流逝的时间，在交换机再发送一个请求到RADIUS服务器前。

终端原因字段显示端口认证失败的原因。

第16步。点击**适用**保存您的配置。

## 运用接口配置于多个接口

此部分说明如何运用端口802.1X身份验证配置于多个端口。

步骤1.登陆到Web配置工具并且选择**安全 > 802.1x > 端口认证**。端口认证页打开：

Port Authentication Table											
Entry No.	Port	User Name	Current Port Control	RADIUS VLAN Assignment	Guest VLAN	Authentication Method	Periodic Reauthentication	Reauthentication Period	Authenticator State	Time Range Name	Quiet State
<input checked="" type="radio"/>	1	FE1	Authorized	Disabled	Disabled	802.1x Only	Enabled	3000	Force Authorized	Inactive	100
<input type="radio"/>	2	FE2	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize	Inactive	60
<input type="radio"/>	3	FE3	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize	Inactive	60
<input type="radio"/>	4	FE4	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize	Inactive	60
<input type="radio"/>	5	FE5	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize	Inactive	60
<input type="radio"/>	6	FE6	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize	Inactive	60
<input type="radio"/>	7	FE7	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize	Inactive	60
<input type="radio"/>	8	FE8	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize	Inactive	60
<input type="radio"/>	9	FE9	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize	Inactive	60
<input type="radio"/>	10	FE10	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize	Inactive	60

步骤2.点击接口的单选按钮您要运用身份验证配置于多个接口。

步骤3.点击“Copy”设置。Settings窗口的复制出现。

Copy configuration from entry 1 (GE1)

to:  (Example: 1,3,5-10 or GE1,GE3-GE5)

第 4 步：在对字段，请输入您希望运用在选择的接口配置第2.步接口的范围。您能使用接口号或接口的名字作为输入。您能进入逗号分离的每个接口(例如：1，3，5或者GE1、GE3，GE5)或您能输入接口的范围(例如：1-5或GE1-GE5)。

步骤5.点击适用保存您的配置。

下面的镜像在配置以后表示更改。

Port Authentication Table												
Entry No.	Port	User Name	Current	RADIUS	Guest	Authentication	Periodic	Reauthentication	Authenticator	Time Range	Quiet	
			Port Control	VLAN Assignment	VLAN	Method	Reauthentication	Period	State	Name	State	Period
<input type="radio"/>	1	FE1	Authorized	Disabled	Disabled	802.1x Only	Enabled	3000	Force Authorized	Inactive	100	
<input type="radio"/>	2	FE2	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize	Inactive	60	
<input type="radio"/>	3	FE3	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize	Inactive	60	
<input type="radio"/>	4	FE4	N/A	Disabled	Disabled	802.1x Only	Disabled	3600	Initialize	Inactive	60	
<input type="radio"/>	5	FE5	N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize	Inactive	100	
<input type="radio"/>	6	FE6	N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize	Inactive	100	
<input type="radio"/>	7	FE7	N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize	Inactive	100	
<input type="radio"/>	8	FE8	N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize	Inactive	100	
<input type="radio"/>	9	FE9	N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize	Inactive	100	
<input type="radio"/>	10	FE10	N/A	Disabled	Disabled	802.1x Only	Enabled	3000	Initialize	Inactive	100	