

在Cisco Sx220系列智能交换机上配置802.1X端口身份验证

目标

本文的目的是向您展示如何在Sx220系列智能交换机上配置端口身份验证。

802.1X端口身份验证支持为设备上的每个端口配置802.1X参数。请求身份验证的端口称为请求方。身份验证器是充当请求方网络防护的交换机或接入点。身份验证器将身份验证消息转发到RADIUS服务器，以便端口可以进行身份验证并可以发送和接收信息。

适用设备

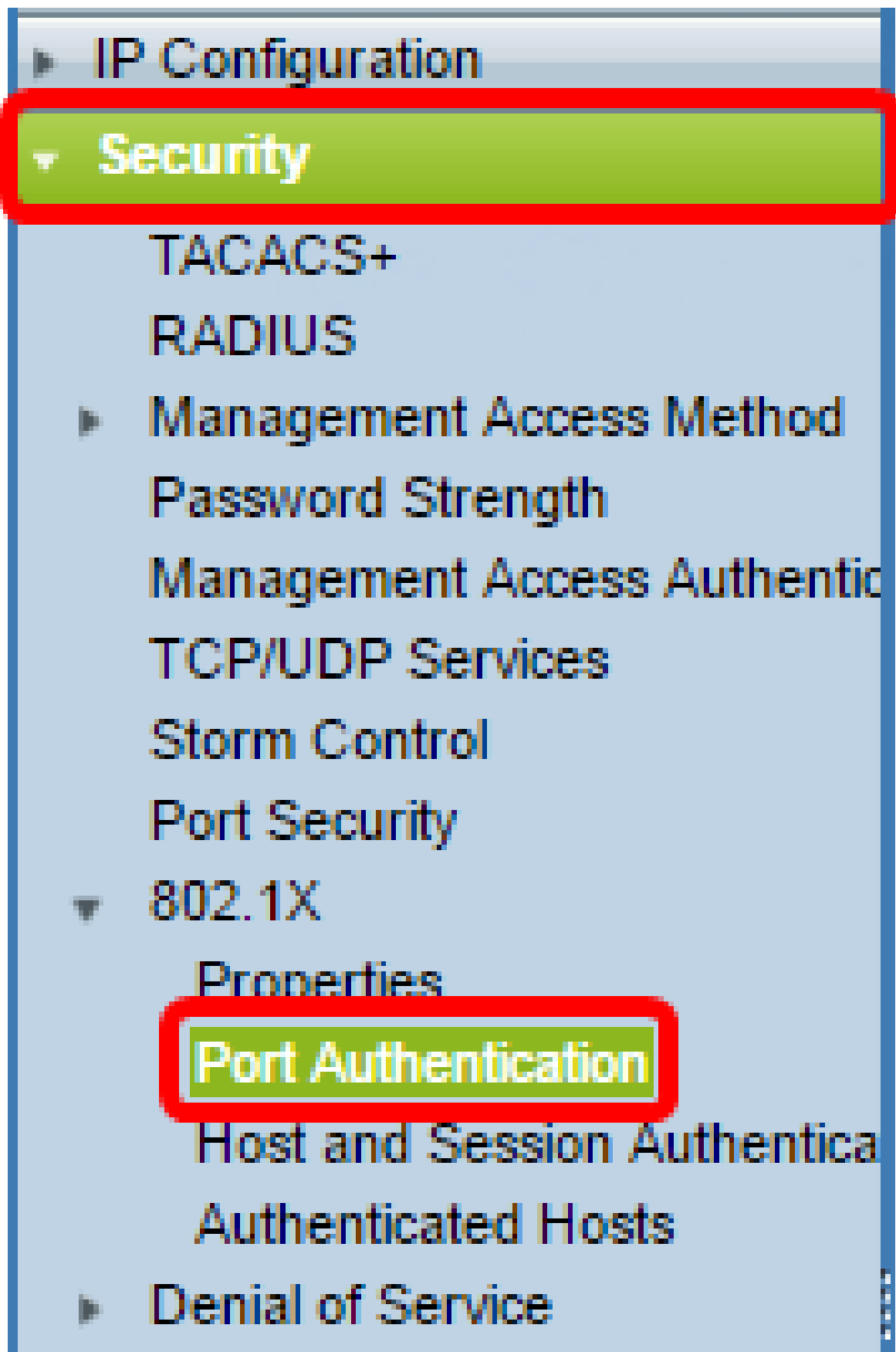
- Sx220系列

软件版本

- 1.1.0.14

配置端口身份验证

步骤1:登录到交换机基于Web的实用程序，并选择安全> 802.1X >端口身份验证。



第二步：点击要配置的端口的单选按钮，然后点击编辑。

<input type="radio"/>	3	GE3	N/A	Disabled	Disabled	Disabled	Enabled
<input checked="" type="radio"/>	4	GE4	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	5	GE5	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	6	GE6	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	7	GE7	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	8	GE8	N/A	Auto	Disabled	Enabled	Enabled
<input type="radio"/>	9	GE9	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	10	GE10	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	11	GE11	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	12	GE12	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	13	GE13	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	14	GE14	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	15	GE15	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	16	GE16	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	17	GE17	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	18	GE18	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	19	GE19	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	20	GE20	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	21	GE21	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	22	GE22	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	23	GE23	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	24	GE24	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	25	GE25	N/A	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	26	GE26	N/A	Disabled	Disabled	Disabled	Enabled

Copy Settings... Edit...

注意：在本示例中，选择了端口GE4。

第三步：系统将弹出Edit Port Authentication窗口。从Interface下拉列表中，确保指定的端口是您在第2步中选择的端口。否则，请点击下拉箭头并选择正确的端口。

Interface: Port GE4 ▼

Administrative Port Control: Disabled
 Force Unauthorized
 Auto
 Force Authorized

RADIUS VLAN Assignment: Disabled
 Reject
 Static

Guest VLAN: Enable

第四步：选择管理端口控制的单选按钮。这将确定端口授权状态。选项有：

- 已禁用 — 禁用802.1X。这是默认状态。
- Force Unauthorized — 通过将接口移至未授权状态来拒绝接口访问。交换机不通过接口向客户端提供身份验证服务。
- 自动 — 在交换机上启用基于端口的身份验证和授权。根据交换机和客户端之间的身份验证交换，接口在已授权或未授权状态之间移动。
- Force Authorized — 授权接口而不进行身份验证。

Interface: Port GE4 ▼

Administrative Port Control: Disabled
 Force Unauthorized
 Auto
 Force Authorized

RADIUS VLAN Assignment: Disabled
 Reject
 Static

Guest VLAN: Enable

注意：在本示例中，选择Auto。

步骤5. (可选) 为RADIUS VLAN分配选择单选按钮。这将启用指定端口上的动态VLAN分配。选项有：

- 已禁用 — 忽略VLAN授权结果并保留主机的原始VLAN。这是默认操作。
- 拒绝 — 如果指定端口收到VLAN授权信息，它将使用该信息。但是，如果没有VLAN授权信息，它将拒绝主机并使其处于未授权状态。
- 静态 — 如果指定端口收到VLAN授权信息，它将使用该信息。但是，如果没有VLAN授权信息，它将保留主机的原始VLAN。

注意：如果存在来自RADIUS的VLAN授权信息，但未在测试设备(DUT)上管理性创建VLAN，则会自动创建VLAN。在本例中，选择Static。

Interface:	Port <input type="text" value="GE4"/>
Administrative Port Control:	<input type="radio"/> Disabled <input type="radio"/> Force Unauthorized <input checked="" type="radio"/> Auto <input type="radio"/> Force Authorized
RADIUS VLAN Assignment:	<input type="radio"/> Disabled <input type="radio"/> Reject <input checked="" type="radio"/> Static
Guest VLAN:	<input type="checkbox"/> Enable

快速提示：要使动态VLAN分配功能正常工作，交换机需要由RADIUS服务器发送以下VLAN属性：

- [64]隧道类型= VLAN (类型13)
- [65] Tunnel-Medium-Type = 802 (类型6)
- [81]隧道专用组Id = VLAN ID

步骤6. (可选) 选中Enable复选框，使访客VLAN将访客VLAN用于未授权的端口。


Interface:	Port	GE4 ▼
Administrative Port Control:	<input type="radio"/>	Disabled
	<input type="radio"/>	Force Unauthorized
	<input checked="" type="radio"/>	Auto
	<input type="radio"/>	Force Authorized
RADIUS VLAN Assignment:	<input type="radio"/>	Disabled
	<input type="radio"/>	Reject
	<input checked="" type="radio"/>	Static
Guest VLAN:	<input checked="" type="checkbox"/>	Enable

步骤 7. 选中Enable复选框以定期重新进行身份验证。这将启用端口重新身份验证尝试（在指定的重新身份验证时间段之后）。

Interface:	Port	GE4 ▼
Administrative Port Control:	<input type="radio"/>	Disabled
	<input type="radio"/>	Force Unauthorized
	<input checked="" type="radio"/>	Auto
	<input type="radio"/>	Force Authorized
RADIUS VLAN Assignment:	<input type="radio"/>	Disabled
	<input type="radio"/>	Reject
	<input checked="" type="radio"/>	Static
Guest VLAN:	<input checked="" type="checkbox"/>	Enable
Periodic Reauthentication:	<input checked="" type="checkbox"/>	Enable

注：默认情况下启用此功能。

步骤 8在Reauthentication Period字段中输入值。这是重新验证端口的时间（以秒为单位）。

Interface:	Port	GE4 ▼
Administrative Port Control:	<input type="radio"/>	Disabled
	<input type="radio"/>	Force Unauthorized
	<input checked="" type="radio"/>	Auto
	<input type="radio"/>	Force Authorized
RADIUS VLAN Assignment:	<input type="radio"/>	Disabled
	<input type="radio"/>	Reject
	<input checked="" type="radio"/>	Static
Guest VLAN:	<input checked="" type="checkbox"/>	Enable
Periodic Reauthentication:	<input checked="" type="checkbox"/>	Enable
 Reauthentication Period:	<input type="text" value="3600"/>	
Reauthenticate Now:	<input type="checkbox"/>	

注：在本示例中，使用默认值3600。

步骤9. (可选) 选中Reauthenticate Now复选框以启用立即端口重新身份验证。

注：身份验证器状态字段显示身份验证的当前状态。

Interface:	Port	GE4 ▼
Administrative Port Control:	<input type="radio"/>	Disabled
	<input type="radio"/>	Force Unauthorized
	<input checked="" type="radio"/>	Auto
	<input type="radio"/>	Force Authorized
RADIUS VLAN Assignment:	<input type="radio"/>	Disabled
	<input type="radio"/>	Reject
	<input checked="" type="radio"/>	Static
Guest VLAN:	<input checked="" type="checkbox"/>	Enable
Periodic Reauthentication:	<input checked="" type="checkbox"/>	Enable
Reauthentication Period:	<input type="text" value="3600"/>	
Reauthenticate Now:	<input checked="" type="checkbox"/>	
Authenticator State:	N/A	

注意：如果端口未处于Force Authorized或Force Unauthorized状态，则它处于Auto Mode状态，身份验证器显示正在进行的身份验证的状态。端口通过身份验证后，状态显示为Authenticated。

步骤 10在Max Hosts字段中，输入特定端口上允许的最大身份验证主机数量。此值仅在多会话模式下生效。

Interface:	Port	GE4 ▼
Administrative Port Control:	<input type="radio"/> Disabled	<input type="radio"/> Force Unauthorized
	<input checked="" type="radio"/> Auto	<input type="radio"/> Force Authorized
RADIUS VLAN Assignment:	<input type="radio"/> Disabled	<input type="radio"/> Reject
	<input checked="" type="radio"/> Static	
Guest VLAN:	<input checked="" type="checkbox"/> Enable	
Periodic Reauthentication:	<input checked="" type="checkbox"/> Enable	
⚙️ Reauthentication Period:	<input type="text" value="3600"/>	
Reauthenticate Now:	<input checked="" type="checkbox"/>	
Authenticator State:	N/A	
⚙️ Max Hosts:	<input type="text" value="256"/>	

注：在本示例中，使用默认值256。

步骤 11在Quiet Period字段中，输入身份验证交换失败后交换机保持安静状态的秒数。当交换机处于静默状态时，这意味着交换机没有侦听来自客户端的新身份验证请求。

⚙️ Reauthentication Period:	<input type="text" value="3600"/>
Reauthenticate Now:	<input checked="" type="checkbox"/>
Authenticator State:	N/A
⚙️ Max Hosts:	<input type="text" value="256"/>
⚙️ Quiet Period:	<input type="text" value="60"/>

注：在本示例中，使用默认值60。

步骤 12在重新发送EAP字段中，输入交换机在重新发送请求之前等待来自请求方（客户端）的可扩展身份验证协议(EAP)请求或身份帧的响应的秒数。

⚙️ Reauthentication Period:	<input type="text" value="3600"/>
Reauthenticate Now:	<input checked="" type="checkbox"/>
Authenticator State:	N/A
⚙️ Max Hosts:	<input type="text" value="256"/>
⚙️ Quiet Period:	<input type="text" value="60"/>
⚙️ Resending EAP:	<input type="text" value="30"/>

注：在本示例中，使用默认值30。

步骤 13在Max EAP Requests字段中，输入可以发送的最大EAP请求数。如果在定义的时间段（请求方超时）后未收到响应，则身份验证进程将重新启动。

⚙️ Reauthentication Period:	<input type="text" value="3600"/>
Reauthenticate Now:	<input checked="" type="checkbox"/>
Authenticator State:	N/A
⚙️ Max Hosts:	<input type="text" value="256"/>
⚙️ Quiet Period:	<input type="text" value="60"/>
⚙️ Resending EAP:	<input type="text" value="30"/>
⚙️ Max EAP Requests:	<input type="text" value="2"/>

注：在本示例中，使用默认值2。

步骤 14在Supplicant客户端超时字段中，输入将EAP请求重新发送到请求方之前经过的秒数。

Max Hosts:	<input type="text" value="256"/>
Quiet Period:	<input type="text" value="60"/>
Resending EAP:	<input type="text" value="30"/>
Max EAP Requests:	<input type="text" value="2"/>
Supplicant Timeout:	<input type="text" value="30"/>

注：在本示例中，使用默认值30。

步骤 15在Server Timeout字段中，输入交换机将请求重新发送到身份验证服务器之前经过的秒数。

Max Hosts:	<input type="text" value="256"/>
Quiet Period:	<input type="text" value="60"/>
Resending EAP:	<input type="text" value="30"/>
Max EAP Requests:	<input type="text" value="2"/>
Supplicant Timeout:	<input type="text" value="30"/>
Server Timeout:	<input type="text" value="30"/>

注：在本示例中，使用默认值30。

步骤 16单击 Apply。

现在，您应该已经成功地在交换机上配置了端口身份验证。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。