在思科企业220系列交换机上配置802.1x身份验证

目标

本文旨在向您展示如何在Cisco Business 220系列智能交换机上配置802.1x身份验证。

适用设备 |固件版本

- CBS220系列（产品手册） |2.0.0.17

简介

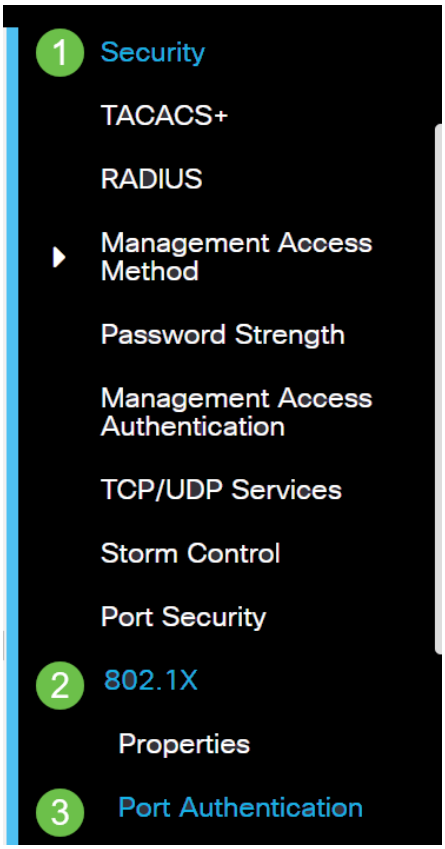
端口身份验证启用每个端口的参数配置。由于某些配置更改仅在端口处于强制授权状态（例如主机身份验证）时才可能发生，因此建议在进行更改之前将端口控制更改为强制授权。配置完成后，将端口控制恢复到其先前状态。

定义了802.1x的端口不能成为LAG的成员。802.1x和端口安全不能同时在同一端口上启用。如果在接口上启用端口安全，则管理端口控制不能更改为自动模式。

配置端口身份验证

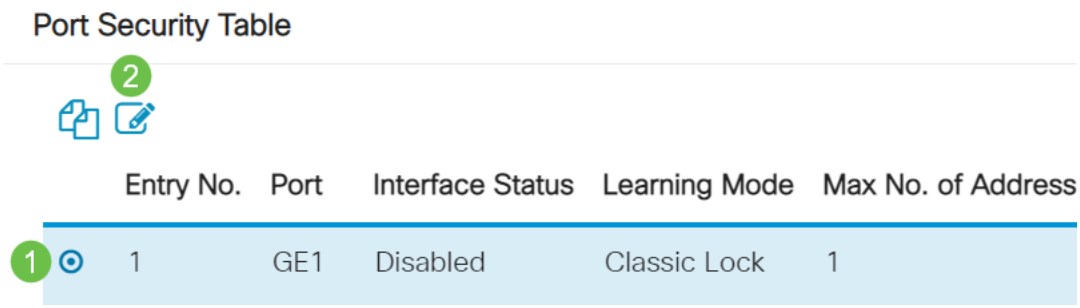
第 1 步

登录到交换机Web用户界面(UI)，然后选择**Security > 802.1x > Port Authentication**。



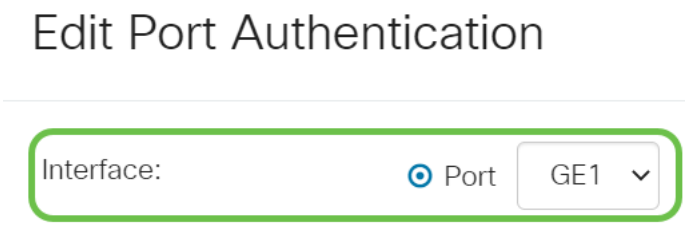
步骤 2

单击要配置的端口的单选按钮，然后单击编辑**图标**。



步骤 3

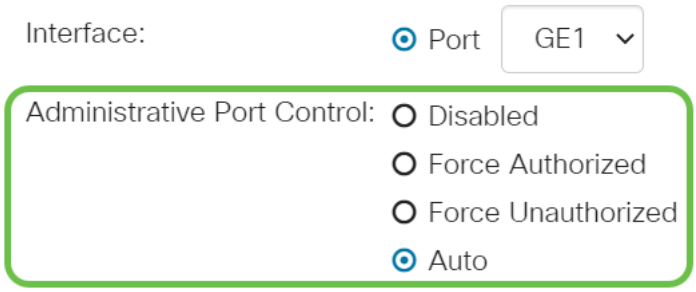
然后会*弹出*"编辑端口身份验证"窗口。从接口下拉列表中，确保指定的端口是您在步骤2中选择的端口。否则，单击下拉箭头并选择正确的端口。



步骤 4

为管理端口控制选择单选按钮。这将确定端口授权状态。选项有：

- **禁用** — 禁用802.1x。这是默认状态。
- **强制未授权**(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。接口根据交换机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**(Force Authorized) — 授权接口而不进行身份验证。

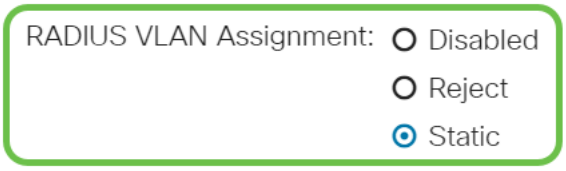


步骤 5（可选）

为RADIUS VLAN分配选择单选按钮。这将在指定端口上启用动态VLAN分配。选项有：

- **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。

如果有来自RADIUS的VLAN授权信息，但VLAN未在测试设备(DUT)上管理性创建，则VLAN将自动创建。



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

- [64]隧道类型= VLAN（类型13）
- [65]隧道中型= 802（类型6）
- [81]隧道专用组ID = VLAN ID

步骤 6（可选）

选中Guest VLAN的**Enable**复选框，以对未授权端口使用访客VLAN。

步骤 7

选中Periodic Reauthentication的**Enable**复选框。这将在指定的重新身份验证时间段后启用端口重新身份验证尝试。

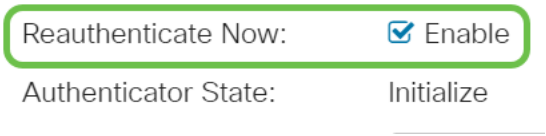
步骤 8

在重新验证期间字*段中输*入值。这是重新验证端口的时间（以秒为单位）。

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。

身份验证器状态字段显示身份验证的当前状态。



如果端口未处于“强制授权”或“强制未授权”状态，则它处于“自动”模式，验证器显示正在进行的身份验证状态。端口经过身份验证后，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经过身份验证的主机的最大数量。此值仅在多会话模式下生效。

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静默状态的秒数。当交换机处于静默状

态时，这意味着交换机不侦听来自客户端的新身份验证请求。

步骤 12

在*Resending 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)请求或身份帧响应的秒数。

步骤 13

在*Max EAP Requests*字段中，输入可发送的EAP请求的最大数量。如果在定义的时间段（请求方超时）后未收到响应，则重新启动身份验证过程。

步骤 14

在*Supplicant Timeout*字段中，输入在EAP请求重新发送到Supplicant客户端之前过期的秒数。

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。

步骤 16

单击 Apply。

现在，您应该已在交换机上成功配置802.1x身份验证。

有关详细配置，请参阅《Cisco Business 220系列交换机管理指南》。

如果您想查看其他文章，请查看Cisco Business 220系列交换机支持页