200/220/300系列交换机上的802.1X主机和会话身份验证配置

目标

802.1X是基于端口的网络访问控制(PNAC)的IEEE标准，为连接到端口的设备提供身份验证方法。交换机的管理GUI中的“主机和会话身份验证”(Host and Session Authentication)页面用于定义每个端口使用的身份验证类型。每个端口身份验证是一项功能，允许网络管理员根据所需的身份验证类型划分交换机端口。Authenticated Hosts页面显示有关已进行身份验证的主机的信息。

本文解释如何按端口配置主机和会话身份验证，以及如何在200/220/300系列管理型交换机的802.1X安全设置中查看经过身份验证的主机。

适用设备

- Sx200系列
- Sx220系列
- Sx300系列

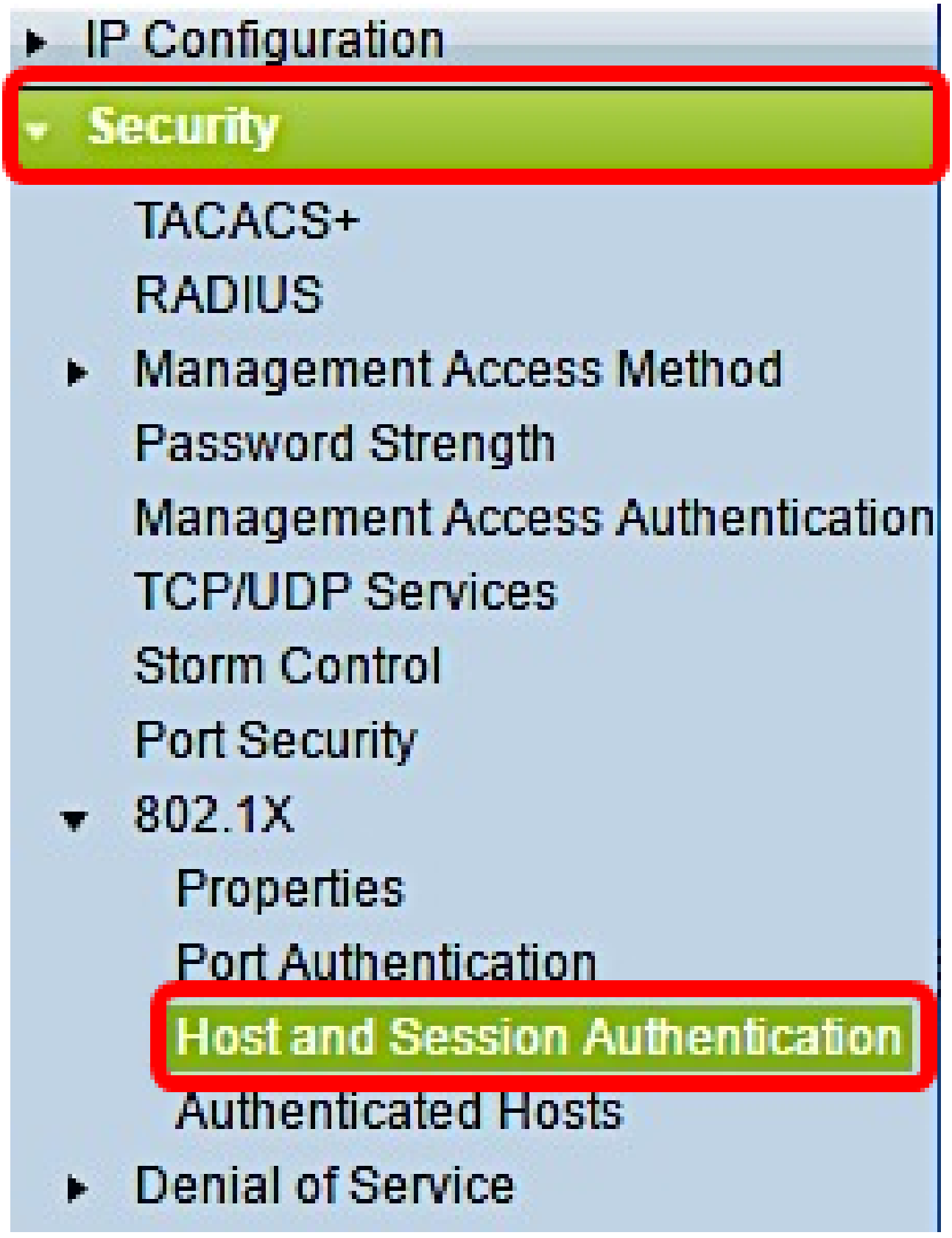
软件版本

- 1.4.5.02 — Sx200系列、Sx300系列
- 1.1.0.14 — Sx220系列

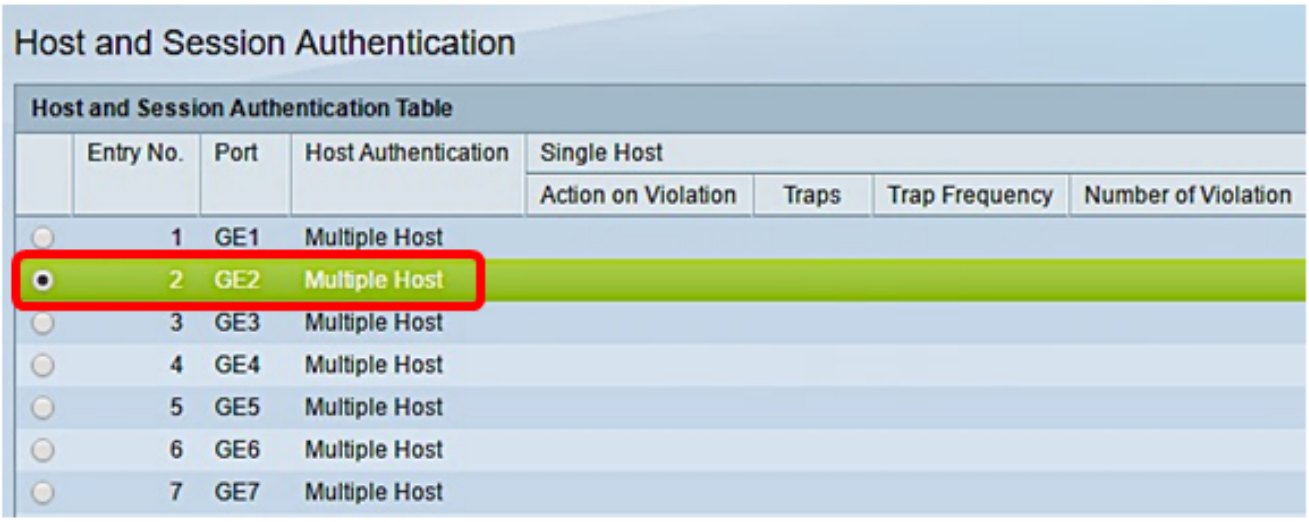
主机和会话身份验证

步骤1:登录基于Web的实用程序，然后选择Security > 802.1X > Host and Session Authentication。

注意：以下图像来自SG220-26P智能交换机。

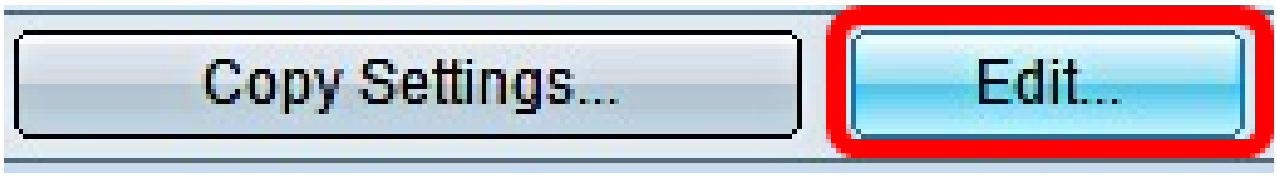


第二步：点击要编辑的端口的单选按钮。

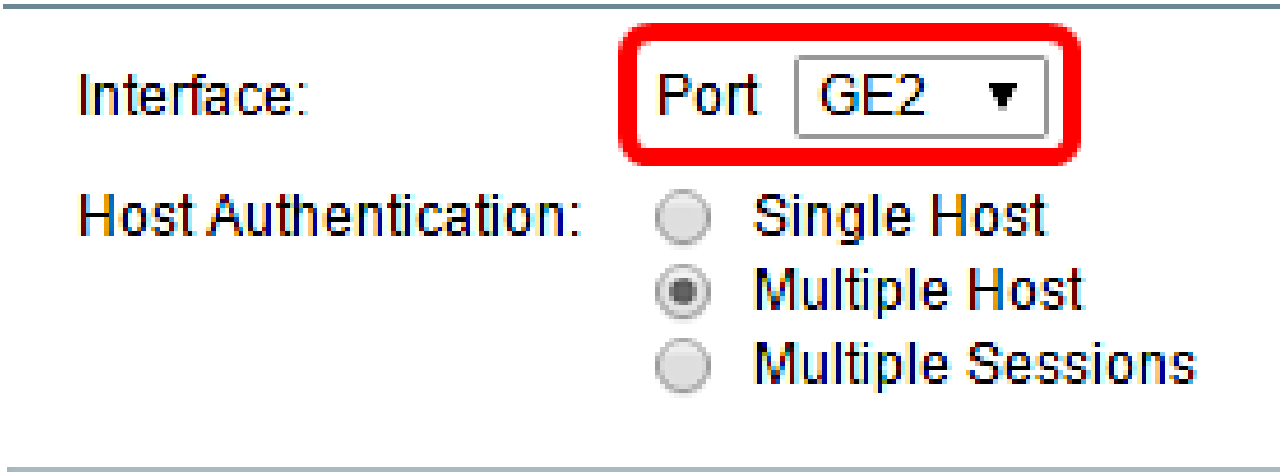


注意：在本示例中，选择了端口GE2。

第三步：单击Edit以编辑指定端口的主机和会话身份验证。



第四步：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。

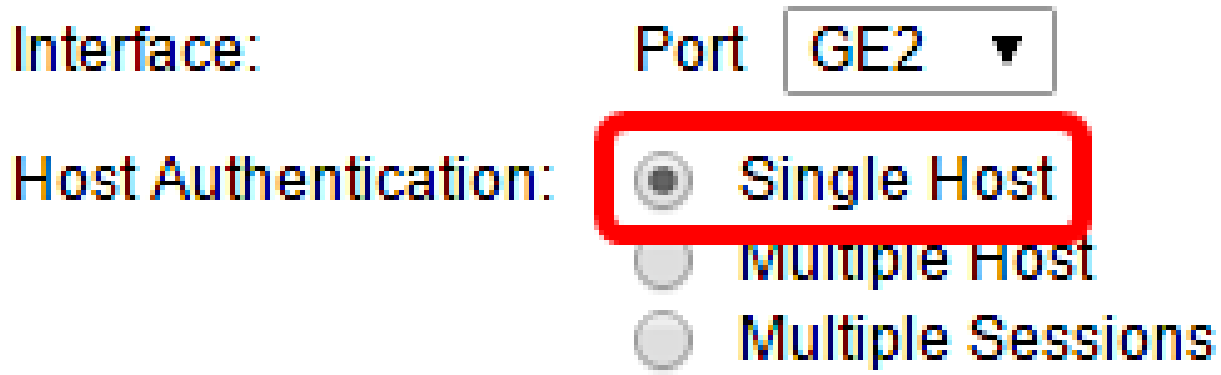


注：如果使用200或300系列，则会出现“编辑主机和会话身份验证”窗口。

第五步：点击与Host Authentication字段中所需的身份验证模式对应的单选按钮。选项有：

- 单个主机 — 交换机仅授予单个授权主机对该端口的访问权限。
- 多主机(802.1X) — 多个主机可以访问单个端口。这是默认模式。交换机只需要授权第一台主机，然后连接到该端口的所有其他客户端都可以访问网络。如果身份验证失败，第一台主机和所有连接的客户端都被拒绝访问网络。
- 多个会话 — 多个主机可以访问单个端口，但每台主机都必须通过身份验证。

注意：在本例中，选择单个主机。

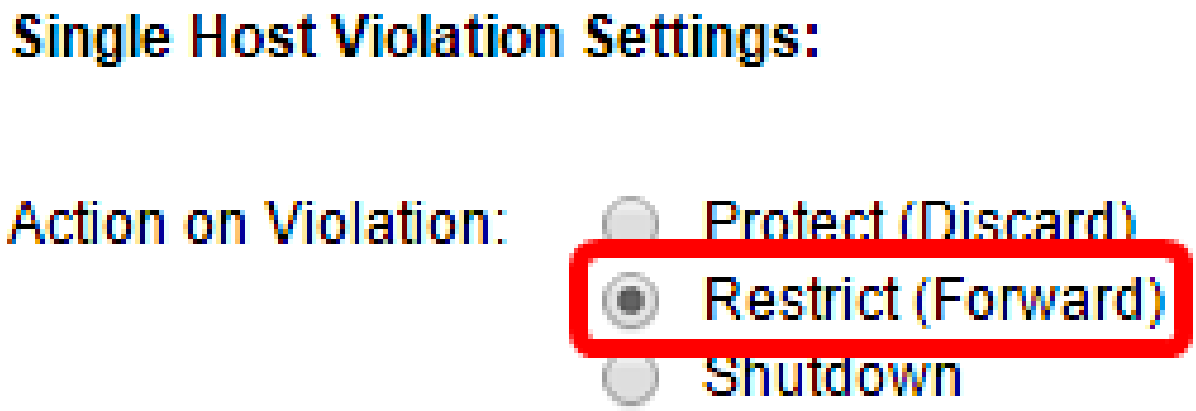


注意：如果选择多个主机或多个会话，请跳至步骤9。

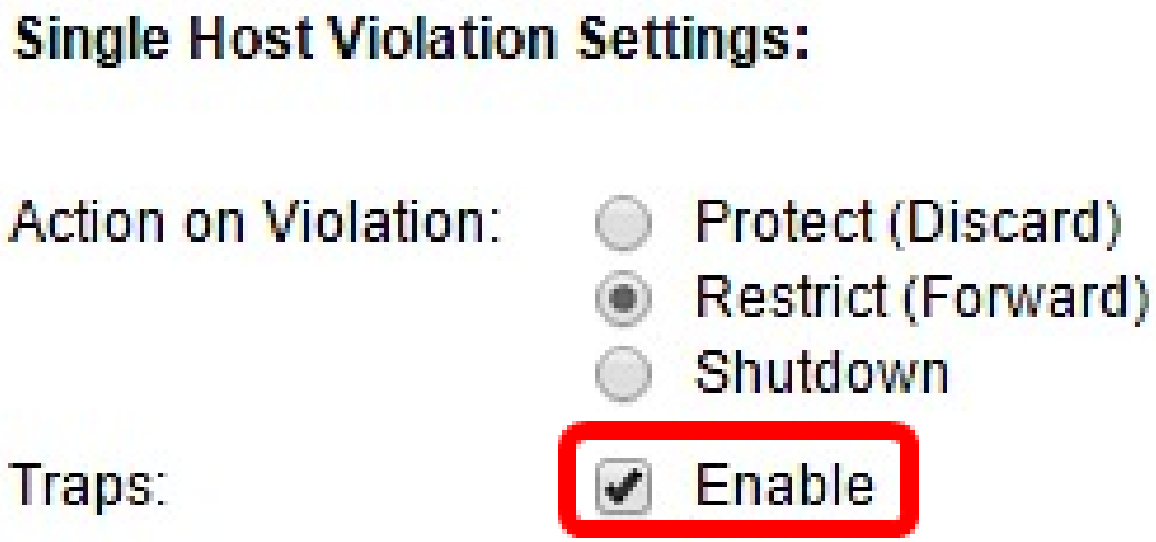
第六步：在Single Host Violation Settings区域中，点击与所需Action on Violation对应的单选按钮。如果数据包来自的MAC地址与原始请求方的MAC地址不匹配的主机，则会发生违规。发生这种情况时，该操作将决定从不属于原始请求方的主机到达的数据包会发生什么情况。选项有：

- 保护（丢弃）— 丢弃数据包。这是默认操作。
- Restrict（转发）— 提供访问并转发数据包。
- Shutdown — 阻止数据包并关闭端口。在重新激活或交换机重新启动之前，端口会保持关闭状态。

注：在本示例中，选择Restrict(Forward)。



步骤7.（可选）选中Traps字段中的Enable以启用陷阱。陷阱是生成的简单网络管理协议(SNMP)消息，用于报告系统事件。当发生违规时，陷阱会发送到交换机的SNMP管理器。



步骤 8在Trap Frequency字段中输入已发送陷阱之间允许的所需时间（以秒为单位）。这定义了陷阱的发送频率。

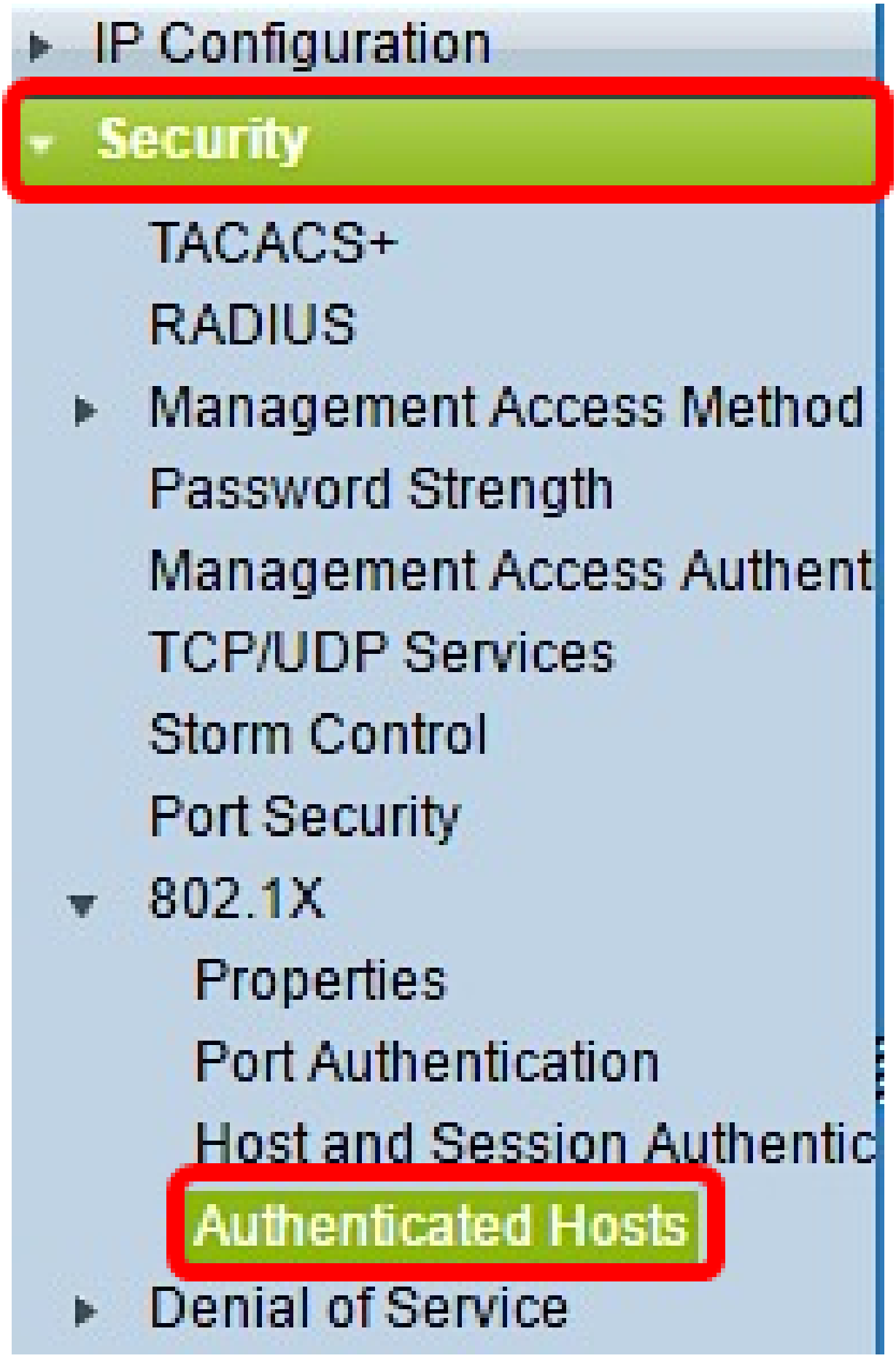
注：在本示例中，使用30秒。

步骤 9单击 Apply。

您现在应该在交换机上配置主机和会话身份验证。

查看经过身份验证的主机

步骤1:登录到基于Web的实用程序，然后选择Security > 802.1X > Authenticated Host。


IP Configuration
Security
TACACS+
RADIUS
Management Access Method
Password Strength
Management Access Authent
TCP/UDP Services
Storm Control
Port Security
802.1X
Properties
Port Authentication
Host and Session Authentic
Authenticated Hosts
Denial of Service

“已验证主机”(Authenticated Hosts)表显示已验证主机的以下信息。

- User Name — 指定在端口上经过身份验证的请求方名称。
- Port — 指定请求方连接的端口号。
- 会话时间 — 指定请求方连接到端口的完整时间。格式为 DD:HH:MM:SS(Day:Hour:Minute:Second)。
- Authentication Method — 指定用于进行身份验证的方法。可能的值为：
- None — 指定请求方未进行身份验证。
- Radius — 指定请求方已由RADIUS服务器进行身份验证。
- MAC地址 — 指定请求方的MAC地址。
- VLAN ID — 指定主机所属的VLAN。VLAN ID列仅在220系列增强型智能交换机中可用。

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）。