在SG300系列交换机上配置802.1X

目标

802.1X是实施基于端口的身份验证的IEEE标准。如果端口使用802.1X，则使用该端口的任何客户端（称为请求方）必须提供正确的凭证，才能授予对网络的访问权限。实施802.1X的设备（称为验证器）必须能够与网络中其他位置的RADIUS（远程身份验证拨入用户服务）服务器通信。此服务器包含允许访问网络的有效用户列表；身份验证器发送的任何凭证（请求方向其提供）必须与RADIUS服务器保留的凭证匹配。如果是，服务器会通知身份验证器授予用户访问权限；否则，验证器将拒绝访问。

802.1X标准是防止不需要的用户通过插入物理端口访问网络的良好安全措施。请注意，要使802.1X正常工作，必须在网络的其他位置配置RADIUS服务器，并且身份验证器必须能够与其通信。

本文档的目标是向您展示如何在SG300系列交换机上设置802.1X。

适用设备

·SG300系列交换机

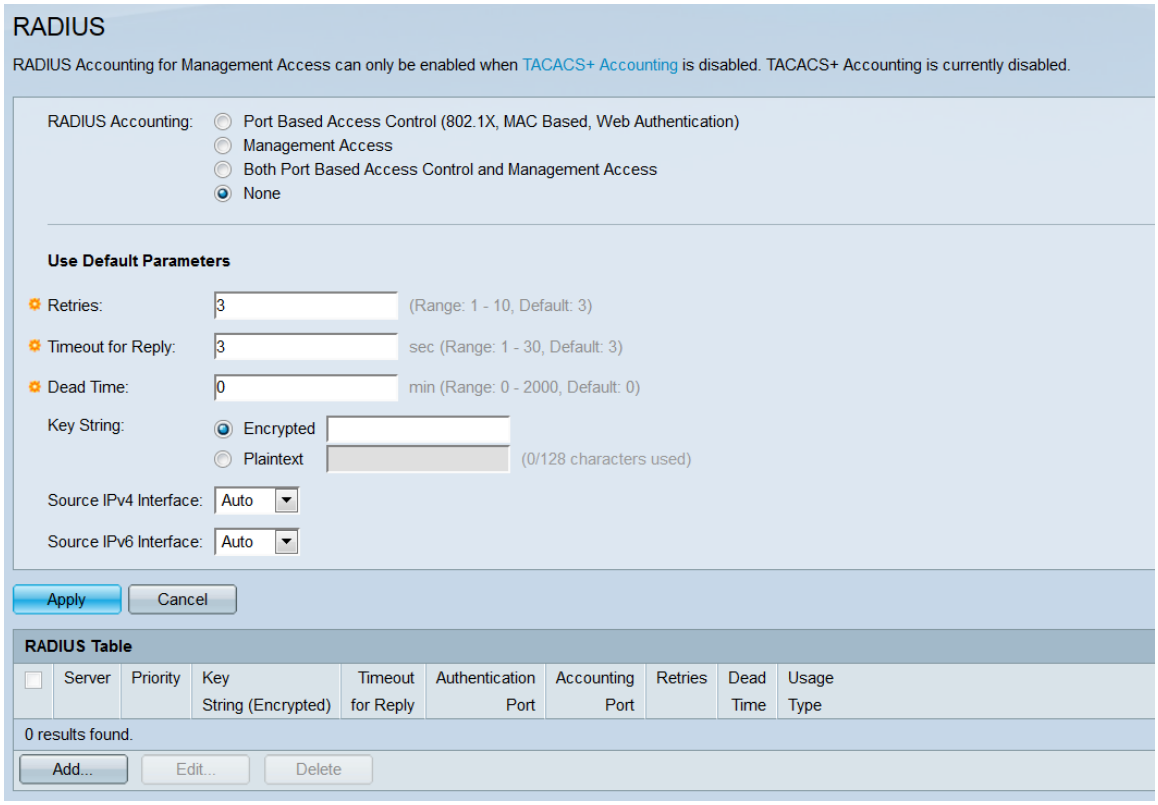
软件版本

•v1.4.1.3

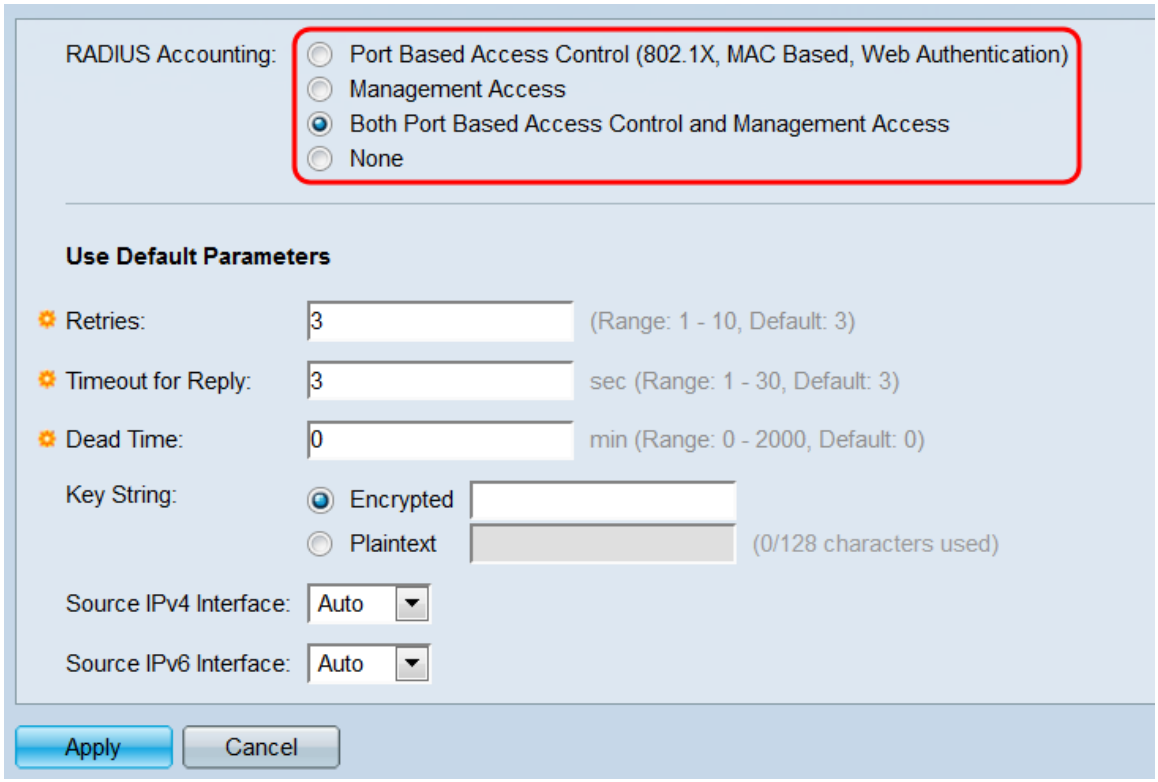
设置802.1X身份验证

添加RADIUS服务器

步骤1.登录Web配置实用程序，然后选择**Security > RADIUS**。将打*开RADIUS*页面。



步骤2.在RADIUS记*帐字段*中，选择单选按钮以选择RADIUS服务器将提供的记帐信息的类型。RADIUS服务器可以获得记帐信息，用于跟踪用户的会话时间、他们使用的资源以及其他事项。此处选择的选项不会影响802.1X的性能。



选项有：

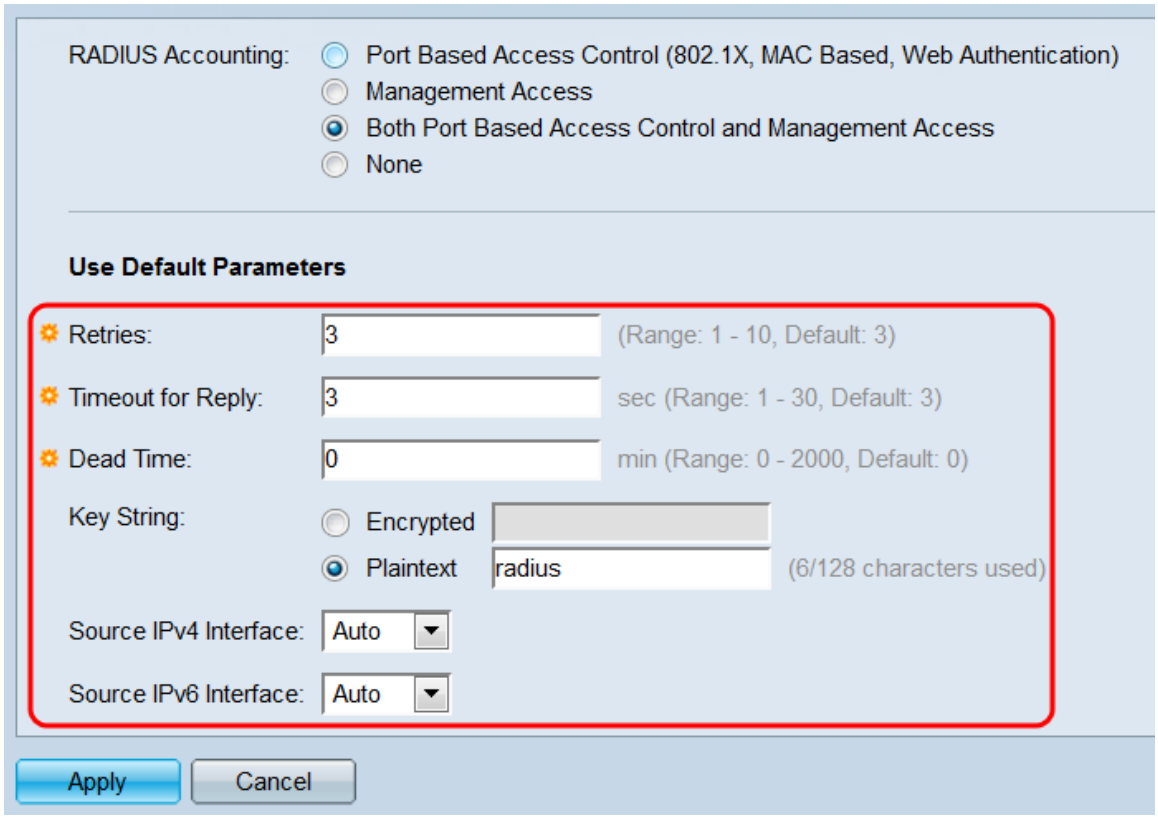
·基于端口的访问控制 — 此选项将有关基于端口的已验证会话的记帐信息发送到RADIUS服务器。

·管理访问 — 此选项将有关交换机管理会话的记帐信息发送到RADIUS服务器。

·基于端口的访问控制和管理访问 — 此选项将两种类型的记帐信息发送到RADIUS服务器。

·无 — 不向RADIUS服务器发送记帐信息。

步骤3.在“使用*默认参数*”区域中，配置默认使用的设置，除非已添加的RADIUS服务器配置了自己的特定设置；添加到交换机的每个单独服务器条目都可以使用默认设置或单独的唯一设置。对于本文，我们将使用本节中定义的默认设置。



配置以下设置：

·重试 — 输入交换机在转到下一台服务器之前尝试联系RADIUS服务器的次数。默认值为 3。

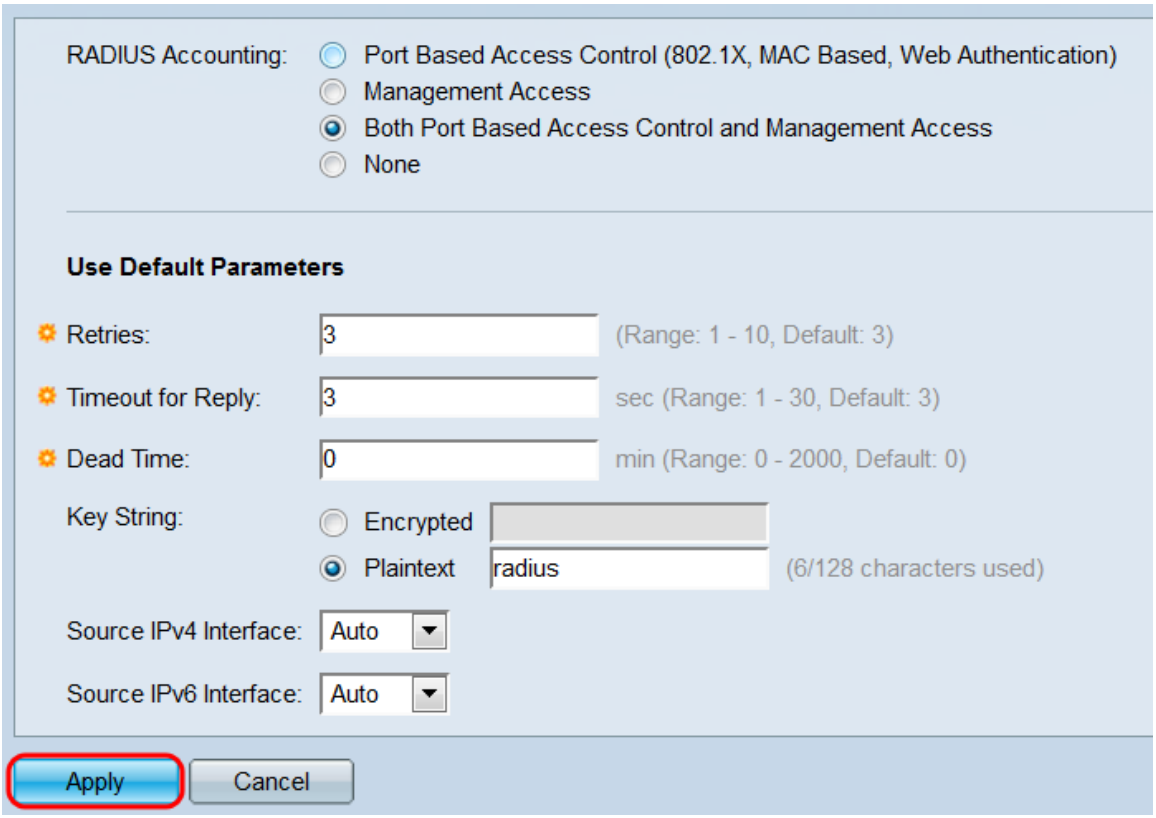
·回复超时 — 输入交换机在执行进一步操作（重试或放弃）之前等待RADIUS服务器回复的秒数。 默认值为 3。

·Dead Time — 输入在服务请求传递无响应RADIUS服务器之前经过的分钟数。默认值为 0;此值表示不会绕过服务器。

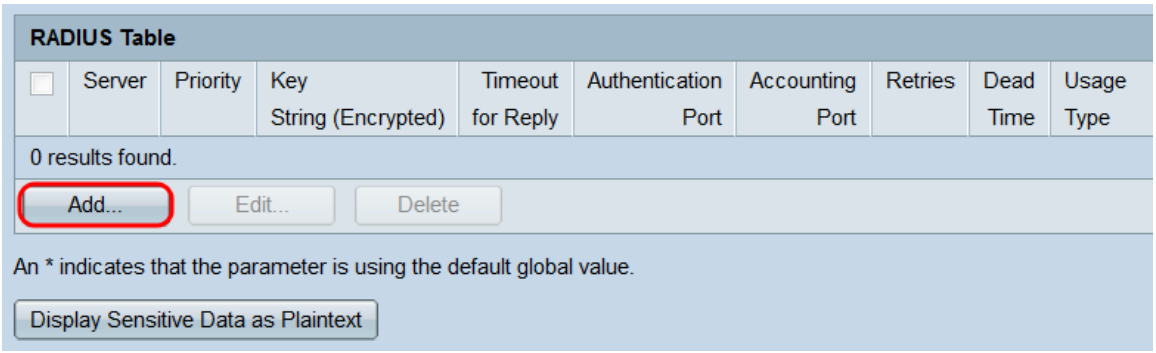
·密钥字符串 — 输入用于在交换机和RADIUS服务器之间进行身份验证的密钥。如果您有加密密钥，请使用“加密”单选按钮**输入**该密钥；否则，请使用“明文”单选按钮**输入明**文密钥。

·源IPv4/IPv6接口 — 使用这些下拉列表选择在与RADIUS服务器通信时将使用哪个IPv4/IPv6源接口。默认值为Auto，它将使用在传出接口上定义的默认源IP地址。

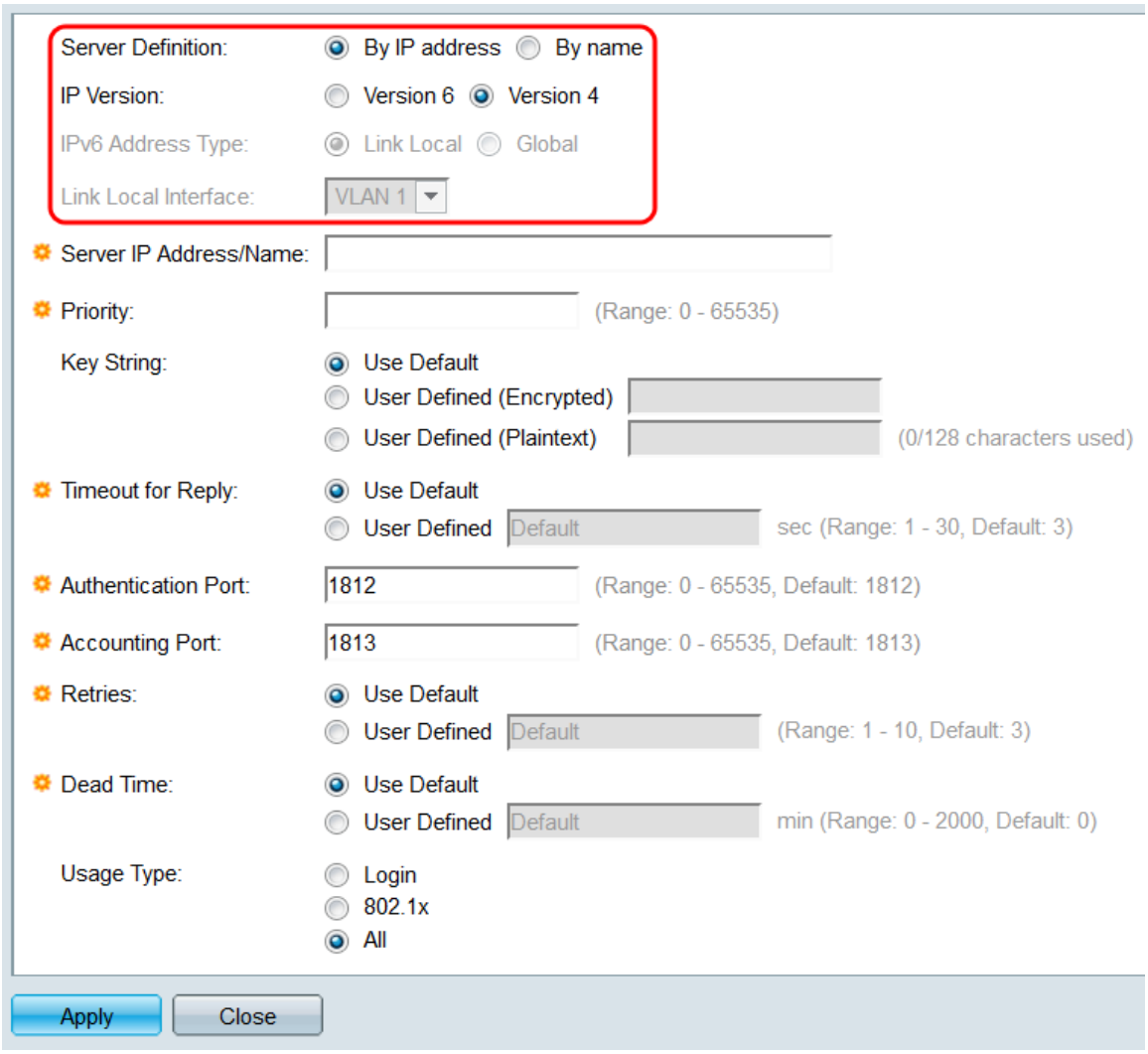
步骤4.单击“**应用**”。将应用默认设置。



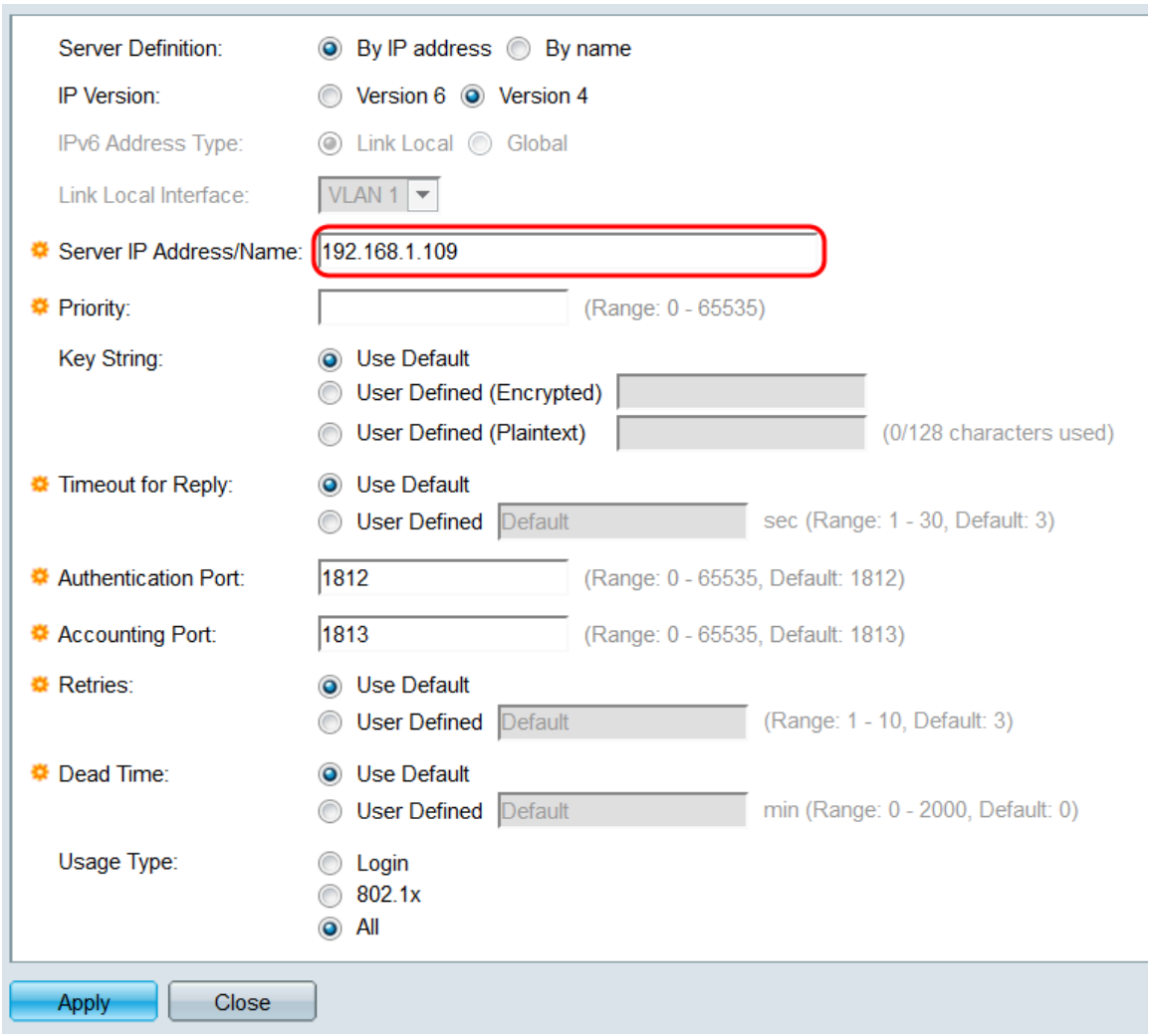
步骤5. RADIUS表*将显示*交换机上当前配置的RADIUS服务器条目。要添加新条目，请单击**Add...按**钮。将会*打开"添加*RADIUS服务器"窗口。



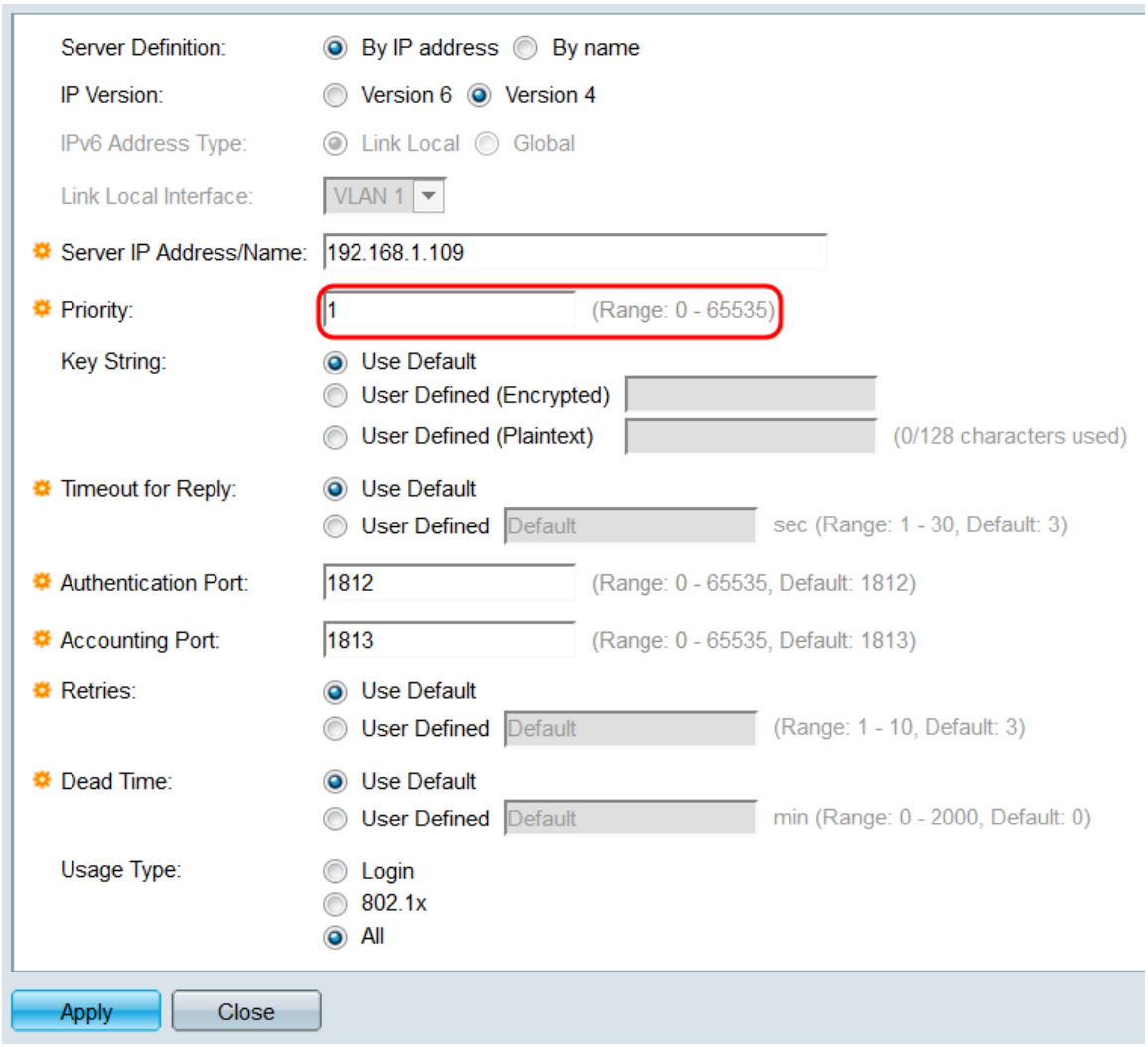
步骤6.在"*服务器定义*"字段中，选择是按IP地址**联系RADIUS服务器**还是**按名称**（主机名）。如果选择**按IP地址**，请选择使用IPv6(**版本6**)或IPv4(版**本4**)。 如果选择**版本6**，请使用*IPv6地址类型*和*链路本地接口*指定将要使用的IPv6地址。



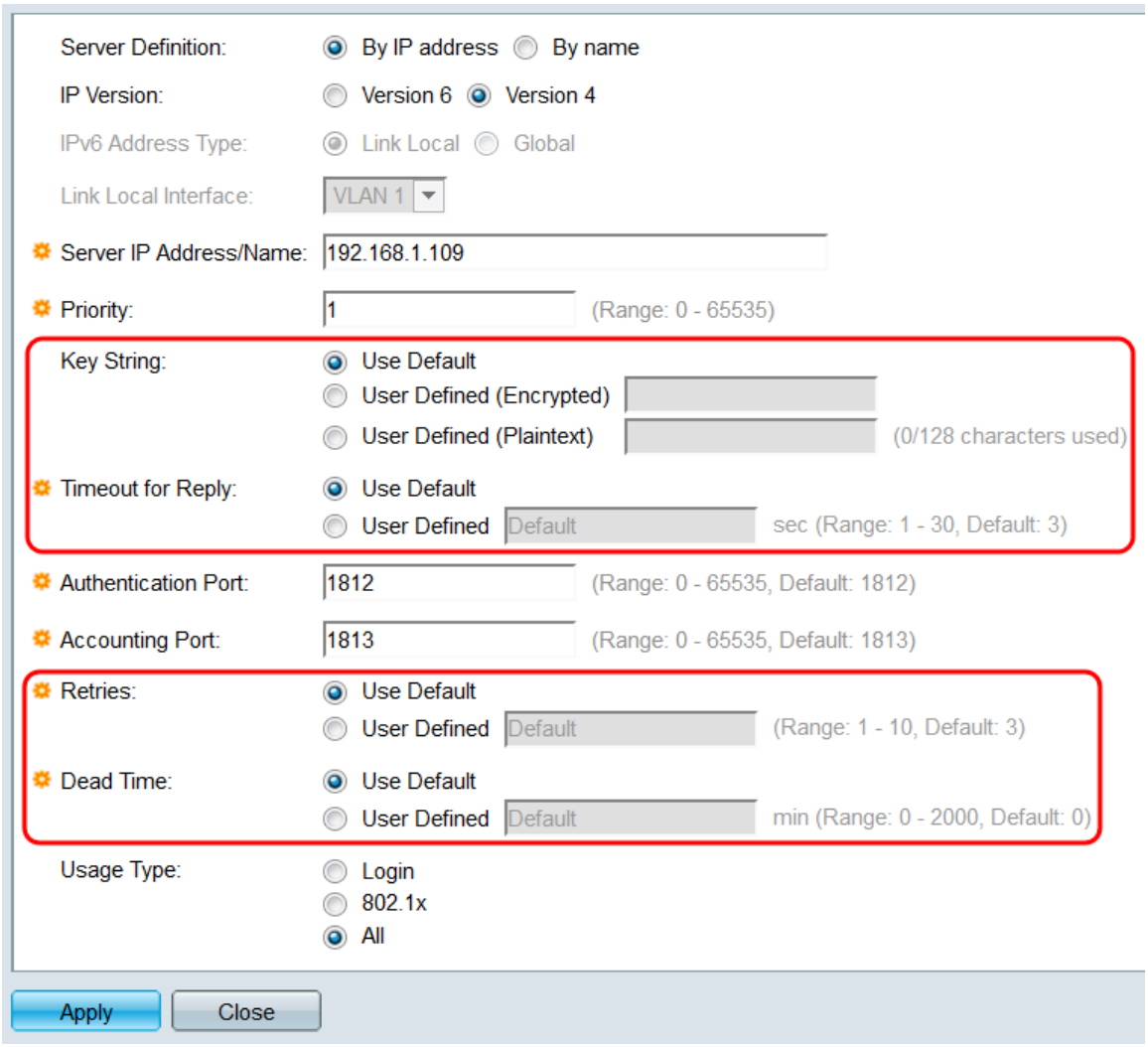
步骤7.在Server *IP Address/Name*字段中，输入RADIUS服务器的IP地址或主机名。



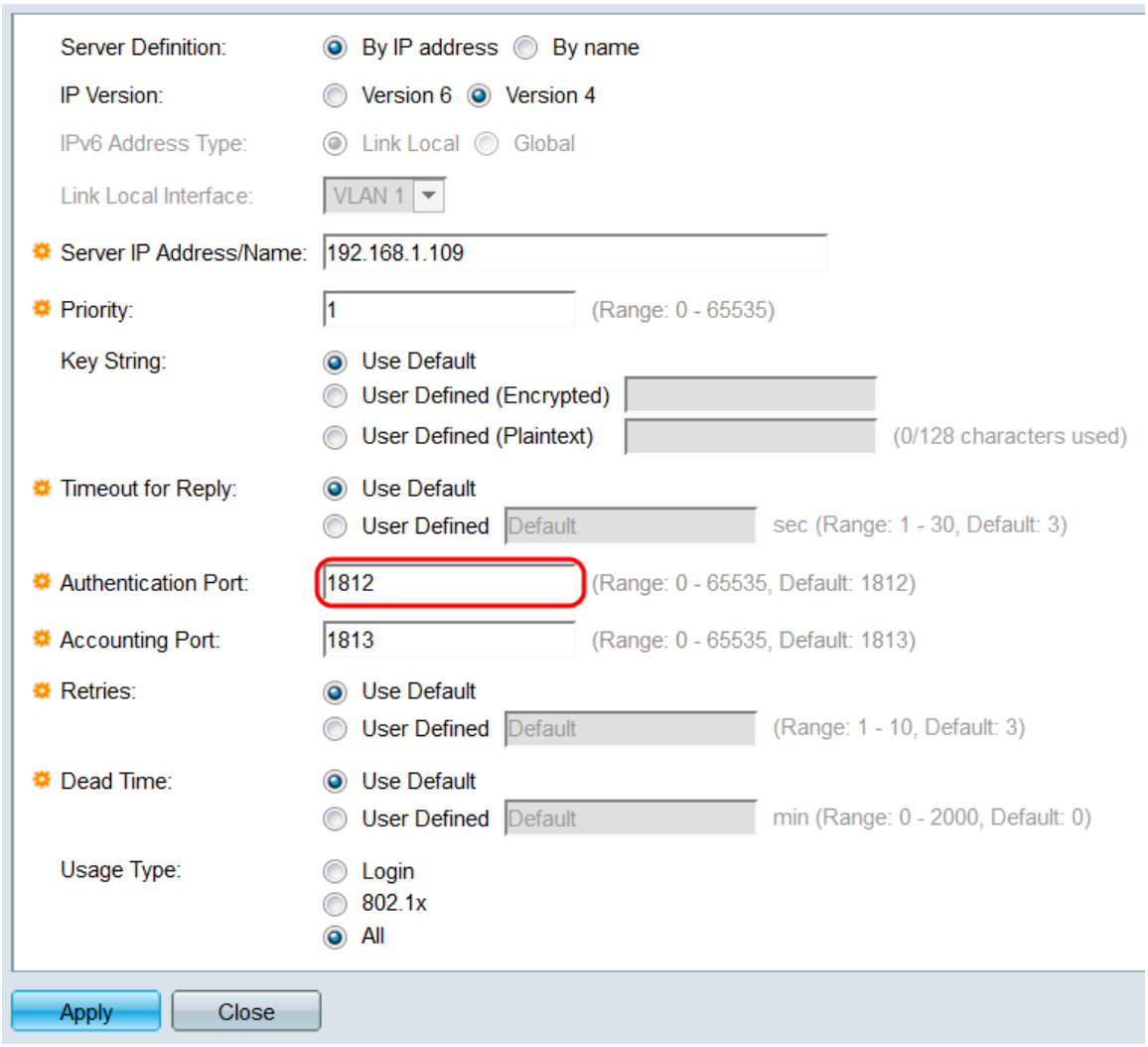
步骤8.在“优先级”*字段*中，输入要分配给此服务器的优先级；交换机将尝试与优先级最高的服务器联系，并继续沿列表向下，直到遇到响应式服务器。范围是0 - 65535，其中0是最高优先级。



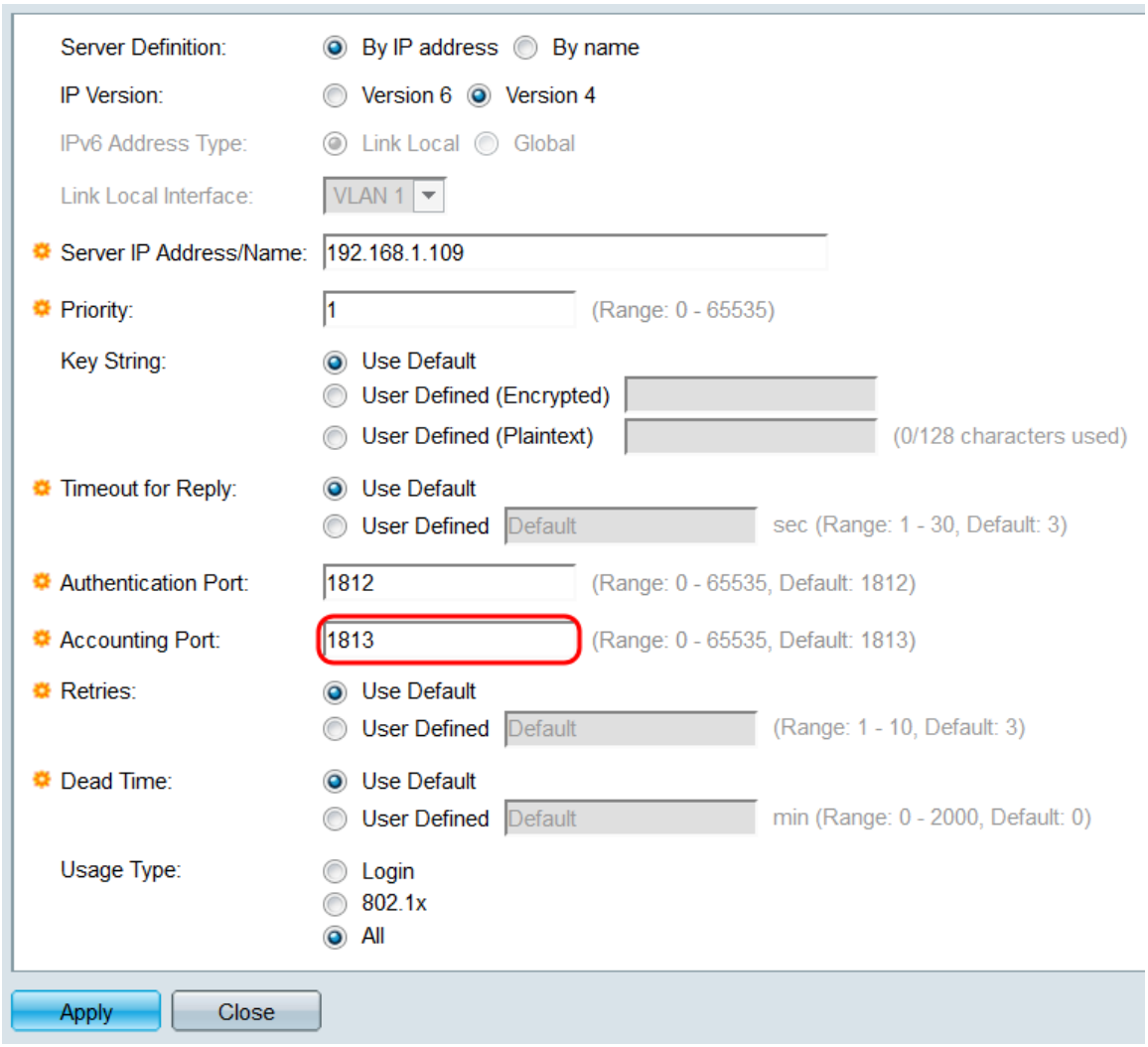
步骤9.在Key String、Timeout for Reply、*Retries* 和Dead Time 字段中选择Use Default单选按钮，以使用RADIUS页中先前配置的设置。您还可以选择“用户**定义**”单选按钮以配置与默认设置不同的设置；如果执行此操作，这些设置将仅用于此特定RADIUS服务器。



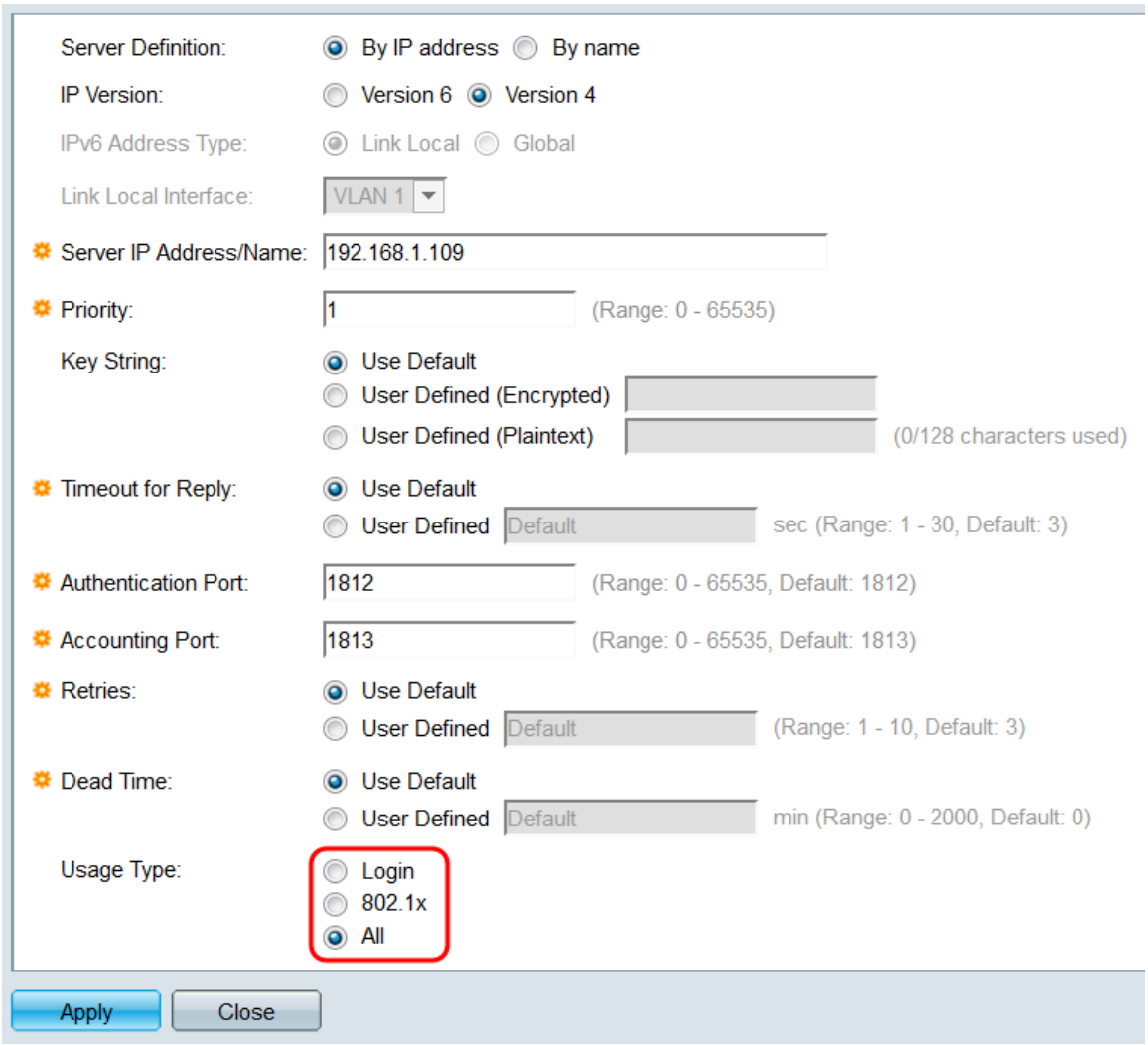
步骤10.在*Authentication Port*字段中，指定将用于与RADIUS服务器进行身份验证通信的端口。建议将其保留在默认端口1812上。



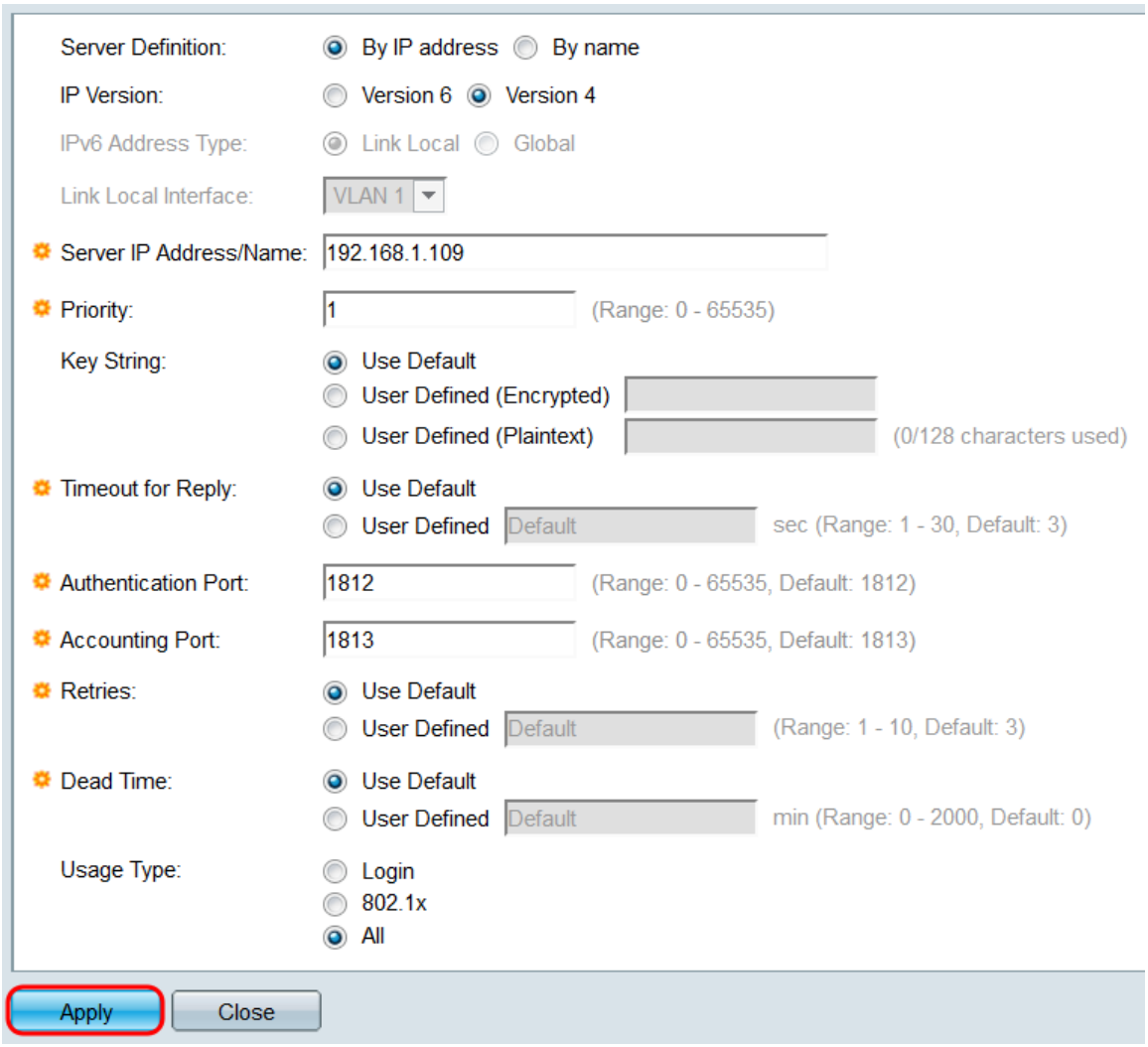
步骤11.在*Accounting Port*字段中，指定将用于与RADIUS服务器进行记帐通信的端口。建议将其保留在默认端口1813上。



步骤12.在“使用类*型*”字段中，选择RADIUS服务器将用于什么。配置802.1X时，选择**802.1x**或**All**单选按钮以使用RADIUS服务器进行802.1X端口身份验证。

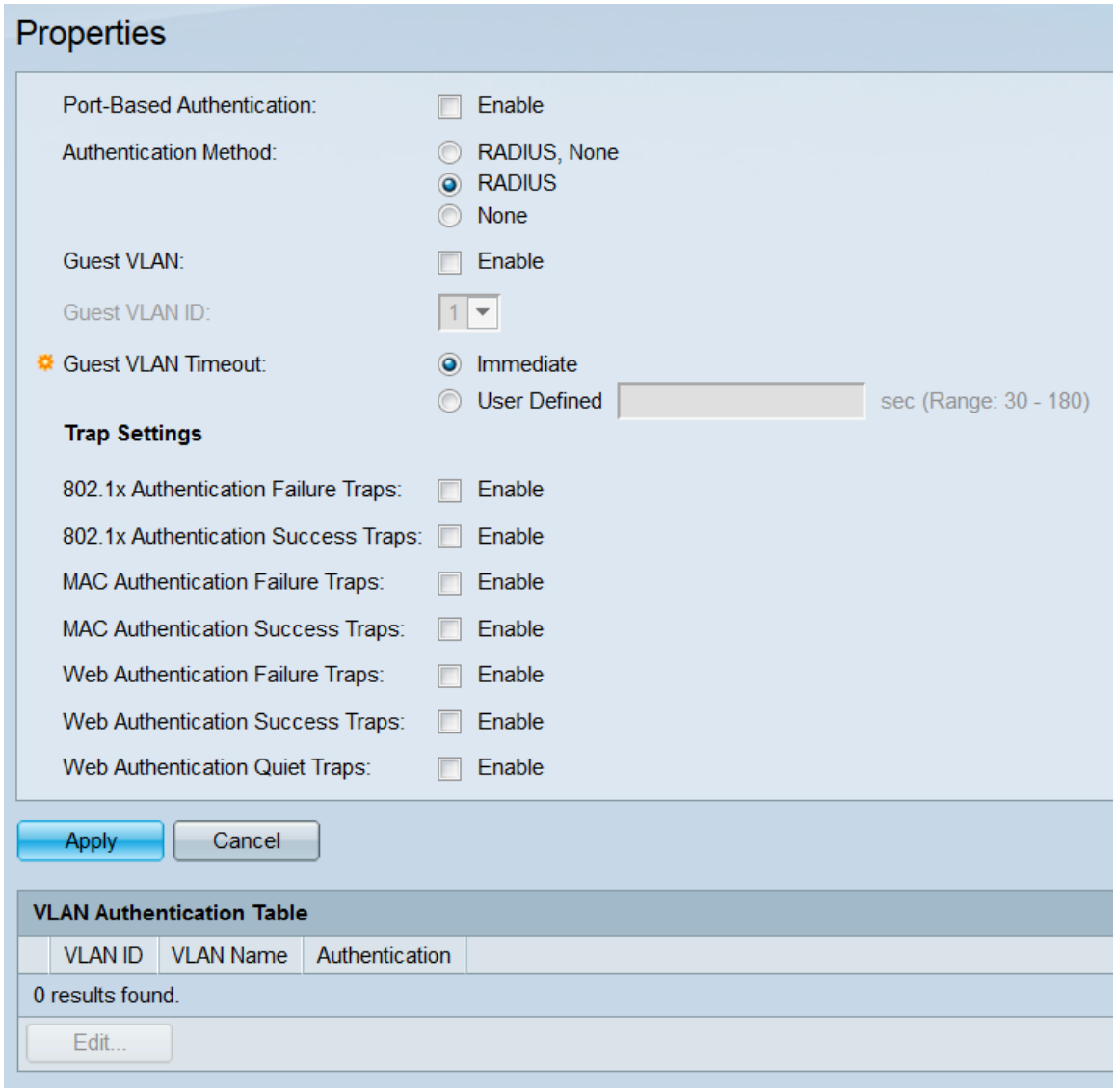


步骤13.单击“**应用**”。服务器将添加到*RADIUS*表。要启用基于端口的802.1X身份验证，请继续下一节。

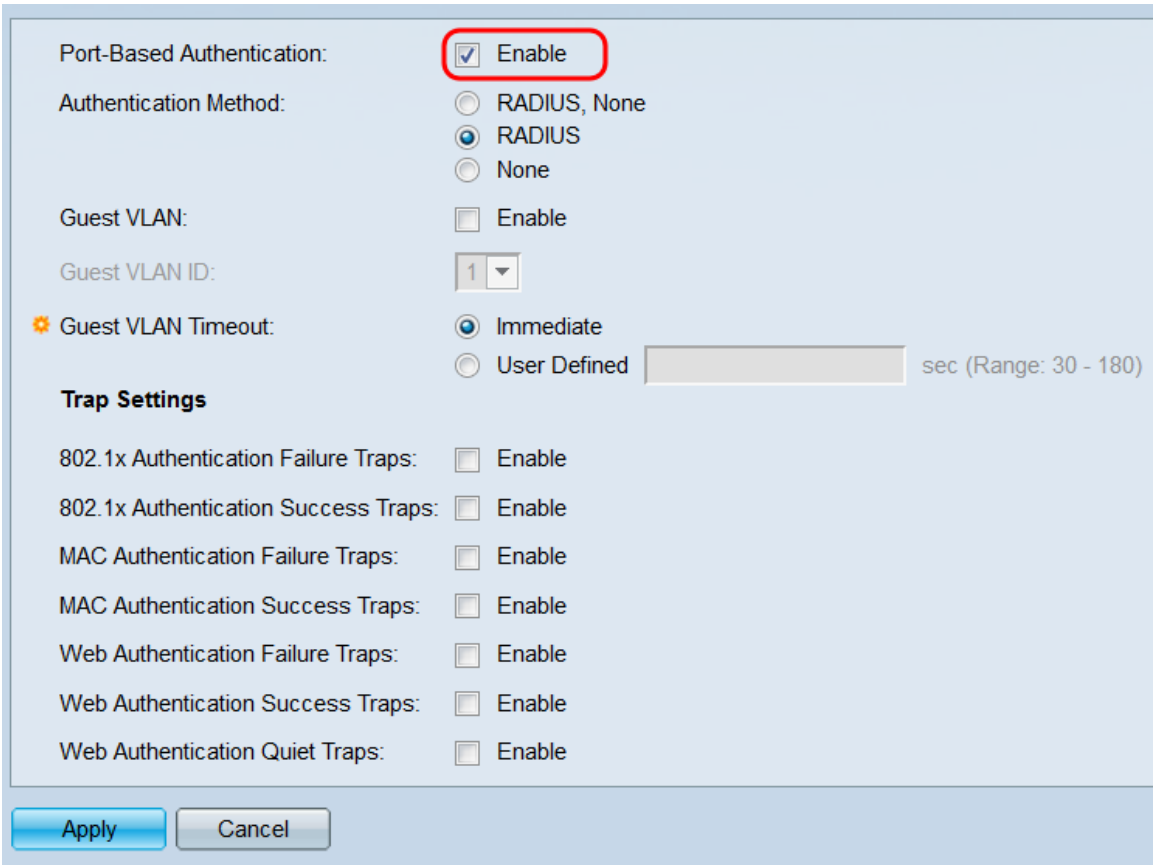


启用基于端口的身份验证

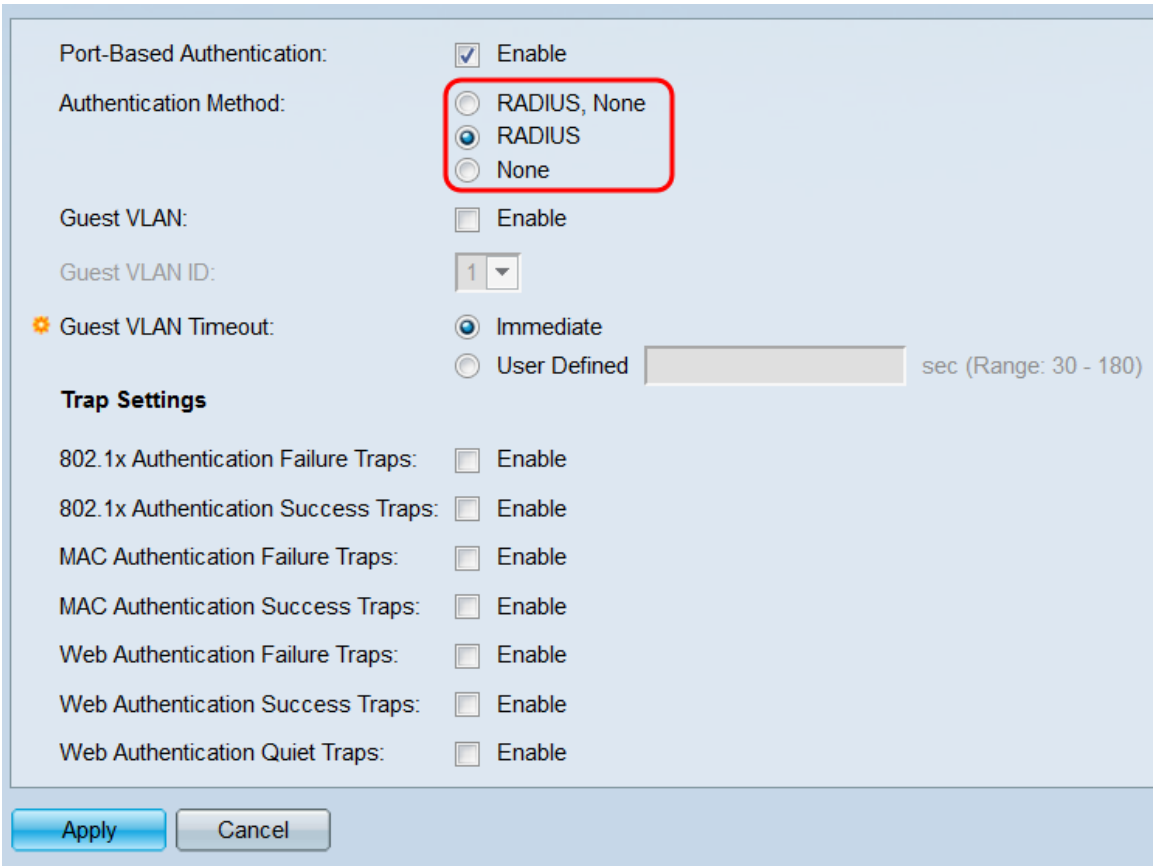
步骤1.在Web配置实用程序中，转到**Security > 802.1X/MAC/Web Authentication > Properties**。将打开“属性”页。



步骤2.在Port-*Based Authentication字段*中，选中**Enable** 复选框以启用基于端口的身份验证。默认情况下启用该接口。



步骤3.在Authentication Method字*段中*，选择单选按钮以确定基于端口的身份验证的工作方式。



选项有：

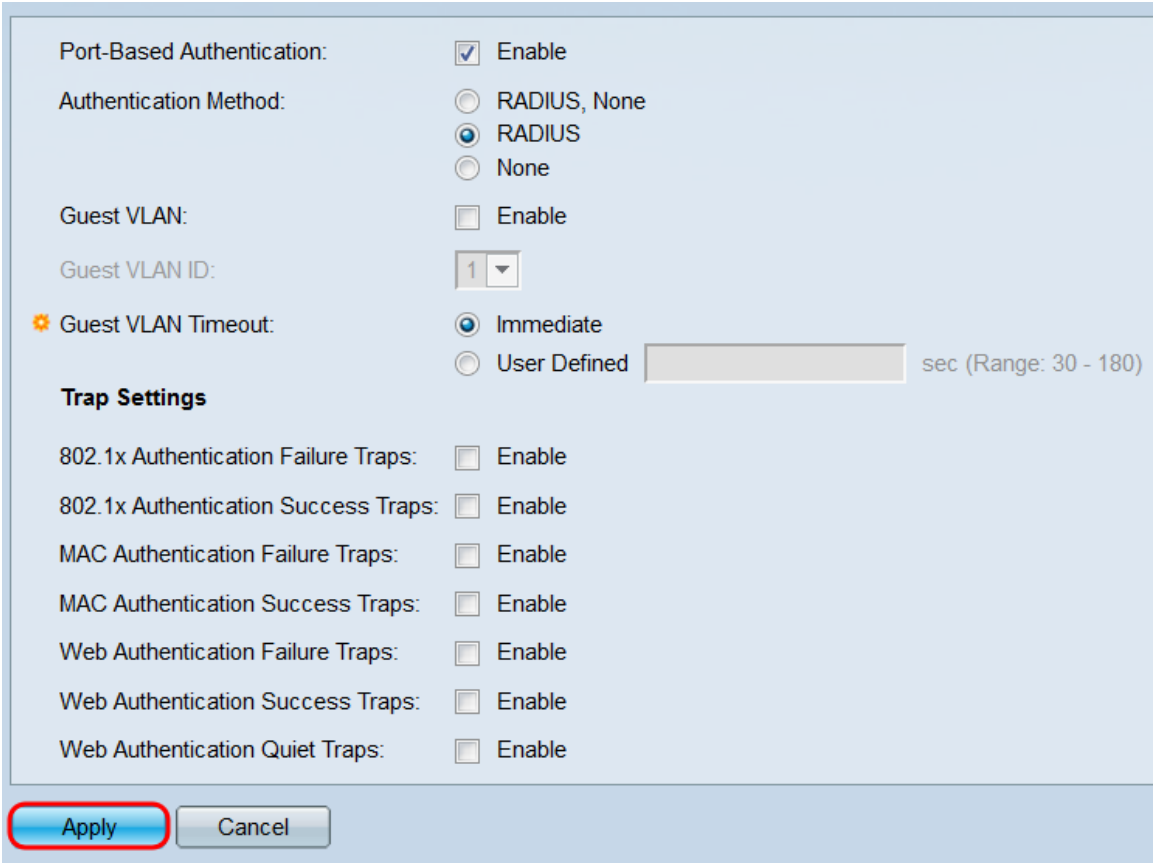
·RADIUS， None — 交换机将尝试联系在RADIUS页面上定义的RADIUS服务*器*。如果没有从服务器收到响应，则不执行身份验证，并允许会话。如果服务器响应，且凭证不正确，则会拒

绝会话。

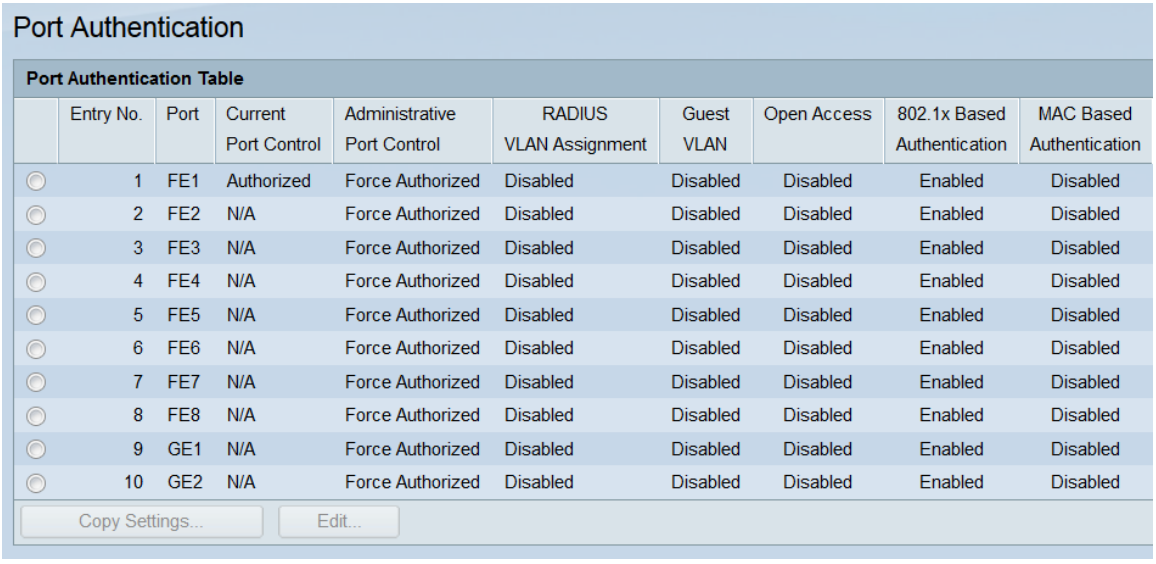
·RADIUS — 交换机将尝试联系在RADIUS页面上定义的*RADIUS服*务器。如果未从服务器收到响应，则会拒绝会话。对于最安全的802.1X实施，建议使用此选项。

·无 — 不执行身份验证。将允许所有会话。此选项不实施802.1X。

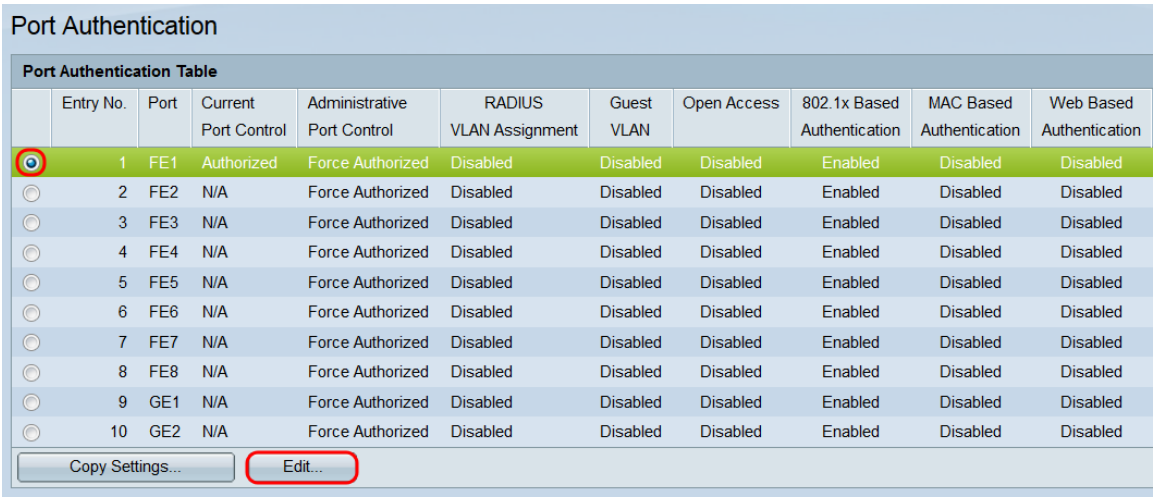
步骤4.单击“**应用**”。



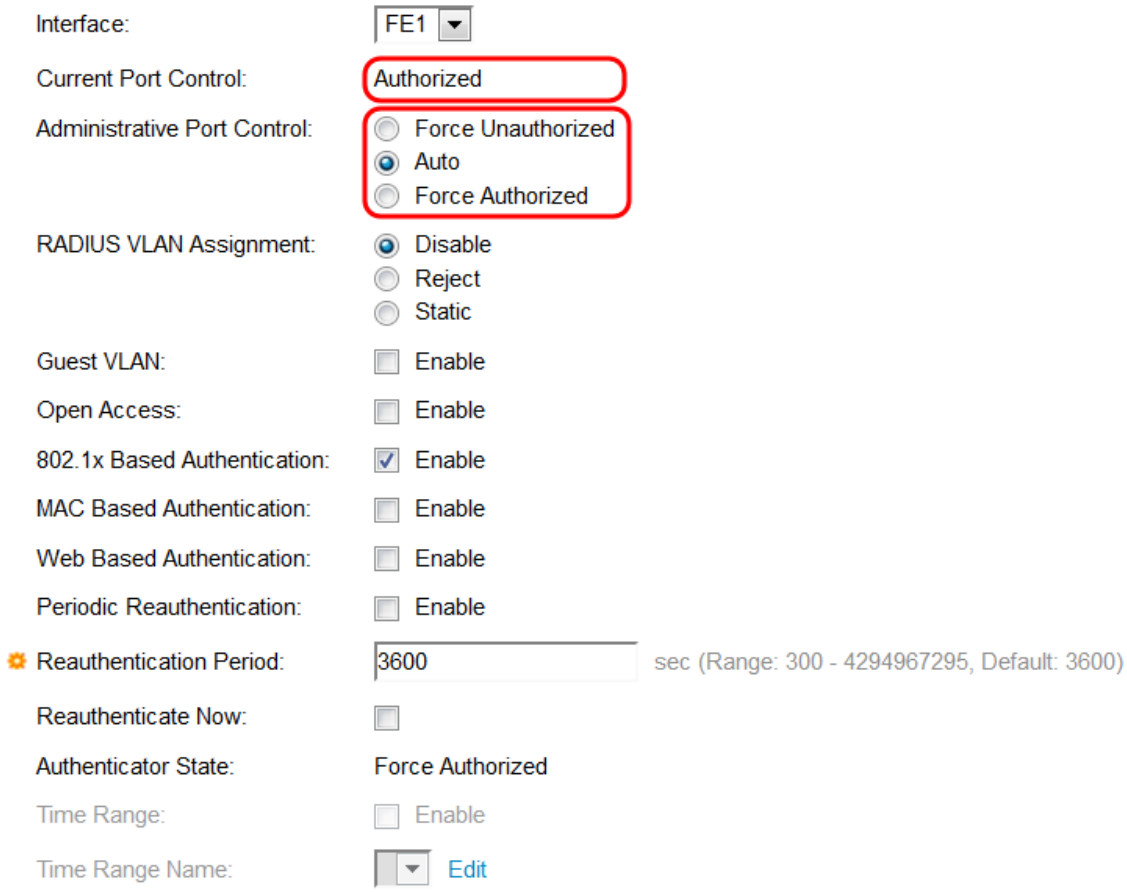
步骤5.导航至**Security > 802.1X/MAC/Web Authentication > Port Authentication**。将打*开“端口身份验证”*页。



步骤6.通过在端口身份验证表中选择其单选按钮并单击编辑.....按钮，*选择要*配置的**端口**。“编辑*端口身份验证*”窗口打开。



步骤7.在Administrative Port Control(管*理端口控制*)字段中，选择一个单选按钮以确定端口将如何授权会话。“当*前端口控制*”字段显示所选端口的当前授权状态。



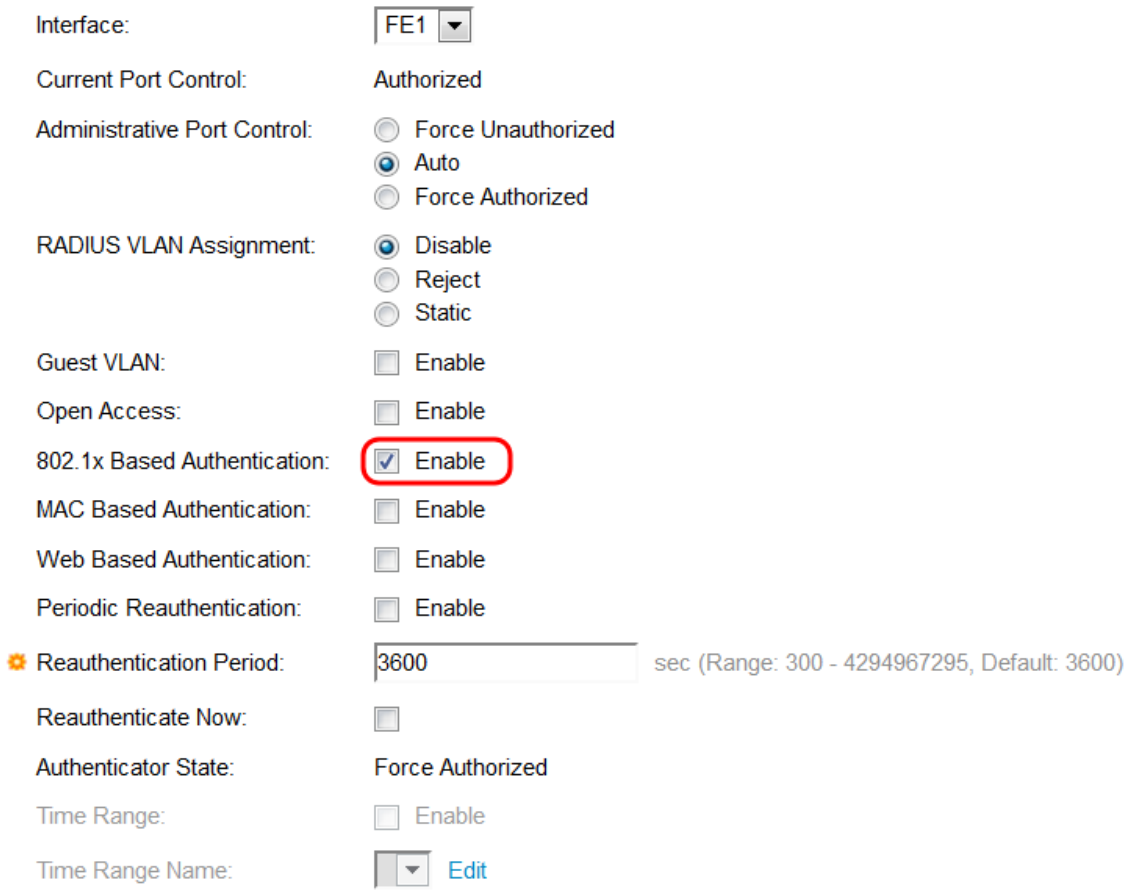
选项有：

·强制未授权 — 将接口移至未授权状态。设备不向连接到此端口的任何客户端提供身份验证，并拒绝访问。

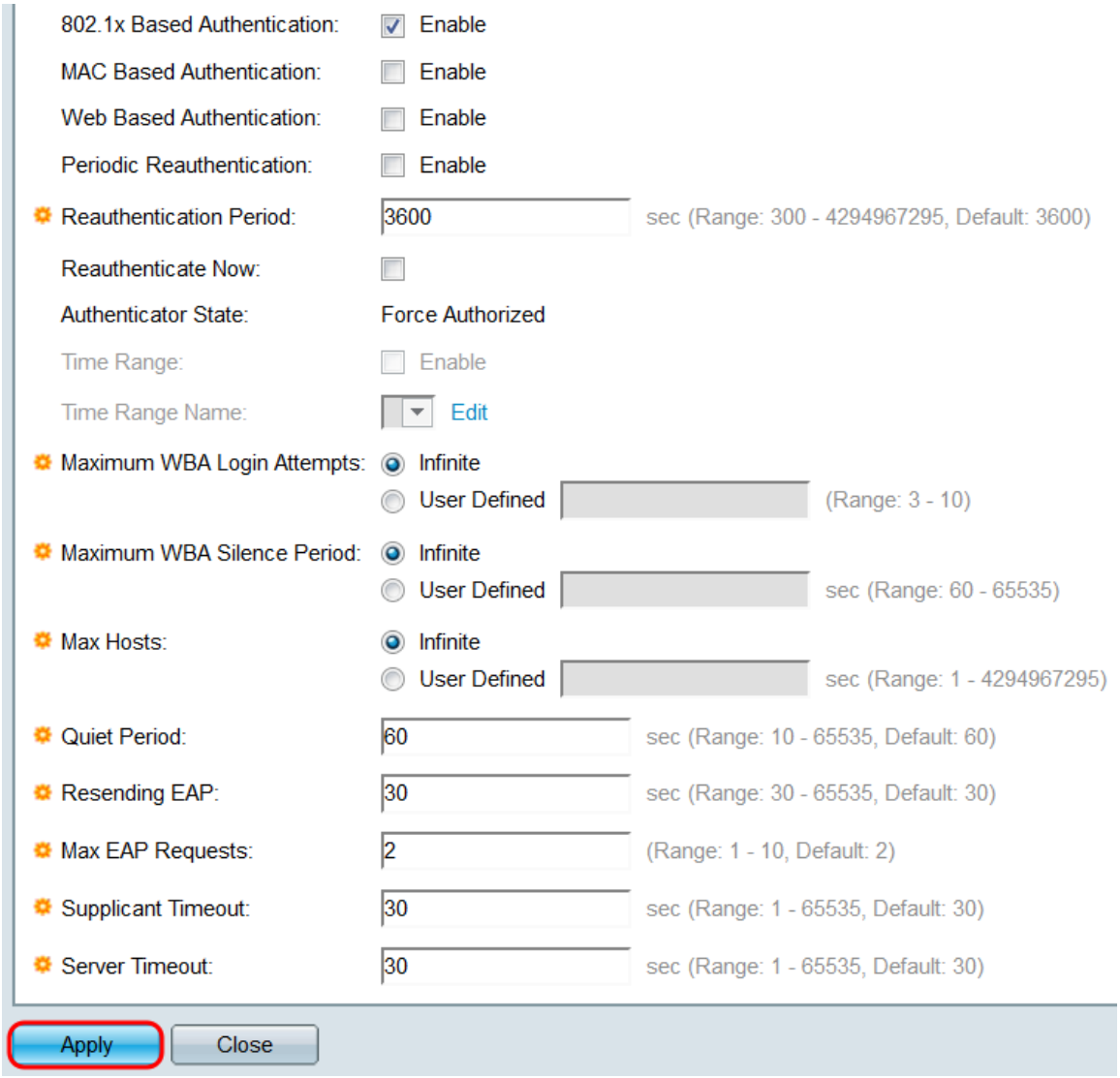
·自动 — 为所选端口启用基于端口的身份验证。根据身份验证过程的结果在授权和未授权之间移动接口。选择此选项以实施802.1X。

·强制授权 — 将接口移入授权状态。设备将提供对连接到此端口的任何客户端的访问，而无需身份验证。

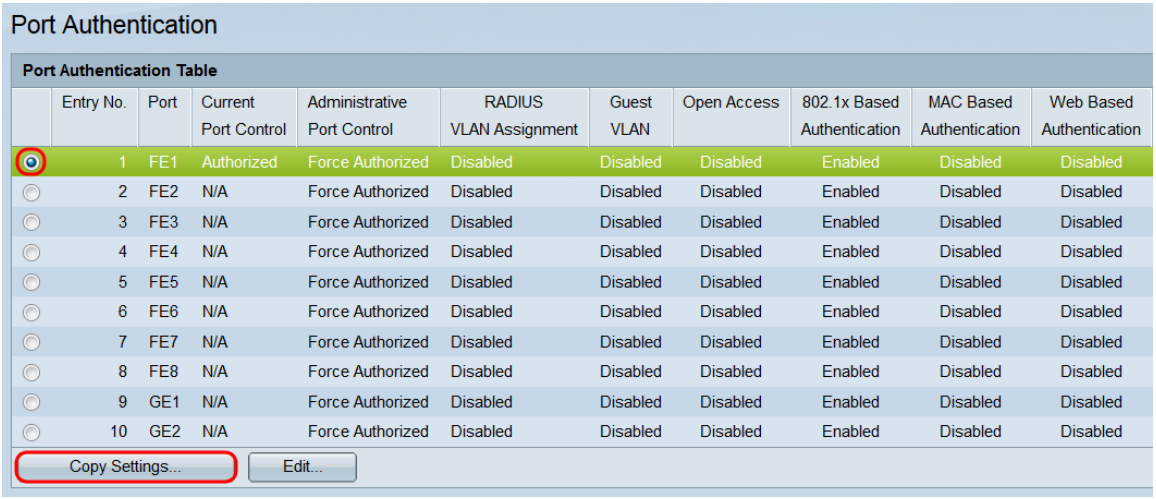
步骤8.选中*802.1X Based Authentication*字段中的**Enable**复选框，以为所选端口启用802.1X身份验证。



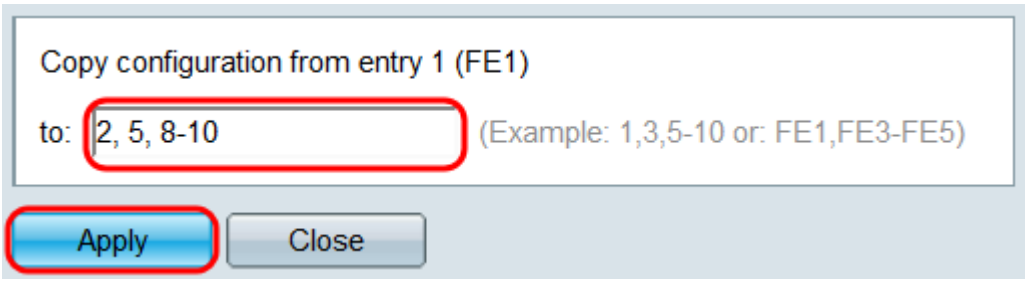
步骤9.单击“**应用**”。现在，应该已完全配置该端口以进行基于802.1X端口的身份验证，并准备开始对连接到该端口的任何客户端进行身份验证。使用*Interface*字段选择要配置的不同端口，而不返回Port Authentication*页面*。



步骤10.如果要快速将端口设置复制到另一个端口或端口范围，请单击*Port Authentication Table*中要复制的端口的单选按钮，然后单击**Copy Settings...**按钮。“复制设置”窗口打开。



步骤11.在文本字段中，输入要将设置复制到的端口（用逗号隔开）。您还可以指定端口范围。然后，单击**Apply**以复制设置。



查看与本文相关的视频……

[单击此处查看思科提供的其他技术讲座]