



## Firepower 1010 交换机端口的基本接口配置

可以将各 Firepower 1010 接口配置为作为常规防火墙接口或第 2 层硬件交换机端口运行。本章节包括用于启动交换机端口配置的任务，包括启用或禁用交换模式以及创建 VLAN 接口和将它们分配给 VLAN。本章节还介绍如何在受支持接口上自定义以太网供电 (PoE)。

- [关于 Firepower 1010 交换机端口，第 1 页](#)
- [Firepower 1010 交换机端口准则和限制，第 2 页](#)
- [配置交换机端口和以太网供电，第 4 页](#)
- [监控交换机端口，第 8 页](#)
- [交换机端口历史记录，第 9 页](#)

### 关于 Firepower 1010 交换机端口

本节介绍 Firepower 1010 的交换机端口。

### 了解 Firepower 1010 端口和接口

#### 端口和接口

对于各物理 Firepower 1010 接口，可以将其操作设置为防火墙接口或交换机端口。请参阅以下有关物理接口和端口类型的信息，以及为其分配交换机端口的逻辑 VLAN 接口：

- **物理防火墙接口** - 在路由模式下，这些接口使用已配置的安全策略在第 3 层网络之间转发流量，以应用防火墙和 VPN 服务。在透明模式下，这些接口是桥接组成员，用于在第 2 层同一网络上的接口之间转发流量，使用已配置的安全策略应用防火墙服务。在路由模式下，还可以将集成路由和桥接与某些接口一起用作桥接组成员，将其他接口用作第 3 层接口。默认情况下，以太网 1/1 接口配置为防火墙接口。
- **物理交换机端口** - 交换机端口使用硬件中的交换功能在第 2 层转发流量。同一 VLAN 上的交换机端口可使用硬件交换互相通信，且流量不受 ASA 安全策略的限制。接入端口仅接受未标记流量，可以将其分配给单个 VLAN。中继端口接受未标记和已标记流量，且可以属于多个 VLAN。默认情况下，以太网 1/2 至 1/8 配置为 VLAN 1 上的接入交换机端口。不能将管理接口配置为交换机端口。

- 逻辑 VLAN 接口 - 这些接口的运行方式与物理防火墙接口相同，但不同的是，无法创建子接口或 EtherChannel 接口。如果交换机端口需要与另一个网络进行通信，则 ASA 设备将安全策略应用至 VLAN 接口，并路由至另一个逻辑 VLAN 接口或防火墙接口。甚至可以将集成路由和桥接与 VLAN 接口一起用作桥接组成员。同一 VLAN 上的交换机端口之间的流量不受安全策略 ASA 的限制，但桥接组中 VLAN 之间的流量会受到安全策略的限制，因此，可以选择将桥接组和交换机端口进行分层，以在某些分段之间实施安全策略。

### 以太网供电

以太网 1/7 和以太网 1/8 支持以太网供电+ (PoE+)。

## Auto-MDI/MDIX 功能

如果是所有 Firepower 1010 接口，默认的自动协商设置还包括 Auto-MDI/MDIX 功能。Auto-MDI/MDIX 在自动协商阶段检测直通电缆时执行内部交叉，从而消除交叉布线的需要。如要启用接口的 Auto-MDI/MDIX，必须将速度或双工设置为自动协商。如果将速度和双工明确设置为固定值，从而禁用了两种设置的自动协商，则 Auto-MDI/MDIX 也将被禁用。当速度和双工被设置为 1000 和全值时，接口始终会自动协商；因此，Auto-MDI/MDIX 始终会启用，且您无法禁用它。

## Firepower 1010 交换机端口准则和限制

### 情景模式

Firepower 1010 不支持多情景模式。

### 故障转移和集群

- 无集群支持。
- 仅支持主用/备用故障转移。
- 使用故障转移时，不应使用交换机端口功能。由于交换机端口在硬件中运行，因此会继续在主用设备和备用设备上传输流量。故障转移旨在防止流量通过备用设备，但此功能不会扩展至交换机端口。在正常故障转移网络设置中，两台设备上的活动交换机端口将导致网络环路。建议将外部交换机用于任何交换功能。请注意，VLAN 接口可通过故障转移监控，而交换机端口无法通过故障转移监控。理论上，您可以将单个交换机端口置于 VLAN 上并成功使用故障转移，但更简单的设置是改用物理防火墙接口。
- 仅可使用防火墙接口作为故障转移链路。

### 逻辑 VLAN 接口

- 您可以创建多达 60 个 VLAN 接口。
- 如果还在防火墙接口上使用 VLAN 子接口，则无法使用与逻辑 VLAN 接口相同的 VLAN ID。

- MAC 地址：
  - 路由防火墙模式 - 所有 VLAN 接口共享一个 MAC 地址。确保所有连接的交换机均可支持此方案。如果连接的交换机需要唯一 MAC 地址，可手动分配 MAC 地址。请参阅[配置手动 MAC 地址、MTU 和 TCP MSS](#)。
  - 透明防火墙模式 - 每个 VLAN 接口都有唯一的 MAC 地址。如有需要，您可通过手动分配 MAC 地址覆盖生成的 MAC 地址。请参阅[配置手动 MAC 地址、MTU 和 TCP MSS](#)。

### 网桥组

您不能将逻辑 VLAN 接口和物理防火墙接口混合在同一个网桥组中。

### VLAN 接口和交换机端口不支持的功能

VLAN 接口和交换机端口不支持：

- 动态路由
- 组播路由
- 基于策略的路由
- 等价多路径路由 (ECMP)
- VXLAN
- EtherChannel
- 故障转移和状态链路
- 流量区域
- 安全组标记 (SGT)

### 其他准则和限制

- 您最多可以在 Firepower 1010 上配置 60 个命名接口。
- 不能将 管理接口配置为交换机端口。

### 默认设置

- 以太网 1/1 是一个防火墙接口。
- 以太网 1/2 至以太网 1/8 是分配给 VLAN 1 的交换机端口。
- 默认速度和复用 - 默认情况下，速度和复用设置为自动协商。

## 配置交换机端口和以太网供电

要配置交换机端口和 PoE，请完成以下任务。

### 配置 VLAN 接口

本节介绍如何配置 VLAN 接口以用于关联交换机端口。

#### 过程

**步骤 1** 依次选择配置 > 设备设置 > 接口设置 > 接口，然后选择添加 > VLAN 接口。

**步骤 2** 在 VLAN ID 字段中，输入此接口的 VLAN ID（介于 1 和 4070 之间），不包括 3968 到 4047 范围内的 ID（保留供内部使用）。

**步骤 3**（可选）在“阻止来自接口的流量流向”下拉列表中，选择此 VLAN 接口无法向其发起流量的 VLAN。

例如，您有一个 VLAN 分配给外部以供互联网访问，另一个 VLAN 分配给内部企业网络，第三个 VLAN 分配给您的家庭网络。家庭网络无需访问企业网络，因此，您可以使用此接口上的阻止流量来选择家庭 VLAN；企业网络可以访问家庭网络，但家庭网络不能访问企业网络。

**步骤 4** 点击确定。

**步骤 5** 点击应用。

### 将交换机端口配置为接入端口

要将交换机端口分配给单个 VLAN，请将其配置为接入端口。接入端口仅接受未标记流量。默认情况下，以太网 1/2 至以太网 1/8 交换机端口已启用并分配给 VLAN 1。

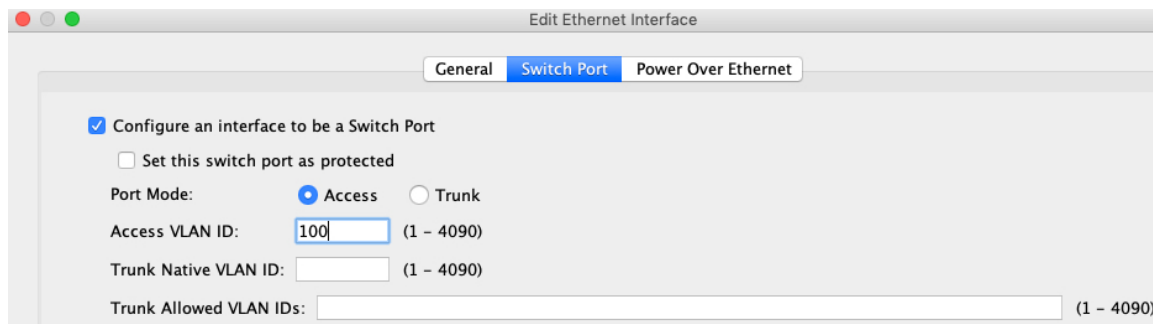


**注释** Firepower 1010 不支持在网络中进行环路检测的生成树协议。因此，您必须确保与 ASA 的任何连接均不会在网络环路中结束。

#### 过程

**步骤 1** 依次选择配置 > 设备设置 > 接口设置 > 接口，选择要编辑的接口，然后点击编辑。

**步骤 2** 点击交换机端口。



**步骤 3** 选中“将一个接口配置为交换机端口”复选框。

**步骤 4** (可选) 选中将此交换机端口设置为受保护复选框以将此交换机端口设置为受保护端口，因此您可以阻止交换机端口与同一 VLAN 上的其他受保护交换机端口进行通信。

在以下情况下，您可能想要防止交换机端口相互之间进行通信：主要从其他 VLAN 访问这些交换机端口上的设备；您不需要允许 VLAN 间访问；如出现病毒感染或其他安全漏洞，则需要将设备相互隔离开。例如，如果具有托管 3 台 Web 服务器的 DMZ，则在您将此交换机端口设置为受保护选项应用于各交换机端口后，则可以将 Web 服务器相互隔离。内部网络和外部网络均可以与这 3 台网络服务器进行通信，反之亦然，但这些网络服务器相互之间无法进行通信。

**步骤 5** 端口模式 (Port Mode) 下，点击访问 (Access) 单选按钮。

**步骤 6** 输入与此交换机端口关联的接入 VLAN ID (介于 1 和 4070 之间)。

默认值为 VLAN 1。

**步骤 7** 点击“常规”。

**步骤 8** 选中启用接口。

注释 “常规”页面上的其他字段 (例如“接口名称”) 不适用于交换机端口。

**步骤 9** (可选) 设置硬件属性。

a) 点击“配置硬件属性”。

b) 选择“双工”。

默认为自动。

c) 选择速度。

默认为自动。

d) 点击点击。

**步骤 10** 点击确定。

**步骤 11** 点击应用。

## 将交换机端口配置为中继端口

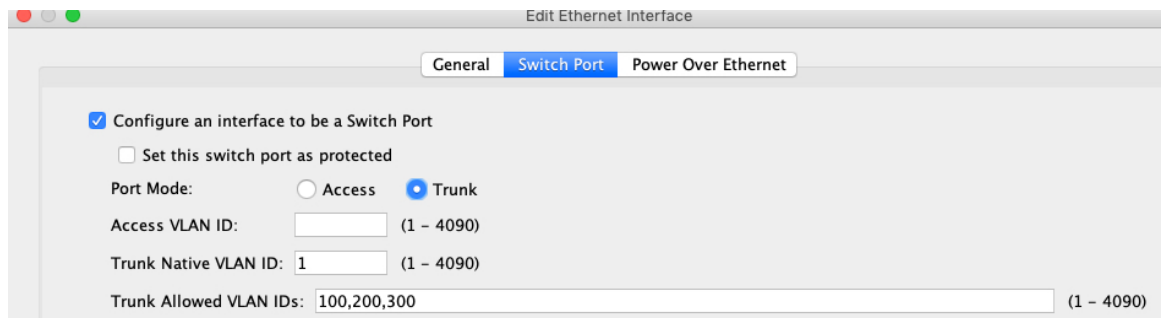
此程序介绍如何创建可以使用 802.1 Q 标记传输多个 VLAN 的中继端口。中继端口接受未标记和标记流量。允许的 VLAN 上的流量通过中继端口保持不变。

中继端口接收未标记流量后将其标记为本地 VLAN ID，以便 ASA 可以将流量转发至正确交换机端口，或可以将流量路由至另一个防火墙接口。如果 ASA 从中继端口发送本地 VLAN ID 流量，则会删除 VLAN 标记。请务必在另一台交换机上的中继端口上设置相同的本地 VLAN，以便将未标记流量标记至同一 VLAN。

### 过程

**步骤 1** 依次选择配置 > 设备设置 > 接口设置 > 接口，选择要编辑的接口，然后点击编辑。

**步骤 2** 点击交换机端口。



**步骤 3** 选中“将一个接口配置为交换机端口”复选框。

**步骤 4** （可选）选中将此交换机端口设置为受保护复选框以将此交换机端口设置为受保护端口，因此您可以阻止交换机端口与同一 VLAN 上的其他受保护交换机端口进行通信。

在以下情况下，您可能想要防止交换机端口相互之间进行通信：主要从其他 VLAN 访问这些交换机端口上的设备；您不需要允许 VLAN 间访问；如出现病毒感染或其他安全漏洞，则需要将设备相互隔离开。例如，如果具有托管 3 台 Web 服务器的 DMZ，则在您将**将此交换机端口设置为受保护**选项应用于各交换机端口后，则可以将 Web 服务器相互隔离。内部网络和外部网络均可以与这 3 台网络服务器进行通信，反之亦然，但这些网络服务器相互之间无法进行通信。

**步骤 5** 端口模式下，点击中继单选按钮。

**步骤 6** 输入设置介于 1 和 4070 之间的 **Trunk Native VLAN ID**。默认值为 VLAN 1。

每个端口只能有一个本地 VLAN，但各端口的本地 VLAN 可以相同也可以不同。

**步骤 7** 输入与此交换机端口关联的**中继允许的 VLAN ID**，用 1 到 4070 之间的逗号分隔。

如果在此字段中包含本地 VLAN，则将忽略该本地 VLAN；从端口发送本地 VLAN 流量时，中继端口始终会删除 VLAN 标记。此外，不会接收仍具有 VLAN 标记的流量。

**步骤 8** 点击“常规”。

**步骤 9** 选中启用接口。

注释 “常规” 页面上的其他字段（例如“接口名称”）不适用于交换机端口。

**步骤 10** （可选） 设置硬件属性。

a) 点击“配置硬件属性”。

b) 选择“双工”。

默认为自动。

c) 选择速度。

默认为自动。

d) 点击点击。

**步骤 11** 点击确定。

**步骤 12** 点击应用。

## 配置以太网供电

以太网 1/7 和以太网 1/8 支持 IP 电话或无线接入点等设备的以太网供电 (PoE)。Firepower 1010 支持 IEEE 802.3af (PoE) 和 802.3at (PoE+)。PoE+ 使用链路层发现协议 (LLDP) 来协商功率级别。PoE+ 可以为受电设备提供 30 瓦的功率。仅在需要时提供功率。

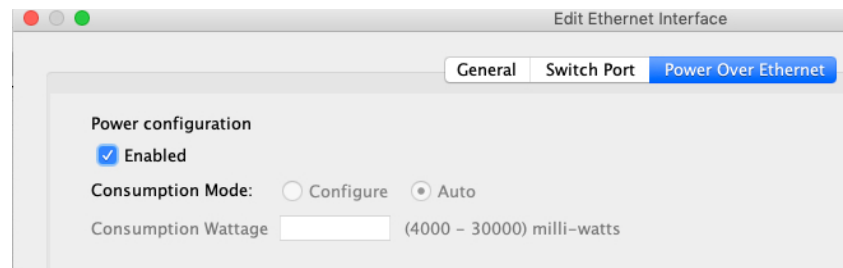
如果关闭接口，则会禁用设备电源。

默认情况下，在以太网 1/7 和以太网 1/8 上启用 PoE。此过程介绍如何禁用和启用 PoE 以及如何设置可选参数。

### 过程

**步骤 1** 依次选择配置 > 设备设置 > 接口设置 > 接口，选择要编辑的接口（以太网 1/7 或 1/8），然后点击编辑。

**步骤 2** 点击以太网供电。



**步骤 3** 点击已启用。

**步骤 4** 点击“功耗模式：配置”或“自动”单选按钮。

- **Auto-PoE** 使用适合受电设备类别的瓦数将电源自动传送至受电设备。Firepower 1010 使用 LLDP 进一步协商正确的瓦数。
- **配置** - 手动在“**功耗（瓦数）**”字段中指定以瓦为单位的瓦数，范围为 4000 至 30000。如果要手动设置瓦数并禁用 LLDP 协商，请使用此选项。

**步骤 5** 点击确定。

**步骤 6** 点击应用。

**步骤 7** 依次选择**监控 > 接口 > 以太网供电**以查看当前 PoE+ 状态。

---

## 监控交换机端口

- **监控 > 接口 > ARP 表**

显示 ARP 表，包括静态和动态条目。ARP 表包含将给定接口的 MAC 地址映射到 IP 地址的条目。

- **监控 > 接口 > MAC 地址表**

显示静态和动态 MAC 地址条目。

- **监控 > 接口 > 接口图形**

以图形或表格形式显示接口统计信息。

- **监控 > 接口 > L2 交换机**

显示 VLAN 到路由器的关联，以及静态和动态 MAC 地址条目。

- **监控 > 接口 > 以太网供电**

显示 PoE+ 状态。



## 交换机端口历史记录

表 1: 交换机端口历史记录

功能名称	版本	功能信息
Firepower 1010 硬件交换机支持	9.13(1)	<p>Firepower 1010 支持将各以太网接口设置为交换机端口或防火墙接口。</p> <p>新增/修改的屏幕:</p> <ul style="list-style-type: none"><li>• 配置 &gt; 设备设置 &gt; 接口设置 &gt; 接口 &gt; 编辑 &gt; 交换端口</li><li>• 配置 &gt; 设备设置 &gt; 接口设置 &gt; 接口 &gt; 添加 VLAN 接口</li><li>• 监控 &gt; 接口 &gt; L2 交换机</li></ul>
Firepower 1010 PoE+ 支持以太网 1/7 和以太网 1/8	9.13(1)	<p>Firepower 1010 支持以太网接口 1/7 和 1/8 上的增强型以太网供电+ (PoE+)。</p> <p>新增/修改的屏幕:</p> <ul style="list-style-type: none"><li>• 配置 &gt; 设备设置 &gt; 接口设置 &gt; 接口 &gt; 编辑 &gt; 关闭以太网电源</li><li>• 监控 &gt; 接口 &gt; 以太网供电</li></ul>



## 当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。