



## VLAN 子接口

本章说明如何配置 VLAN 子接口。



**注释** 在多情景模式下，请在系统执行空间中完成本节所述的所有任务。如果您尚未进入系统执行空间，请在 **Configuration > Device List** 窗格中双击主用设备 IP 地址下的 **System**。

- [关于 VLAN 子接口，第 1 页](#)
- [VLAN 子接口的许可，第 1 页](#)
- [VLAN 子接口的准则和限制，第 2 页](#)
- [VLAN 子接口的默认设置，第 3 页](#)
- [配置 VLAN 子接口和 802.1Q 中继，第 3 页](#)
- [VLAN 子接口示例，第 4 页](#)
- [VLAN 子接口历史记录，第 6 页](#)

## 关于 VLAN 子接口

通过 VLAN 子接口，您可以将物理接口或 EtherChannel 接口划分为标记有不同 VLAN ID 的多个逻辑接口。带有一个或多个 VLAN 子接口的接口将自动配置为 802.1Q 中继。由于 VLAN 允许您在特定物理接口上将流量分开，所以您可以增加网络中可用的接口数量，而无需增加物理接口或 ASA。此功能对多情景模式尤其有用，使得可以向每个情景分配唯一的接口。

可以配置主 VLAN，以及一个或多个辅助 VLAN。当 ASA 接收到辅助 VLAN 上的流量时，它会将该流量映射到主 VLAN。

## VLAN 子接口的许可

型号	许可证要求
Firepower 1010	基础许可证：60

型号	许可证要求
Firepower 1120	基础许可证: 512
Firepower 1140 和 1150	基础许可证: 1024
Firepower 2100	基础许可证: 1024
Secure Firewall 3100	基础许可证: 1024
Firepower 4100	基础许可证: 1024
Firepower 9300	基础许可证: 1024
ASA Virtual	吞吐量: 100 Mbps: 25 1 Gbps: 50 2 Gbps: 200 10 Gbps: 1024
ISA 3000	基础许可证: 5 增强型安全许可证: 100



注释 对于根据 VLAN 限制计数的接口，您必须向其分配 VLAN。

## VLAN 子接口的准则和限制

### 型号支持

- Firepower 1010 - 交换机端口或 VLAN 接口上不支持 VLAN 子接口。
- 对于 ASA 型号，您无法在管理接口上配置子接口。请参阅 [管理插槽/端口接口](#) 了解子接口支持。

### 其他准则

- 防止物理接口上的未标记数据包 - 如果使用子接口，则通常表明也不希望物理接口传递流量，因为物理接口会传递未标记的数据包。此属性的主用物理接口以及 EtherChannel 链路同样适用。由于必须启用物理接口或 EtherChannel 接口才能使子接口传递流量，请通过不为接口配置名称省略 `nameif` 命令不传递流量。如果要使物理接口或 EtherChannel 接口传递未标记的数据包，您可以照常配置名称。

- 同一父接口上的所有子接口必须为网桥组成员或路由接口；您无法混合搭配。
- ASA 不支持动态中继协议 (DTP)，因此您必须无条件地将连接的交换机端口配置到中继上。
- 您可能想要为 ASA 上定义的子接口分配唯一 MAC 地址，因为它们使用父接口上相同的固化 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 ASA 上特定实例内发生流量中断。您可以自动生成唯一的 MAC 地址；请参阅[分配 MAC 地址](#)。

## VLAN 子接口的默认设置

本节列出了接口的默认设置（如果没有出厂默认配置）。

### 接口的默认状态

接口的默认状态取决于类型和情景模式。

在多情景模式下，默认启用所有已分配的接口，而不考虑接口在系统执行空间中的状态。但是，要使流量通过该接口，还必须在系统执行空间中启用该接口。如果您在系统执行空间中关闭了一个接口，则该接口在所有共享它的情景中都会关闭。

在单模式下或在系统执行空间中，接口具有以下默认状态：

- 物理接口 - 已禁用。
- VLAN 子接口 - 已启用。但是，要使流量通过子接口，还必须启用物理接口。

## 配置 VLAN 子接口和 802.1Q 中继

向物理接口或 EtherChannel 接口添加 VLAN 子接口。

### 开始之前

对于多情景模式，请在系统执行空间中完成本程序。如果您尚未进入系统配置模式，请在 **Configuration > Device List** 窗格中双击主用设备 IP 地址下的 **System**。

### 过程

**步骤 1** 视情景模式而定：

- 对于单情景模式，请依次选择 **Configuration > Device Setup > Interface Settings > Interfaces** 窗格。
- 对于多情景模式，请在系统执行空间中依次选择 **配置 > 上下文管理 > 接口** 窗格。

**步骤 2** 依次选择 **添加 > 接口**。

系统将显示 **Add Interface** 对话框。

**注释** 在单情景模式中，此程序仅涉及 **Edit Interface** 对话框上参数的子集；要配置其他参数，请参阅[路由模式接口](#)和[透明模式接口](#)。请注意，在多情景模式下，完成接口配置之前，您需要将接口分配到情景。请参阅[配置多情景](#)。

**步骤 3** 从 **Hardware Port** 下拉列表中，选择要添加子接口的物理接口或端口通道接口。

**步骤 4** 如果该接口尚未启用，请选中 **Enable Interface** 复选框。

默认情况下，该接口已启用。

**步骤 5** 在 **VLAN ID** 字段中，输入介于 1 和 4094 之间的 VLAN ID。

某些 VLAN ID 可能是连接的交换机中的保留 VLAN ID，因此请查看交换机文档以了解详细信息。对于多情景模式，您只能在系统配置中设置 VLAN。

**步骤 6** 在 **Secondary VLAN ID** 字段中，输入一个或多个使用空格、逗号或连字符（适用于连续范围）分隔的 VLAN ID。

当 ASA 接收到辅助 VLAN 的流量时，它会将流量映射到主 VLAN。

**步骤 7** 在 **Subinterface ID** 字段中，输入子接口 ID（介于 1 到 4294967293 之间的整数）。

允许的子接口数因平台而异。此 ID 一旦设置便不可更改。

**步骤 8** （可选）在 **Description** 字段中，输入此接口的说明。

一行说明最多可包含 240 个字符（不包括回车符）。对于多情景模式，系统说明与情景说明无关。例如，对于故障转移或状态链路，说明固定为“LAN Failover Interface”、“STATE Failover Interface”或“LAN/STATE Failover Interface”。您无法编辑此说明。如果将此接口设为故障转移或状态链路，则固定说明将覆盖在此处输入的任何说明。

**步骤 9** 点击确定 (OK)。

系统将返回到 **Interfaces** 窗格。

---

#### 相关主题

[VLAN 子接口的许可](#)，第 1 页

## VLAN 子接口示例

以下示例在单模式下配置子接口的参数：

```
interface gigabitethernet 0/1
  no nameif
  no security-level
  no ip address
  no shutdown
interface gigabitethernet 0/1.1
```

```
vlan 101
nameif inside
security-level 100
ip address 192.168.6.6 255.255.255.0
no shutdown
```

以下示例显示 VLAN 映射如何与 Catalyst 6500 配合使用。请查看 Catalyst 6500 配置指南，了解如何将节点连接到 PVLANS。

#### ASA Configuration

```
interface GigabitEthernet1/1
  description Connected to Switch GigabitEthernet1/5
  no nameif
  no security-level
  no ip address
  no shutdown
!
interface GigabitEthernet1/1.70
  vlan 70 secondary 71 72
  nameif vlan_map1
  security-level 50
  ip address 10.11.1.2 255.255.255.0
  no shutdown
!
interface GigabitEthernet1/2
  nameif outside
  security-level 0
  ip address 172.16.171.31 255.255.255.0
  no shutdown
```

#### Catalyst 6500 Configuration

```
vlan 70
  private-vlan primary
  private-vlan association 71-72
!
vlan 71
  private-vlan community
!
vlan 72
  private-vlan isolated
!
interface GigabitEthernet1/5
  description Connected to ASA GigabitEthernet1/1
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 70-72
  switchport mode trunk
!
```

## VLAN 子接口历史记录

表 1: VLAN 子接口历史记录

功能名称	版本	功能信息
增加了 VLAN 数量	7.0(5)	提高了以下限制： <ul style="list-style-type: none"> <li>• ASA5510 基础许可证的 VLAN 数量从 0 增加到 10。</li> <li>• ASA5510 增强型安全许可证 VLAN 数量从 10 增加到 25。</li> <li>• ASA5520 VLAN 数量从 25 增加到 100。</li> <li>• ASA5540 VLAN 数量从 100 增加到 200。</li> </ul>
增加了 VLAN 数量	7.2(2)	提高了以下型号的 VLAN 限制：ASA 5510（对于基础许可证，从 10 提高到 50；对于增强型安全许可证，从 25 提高到 100）、ASA 5520（从 100 提高到 150）、ASA 5550（从 200 提高到 250）。
增加了 ASA 5580 的 VLAN 数量	8.1(2)	在 ASA 5580 上支持的 VLAN 数量从 100 增加到 250。
支持将辅助 VLAN 映射到主 VLAN	9.5(2)	现在您可以为一个子接口配置一个或多个辅助 VLAN。当 ASA 接收到辅助 VLAN 的流量时，它会将流量映射到主 VLAN。  修改了以下菜单项： <b>配置 &gt; 设备设置 &gt; 接口设置 &gt; 接口配置 &gt; 设备设置 &gt; 接口设置 &gt; 接口 &gt; 添加接口 &gt; 通用</b>
为 ISA 3000 增加了 VLAN	9.13(1)	拥有增强型安全许可证的 ISA 3000 的最大 VLAN 数量从 25 增加到 100。

## 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。