Firepower 1010 和 Cisco Secure Firewall 1210/1220 交换机端口的基本接口配置

可以将各 Firepower 1010 或 Cisco Secure Firewall 1210/1220 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 和 Cisco Secure Firewall 1210/1220 交换机端口

本节介绍 Firepower 1010 和 Cisco Secure Firewall 1210/1220的交换机端口。

了解交换机端口和接口

端口和接口

对于各物理 Firepower 1010 或 Cisco Secure Firewall 1210/1220 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 (1010 和 1210) 或以太网 1/2 至 1/10 (1220) 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

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+)。

Auto-MDI/MDIX 功能

如果是所有交换机口，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。

交换机端口准则和限制

情景模式

- Firepower 1010 不支持多情景模式。
- Cisco Secure Firewall 1210/1220 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 (SVI)

- 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。请参阅手动配置 MAC 地址。
  - 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。请参阅手动配置 MAC 地址。

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 和 Cisco Secure Firewall 1210/1220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。
- 在 Firepower 1010 和 Cisco Secure Firewall 1210，以太网 1/2 至以太网 1/8 是分配给 VLAN 1 的交换机端口。
- 在 Cisco Secure Firewall 1220，以太网 1/2 至以太网 1/8 交换机端口会被分配给 VLAN 1。
- 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。

启用或禁用交换机端口模式

您可以将每个接口单独设置为防火墙接口或交换机端口。默认情况下，以太网 1/1 是防火墙接口，而剩余的以太网接口则配置为交换机端口。

过程

步骤 1 进入接口配置模式。

interface ethernet1/端口

- 端口，用于设置端口号，从 1 到 8。

您无法将 Management 1/1 接口设置为交换机端口模式。

示例：

```
ciscoasa(config)# interface ethernet1/4
ciscoasa(config-if)#
```

步骤 2 启用交换机端口模式。

switchport

如果此接口已处于交换机端口模式，系统会提示您输入交换机端口参数，而不是更改模式。

```
ciscoasa(config-if)# switchport
ciscoasa(config-if)# switchport ?
interface mode commands/options:
  access         Set access mode characteristics of the interface
  mode           Set trunking mode of the interface
  monitor        Monitor another interface
  protected      Configure an interface to be a protected port
  trunk          Set trunking characteristics of the interface
<cr>
```

```
ciscoasa(config-if)#
```

步骤 3 禁用交换机端口模式。

no switchport

```
ciscoasa(config-if)# no switchport
ciscoasa(config-if)# switchport ?

interface mode commands/options:
<cr>
```

示例

以下示例将以太网 1/3 和 1/4 设置为防火墙模式：

```
ciscoasa(config)# interface ethernet1/3
ciscoasa(config-if)# no switchport
ciscoasa(config-if)# interface ethernet1/3
ciscoasa(config-if)# no switchport
ciscoasa(config-if)#
```

配置 VLAN 接口

本节介绍如何配置 VLAN 接口 (SVI) 以用于关联交换机端口。您最多可以创建 60 个与交换机端口相关联的 VLAN 接口。

过程

步骤 1 添加 VLAN 接口。

interface vlan *id*

- *id* - 设置此接口的 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）。

示例：

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)#
```

步骤 2 （可选） 禁用转发到另一个 VLAN。

no forward interface *vlan_id*

- *vlan_id* - 为不能发起到其它 VLAN 流量的 VLAN 接口的 VLAN ID。

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 **no forward interface** 命令来选择家庭 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。

示例：

```
ciscoasa(config-if)# no forward interface 200
ciscoasa(config-if)#
```

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 交换机端口会被启用并分配给 的 VLAN 1。在 Cisco Secure Firewall 1220 上，以太网 1/2 至以太网 1/10 交换机端口会被默认启用并分配给 VLAN 1。

注释 设备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 进入接口配置模式。

interface ethernet1/端口

- 端口，用于设置端口号，从 1 到 8。

示例：

```
ciscoasa(config)# interface ethernet1/4
ciscoasa(config-if)#
```

步骤 2 将此交换机端口分配给 VLAN。

switchport access vlan编号

- *number* - 设置介于 1 和 4070 之间的 VLAN ID。默认值为 VLAN 1。

示例：

```
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)#
```

步骤 3 （可选） 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。

switchport protected

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 **switchport protected** 命令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。

示例：

```
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)#
```

步骤 4 （可选） 设置速度。

speed {**auto** | **10** | **100** | **1000**}

默认值为 **auto**。

示例：

```
ciscoasa(config-if)# speed 100
ciscoasa(config-if)#
```

步骤 5 （可选） 设置双工。

duplex {**auto** | **full** | **half**}

默认值为 **auto**。

示例：

```
ciscoasa(config-if)# duplex half
ciscoasa(config-if)#
```

步骤 6 启用交换机端口。

no shutdown

要禁用此交换机端口，请输入 **shutdown** 命令。

示例：

```
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)#
```

示例

以下示例将以太网 1/3、以太网 1/4 和以太网 1/5 的比例分配给 VLAN 101，并将以太网 1/3 和以太网 1/4 的比例设置为受保护：

```
ciscoasa(config)# interface ethernet1/3
ciscoasa(config-if)# switchport access vlan 101
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet1/4
ciscoasa(config-if)# switchport access vlan 101
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet1/5
ciscoasa(config-if)# switchport access vlan 101
ciscoasa(config-if)# no shutdown
```

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 进入接口配置模式。

interface ethernet1/端口

- 端口，用于设置端口号，从 1 到 8。

示例：

```
ciscoasa(config)# interface ethernet1/4
ciscoasa(config-if)#
```

步骤 2 使此交换机端口成为中继端口。

switchport mode trunk

要将此端口恢复为接入模式，请输入 **switchport mode access** 命令。

示例：

```
ciscoasa(config-if)# switchport mode trunk
```

```
ciscoasa(config-if)#
```

步骤 3 将 VLAN 分配给此中继。

switchport trunk allowed vlan *vlan_range*

- *vlan_range* - 设置介于 1 和 4070 之间的 VLAN ID。您可以通过以下方式之一识别最多 20 个ID：
  - 单一编号 (n)
  - 范围 (n-x)
  - 用逗号将编号和范围隔开，例如：

    5,7-10,13,45-100

可以用空格代替逗号，但此命令保存到配置中后，其中的空格将会变成逗号。

如果在此命令中包含本地 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。

示例：

```
ciscoasa(config-if)# switchport trunk allowed vlan 100,200,300
ciscoasa(config-if)#
```

步骤 4 设置本地 VLAN。

switchport trunk native vlan *vlan_id*

- *vlan_range* - 设置介于 1 和 4070 之间的 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。

示例：

```
ciscoasa(config-if)# switchport trunk native vlan 2
ciscoasa(config-if)#
```

步骤 5 （可选） 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。

switchport protected

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 **switchport protected** 命令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。

示例：

```
ciscoasa(config-if)# switchport protected
```

```
ciscoasa(config-if)#
```

步骤 6 （可选） 设置速度。

speed {**auto** | **10** | **100** | **1000**}

默认值为 **auto**。

示例：

```
ciscoasa(config-if)# speed 100
ciscoasa(config-if)#
```

步骤 7 （可选） 设置双工。

duplex {**auto** | **full** | **half**}

默认值为 **auto**。

示例：

```
ciscoasa(config-if)# duplex half
ciscoasa(config-if)#
```

步骤 8 启用交换机端口。

no shutdown

要禁用此交换机端口，请输入 **shutdown** 命令。

示例：

```
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)#
```

示例

以下示例将以太网 1/6 设置为 VLAN 为 20 到 30 的中继端口，并将本地 VLAN 设置为 4：

```
ciscoasa(config)# interface ethernet1/6
ciscoasa(config-if)# switchport mode trunk
ciscoasa(config-if)# switchport trunk allowed vlan 20-30
ciscoasa(config-if)# switchport trunk native vlan 4
ciscoasa(config-if)# no shutdown
```

配置以太网供电

在 Firepower 1010， 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)。在 Cisco Secure Firewall 1210CP 上，以太网 1/5-1/8 支持 PoE。Firepower 1010 和 Cisco Secure Firewall

1210CP 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。

在 Firepower 1010， 在以太网 1/7 和以太网 1/8 上启用 PoE。在 Cisco Secure Firewall 1210CP 上，以太网 1/5-1/8 上的 PoE 默认启用。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 进入接口配置模式。

interface ethernet1/5（仅限 1210CP）|（仅限 1210CP）**6**（仅限 1210CP）**7** | **8**}

示例：

```
ciscoasa(config)# interface ethernet1/7
ciscoasa(config-if)#
```

步骤 2 启用或禁用 PoE+。

power inline {**auto** | **never** | **consumption wattage** *milliwatts*}

- **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 和 Cisco Secure Firewall 1210CP 使用 LLDP 进一步协商正确的瓦数。
- **never** - 禁用 PoE。
- **consumption wattage***millipowers* - 手动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，请使用此命令。

使用 **show power inline** 命令查看当前 PoE+ 状态。

示例：

```
ciscoasa(config-if)# power inline auto
ciscoasa(config-if)# show power inline
Interface     Power   Class   Current (mA)   Voltage (V)
   ---------     -----   -----   ------------   -----------
   Ethernet1/1   n/a     n/a     n/a            n/a
   Ethernet1/2   n/a     n/a     n/a            n/a
   Ethernet1/3   n/a     n/a     n/a            n/a
   Ethernet1/4   n/a     n/a     n/a            n/a
   Ethernet1/5   n/a     n/a     n/a            n/a
   Ethernet1/6   n/a     n/a     n/a            n/a
   Ethernet1/7   On      4       121.00         53.00
   Ethernet1/8   On      4       88.00          53.00
```

示例

以下示例为以太网 1/7 手动设置功率，为以太网 1/8 设置功率为自动：

```
ciscoasa(config)# interface ethernet1/7
ciscoasa(config-if)# power inline consumption wattage 10000
ciscoasa(config-if)# interface ethernet1/8
ciscoasa(config-if)# power inline auto
ciscoasa(config-if)#
```

监控交换机端口

- **show interface**

  显示接口统计信息。

- **show interface ip brief**

  显示接口的 IP 地址和状态。

- **show switch vlan**

  显示 VLAN 到交换机端口的关联。

```
ciscoasa# show switch vlan
VLAN Name                 Status    Ports
---- -------------------- --------- --------------------
1    -                     down      Ethernet1/3,
                                     Ethernet1/4,
                                     Ethernet1/5,
                                     Ethernet1/6
                                     Ethernet1/7,
                                     Ethernet1/8
10   inside                up        Ethernet1/1
20   outside               up        Ethernet1/2
```

- **show switch mac-address-table**

  显示静态和动态 MAC 地址条目。

```
ciscoasa# show switch mac-address-table
Legend: Age - entry expiration time in seconds
  Mac Address  | VLAN |       Type       | Age | Port
-----------------------------------------------------
0c75.bd11.c504 | 0010 |     dynamic      | 330 | In0/0
885a.92f6.c6e3 | 0010 |     dynamic      | 330 | Et1/1
0c75.bd11.c504 | 0020 |     dynamic      | 330 | In0/0
885a.92f6.c45b | 0020 |     dynamic      | 330 | Et1/2
```

- **show arp**

显示动态、静态和代理 ARP 条目。动态 ARP 条目包括 ARP 条目时限（秒）。静态 ARP 条目以短划线 (-) 取代时限，代理 ARP 条目则显示“别名”。以下是 **show arp** 命令的输出示例。第一个条目是时限为 2 秒的动态条目。第二个条目是静态条目，第三个条目来自代理 ARP。

```
ciscoasa# show arp
outside 10.86.194.61 0011.2094.1d2b 2
outside 10.86.194.1 001a.300c.8000 -
outside 10.86.195.2 00d0.02a8.440a alias
```

- **show power inline**

  显示 PoE+ 状态。

```
ciscoasa# show power inline
   Interface     Power   Class   Current (mA)   Voltage (V)
   ---------     -----   -----   ------------   -----------
   Ethernet1/1   n/a     n/a     n/a            n/a
   Ethernet1/2   n/a     n/a     n/a            n/a
   Ethernet1/3   n/a     n/a     n/a            n/a
   Ethernet1/4   n/a     n/a     n/a            n/a
   Ethernet1/5   n/a     n/a     n/a            n/a
   Ethernet1/6   n/a     n/a     n/a            n/a
   Ethernet1/7   On      4       121.00         53.00
   Ethernet1/8   On      4       88.00          53.00
```

交换机端口示例

以下主题提供在路由和透明模式下配置交换机端口的示例。

路由模式示例

以下示例创建两个 VLAN 接口，并将两个交换机端口分配给内部接口，一个分配给外部接口。

```
interface Vlan11
nameif inside
security-level 100
ip address 10.11.11.1 255.255.255.0
no shutdown
!
interface Vlan20
nameif outside
security-level 0
ip address 10.20.20.1 255.255.255.0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
```

```
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 11
no shutdown
```

透明模式示例

以下示例在网桥组 1 中创建两个 VLAN 接口，并将两个交换机端口分配给内部接口，一个分配给外部接口。

```
firewall transparent
!
interface BVI1
ip address 10.20.20.1 255.255.255.0
!
interface Vlan11
bridge-group 1
nameif inside
security-level 100
no shutdown
!
interface Vlan20
bridge-group 1
nameif outside
security-level 0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 11
no shutdown
```

混合防火墙接口/交换机端口示例

以下示例为内部接口创建一个 VLAN 接口，为外部和 dmz 创建两个防火墙接口。

```
interface Vlan11
nameif inside
security-level 100
ip address 10.11.11.1 255.255.255.0
no shutdown
!
interface Ethernet1/1
switchport
```

```
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/4
nameif outside
security-level 0
ip address 10.12.11.1 255.255.255.0
no shutdown
!
interface Ethernet1/5
nameif dmz
security-level 50
ip address 10.13.11.1 255.255.255.0
no shutdown
```

集成的路由和桥接示例

以下示例创建两个网桥组，其中两个VLAN接口（inside_1和inside_2）在网桥组1中，一个（外部）在网桥组2中。第四个VLAN接口不属于网桥组，而是常规路由接口。同一VLAN上交换机端口之间的流量不受ASA的安全策略限制。但网桥组中VLAN之间的流量会受到安全策略的限制，因此，可以选择将网桥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。

```
interface BVI1
nameif inside_bvi
security-level 100
ip address 10.30.1.10 255.255.255.0
!
interface BVI2
nameif outside_bvi
security-level 0
ip address 10.40.1.10 255.255.255.0
!
interface Vlan10
bridge-group 1
nameif inside_1
security-level 100
no shutdown
!
interface Vlan20
bridge-group 2
nameif outside
security-level 0
no shutdown
!
interface Vlan30
bridge-group 1
nameif inside_2
security-level 100
no shutdown
```

```
!
interface Vlan 100
nameif dmz
security-level 0
ip address 10.1.1.1 255.255.255.0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 10
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 30
no shutdown
!
interface Ethernet1/4
switchport
switchport access vlan 20
security-level 100
no shutdown
!
interface Ethernet1/5
switchport
switchport access vlan 100
no shutdown
!
interface Ethernet1/6
switchport
switchport access vlan 10
no shutdown
!
interface Ethernet1/7
switchport
switchport access vlan 30
no shutdown
!
interface Ethernet1/8
switchport
switchport access vlan 100
no shutdown
```

故障转移示例

以下示例将以太网 1/3 配置为故障转移接口。

```
interface Vlan11
nameif inside
security-level 100
ip address 10.11.11.1 255.255.255.0 standby 10.11.11.2
no shutdown
!
interface Vlan20
nameif outside
```

```
security-level 0
ip address 10.20.20.1 255.255.255.0 standby 10.20.20.2
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
description LAN/STATE Failover Interface
no shutdown
!
failover
failover lan unit primary
failover lan interface folink Ethernet1/3
failover replication http
failover link folink Ethernet1/3
failover interface ip folink 10.90.90.1 255.255.255.0 standby 10.90.90.2
```

交换机端口的历史记录

表 *1:* 交换机端口的历史记录

功能名称	版本	功能信息
Cisco Secure Firewall 1210/1220 硬件交换机支持	9.22(1)	Cisco Secure Firewall 1210/1220 支持将各以太网接口设置为交换机端口或防火墙接口。
以太网端口 1/5-1/8 上的 Cisco Secure Firewall 1210CP PoE+ 支持	9.22(1)	Cisco Secure Firewall 1210CP 在以太网端口 1/5-1/8 上支持以太网供电+ (PoE+)。
Firepower 1010 硬件交换机支持	9.13(1)	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。 新增/修改的命令：forward interface、interface vlan、show switch mac-address-table、show switch vlan、switchport、switchport access vlan、switchport mode、switchport trunk allowed vlan
Firepower 1010 PoE + 支持以太网 1/7 和以太网 1/8	9.13(1)	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+)。 新增/修改的命令：**power inline**、**show power inline**

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。