# FPR1010上的L2交换机，架构、验证和故障排除

## 目录


简介
先决条件
要求
使用的组件
背景信息
Firepower 6.5附件
FMC附件
工作原理
FP1010架构
数据包处理
FP1010端口模式
FP1010案例1.路由端口（IP路由）
FP1010案例2.网桥组模式（桥接）
FP1010机箱3.接入模式下的交换机端口（硬件交换）
过滤VLAN内流量
FP1010机箱4.交换机端口（中继）
FP1010案例5.交换机端口（VLAN间）
FP1010案例6. VLAN间过滤器
案例研究 — FP1010。桥接与硬件交换+桥接
FP1010设计注意事项
FXOS REST API
故障排除/诊断
诊断概述
FP1010后端
收集FPRM show技术（在FP1010上）
限制详细信息、常见问题和解决方法
相关信息


## 简介

本文档介绍FP1010设备上的L2交换机。具体来说，它主要涵盖实施中的安全服务平台(SSP)/Firepower广泛操作系统(FXOS)部分。在6.5版本中，Firepower 1010（桌面型号）在内置第2层硬件交换机上启用了交换功能。这有助于避免额外的硬件交换机，并降低成本。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 背景信息

- FP1010是一种桌面型小型办公室家庭办公室(SOHO)，可替代ASA5505和ASA5506-X平台。
- 对由Firepower管理中心(FMC)、Firepower设备管理器(FDM)或云防御协调器(CDO)管理的FTD映像(6.4+)的软件支持。
- 对由CSM、ASDM或CLI管理的ASA映像(9.13+)的软件支持。
- 操作系统(OS)、ASA或FTD是FXOS捆绑包（类似于FP21xx）。
- 8个10/100/1000 Mbps数据端口。
- 端口E1/7、E1/8支持PoE+。
- 硬件交换机允许端口之间的线速通信(例如：摄像头进入本地服务器)。


### Firepower 6.5附件

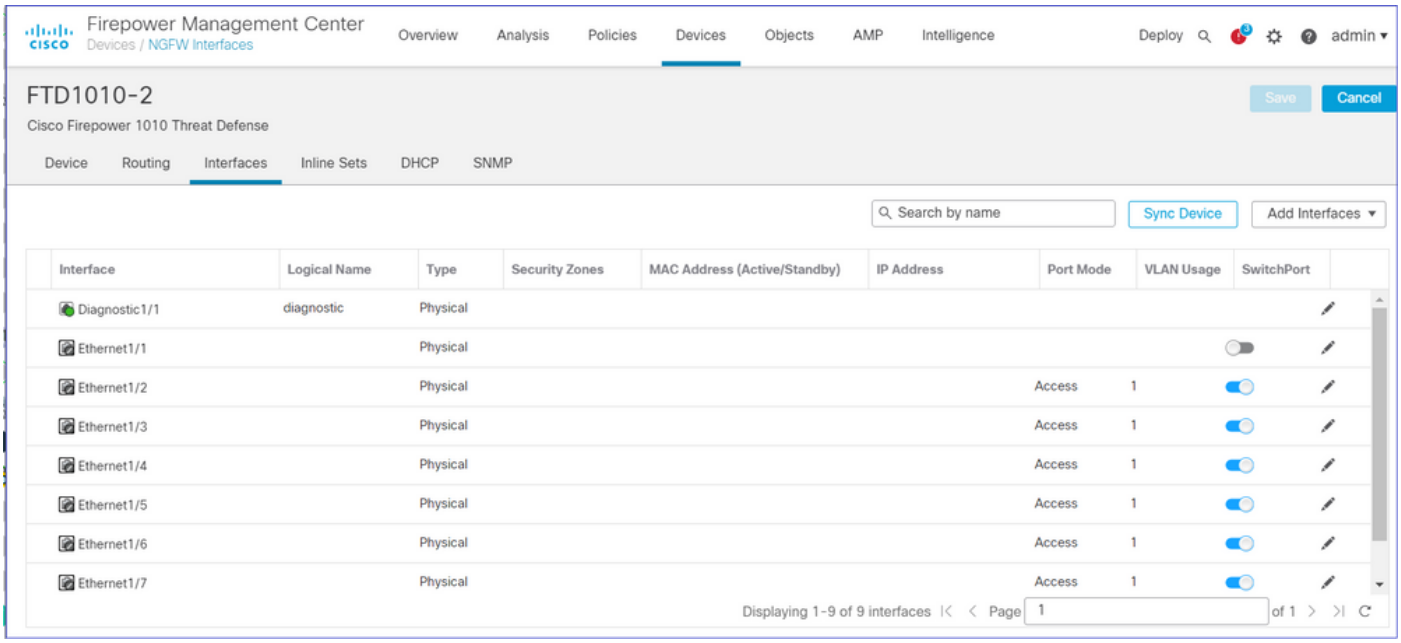
- 介绍一种称为交换虚拟接口(SVI)的新型接口。
- 混合模式:接口可以在交换(L2)或非交换(L3)模式下配置。
- L3模式接口将所有数据包转发到安全应用。
- 如果两个端口属于同一VLAN，则L2模式端口可以在硬件中切换，从而提高吞吐量和延迟。需要路由或桥接的数据包将到达安全应用(例如：摄像头从互联网下载新固件)，并根据配置进行安全检查。
- L2物理接口可以与一个或多个SVI接口关联。
- L2模式接口可以处于接入或中继模式。
- 接入模式L2接口仅允许未标记流量。
- 中继模式L2接口允许标记流量。
- 本征VLAN支持中继模式L2接口。
- ASA CLI、ASDM、CSM、FDM、FMC经过增强，可支持新功能。

### FMC附件

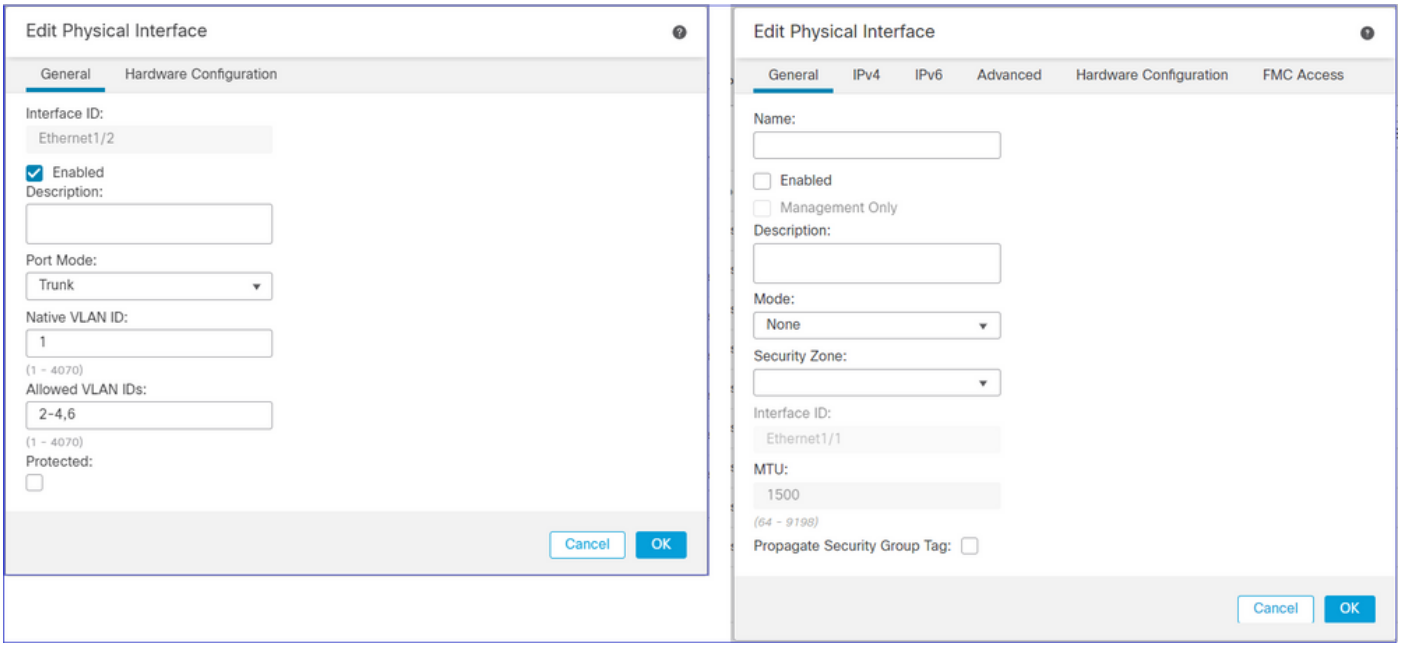
- 为物理接口引入了称为switchport的新接口模式，用于识别物理接口是L3接口还是L2接口。
- L2物理接口可以根据接入或中继模式与一个或多个VLAN接口关联。
- Firepower 1010在最后两个数据接口（即Ethernet1/7和Ethernet1/8）上支持以太网供电(PoE)配置。
- 交换和非交换之间的接口更改会清除除PoE和硬件配置之外的所有配置。

## 工作原理

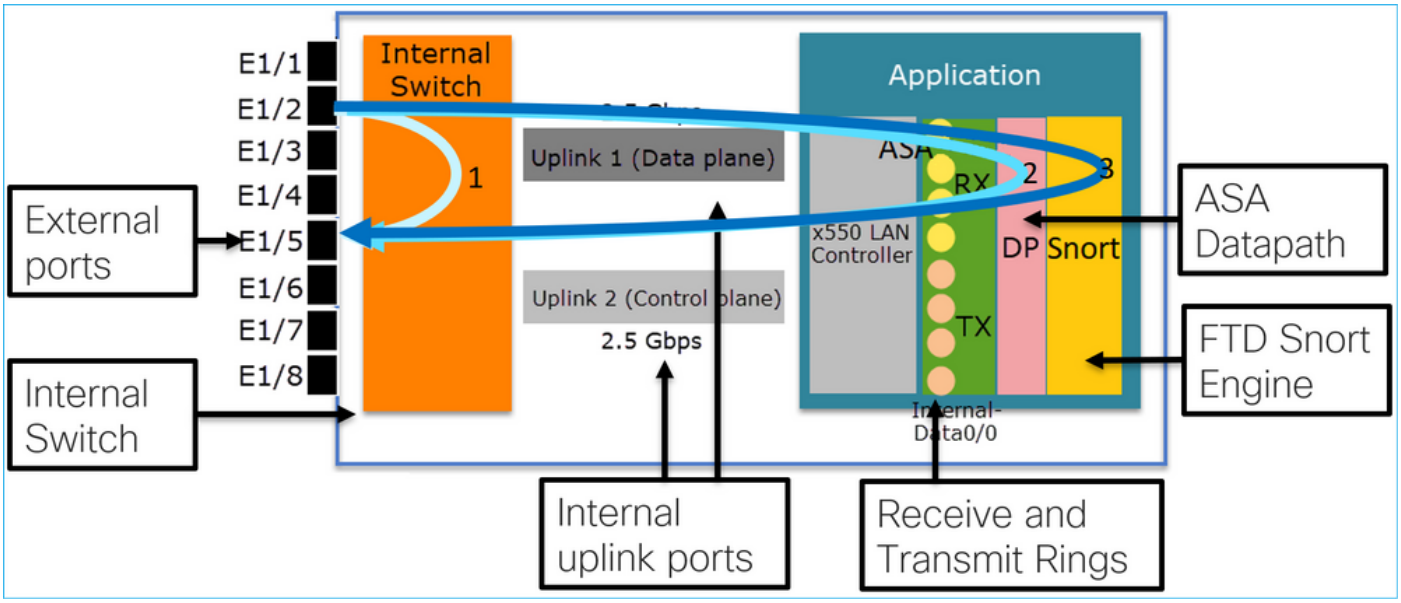
此功能只是对FMC(设备管理>接口页面)上现有接口支持的增强。




物理接口视图（L2和L3）




## FP1010架构




- 8个外部数据端口。
- 1个内部交换机。
- 3个上行链路端口（图中显示其中2个），一个用于数据平面，一个用于控制平面，一个用于配置。
- x550 LAN控制器（应用和上行链路之间的接口）。
- 4个接收(RX)和4个发送(TX)环。
- 数据路径进程（在ASA和FTD上）。
- Snort进程（在FTD上）。

### 数据包处理

影响数据包处理的两个主要因素：

1.接口/端口模式

2.应用的策略

数据包可以通过3种不同方式穿越FP1010:

1.仅由内部交换机处理

2.转发到应用(ASA/FTD)，仅由数据路径进程处理

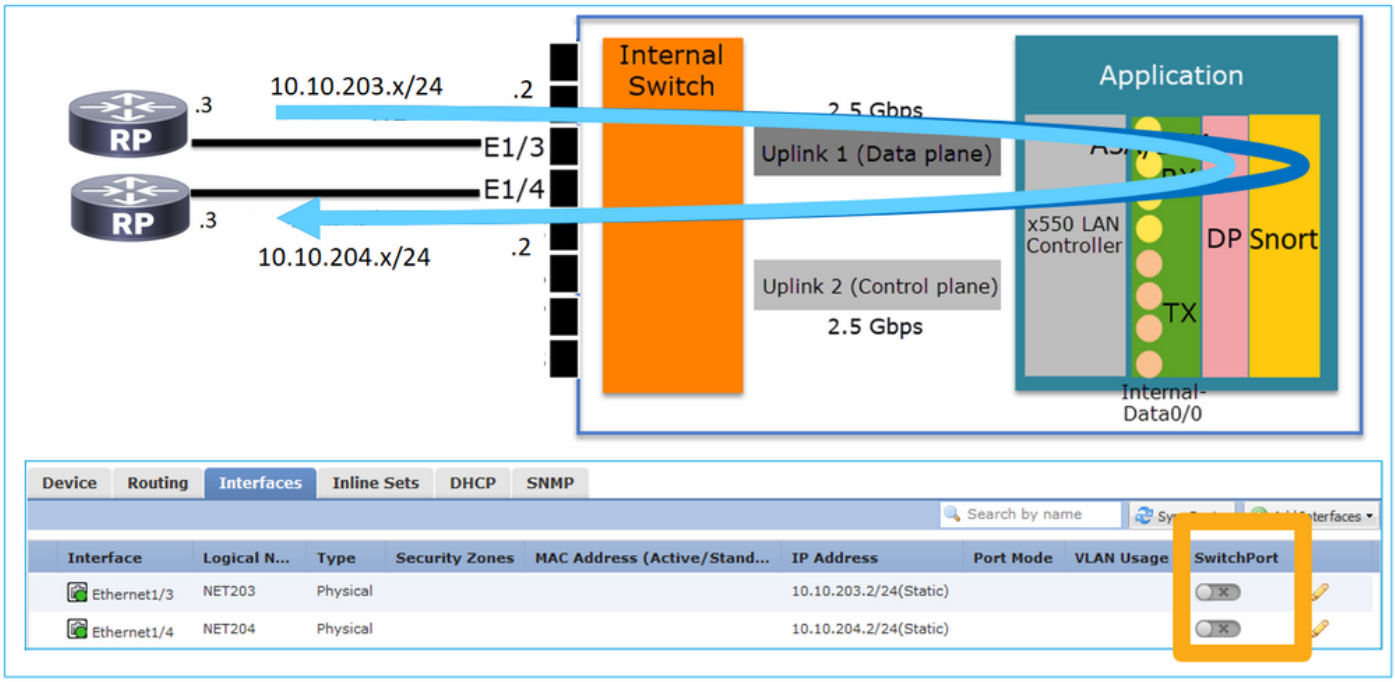
3.向上转发到应用(FTD)，并由数据路径和Snort引擎处理

## FP1010端口模式

UI示例用于FMC，CLI示例用于FTD。大多数概念也完全适用于ASA。

### FP1010案例1.路由端口（IP路由）

#### 配置和操作



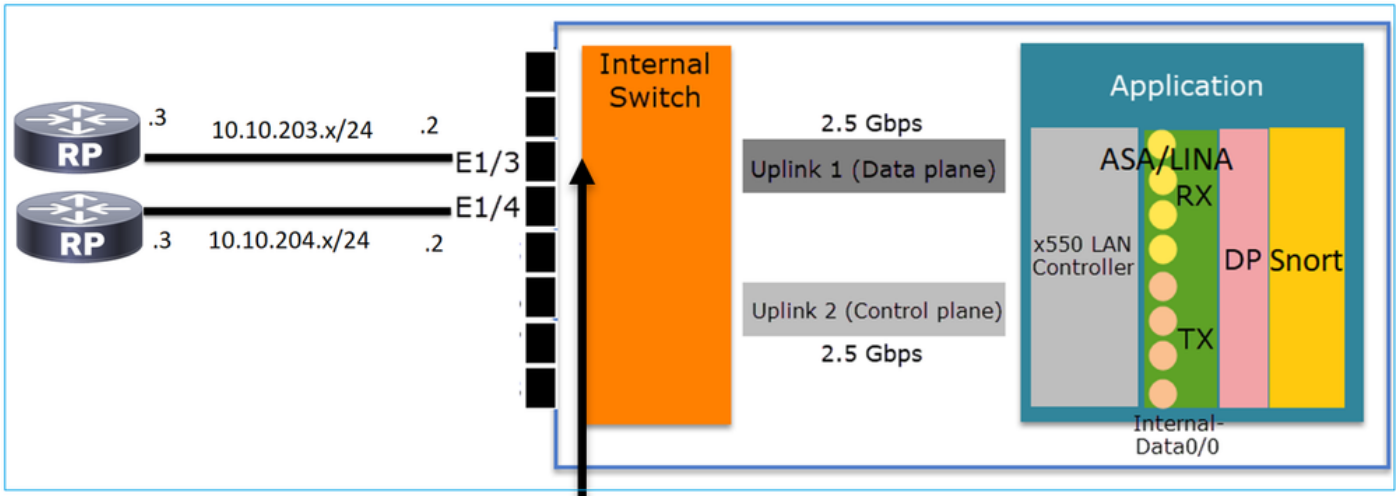

## 要点

- 从设计角度来看，这2个端口属于2个不同的L2子网。
- 在路由模式下配置端口时，数据包由应用（ASA或FTD）处理。
- 对于FTD，根据规则操作（例如ALLOW），数据包甚至可以由Snort引擎检查。

## FTD接口配置

```
interface Ethernet1/3 nameif NET203
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
security-level 0
 ip address 10.10.203.2 255.255.255.0
!
interface Ethernet1/4 nameif NET204
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
security-level 0
 ip address 10.10.204.2 255.255.255.0
```

## FP1010路由端口验证



从FXOS CLI可以检查物理接口计数器。本示例显示E1/3端口上的入口单播和出口单播计数器：

```
FP1010(local-mgmt)# show portmanager counters ethernet 1 3 | egrep
"stats.ing_unicastframes\|stats.egr_unicastframes"
stats.ing_unicastframes         = 3521254 stats.egr_unicastframes         = 604939
```

可以应用FTD数据路径捕获并跟踪数据包：

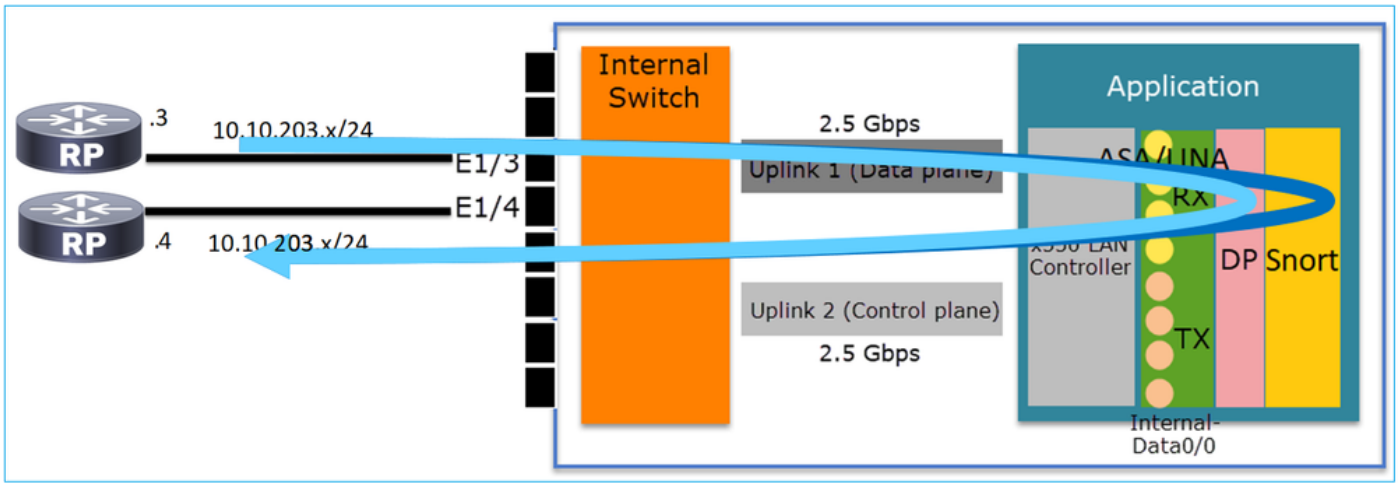
```
FP1010# show capture
capture CAP203 type raw-data trace interface NET203 [Capturing - 185654 bytes]
```

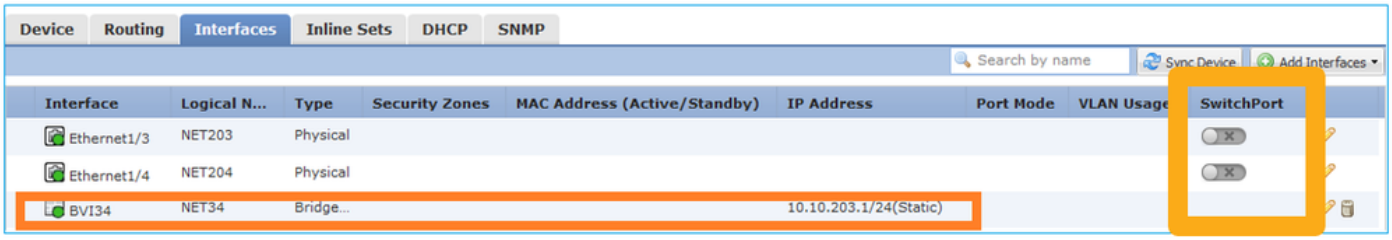
这是捕获片段。如预期，数据包会根据ROUTE LOOKUP进行转发：

```
FP1010# show capture CAP203 packet-number 21 trace

21: 06:25:23.924848       10.10.203.3 > 10.10.204.3 icmp: echo request
…
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.10.204.3 using egress ifc  NET204
```

## FP1010案例2.网桥组模式（桥接）

### 配置和操作




### 要点

- 从设计角度来看，两个端口连接到同一L3子网（类似于透明防火墙），但VLAN不同。
- 在桥接模式下配置端口时，数据包由应用（ASA或FTD）处理。

- 对于FTD，根据规则操作（例如ALLOW），数据包甚至可以由Snort引擎检查。

### FTD接口配置

```
interface Ethernet1/3 bridge-group 34 nameif NET203
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
security-level 0
!
interface Ethernet1/4 bridge-group 34 nameif NET204
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
!
interface BVI34 nameif NET34 security-level 0 ip address 10.10.203.1 255.255.255.0
```

### FP1010网桥组端口验证

此命令显示BVI 34的接口成员：

```
FP1010# show bridge-group 34
 Interfaces:
 Ethernet1/3 Ethernet1/4
 Management System IP Address:  10.10.203.1 255.255.255.0
 Management Current IP Address: 10.10.203.1 255.255.255.0
 Management IPv6 Global Unicast Address(es):    N/A
 Static mac-address entries:  0
 Dynamic mac-address entries: 13
```

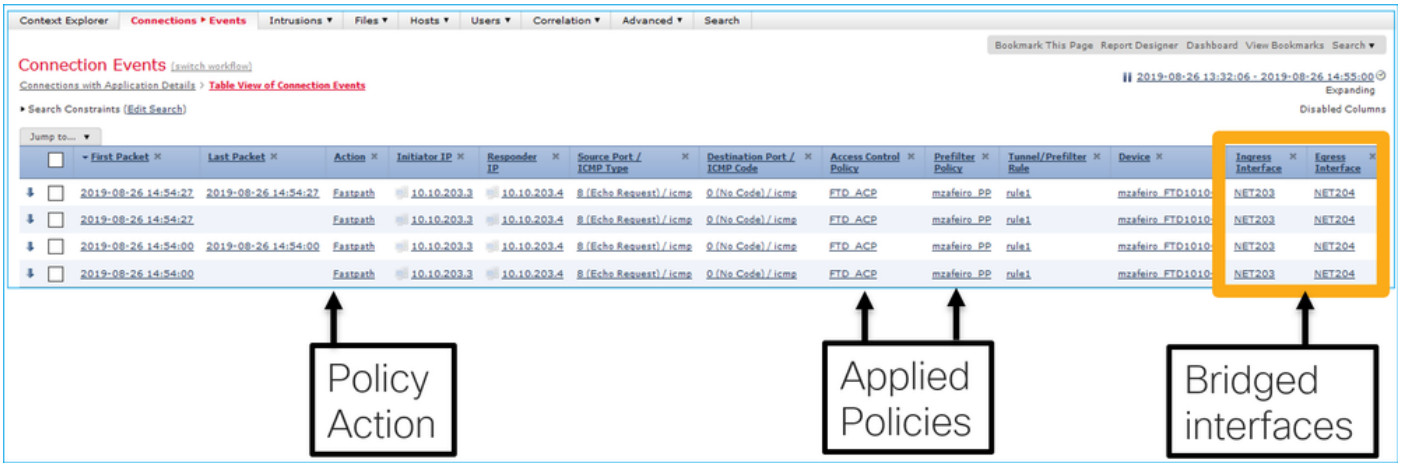
此命令显示ASA/FTD数据路径内容可寻址存储器(CAM)表：

```
FP1010# show mac-address-table
interface mac address     type       Age(min)    bridge-group
-----------------------------------------------------------------
NET203 0050.5685.43f1   dynamic      1             34
NET204 4c4e.35fc.fcd8   dynamic      3             34
NET203                     0050.56b6.2304   dynamic      1             34
NET204                     0017.dfd6.ec00   dynamic      1             34
NET203                     0050.5685.4fda   dynamic      1             34
```

数据包跟踪代码段显示数据包是根据目的MAC L2查找转发的：

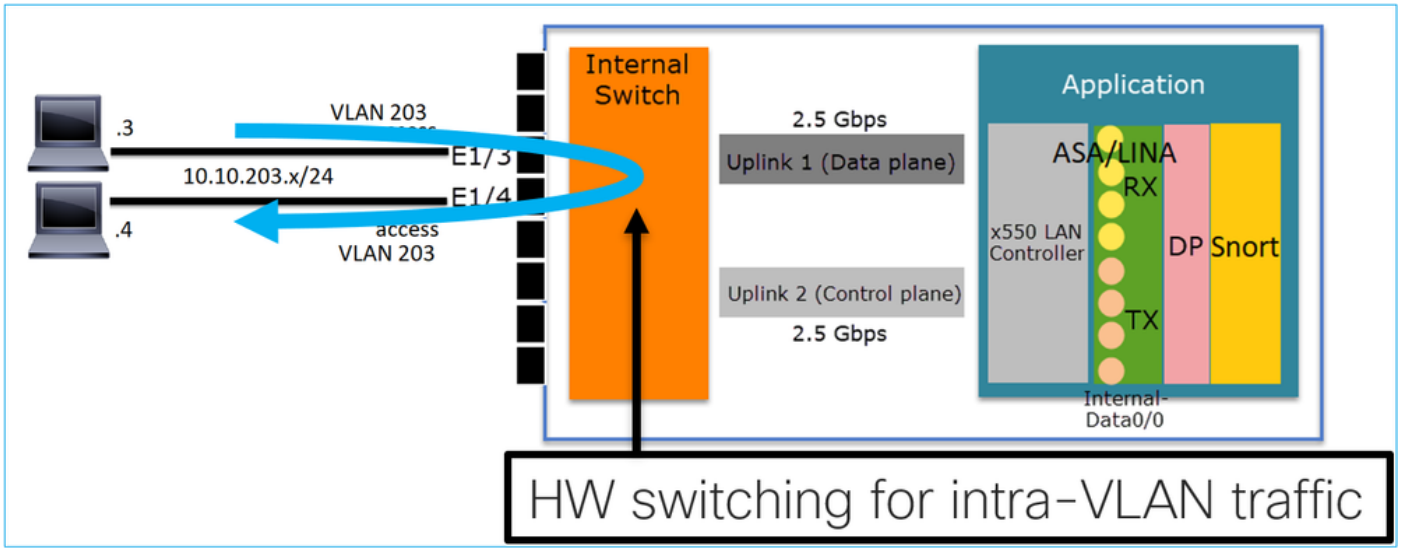
```
FP1010# show cap CAP203 packet-number 1 trace

2 packets captured

1: 11:34:40.277619 10.10.203.3 > 10.10.203.4 icmp: echo request
Phase: 1
Type: L2-EGRESS-IFC-LOOKUP Subtype: Destination MAC L2 Lookup
Result: ALLOW
Config:
Additional Information:
DestinationMAC lookup resulted in egress ifc NET204
```

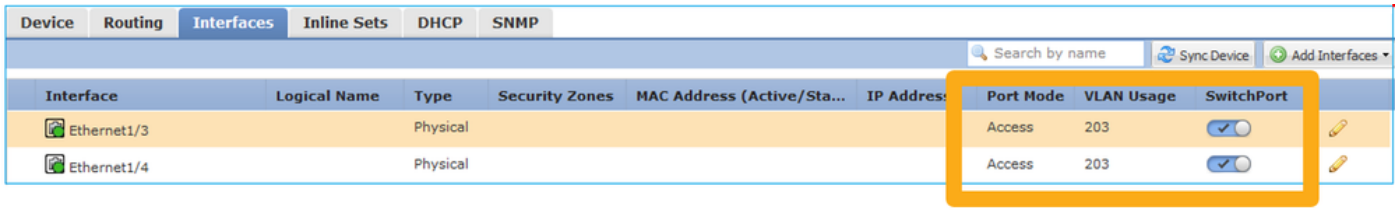
对于FTD，FMC连接事件还可提供有关流量检查和传输网桥组接口的信息：




## FP1010机箱3.接入模式下的交换机端口（硬件交换）

### 配置和操作




### 要点

- 硬件交换是FTD **6.5+和**ASA 9.**13+功**能。
- 从设计角度来看，两个端口连接到同一L3子网和同一VLAN。
- 此场景中的端口在接入模式下运行（仅无标记流量）。
- 在SwitchPort模式下配置的防火墙端口没有配置逻辑名称(nameif)。
- 当端口在交换模式下配置并属于同一VLAN（VLAN内流量）时，数据包仅由FP1010内部交换机处理。

### FTD接口配置

从CLI的角度来看，配置与L2交换机非常相似：

```
interface Ethernet1/3 switchport switchport access vlan 203 ! interface Ethernet1/4 switchport
```

```
switchport access vlan 203
```

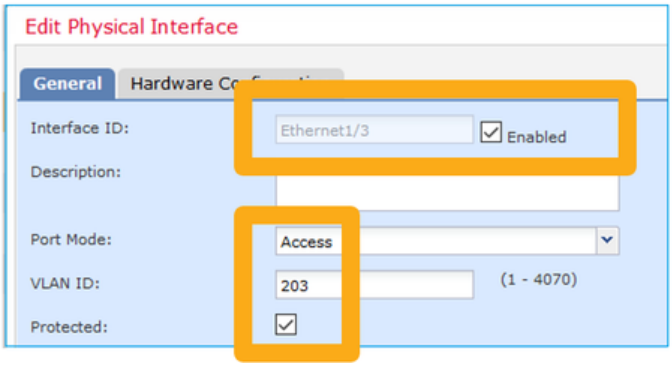
## 过滤VLAN内流量

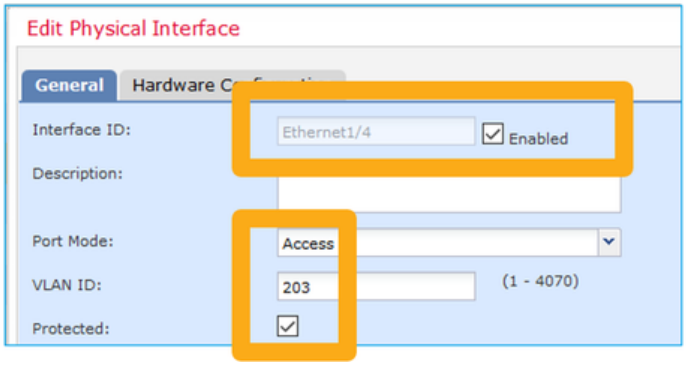
挑战:**ACL无法过滤VLAN内流量！**

解决方案:**受保护**端口

原则很简单：2个配置为“受保护”的端口无法相互通信。

FMC UI（在受保护端口的情况下）：




## FTD接口配置

命令**switchport protected**在接口下配置：

```
interface Ethernet1/3
 switchport
 switchport access vlan 203
 switchport protected
!
interface Ethernet1/4
 switchport
 switchport access vlan 203
 switchport protected
```

## FP1010交换机端口验证

在本示例中，发送了1000个单播数据包(ICMP)，其大小为特定大小（1100字节）：

```
router# ping 10.10.203.4 re 1000 timeout 0 size 1100
```

要检查中转接口的入口和出口单播计数器，请使用以下命令：

```
FP1010(local-mgmt)# show portmanager counters ethernet 1 3 | egrep
"stats.ing_unicastframes\|stats.bytes_1024to1518_frames"
stats.ing_unicastframes         = 146760
stats.bytes_1024to1518_frames   = 0
FP1010(local-mgmt)# show portmanager counters ethernet 1 4 | egrep
"stats.egr_unicastframes\|stats.bytes_1024to1518_frames"
stats.bytes_1024to1518_frames   = 0
stats.egr_unicastframes         = 140752
FP1010(local-mgmt)# show portmanager counters ethernet 1 3 | egrep
"stats.ing_unicastframes\|stats.bytes_1024to1518_frames"
```

```
stats.ing_unicastframes        = 147760 <------------------ Ingress Counters got increased by
1000
stats.bytes_1024to1518_frames  = 1000 <------------------ Ingress Counters got increased by 1000
FP1010(local-mgmt)# show portmanager counters ethernet 1 4 | egrep
"stats.egr_unicastframes\|stats.bytes_1024to1518_frames"
stats.bytes_1024to1518_frames  = 0 <------------------ No egress increase
stats.egr_unicastframes        = 140752 <------------------ No egress increase
```

此命令显示内部交换机VLAN状态：

```
FP1010# show switch vlan
VLAN Name            Status    Ports
---- --------------- --------- ----------------------
1     -              down
203 - up Ethernet1/3, Ethernet1/4
```

只要至少为VLAN分配一个端口，VLAN的状态就为UP

如果端口管理性关闭或连接的交换机端口关闭/电缆断开，并且这是分配给VLAN的唯一端口，则VLAN状态也关闭：

```
FP1010-2# show switch vlan
VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    -                                   down 201  net201                                down
Ethernet1/1 <--- e1/1 was admin down 202  net202                              down Ethernet1/2 <---
upstream switch port is admin down
```

此命令显示内部交换机的CAM表：

```
FP1010-2# show switch mac-address-table
Legend: Age - entry expiration time in seconds

   Mac Address  | VLAN |            Type          | Age | Port
-------------------------------------------------------------
 4c4e.35fc.0033 | 0203 |          dynamic         | 282 | Et1/3
 4c4e.35fc.4444 | 0203 |          dynamic         | 330 | Et1/4
```

内部交换机CAM表默认老化时间为5分30秒。

FP1010包含2个CAM表：

1. **内部交换机CAM表**:用于硬件交换
2. **ASA/FTD数据路径CAM表**:用于桥接

每个通过FP1010的数据包/帧都根据端口模式由单个CAM表(内部交换机或FTD数据**路径**)进行处理。

> **警告**：请勿将SwitchPort模**式中使用的show switch mac-address-table** internal switch CAM表与桥接模**式中使用的**show mac-address-table FTD datapath CAM表混淆

**硬件交换：需要注意的其他事项**

ASA/FTD数据路径日志不显示有关硬件交换流的信息：

```
FP1010# show log
FP1010#
```

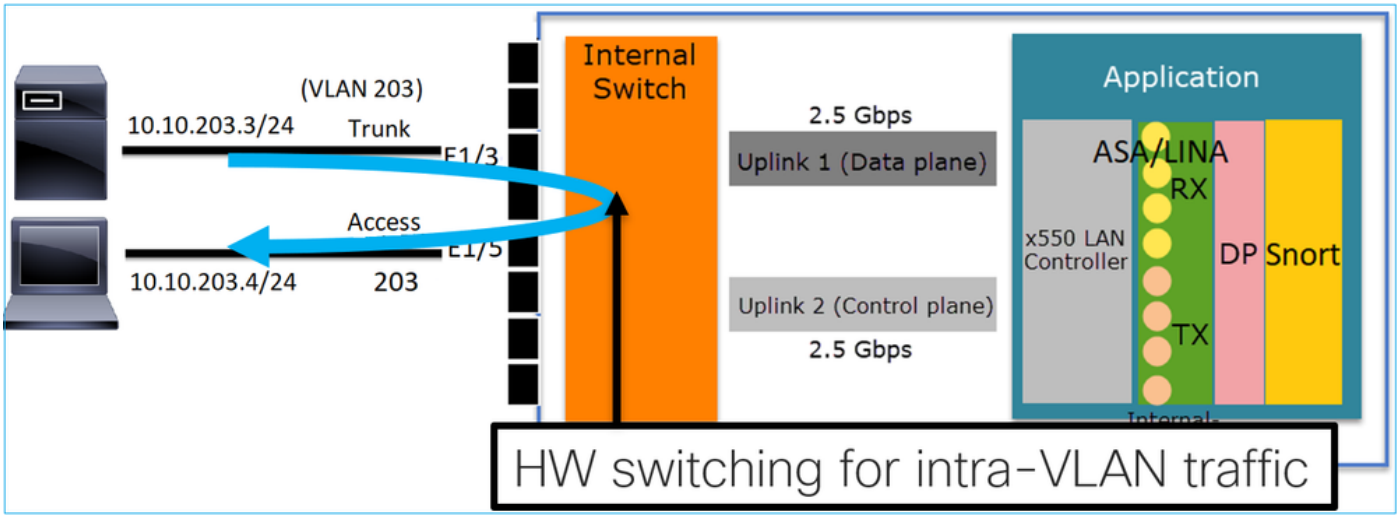
ASA/FTD数据路径连接表不显示硬件交换流：

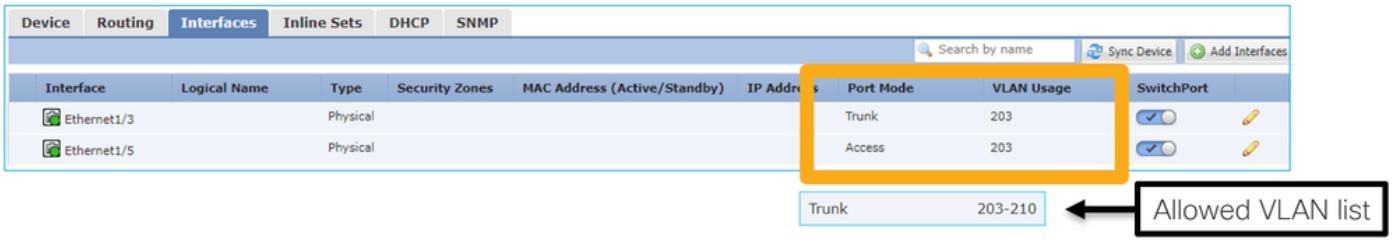
```
FP1010# show conn
0 in use, 3 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect
```

此外，FMC连接事件不显示硬件交换流。

## FP1010机箱4.交换机端口（中继）

### 配置和操作




### 要点

- 硬件交换是FTD 6.5+和ASA 9.13+功能。
- 从设计角度来看，两个端口连接到同一L3子网和同一VLAN。
- 中继端口接受已标记帧和未标记帧（如果为本征VLAN）。
- 当端口在交换模式下配置并属于同一VLAN（VLAN内流量）时，数据包仅由内部交换机处理。

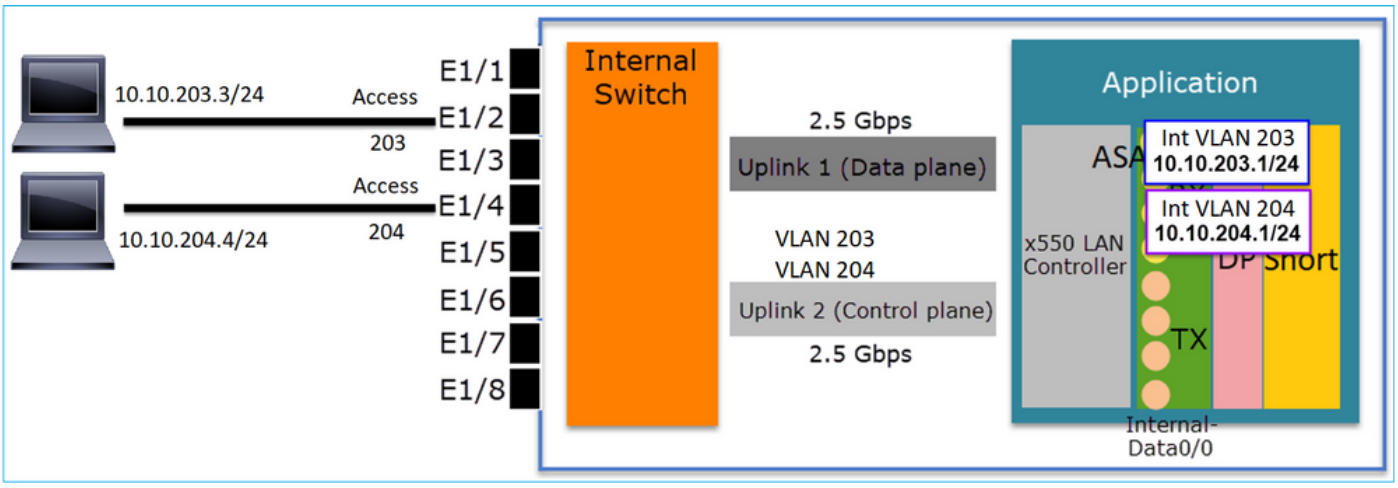
### FTD接口配置

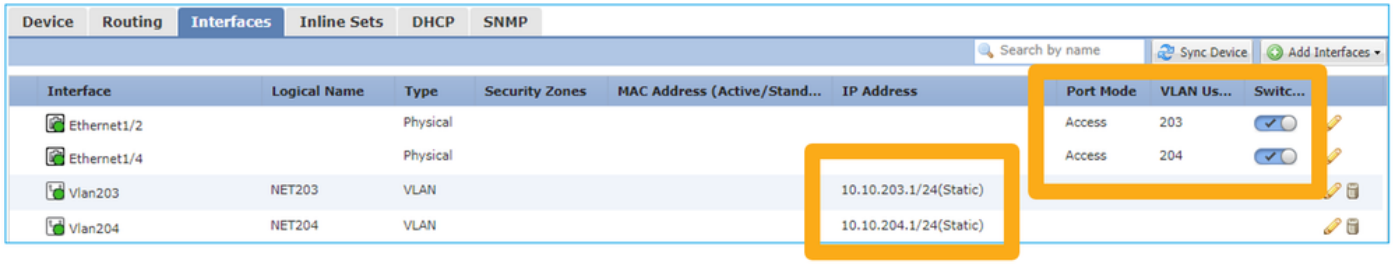
配置类似于第2层交换机端口：

```
interface Ethernet1/3 switchport switchport trunk allowed vlan 203 switchport trunk native vlan
1 switchport mode trunk
!
interface Ethernet1/5
 switchport
 switchport access vlan 203
```

# FP1010案例5.交换机端口（VLAN间）

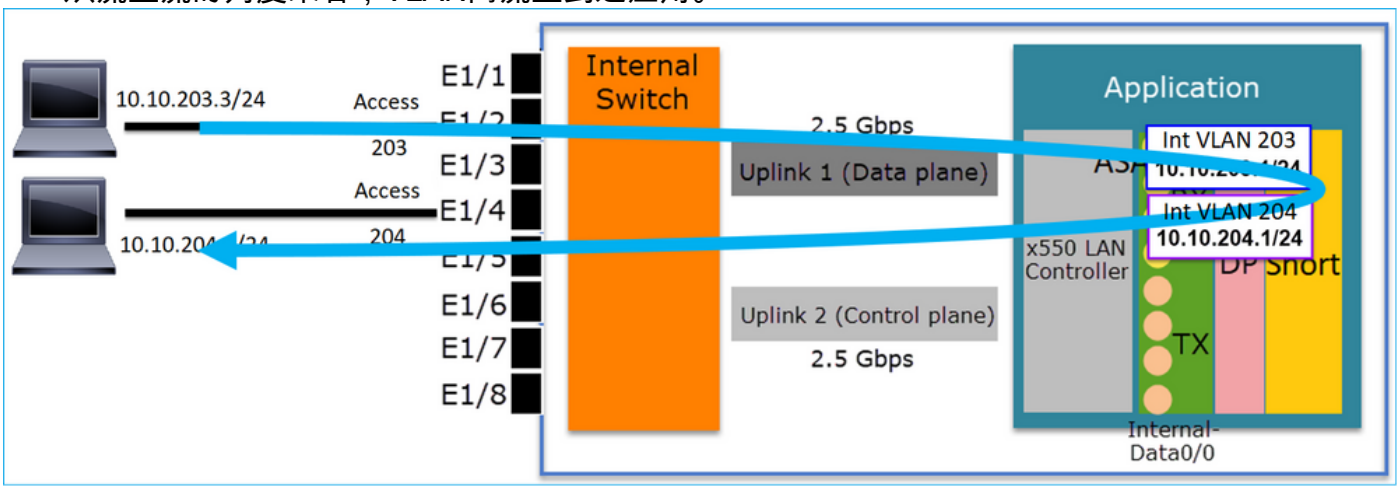
## 配置和操作




## 要点

- 从设计角度来看，2个端口连接到2个不同的L3子网和2个不同的VLAN。
- VLAN之间的流量通过VLAN接口（类似于SVI）。
- 从流量流的角度来看，VLAN间流量到达应用。




## FTD接口配置

配置类似于交换机虚拟接口(SVI):

```
interface Ethernet1/2
 switchport switchport access vlan 203
interface Ethernet1/4
 switchport switchport access vlan 204
!
```

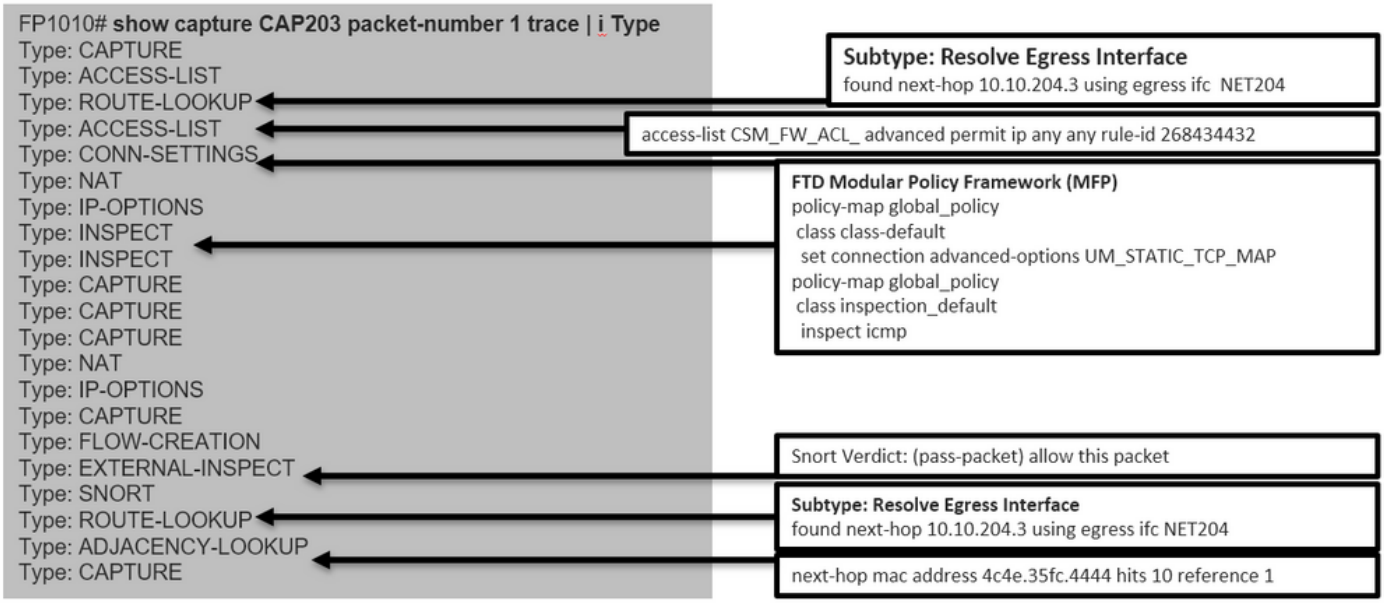
```
interface Vlan203 nameif NET203 security-level 0 ip address 10.10.203.1 255.255.255.0
interface Vlan204 nameif NET204 security-level 0 ip address 10.10.204.1 255.255.255.0
```

### VLAN间流量的数据包处理

这是通过两个不同VLAN的数据包的跟踪：

```
FP1010# show capture CAP203 packet-number 1 trace | include Type
Type: CAPTURE
Type: ACCESS-LIST
Type: ROUTE-LOOKUP
Type: ACCESS-LIST
Type: CONN-SETTINGS
Type: NAT
Type: IP-OPTIONS
Type: INSPECT
Type: INSPECT
Type: CAPTURE
Type: CAPTURE
Type: CAPTURE
Type: NAT
Type: IP-OPTIONS
Type: CAPTURE
Type: FLOW-CREATION
Type: EXTERNAL-INSPECT
Type: SNORT
Type: ROUTE-LOOKUP
Type: ADJACENCY-LOOKUP
Type: CAPTURE
```

数据包流程的主要阶段：




## FP1010案例6. VLAN间过滤器

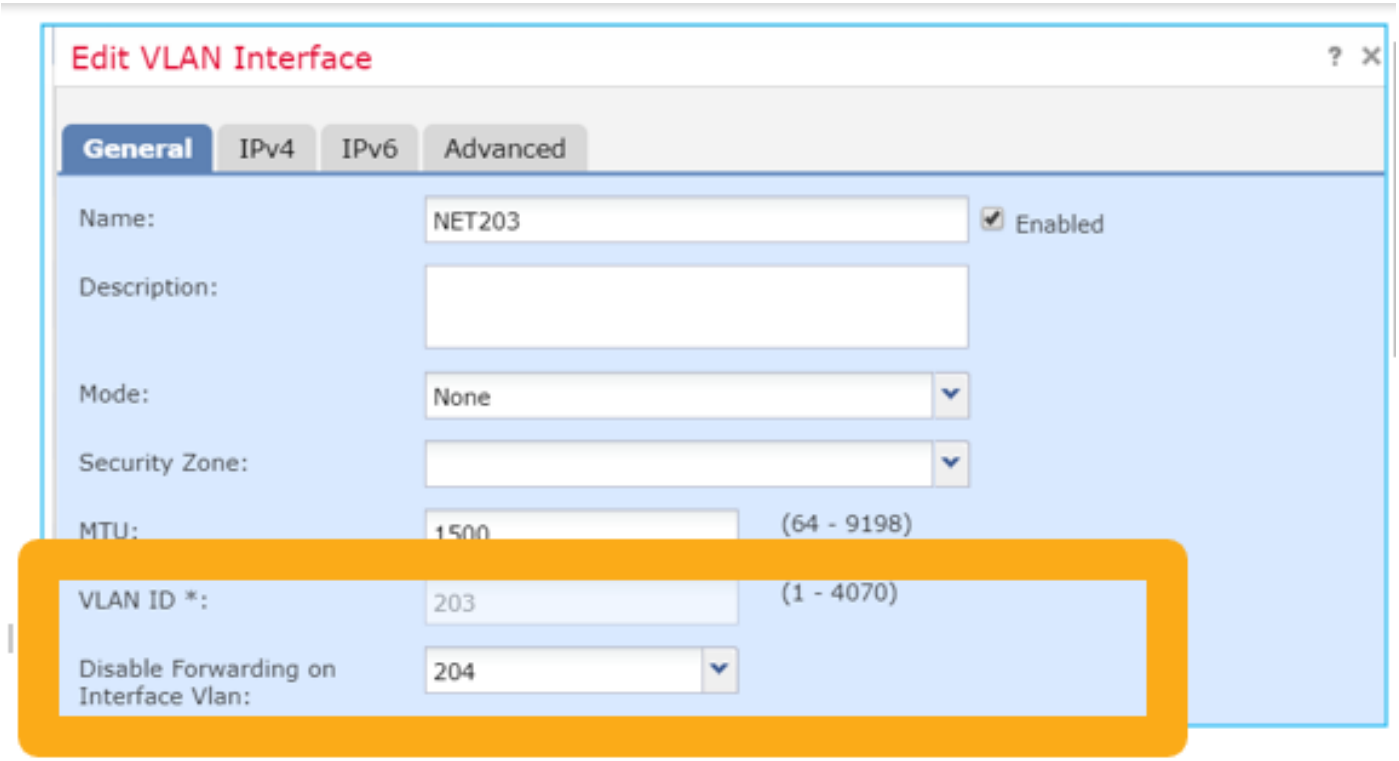
### 配置和操作

过滤VLAN间流量有2个主要选项：

1. 访问控制策略
2. 'no forward'命令

## 使用“no forward”命令过滤VLAN间流量

FMC UI配置：




### 要点

- no forward drop是单向的。
- 它不能应用于两个VLAN接口。
- 在ACL检查之前，将完成no forward检查。

### FTD接口配置

本例中的CLI配置为：

```
interface Vlan203
no forward interface Vlan204
 nameif NET203
 security-level 0
 ip address 10.10.203.1 255.255.255.0
!
interface Vlan204
 nameif NET204
 security-level 0
 ip address 10.10.204.1 255.255.255.0
```

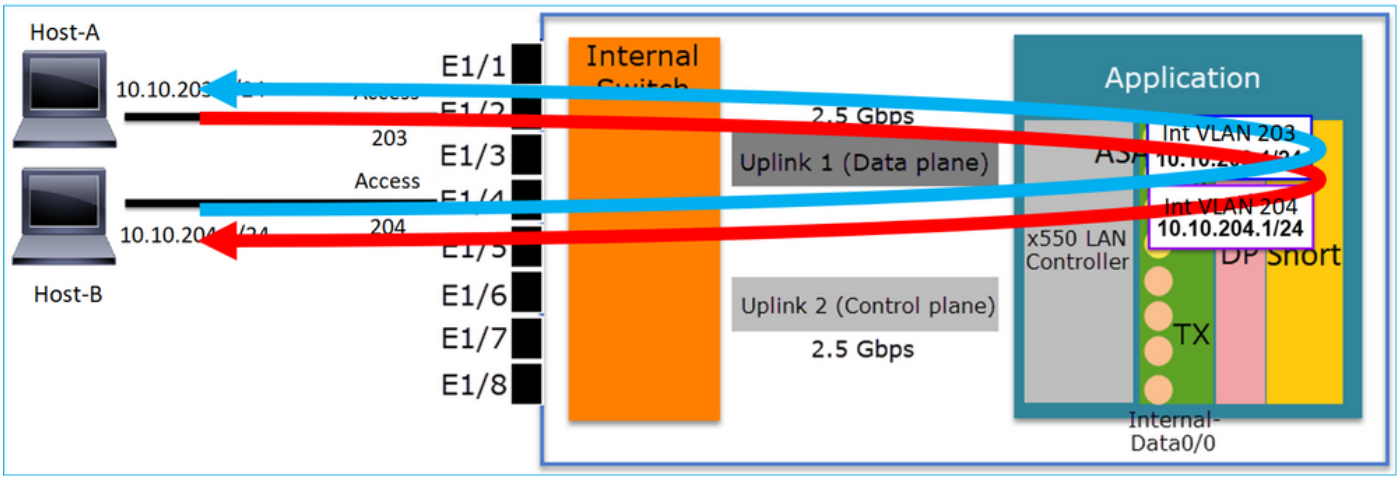
如果数据包被无转发功能丢弃，则生成ASA/FTD数据路径系统日志消息：

```
FP1010# show log
Sep 10 2019 07:44:54: %FTD-5-509001: Connection attempt was prevented by "no forward" command:
icmp src NET203:10.10.203.3 dst NET204:10.10.204.3 (type 8, code 0)
```

从加速安全路径(ASP)下拉视点来看，它被视为ACL下拉：

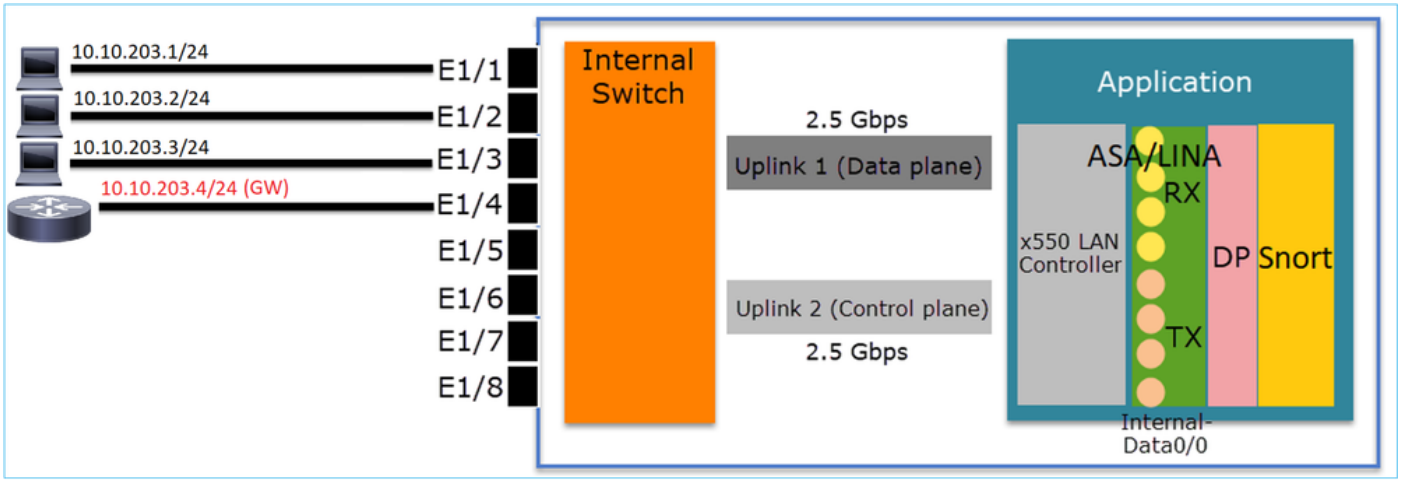
```
FP1010-2# show asp drop
Frame drop:
Flow is denied by configured rule (acl-drop) 1
```

由于丢弃是单向的，因此主机A(VLAN 203)无法发起到主机B(VLAN 204)的流量，但允许相反的流量：




## 案例研究 — FP1010。桥接与硬件交换+桥接

请考虑以下拓扑：



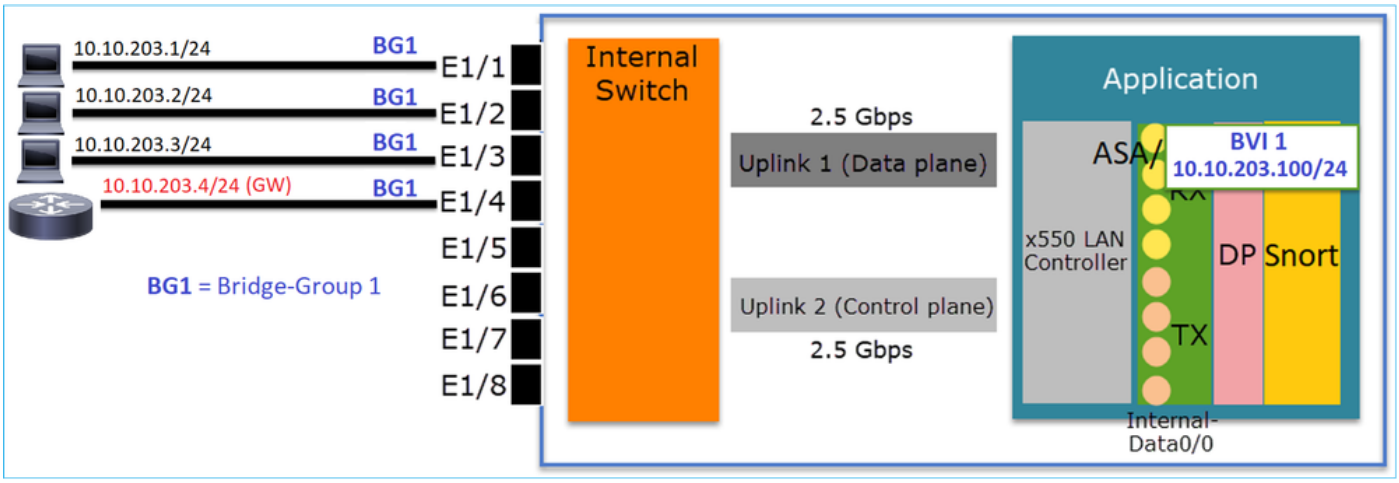

在此拓扑中：

- 三台终端主机属于同一L3子网(10.10.203.x/24)。
- 路由器(10.10.203.4)在子网中充当GW。

在此拓扑中有2个主要设计选项：

1. 桥接
2. 硬件交换+桥接

**设计选项1.桥接**

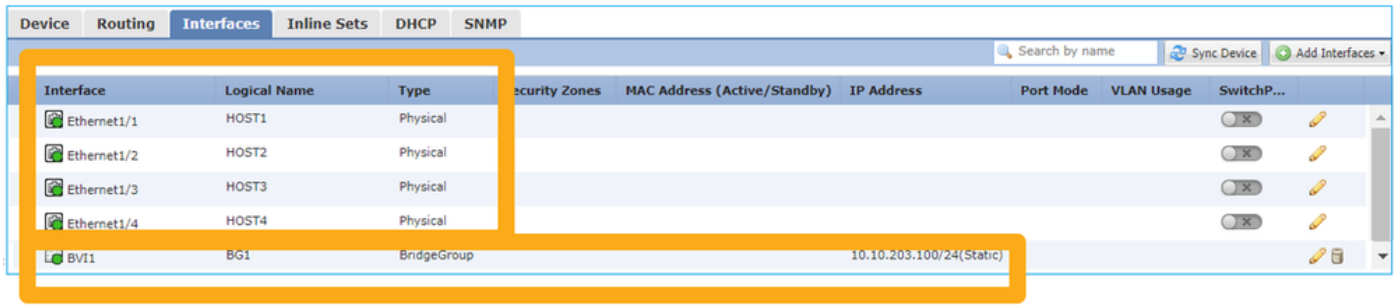



## 要点

本设计的要点是：

- BVI 1与4台连接的设备在同一子网(10.10.203.x/24)中使用IP创建。
- 所有四个端口属于同一网桥组（本例中为组1）。
- 四个端口中的每个端口都配置了名称。
- 主机到主机和主机到网关的通信通过应用（例如FTD）。

从FMC UI的角度来看，配置为：

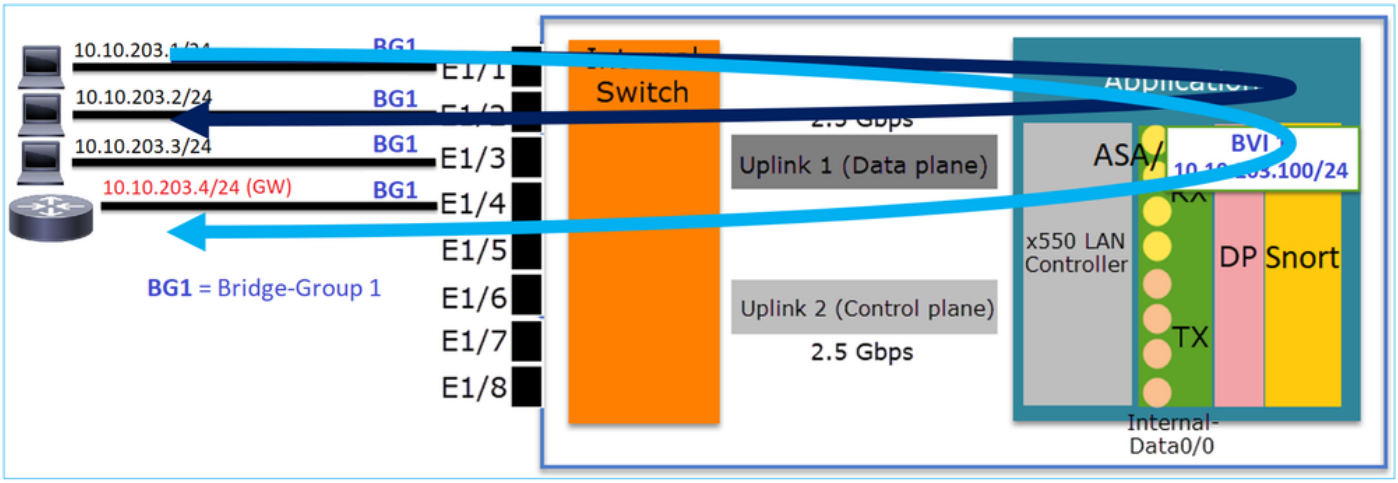



## FTD接口配置

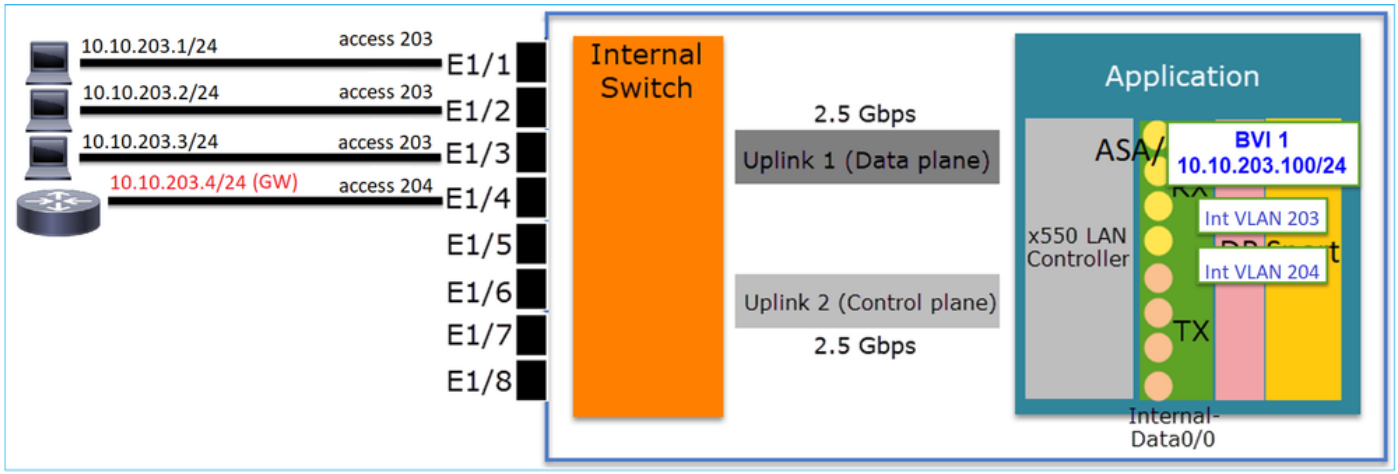
本例中的配置为：

```
interface BVI1 nameif BG1 security-level 0 ip address 10.10.203.100 255.255.255.0
interface Ethernet1/1
 no switchport bridge-group 1 nameif HOST1
interface Ethernet1/2
 no switchport
 bridge-group 1
 nameif HOST2
interface Ethernet1/3
 no switchport
 bridge-group 1
 nameif HOST3
interface Ethernet1/4
 no switchport
 bridge-group 1
 nameif HOST4
```

此场景中的流量：




**设计选项2.硬件交换+桥接**

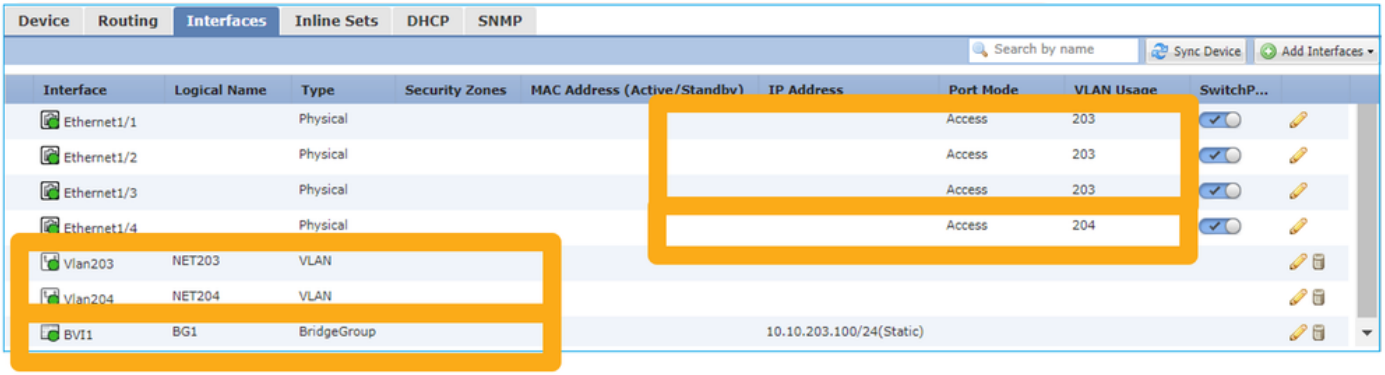



**要点**

本设计的要点是：

- BVI 1与4台连接的设备在同一子网(10.10.203.x/24)中使用IP创建。
- 连接到终端主机的端口在SwitchPort模式下配置，并属于同一VLAN(203)。
- 连接到GW的端口在SwitchPort模式下配置，属于不同的VLAN(204)。
- 有2个VLAN接口(203、204)。 2个VLAN接口没有分配IP，属于网桥组1。
- 主机到主机的通信仅通过内部交换机。
- 主机到网关的通信通过应用（例如FTD）。

FMC UI配置：

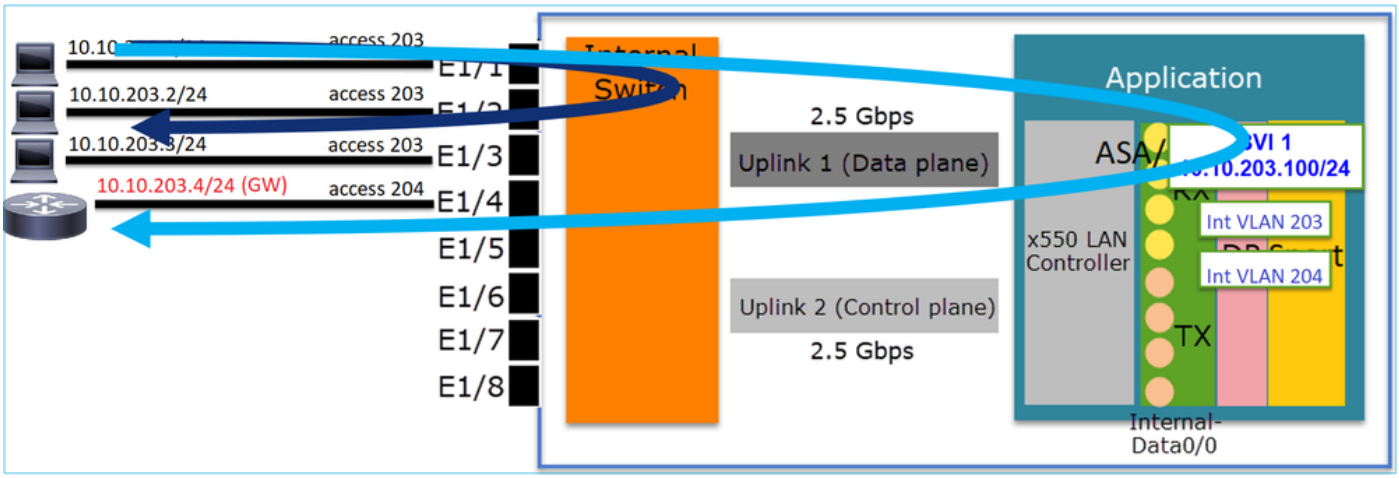


### FTD接口配置

本例中的配置为：

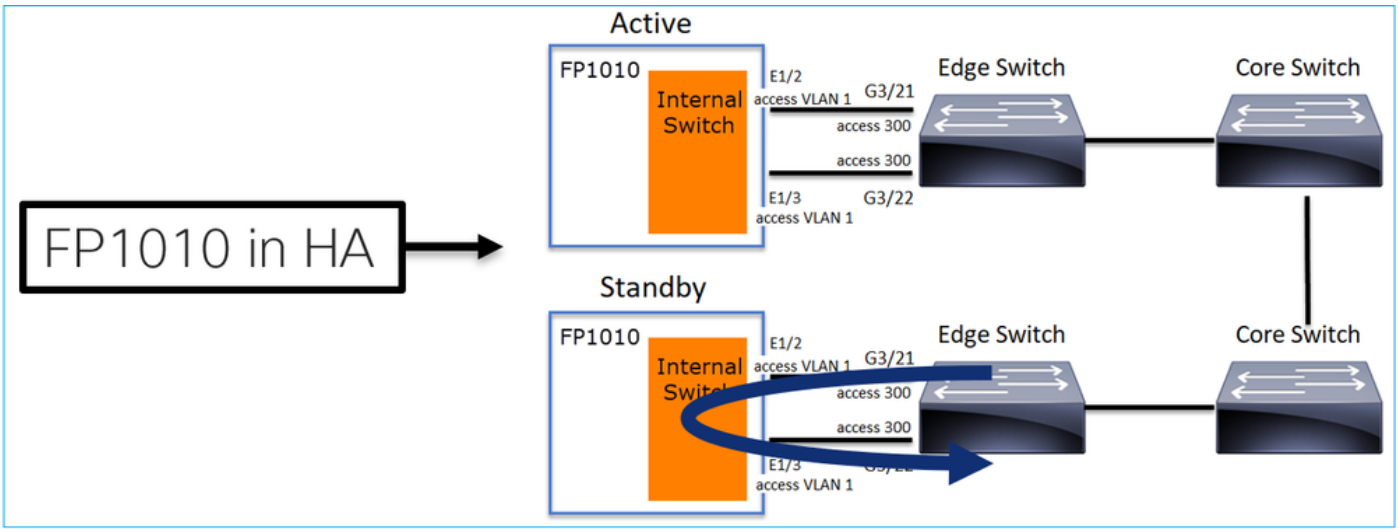
```
interface Ethernet1/1
 switchport switchport access vlan 203
interface Ethernet1/2
 switchport switchport access vlan 203
interface Ethernet1/4
 switchport switchport access vlan 204
!
interface Vlan203
 bridge-group 1 nameif NET203
interface Vlan204
 bridge-group 1 nameif NET204
!
interface BVI1 nameif BG1 ip address 10.10.203.100 255.255.255.0
```

主机到主机通信与主机到GW通信：




## FP1010设计注意事项

### 交换和高可用性(HA)




在HA环境中配置硬件交换时，存在2个主要问题：

1. 备用设备上的HW交换通过设备转发数据包。这可能导致流量环路。

2. 交换机端口不由HA监控

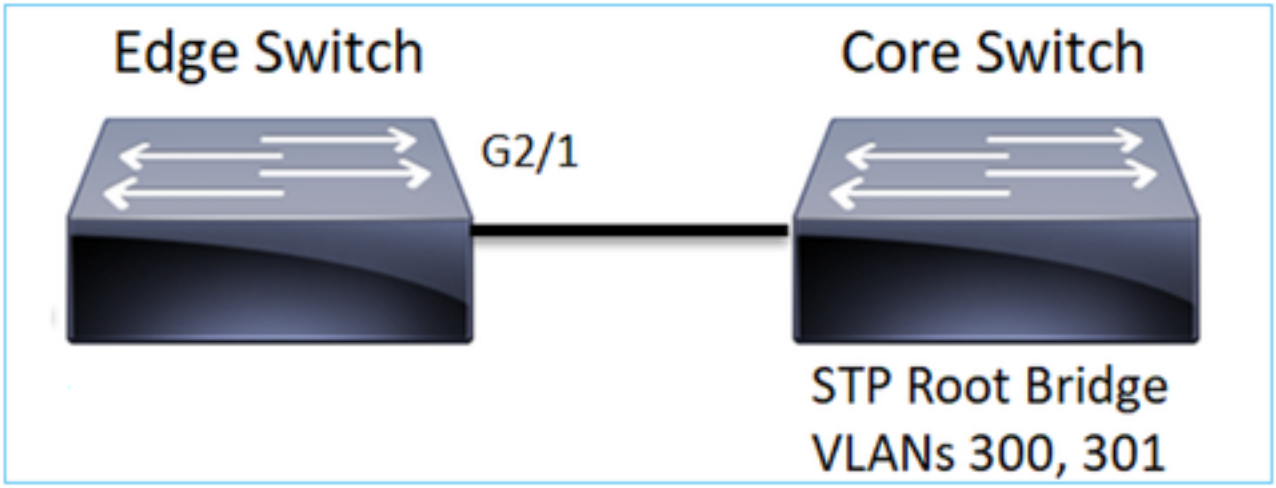
设计要求

- 您不得将SwitchPort功能与ASA/FTD高可用性结合使用。FMC配置指南中记录了以下内容：https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/regular_firewall_interfaces_for_firepower_threat_defense.html#topic_kqm_dgc_b3b


**与生成树协议(STP)的交互**

FP1010内部交换机不运行STP。

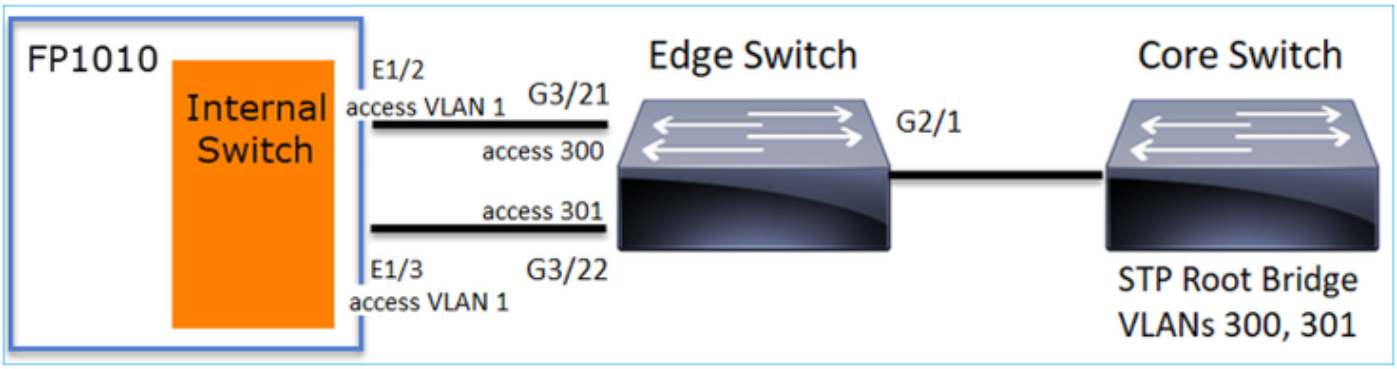
请考虑以下场景：




在边缘交换机上，两个VLAN的根端口是G2/1:

```
Edge-Switch# show spanning-tree root | i 300|301
VLAN0300         33068 0017.dfd6.ec00         4    2   20  15  Gi2/1
VLAN0301  33069 0017.dfd6.ec00         4    2   20  15  Gi2/1
```

将FP1010连接到边缘交换机，并在同一VLAN（硬件交换）中配置两个端口：



问题

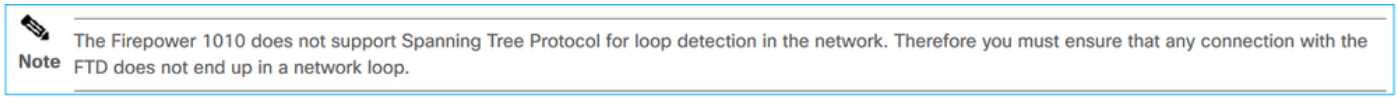
- 由于G3/22上收到的VLAN 301的VLAN泄漏的上级BPDU

```
Edge-Switch# show spanning-tree root | in 300|301
VLAN0300         33068 0017.dfd6.ec00         4    2   20  15  Gi2/1
VLAN0301         33068 0017.dfd6.ec00         8    2   20  15  Gi3/22
```

**警告**：如果将L2交换机连接到FP1010，则可以影响STP域

FMC配置指南中也记录了这一点：

https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/regular_firewall_interfaces_for_firepower_threat_defense.html#task_rzl_bfc_b3b




## FXOS REST API

### FMC REST API

以下是此功能支持的REST API:

- L2物理接口[支持的PUT/GET]

/api/fmc_config/v1/domain/{domainUUID}/devices/devicerecords/{containerUUID}/physicalinterfaces/{objectId}

- VLAN接口[支持POST/PUT/GET/DELETE]

/api/fmc_config/v1/domain/{domainUUID}/devices/devicerecords/{containerUUID}/vlaninterfaces/{objectId}

# 故障排除/诊断

## 诊断概述

- 日志文件在FTD/NGIPS故障排除或show tech输出中捕获。在进行故障排除时，需要查看以下项目以了解更多详细信息：
- /opt/cisco/platform/logs/portmgr.out
- /var/sysmgr/sam_logs/svc_sam_dme.log
- /var/sysmgr/sam_logs/svc_sam_portAG.log
- /var/sysmgr/sam_logs/svc_sam_appAG.log
- ASA运行配置
- /mnt/disk0/log/asa-appagent.log

**从FXOS（设备）— CLI收集数据**

对于FTD(SSH):

```
> connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.

...

FP1010-2# connect local-mgmt
FP1010-2(local-mgmt)#
```

对于FTD（控制台）：

```
> connect fxos
You came from FXOS Service Manager. Please enter 'exit' to go back.
> exit FP1010-2# connect local-mgmt
FP1010-2(local-mgmt)#
```

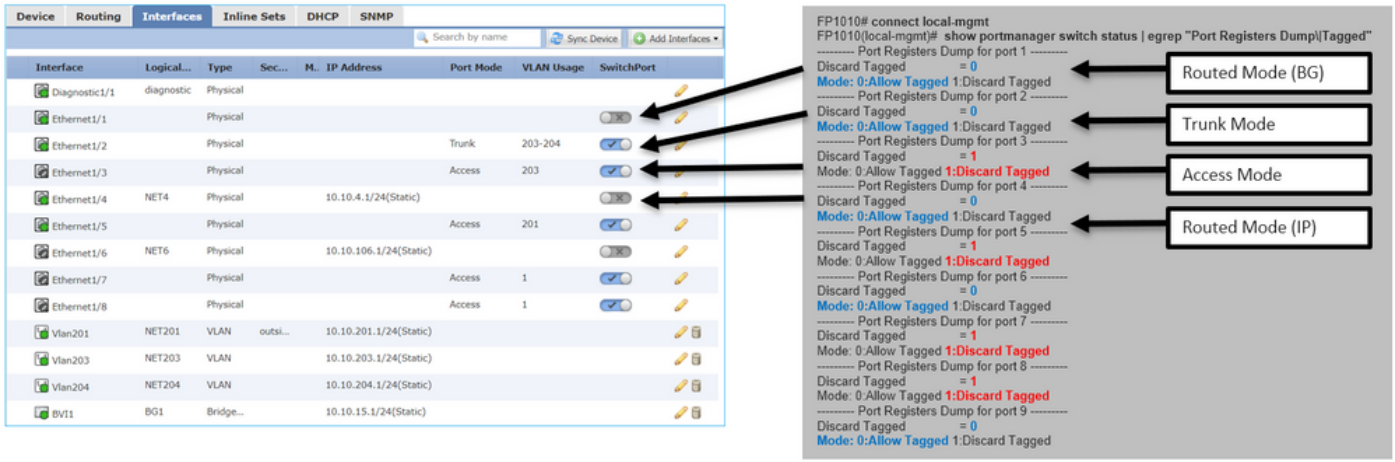
## FP1010后端

端口寄存器定义所有内部交换机和端口功能。

在此屏幕截图中，端口寄存器的“端口控制”部分显示，特别是指示接口上接收的已标记流量必须丢弃(1)还是允许(0)的寄存器。 以下是一个端口的完整注册部分：

```
FP1010-2# connect local-mgmt
FP1010-2(local-mgmt)# show portmanager switch status
...
---Port Control 2            regAddr=8 data=2E80--

Jumbo Mode                    = 2
Mode: 0:1522 1:2048 2:10240

802.1q mode                   = 3
Mode: 0:Disable 1:Fallback 2:Check 3:Secure

Discard Tagged = 1 Mode: 0:Allow Tagged 1:Discard Tagged

Discard Untagged = 0 Mode: 0:Allow Untagged 1:Discard Untagged ARP Mirror = 0 Mode: 1:Enable
0:Disable Egress Monitor Source = 0 Mode: 1:Enable 0:Disable Ingress Monitor Source = 0 Mode:
1:Enable 0:Disable Port default QPri = 0
```

在此屏幕截图中，您可以看到各种端口模式的各种丢弃标记寄存器值：

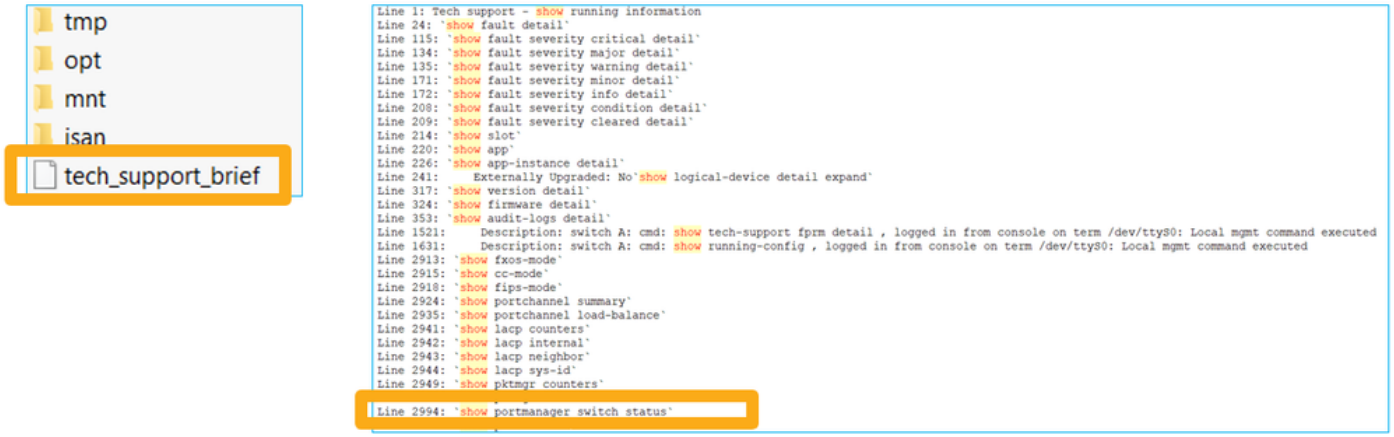



## 收集FPRM show技术（在FP1010上）

要生成FPRM捆绑包并将其上传到FTP服务器，请执行以下操作：

```
FP1010(local-mgmt)# show tech-support fprm detail
FP1010(local-mgmt)# copy workspace:///techsupport/20190913063603_FP1010-2_FPRM.tar.gz
ftp://ftp@10.229.20.96
```

FPRM捆绑包包含一个名为tech_support_brief的文件。tech_support_brief文件包含一系列show命令。其中一个是**show portmanager switch status**:




# 限制详细信息、常见问题和解决方法

### 6.5版本实施的限制

- SVI接口不支持动态路由协议。
- 1010不支持多情景。
- SVI VLAN ID范围限制为1-4070。
- 不支持L2的端口通道。
- 不支持将L2端口用作故障切换链路。

**与交换机功能相关的限制**

| 功能 | 描述 | 限制 |
| --- | --- | --- |
| VLAN接口数 | 可创建的VLAN接口总数 | 60 |
| 中继模式VLAN | 中继模式下端口上允许的最大VLAN数 | 20 |
| Native VLAN | 映射所有未标记的数据包在端口上访问端口上配置的本征VLAN | 1 |
| 命名接口 | 包括所有命名接口(接口VLAN、子接口、端口通道、物理接口等) | 60 |

**其它限制**

- 子接口和接口VLAN不能使用相同的VLAN。
- 参与BVI的所有接口必须属于同一类接口。
- BVI可以使用L3模式端口和L3模式端口子接口的组合创建。
- 可以使用接口VLAN的组合创建BVI。
- 无法通过混合L3模式端口和接口VLAN创建BVI。

## 相关信息

- 思科Firepower 1010安全设备
- 配置指南