

FPR1010上的L2交換機，架構，驗證和故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[Firepower 6.5新增功能](#)

[FMC增加](#)

[工作原理](#)

[FP1010架構](#)

[封包處理](#)

[FP1010埠模式](#)

[FP1010案例1.路由埠 \(IP路由 \)](#)

[FP1010案例2.網橋組模式 \(橋接 \)](#)

[FP1010案例3.接入模式下的交換機埠 \(硬體交換 \)](#)

[過濾VLAN內流量](#)

[FP1010案例4.交換機埠 \(中繼 \)](#)

[FP1010案例5.交換器連線埠 \(VLAN間 \)](#)

[FP1010案例6. VLAN間過濾器](#)

[案例研究 — FP1010。橋接與硬體交換+橋接](#)

[FP1010設計注意事項](#)

[FXOS REST API](#)

[疑難排解/診斷](#)

[診斷概述](#)

[FP1010後端](#)

[收集FP1010上的FPRM show tech](#)

[限制詳細資訊、常見問題和解決方法](#)

[相關資訊](#)

簡介

本文檔介紹FP1010裝置上的L2交換機。具體來說，它主要包括安全服務平台(SSP)/Firepower擴展作業系統(FXOS)部分的實現。在6.5版本中，Firepower 1010 (台式機型號) 在內建L2硬體交換機上啟用交換功能。這有助於您避免額外的硬體交換機，從而降低成本。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

- FP1010是桌上型小型辦公室家庭辦公室(SOHO)，可替代ASA5505和ASA5506-X平台。
- 適用於FTD映像(6.4+)的軟體支援，由Firepower管理中心(FMC)、Firepower裝置管理器(FDM)或Cloud Defense Orchestrator(CDO)管理。
- ASA映像(9.13+)的軟體支援由CSM、ASDM或CLI管理。
- 作業系統(OS) (ASA或FTD) 捆綁了FXOS (類似於FP21xx) 。
- 8個10/100/1000 Mbps資料埠。
- 埠E1/7、E1/8支援PoE+。
- 硬體交換機允許埠之間的線速通訊(例如：監視器輸入本地伺服器)。

ASA5505



ASA5506X



FP1010

Firepower 6.5新增功能

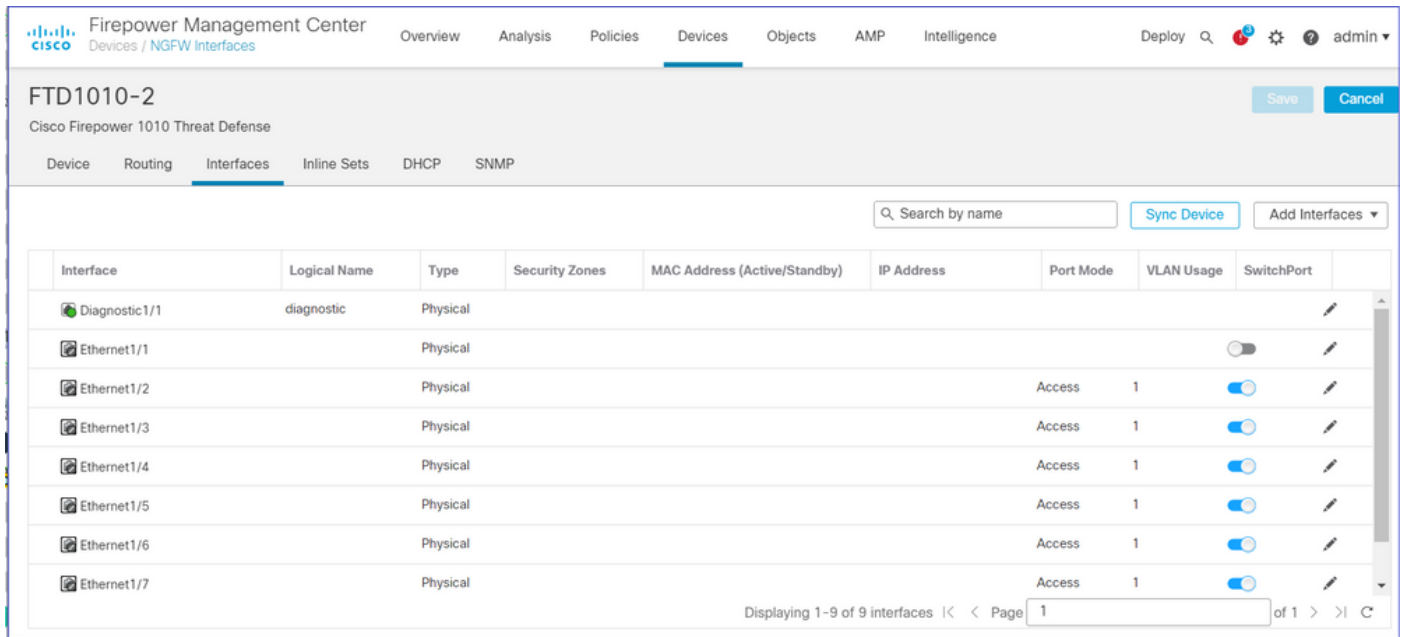
- 介紹一種稱為交換虛擬介面(SVI)的新型介面。
- 混合模式：介面可以在交換(L2)或非交換(L3)模式下配置。
- L3模式介面將所有資料包轉發到安全應用程式。
- 如果兩個連線埠屬於同一個VLAN，可改善輸送量和延遲，則L2模式連線埠可以在硬體中交換。需要路由或橋接的資料包將到達安全應用(例如：照相機從網際網路下載新韌體)並根據配置進行安全檢查。
- L2物理介面可以與一個或多個SVI介面關聯。
- L2模式介面可以處於接入模式或中繼模式。
- 接入模式L2介面僅允許未標籤的流量。
- 中繼模式L2介面允許標籤流量。
- 中繼模式L2介面的本徵VLAN支援。
- ASA CLI、ASDM、CSM、FDM和FMC已增強以支援新功能。

FMC增加

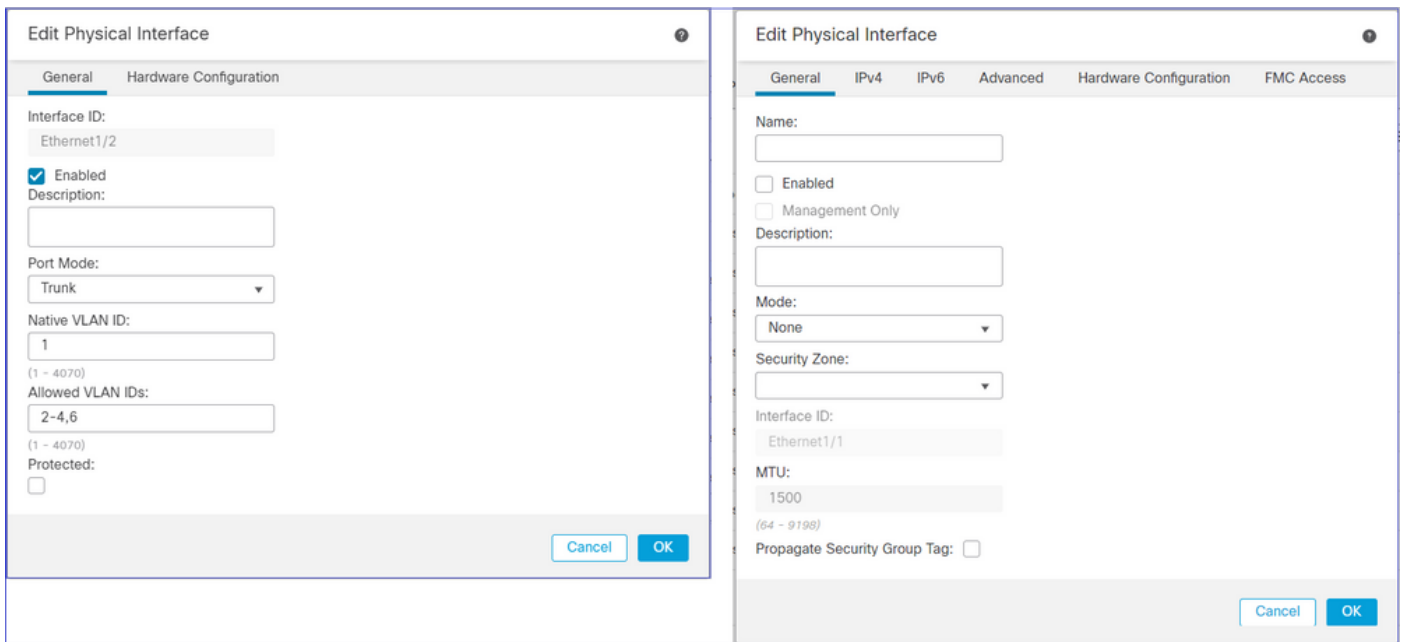
- 為物理介面引入了一種稱為switchport的新介面模式，用於標識物理介面是L3介面還是L2介面。
- 根據訪問或中繼模式，L2物理介面可以與一個或多個VLAN介面關聯。
- Firepower 1010支援最後兩個資料介面 (即Ethernet1/7和Ethernet1/8) 上的乙太網供電(PoE)配置。
- 交換和非交換之間的介面更改會清除除PoE和硬體配置之外的所有配置。

工作原理

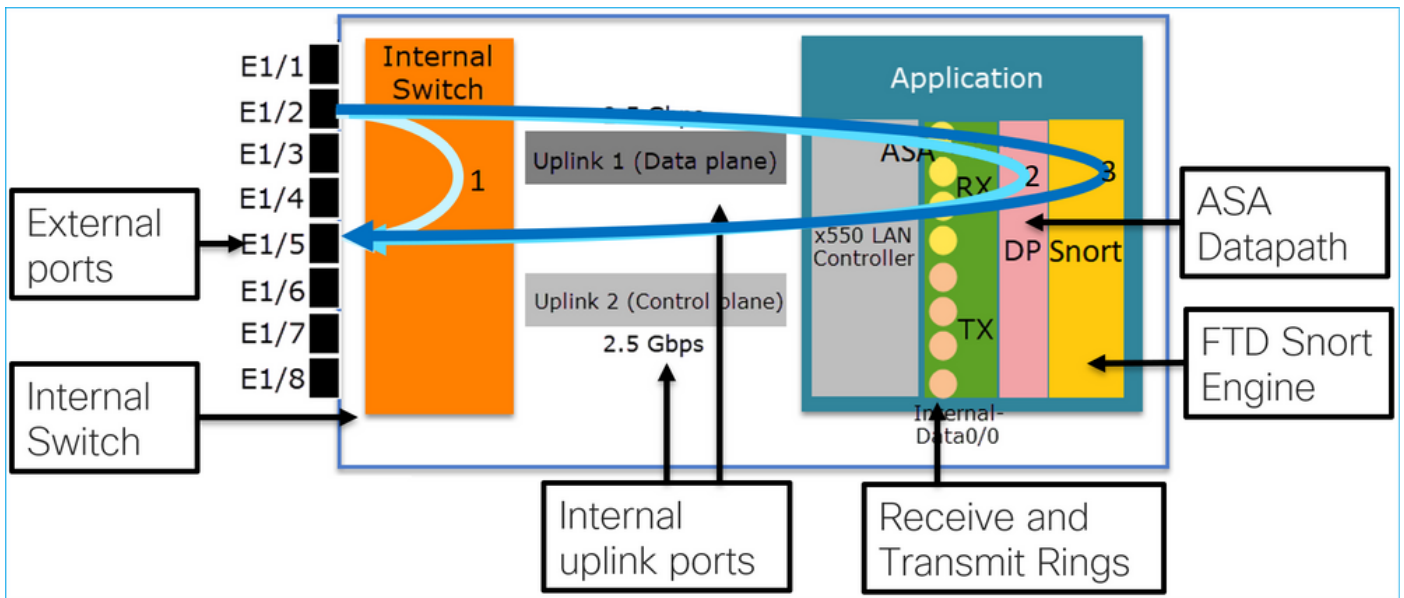
此功能僅增強了FMC(Device Management > Interface Page)上現有的介面支援。



物理介面檢視 (L2和L3)



FP1010架構



- 8個外部資料埠。
- 1個內部交換機。
- 3個上行鏈路埠（其中2個顯示在圖中），一個用於資料平面，一個用於控制平面，一個用於配置。
- x550 LAN控制器（應用與上行鏈路之間的介面）。
- 4個接收(RX)和4個傳輸(TX)環路。
- 資料路徑進程（在ASA和FTD上）。
- Snort程式（在FTD上）。

封包處理

影響資料包處理的主要因素有兩個：

1. 介面/埠模式
2. 適用的政策

資料包可以通過FP1010的方式有3種：

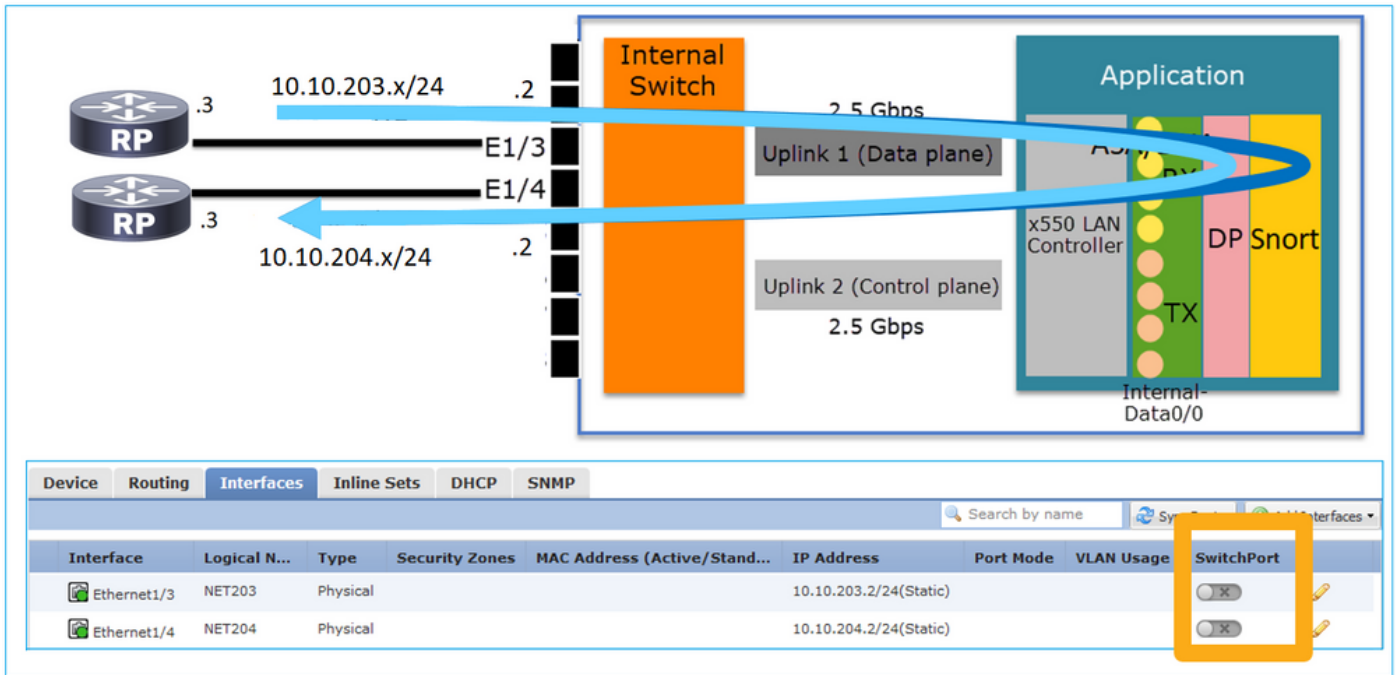
1. 僅由內部交換機處理
2. 轉發到應用程式(ASA/FTD)，僅由資料路徑進程處理
3. 轉發到應用程式(FTD)並由資料路徑和Snort引擎處理

FP1010埠模式

UI示例用於FMC，CLI示例用於FTD。大多數概念也完全適用於ASA。

FP1010案例1.路由埠（IP路由）

組態與操作



要點

- 從設計的角度來看，這2個埠屬於2個不同的L2子網。
- 當連線埠設定為路由模式時，封包會由應用程式（ASA或FTD）處理。
- 在FTD的情況下，根據規則動作（例如ALLOW），封包甚至可由Snort引擎檢查。

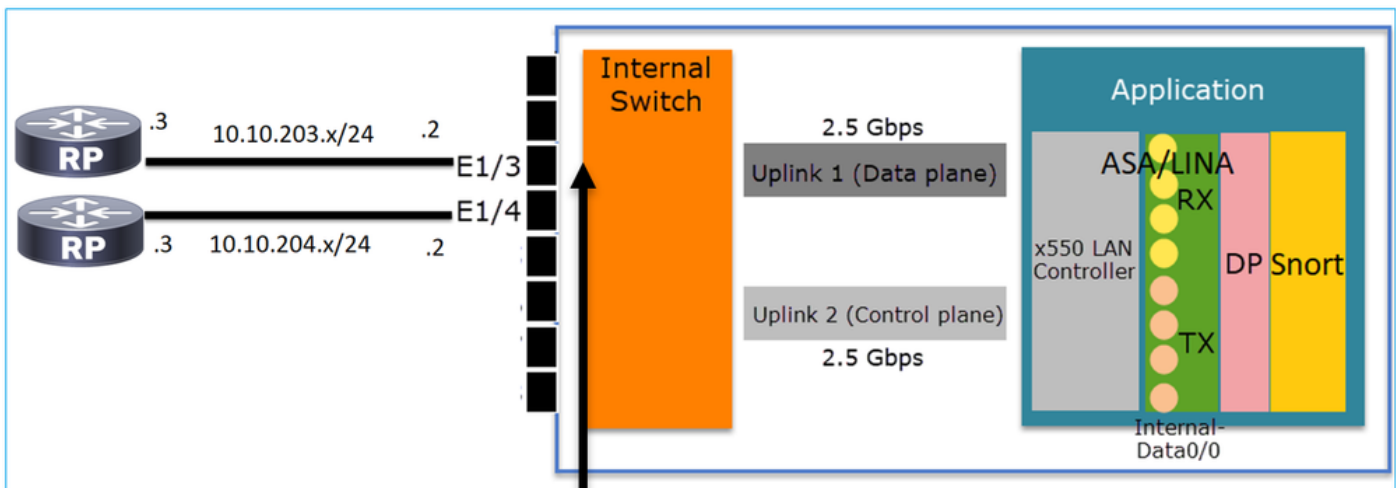
FTD介面組態

```

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路由連線埠驗證



您可以在FXOS CLI中檢查實體介面計數器。此範例顯示E1/3連線埠上的輸入單播和輸出單播計數器：

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

可以應用FTD資料路徑擷取，且可以追蹤封包：

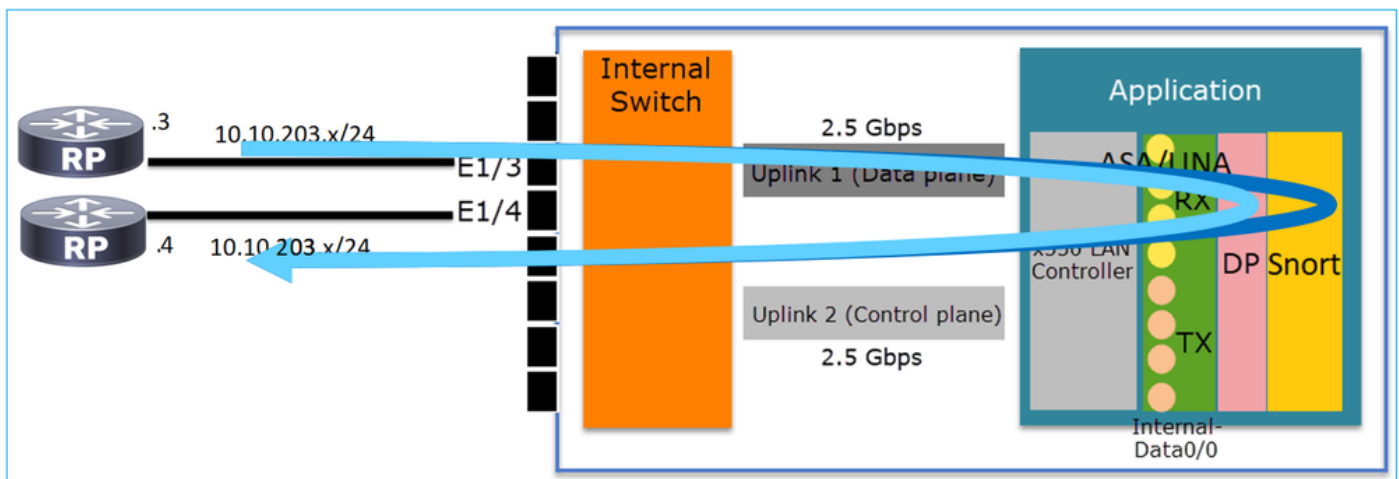
```
FP1010# show capture
capture CAP203 type raw-data trace interface NET203 [Capturing - 185654 bytes]
這是一個捕獲片段。如預期的那樣，資料包將根據ROUTE LOOKUP轉發：
```

```
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.網橋組模式 (橋接)

組態與操作



Device	Routing	Interfaces	Inline Sets	DHCP	SNMP				
		Ethernet1/3	NET203	Physical					
		Ethernet1/4	NET204	Physical					
		BVI134	NET34	Bridge...		10.10.203.1/24(Static)			

要點

- 從設計的角度來看，這2個連線埠連線到相同的L3子網路（類似於透明防火牆），但不同的

VLAN。

- 當連線埠設定為橋接模式時，封包會由應用程式 (ASA或FTD) 處理。
- 在FTD的情況下，根據規則動作 (例如ALLOW) ，封包甚至可由Snort引擎檢查。

FTD介面組態

```
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網橋組埠驗證

此命令顯示BVI 34的介面成員：

```
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
```

此命令顯示ASA/FTD資料路徑內容可定址記憶體(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
```

封包追蹤片段顯示封包是根據目的地MAC L2查詢轉送的：

```
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
```

在FTD的情況下，FMC連線事件還可以提供有關流量檢查和傳輸網橋組介面的資訊：

Context Explorer **Connections > Events** Intrusions Files Hosts Users Correlation Advanced Search

Connection Events [\[switch workflow\]](#)

Connections with Application Details [Table View of Connection Events](#)

Search Constraints (Edit Search)

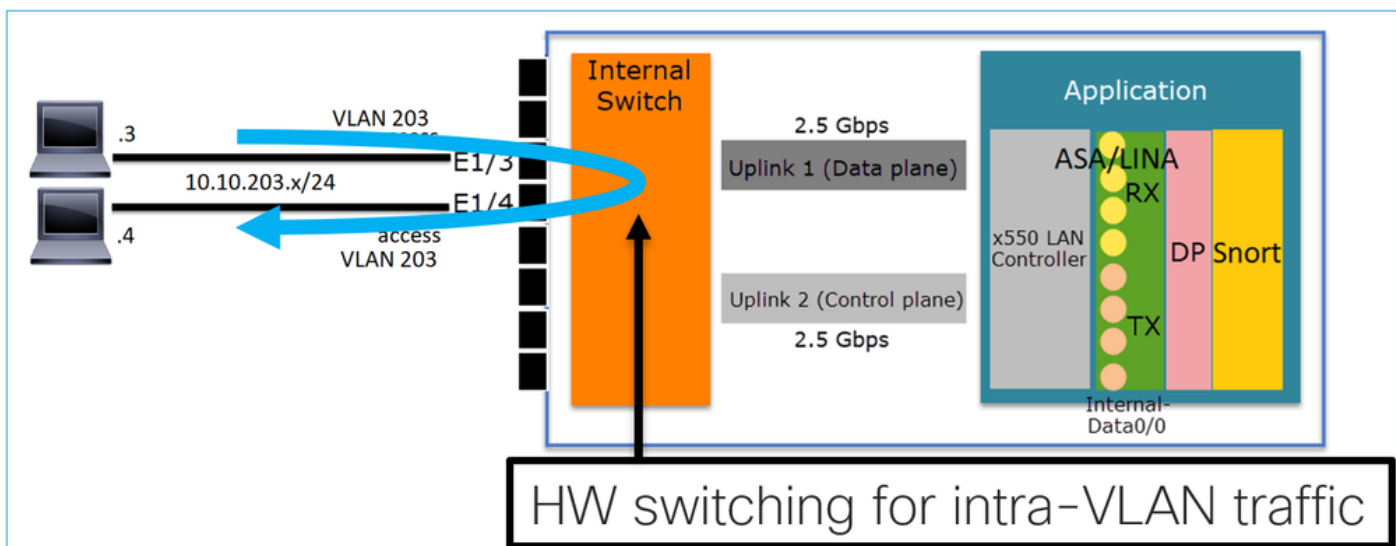
Jump to...

First Packet	Last Packet	Action	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Access Control Policy	Prefilter Policy	Tunnel/Prefilter Rule	Device	Ingress Interface	Egress Interface
2019-08-26 14:54:27	2019-08-26 14:54:27	Fastpath	10.10.203.3	10.10.203.4	8 (Echo Request) / icmp	0 (No Code) / icmp	FTD_ACP	mzafeiro_PP	rule1	mzafeiro_FTD1010	NET203	NET204
2019-08-26 14:54:27	2019-08-26 14:54:27	Fastpath	10.10.203.3	10.10.203.4	8 (Echo Request) / icmp	0 (No Code) / icmp	FTD_ACP	mzafeiro_PP	rule1	mzafeiro_FTD1010	NET203	NET204
2019-08-26 14:54:00	2019-08-26 14:54:00	Fastpath	10.10.203.3	10.10.203.4	8 (Echo Request) / icmp	0 (No Code) / icmp	FTD_ACP	mzafeiro_PP	rule1	mzafeiro_FTD1010	NET203	NET204
2019-08-26 14:54:00	2019-08-26 14:54:00	Fastpath	10.10.203.3	10.10.203.4	8 (Echo Request) / icmp	0 (No Code) / icmp	FTD_ACP	mzafeiro_PP	rule1	mzafeiro_FTD1010	NET203	NET204

Policy Action Applied Policies Bridged interfaces

FP1010案例3.接入模式下的交換機埠 (硬體交換)

組態與操作



Device	Routing	Interfaces	Inline Sets	DHCP	SNMP
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Sta...	IP Address
Ethernet1/3		Physical			
Ethernet1/4		Physical			

Port Mode	VLAN Usage	SwitchPort
Access	203	<input checked="" type="checkbox"/>
Access	203	<input checked="" type="checkbox"/>

要點

- 硬體交換是FTD 6.5+和ASA 9.13+功能。
- 從設計的角度來看，這2個連線埠連線到相同的L3子網和相同的VLAN。
- 此案例中的連線埠在存取模式下運作 (僅限未標籤的流量) 。
- 在SwitchPort模式下配置的防火牆埠沒有配置邏輯名稱(nameif)。
- 當連線埠設定為交換模式且屬於同一VLAN (VLAN內流量) 時，封包只會由FP1010內部交換器處理。

FTD介面組態

從CLI的角度來看，此配置看起來與L2交換機非常相似：

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



```
switchport access vlan 203
```

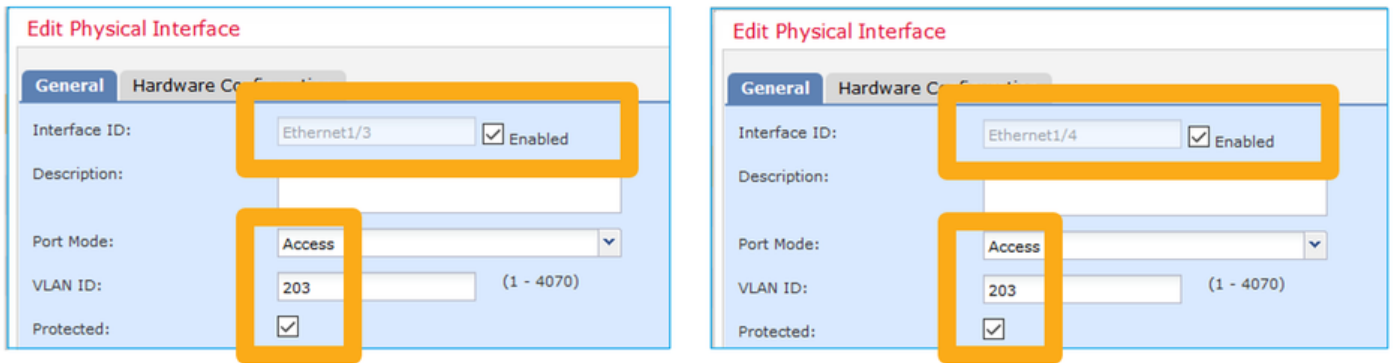
過濾VLAN內流量

挑戰：ACL無法過濾VLAN內流量！

解決方案：受保護的埠

其中的原理非常簡單：2個配置為受保護狀態的埠不能相互通訊。

FMC UI (在受保護埠的情況下)：



FTD介面組態

switchport protected命令是在介面下設定的：

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

FP1010交換器連線埠驗證

在本範例中，有1000個以特定大小（1100位元組）傳送的單點傳播封包(ICMP):

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

若要檢查傳輸介面的輸入和輸出單點傳播計數器，請使用以下命令：

```
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

```

此指令會顯示內部交換器VLAN狀態：

```

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

```

只要至少有一個埠分配給VLAN，VLAN的狀態即為UP

如果埠管理性關閉或連線的交換機埠關閉/斷開電纜連線，並且這是唯一分配給VLAN的埠，則VLAN狀態也為down:

```

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

```

此命令顯示內部交換機的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

內部交換機CAM表的預設老化時間為5分鐘30秒。

FP1010包含2個CAM表：

1. 內部交換機CAM表:用於硬體交換
2. ASA/FTD資料路徑CAM表:用於橋接

通過FP1010的每個資料包/幀由單個CAM表（內部交換機或FTD資料路徑）根據埠模式進行處理。

注意：請勿將SwitchPort模式中使用的show switch mac-address-table內部交換機CAM表與橋接模式中使用的show mac-address-table FTD資料路徑CAM表混淆

硬體交換：需要注意的其他事項

ASA/FTD資料路徑日誌不顯示有關硬體交換流的資訊：

```

FP1010# show log
FP1010#

```

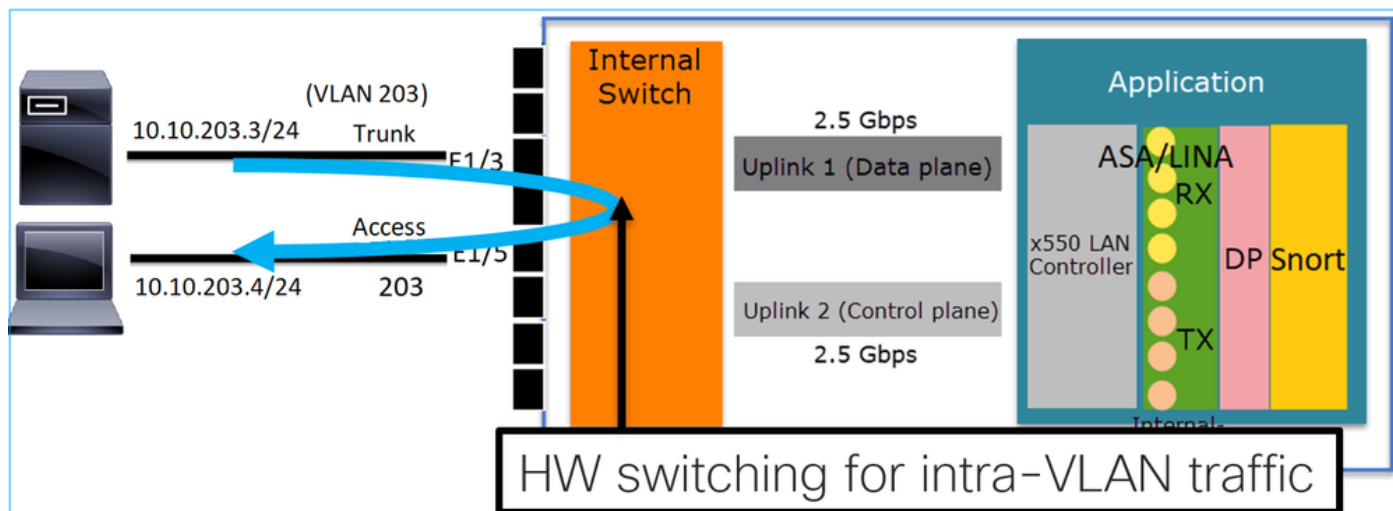
ASA/FTD資料路徑連線表不顯示硬體交換流：

```
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連線事件不顯示硬體交換流。

FP1010案例4.交換機埠 (中繼)

組態與操作



Device	Routing	Interfaces	Inline Sets	DHCP	SNMP
Ethernet1/3		Physical			
Ethernet1/5		Physical			

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Port Mode	VLAN Usage	SwitchPort
Ethernet1/3		Physical				Trunk	203	<input checked="" type="checkbox"/>
Ethernet1/5		Physical				Access	203	<input checked="" type="checkbox"/>

Trunk 203-210 ← Allowed VLAN list

要點

- 硬體交換是FTD 6.5+和ASA 9.13+功能。
- 從設計的角度來看，這2個連線埠連線到相同的L3子網和相同的VLAN。
- Trunk埠接受已標籤幀和未標籤幀 (在本徵VLAN的情況下)。
- 當連線埠設定為交換模式且屬於同一VLAN (VLAN內流量)時，封包只會由內部交換器處理。

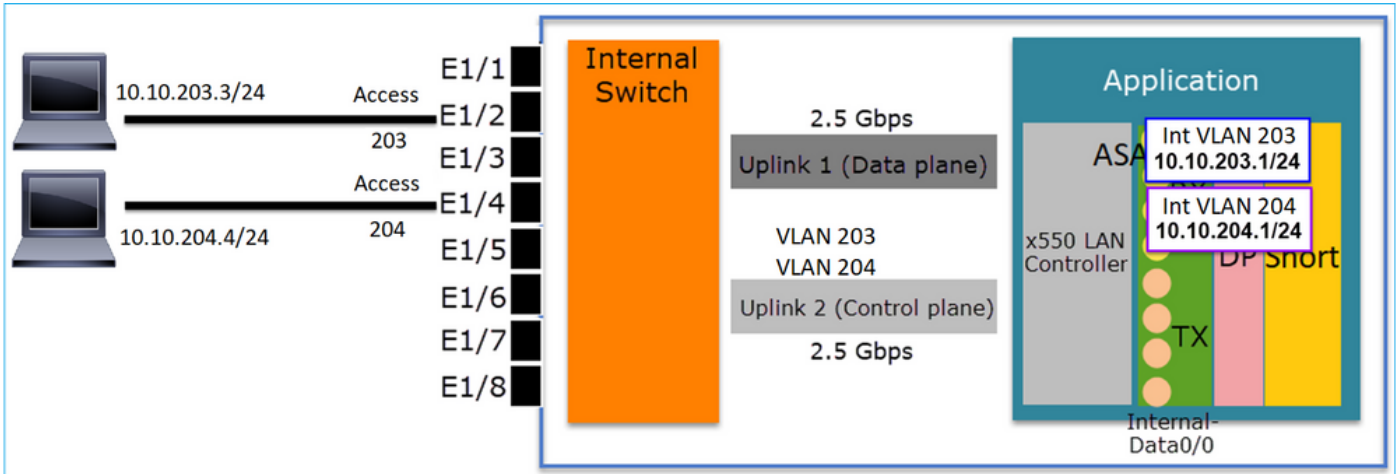
FTD介面組態

此組態類似於第2層交換器連線埠：

```
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.交換器連線埠 (VLAN間)

組態與操作

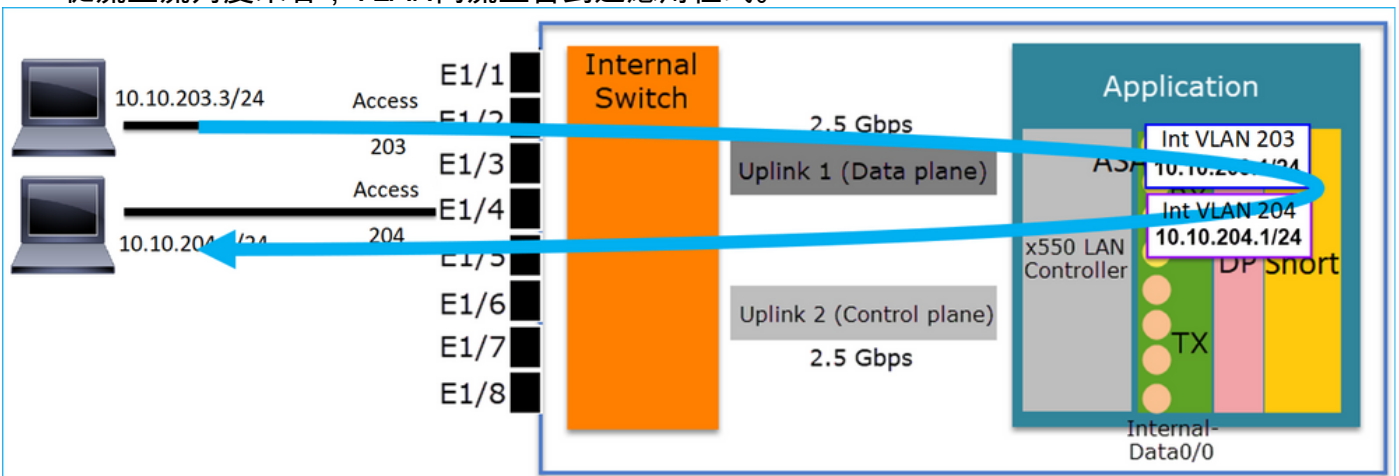


Device	Routing	Interfaces	Inline Sets	DHCP	SNMP
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Stand...)	IP Address
Ethernet1/2		Physical			
Ethernet1/4		Physical			
Vlan203	NET203	VLAN			10.10.203.1/24(Static)
Vlan204	NET204	VLAN			10.10.204.1/24(Static)

Port Mode	VLAN Us...	Switc...
Access	203	<input checked="" type="checkbox"/>
Access	204	<input checked="" type="checkbox"/>

要點

- 從設計的角度來看，2個埠連線到2個不同的L3子網和2個不同的VLAN。
- VLAN之間的流量通過VLAN介面（類似於SVI）。
- 從流量流角度來看，VLAN間流量會到達應用程式。



FTD介面組態

組態類似於交換器虛擬介面(SVI):

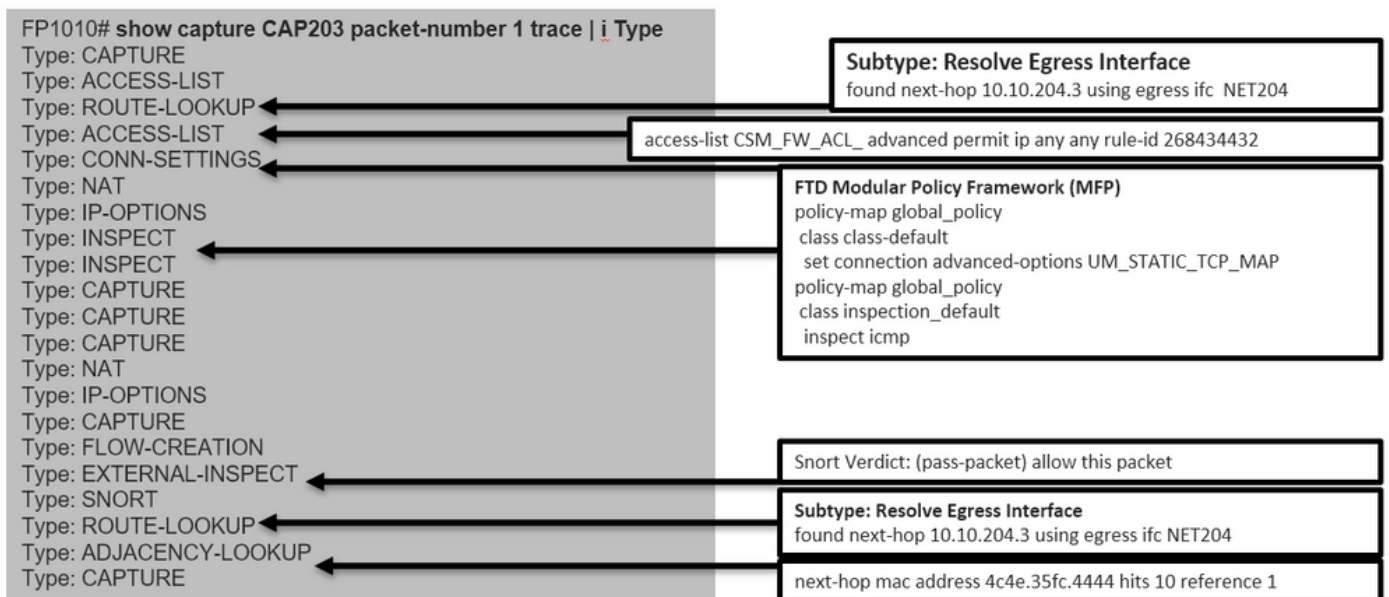
```
interface Ethernet1/2
  switchport switchport access vlan 203
interface Ethernet1/4
  switchport switchport access vlan 204
!
interface Vlan203 nameif NET203 security-level 0 ip address 10.10.203.1 255.255.255.0
interface Vlan204 nameif NET204 security-level 0 ip address 10.10.204.1 255.255.255.0
```

VLAN間流量的封包處理

以下是經過兩個不同VLAN的封包的追蹤軌跡：

```
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
```

資料包過程的主要階段：



FP1010案例6. VLAN間過濾器

組態與操作

有兩種主要選項可過濾VLAN間流量：

1. 訪問控制策略
2. 'no forward'指令

使用「no forward」指令篩選VLAN間流量

FMC UI配置：

The screenshot shows the 'Edit VLAN Interface' configuration window. The 'General' tab is selected. The configuration includes:

- Name: NET203 (with an 'Enabled' checkbox)
- Description: (empty text box)
- Mode: None (dropdown menu)
- Security Zone: (dropdown menu)
- MTU: 1500 (range 64 - 9198)
- VLAN ID *: 203 (range 1 - 4070)
- Disable Forwarding on Interface Vlan: 204 (dropdown menu)

The 'VLAN ID *' and 'Disable Forwarding on Interface Vlan' fields are highlighted with an orange box.

要點

- no forward drop是單向的。
- 不能同時應用於兩個VLAN介面。
- no forward check在ACL檢查之前完成。

FTD介面組態

在此案例中，CLI配置如下：

```
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
```

如果資料包被無轉發功能丟棄，則會生成ASA/FTD資料路徑系統日誌消息：

```
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)
```

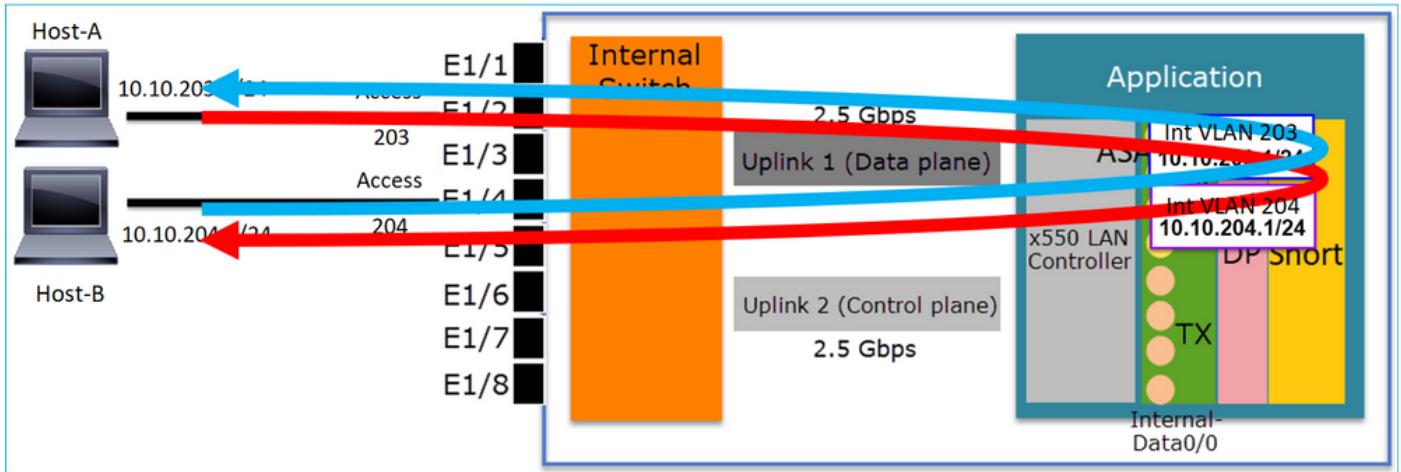
從加速安全路徑(ASP)放置的角度來看，它被視為一個ACL放置：

```
FP1010-2# show asp drop
```

```
Frame drop:
```

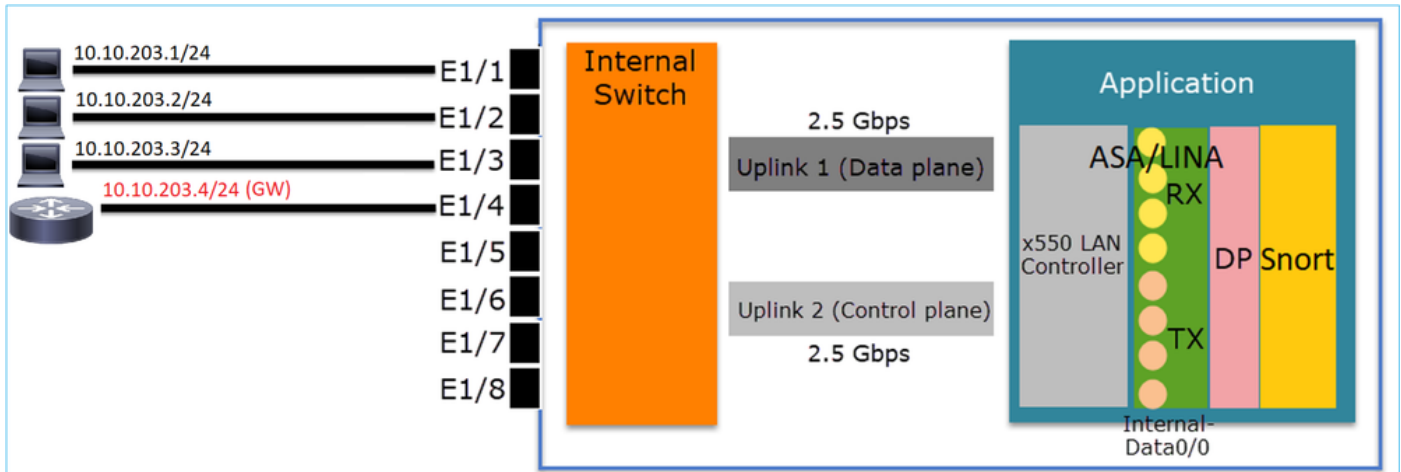
```
Flow is denied by configured rule (acl-drop) 1
```

由於捨棄是單向的，因此主機A(VLAN 203)無法起始流量到主機B(VLAN 204)，但允許相反的流量：



案例研究 — FP1010。橋接與硬體交換+橋接

請考慮以下拓撲：



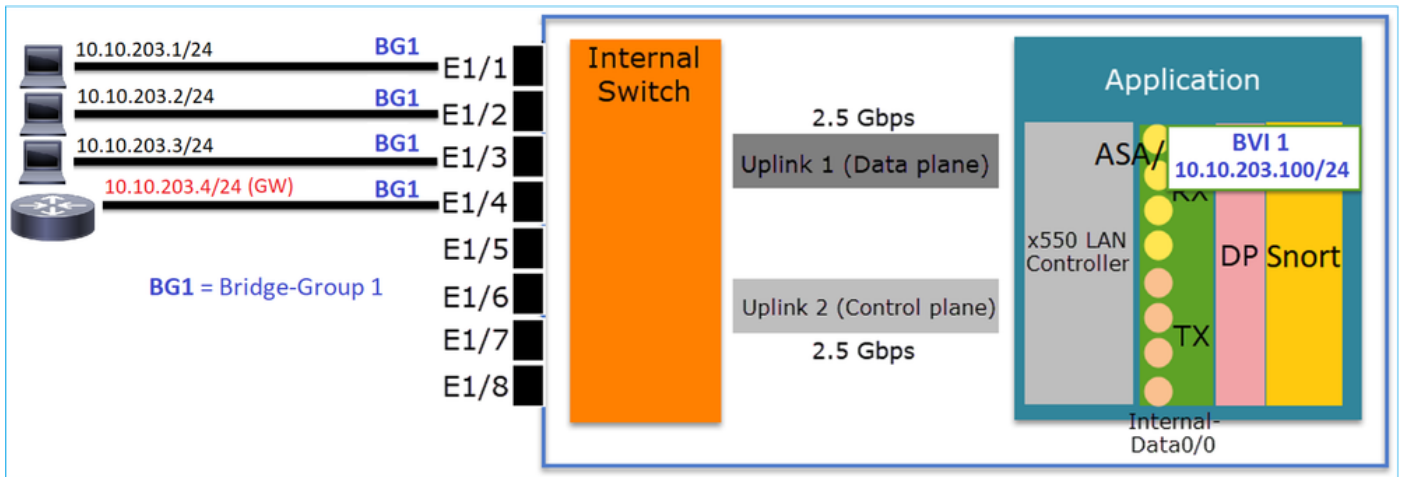
在此拓撲中：

- 三個終端主機屬於同一個L3子網(10.10.203.x/24)。
- 路由器(10.10.203.4)用作子網中的GW。

在此拓撲中，有兩種主要設計選項：

1. 橋接
2. 硬體交換+橋接

設計選項1.橋接



要點

本設計的要點是：

- BVI 1 是使用IP建立的，與4個連線的裝置位於同一子網(10.10.203.x/24)中。
- 所有四個連線埠都屬於同一個橋接器群組（在本案例中為群組1）。
- 四個連線埠中的每個連線埠都設定了名稱。
- 主機到主機和主機到GW的通訊通過應用程式（如FTD）。

從FMC UI的角度來看，配置為：

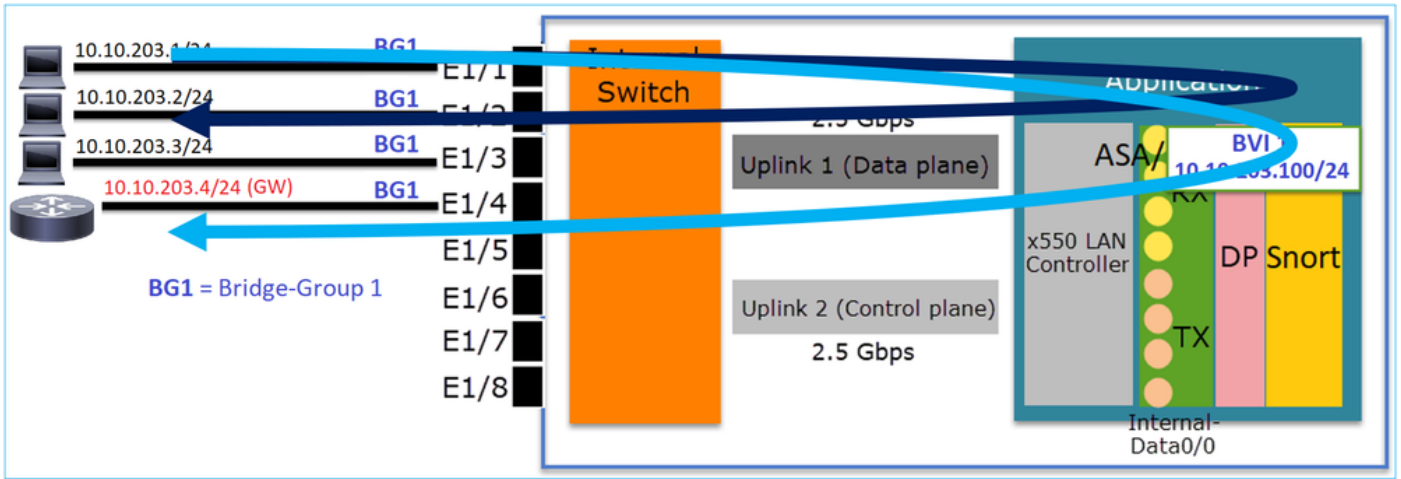
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Port Mode	VLAN Usage	SwitchP...
Ethernet1/1	HOST1	Physical						
Ethernet1/2	HOST2	Physical						
Ethernet1/3	HOST3	Physical						
Ethernet1/4	HOST4	Physical						
BVI1	BG1	BridgeGroup			10.10.203.100/24(Static)			

FTD介面組態

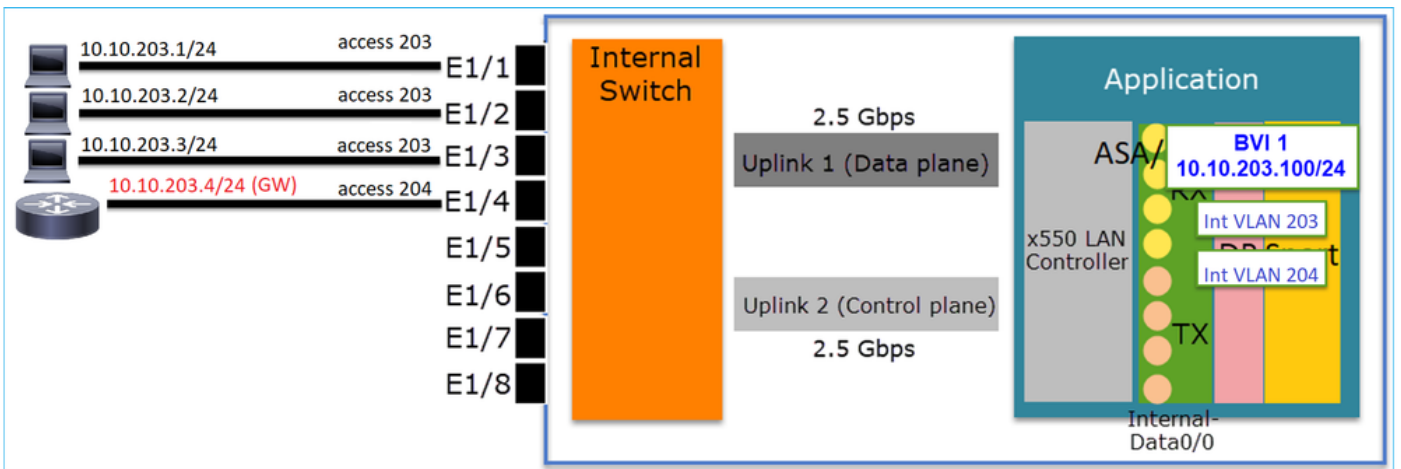
此案例中的設定如下：

```
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
```

此案例中的流量：



設計選項2.硬體交換+橋接



要點

本設計的要點是：

- BVI 1是使用IP建立的，與4個連線的裝置位於同一子網(10.10.203.x/24)中。
- 連線到終端主機的埠配置為SwitchPort模式並屬於同一個VLAN(203)。
- 連線到GW的埠配置為交換機埠模式，屬於不同的VLAN(204)。
- 有2個VLAN介面(203、204)。2個VLAN介面未分配IP，屬於網橋組1。
- 主機到主機的通訊僅通過內部交換機。
- 主機到GW的通訊通過應用程式 (如FTD) 。

FMC UI配置：

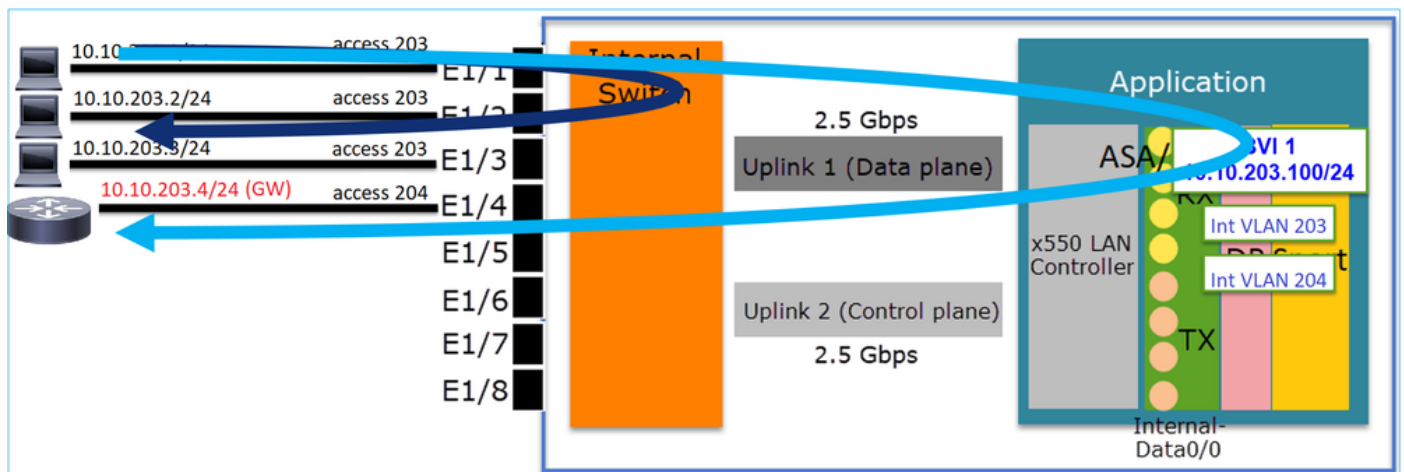
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Port Mode	VLAN Usage	SwitchP...
Ethernet1/1		Physical				Access	203	<input checked="" type="checkbox"/>
Ethernet1/2		Physical				Access	203	<input checked="" type="checkbox"/>
Ethernet1/3		Physical				Access	203	<input checked="" type="checkbox"/>
Ethernet1/4		Physical				Access	204	<input checked="" type="checkbox"/>
Vlan203	NET203	VLAN						<input type="checkbox"/>
Vlan204	NET204	VLAN						<input type="checkbox"/>
BVI1	BG1	BridgeGroup			10.10.203.100/24(Static)			<input type="checkbox"/>

FTD介面組態

此案例中的設定如下：

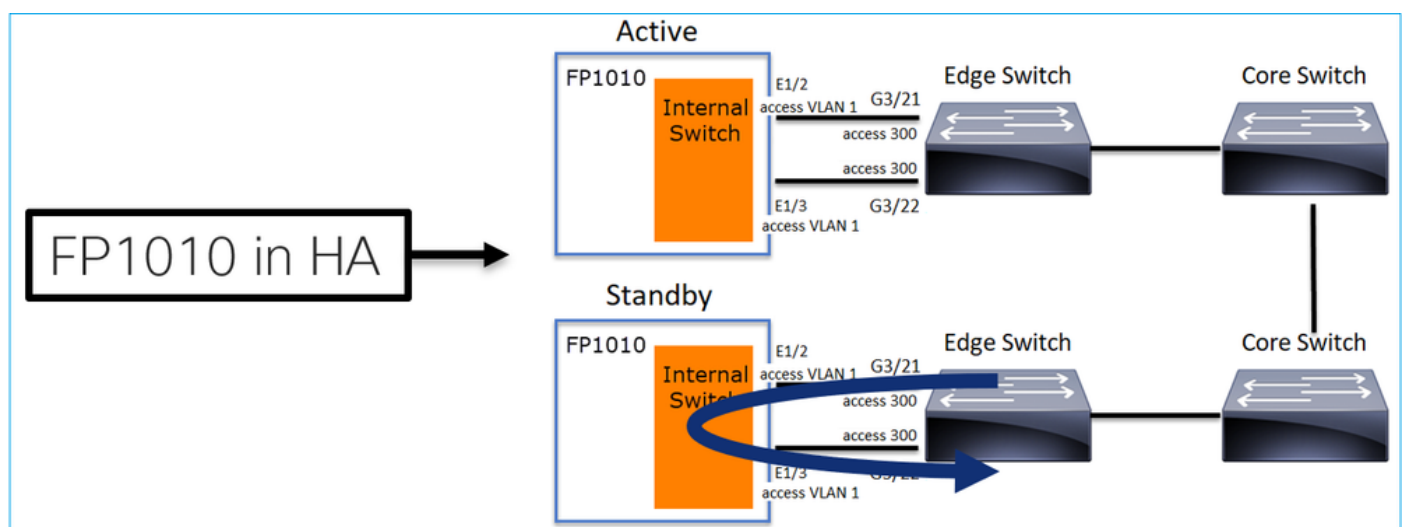
```
interface Ethernet1/1
  switchport switchport access vlan 203
interface Ethernet1/2
  switchport switchport access vlan 203
interface Ethernet1/4
  switchport switchport access vlan 204
!
interface Vlan203
  bridge-group 1 nameif NET203
interface Vlan204
  bridge-group 1 nameif NET204
!
interface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

主機到主機通訊與主機到GW通訊：



FP1010設計注意事項

交換和高可用性(HA)



在HA環境中配置HW交換時存在兩個主要問題：

1. 備用裝置上的HW交換通過裝置轉發資料包。這可能會造成流量回圈。

2. HA不監控SwitchPort

設計要求

- 不能將SwitchPort功能與ASA/FTD高可用性一起使用。FMC配置指南中對此進行了說明：
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

Firepower Threat Defense Interfaces and Device Settings

Interface Overview for Firepower Threat Defense

Regular Firewall Interfaces for Firepower Threat Defense

Inline Sets and Passive Interfaces for Firepower Threat Defense

DHCP and DDNS Services for Threat Defense

Quality of Service (QoS) for Firepower Threat Defense

Firepower Threat Defense High

For all Firepower 1010 interfaces, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled. When the speed and duplex are set to 1000 and full, then the interface always auto-negotiates; therefore Auto-MDI/MDIX is always enabled and you cannot disable it.

Guidelines and Limitations for Firepower 1010 Switch Ports

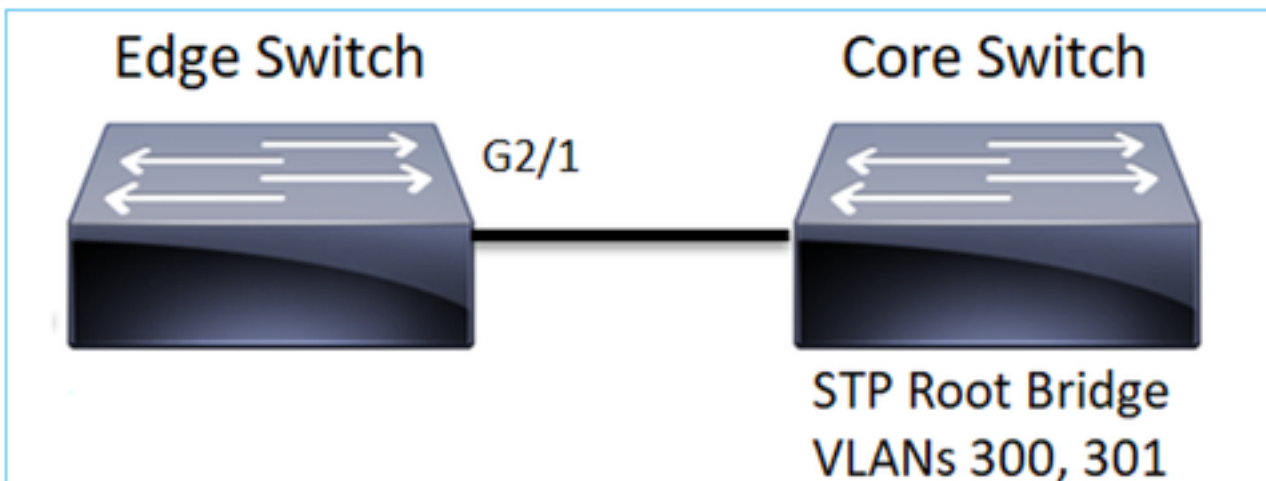
High Availability and Clustering

- No cluster support.
- You should not use the switch port functionality when using High Availability. Because the switch ports operate in hardware, they continue to pass traffic on both the active and the standby units. High Availability is designed to prevent traffic from passing through the standby unit, but this feature does not extend to switch ports. In a normal High Availability network setup, active switch ports on both units will lead to network loops. We suggest that you use external switches for any switching capability. Note that VLAN interfaces can be monitored by failover, while switch ports cannot. Theoretically, you can put a single switch port on a VLAN and successfully use High Availability, but a simpler setup is to use physical firewall interfaces instead.

與生成樹通訊協定(STP)的互動

FP1010內部交換機不運行STP。

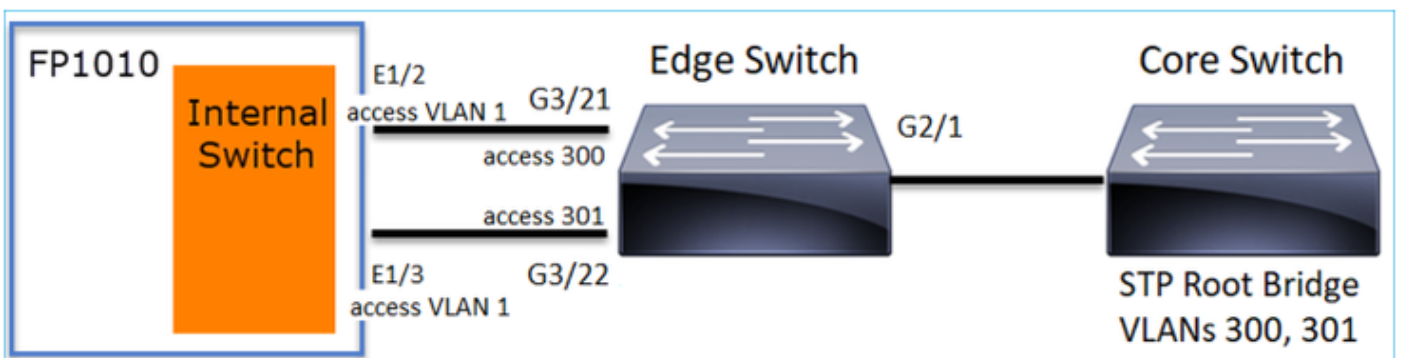
請考慮以下情況：



在邊緣交換機上，兩個VLAN的根埠都是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
```

將FP1010連線到邊緣交換機，並在同一VLAN中配置兩個埠（硬體交換）：



問題

- 由於VLAN洩漏了G3/22上接收的VLAN 301的上級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：如果將L2交換機連線到FP1010，可能會影響STP域

FMC配置指南中也記錄了此資訊：

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

 **Note** The Firepower 1010 does not support Spanning Tree Protocol for loop detection in the network. Therefore you must ensure that any connection with the FTD does not end up in a network loop.

FXOS REST API

FMC REST API

以下是適用於此功能支援的REST API:

- L2實體介面[支援的PUT/GET]

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

- VLAN介面[支援的POST/PUT/GET/DELETE]

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

疑難排解/診斷

診斷概述

- 日誌檔案在FTD/NGIPS故障排除中或show tech輸出中捕獲。以下是進行疑難排解時需要尋找更多詳細資訊的專案：
- /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 running-config
- /mnt/disk0/log/asa-appagent.log

從FXOS (裝置) 收集資料 — CLI

在FTD(SSH)的情況下：

```
> 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)#
```

在FTD的情況下 (主控台) :

```
> 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後端

埠暫存器定義所有內部交換機和埠功能。

在此螢幕截圖中，顯示了埠暫存器的「埠控制」部分，尤其是指示介面上接收的標籤流量必須丟棄(1)或允許(0)的暫存器。 以下是適用於一個連線埠的完整註冊部分：

```
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
```

在此螢幕抓圖中，您可以看到各種埠模式的各種丟棄標籤暫存器值：

The screenshot shows the Cisco Firepower GUI with the 'Interfaces' tab selected. The interface table is as follows:

Interface	Logical...	Type	Sec...	M.	IP Address	Port Mode	VLAN Usage	SwitchPort
Diagnostics/1	diagnostic	Physical						
Ethernet1/1		Physical						
Ethernet1/2		Physical				Trunk	203-204	
Ethernet1/3		Physical				Access	203	
Ethernet1/4	NET4	Physical			10.10.4.1/24(Static)			
Ethernet1/5		Physical				Access	201	
Ethernet1/6	NET6	Physical			10.10.106.1/24(Static)			
Ethernet1/7		Physical				Access	1	
Ethernet1/8		Physical				Access	1	
Vlan201	NET201	VLAN	outs...		10.10.201.1/24(Static)			
Vlan203	NET203	VLAN			10.10.203.1/24(Static)			
Vlan204	NET204	VLAN			10.10.204.1/24(Static)			
BVI1	BG1	Bridge...			10.10.15.1/24(Static)			

The terminal output on the right shows the 'show portmanager switch status' command with 'egrep "Port Registers Dump|Tagged"' filter. Annotations point to specific lines in the terminal output:

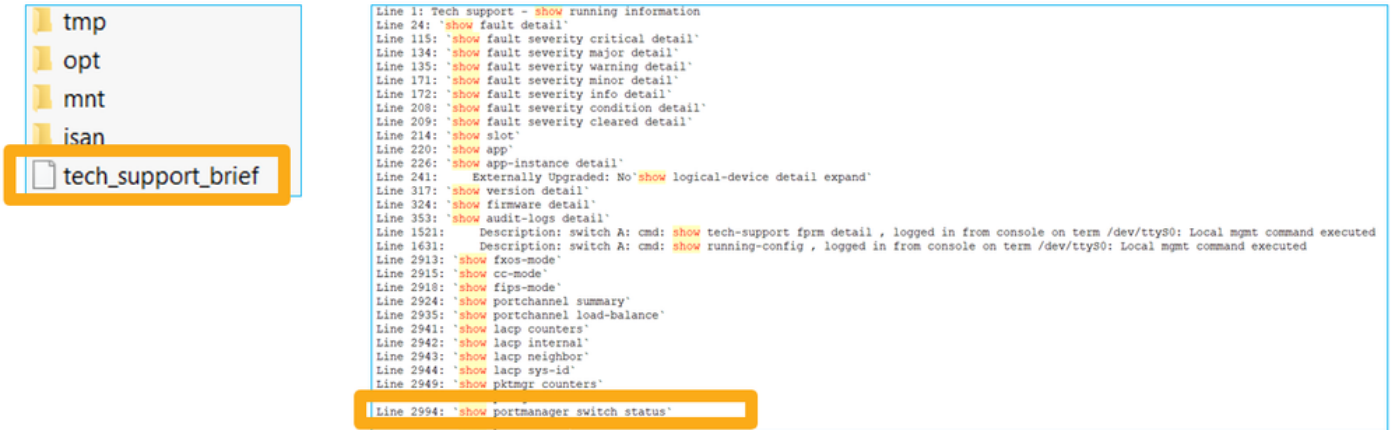
- Routed Mode (BG)**: Points to 'Port Registers Dump for port 1' and 'Discard Tagged = 0'.
- Trunk Mode**: Points to 'Port Registers Dump for port 2' and 'Discard Tagged = 0'.
- Access Mode**: Points to 'Port Registers Dump for port 3' and 'Discard Tagged = 1'.
- Routed Mode (IP)**: Points to 'Port Registers Dump for port 5' and 'Discard Tagged = 1'.

收集FP1010上的FPRM show tech

若要產生FPRM套件組合併將其上傳到FTP伺服器：

```
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套件組合包含名為tech_support_brief的檔案。tech_support_brief檔案包含一系列show命令。其中一個是show portmanager switch status:



限制詳細資訊、常見問題和解決方法

6.5版本實施的限制

- SVI介面不支援動態路由協定。
- 1010不支援多情景。
- SVI VLAN id的範圍限制為1-4070。
- 不支援L2的Port-channel。
- 不支援將第2層埠用作故障切換鏈路。

與交換機功能相關的限制

功能	說明	限制
VLAN介面數量	可建立的VLAN介面總數	60
中繼模式VLAN	處於中繼模式的埠上允許的最大VLAN數	20
本徵VLAN	對映所有未標籤的資料包在埠上連線到埠上配置的本地VLAN	1
命名介面	包括所有命名介面(介面VLAN、子介面、埠通道、物理介面等)	60

其他限制

- 子介面和介面VLAN不能使用同一個VLAN。
- 所有參與BVI的介面必須屬於同一型別的介面。
- 可以使用L3模式埠和L3模式埠子介面的組合建立BVI。
- 可以使用介面VLAN的組合建立BVI。
- 不能通過混合L3模式埠和介面VLAN來建立BVI。

相關資訊

- [Cisco Firepower 1010安全裝置](#)
- [疑難排解技術筆記](#)