使用執行Cisco IOS軟體的Cisco Catalyst 6000/6500進行VACL擷取，以進行詳細流量分析

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[相關產品](#)
[慣例](#)
[背景資訊](#)
[VLAN型SPAN](#)
[VLAN ACL](#)
[使用VACL比VSPAN的優勢](#)
[設定](#)
[網路圖表](#)
[使用基於VLAN的SPAN的組態](#)
[使用VACL的配置](#)
[驗證](#)
[疑難排解](#)
[相關資訊](#)

簡介

本檔案將提供使用VLAN ACL(VACL)擷取連線埠功能的範例組態，以便更精細地進行網路流量分析。本檔案也說明VACL擷取連線埠使用與基於VLAN的SPAN(VSPAN)使用的優點。

要在執行Catalyst OS軟體的Cisco Catalyst 6000/6500上設定VACL擷取連線埠功能，請參閱VACL擷取，以使用執行CatOS軟體的Cisco Catalyst 6000/6500進行精細流量分析。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- IP存取清單：如需詳細資訊，請參閱設定IP存取清單。
- 虛擬LAN:如需詳細資訊，請參閱虛擬LAN/VLAN主幹協定(VLAN/VTP) — 簡介。

採用元件

本文中的資訊係根據以下軟體和硬體版本：執行Cisco IOS® 軟體版本12.2(18)SXF8的Cisco Catalyst 6506系列交換器。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

此組態也可與執行Cisco IOS軟體版本12.1(13)E及更新版本的Cisco Catalyst 6000/6500系列交換器一起使用。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

VLAN型SPAN

SPAN（交換式連線埠分析器）將流量從任何VLAN中的一個或多個來源連線埠或從一個或多個VLAN複製到目的地連線埠進行分析。本地SPAN支援同一Catalyst 6500系列交換器上的來源連線埠、來源VLAN和目的地連線埠。

來源VLAN是受監控以用於網路流量分析的VLAN。VLAN型SPAN(VSPAN)使用VLAN作為SPAN來源。來源VLAN中的所有連線埠均會成為來源連線埠。來源連線埠是受監控以用於網路流量分析的連線埠。主干連線埠可以設定為來源連線埠並與非主幹來源連線埠混合，但SPAN不會從來源主干連線埠複製封裝。

對於已設定輸入和輸出的VSPAN作業階段，如果封包在相同VLAN上交換，便會從目的地連線埠轉送兩個封包（一個為來自輸入連線埠的輸入流量，另一個為來自輸出連線埠的輸出流量）。

VSPAN僅監控離開或進入VLAN中第2層連線埠的流量。

- 如果將VLAN設定為輸入來源，且流量路由到受監控VLAN，則不會監控路由流量，因為路由流量永遠不會顯示為進入VLAN中第2層連線埠的輸入流量。
- 如果將VLAN設定為輸出來源，且流量從受監控VLAN路由出去，則不會監控路由流量，因為路由流量永遠不會顯示為離開VLAN中第2層連線埠的出口流量。

如需來源VLAN的詳細資訊，請參閱來源VLAN的特性。

VLAN ACL

VACL可以為在VLAN中橋接的所有資料包，或者路由到VLAN或WAN介面或傳出VACL捕獲的所有資料包提供訪問控制。與僅配置在路由器介面上且僅應用於路由資料包的常規Cisco IOS標準或擴展ACL不同，VACL適用於所有資料包，可以應用於任何VLAN或WAN介面。VACL在硬體中處理。VACL使用Cisco IOS ACL。VACL會忽略硬體不支援的任何Cisco IOS ACL欄位。

您可以為IP、IPX和MAC層流量配置VACL。應用於WAN介面的VACL僅支援VACL捕獲的IP流量。

當您配置VACL並將其應用到VLAN時，會根據此VACL檢查進入VLAN的所有資料包。如果將

VACL套用到VLAN，將ACL套用到VLAN中的路由介面，則首先根據VACL檢查進入VLAN的封包，如果允許，則在路由介面處理之前，根據輸入ACL檢查進入VLAN的封包。將封包路由到另一個VLAN時，首先根據應用於路由介面的輸出ACL檢查該封包，如果允許，則應用為目的地VLAN設定的VACL。如果為資料包型別配置了VACL，而該型別的資料包與VACL不匹配，則預設操作為deny。以下是VACL中捕獲選項的准則。

- 擷取連線埠不能是ATM連線埠。
- VLAN的捕獲埠需要處於生成樹轉發狀態。
- 交換機對捕獲埠的數量沒有限制。
- 擷取連線埠僅擷取已設定ACL允許的資料包。
- 擷取連線埠僅傳輸屬於擷取連線埠VLAN的流量。將擷取連線埠設定為傳送所需VLAN的中繼，以便擷取前往多個VLAN的流量。

注意：ACL組合不正確可能會中斷流量。在裝置中配置ACL時請特別小心。

註：Catalyst 6000系列交換機上的IPv6不支援VACL。換句話說，VLAN ACL重定向和IPv6不相容，因此ACL不能用於匹配IPv6流量。

使用VACL比VSPAN的優勢

流量分析的VSPAN使用方式存在多個限制：

- 捕獲VLAN中流經的所有第2層流量。這將增加要分析的資料量。
- Catalyst 6500系列交換器上可設定的SPAN作業階段數量有限。如需詳細資訊，請參閱本地SPAN和RSPAN作業階段上限。
- 目的地連接埠接收所有受監控來源連接埠的已傳送和已接收流量的副本。如果目的地連接埠為超額使用，則可能會擁塞。這種擁塞會影響一個或多個來源連接埠上的流量轉送。

VACL捕獲埠功能有助於克服其中一些限制。VACL的主要用途並非監控流量，但是，由於具備對流量進行分類的多種功能，因此引入了捕獲埠功能，從而使網路流量分析變得更加簡單。以下是VACL擷取連線埠使用VSPAN的優勢：

- 精細流量分析VACL可以根據源IP地址、目標IP地址、第4層協定型別、源和目標第4層埠以及其他資訊匹配。此功能使VACL非常適用於精細流量識別和過濾。
- 作業階段數量VACL在硬體中實施；可以建立的訪問控制條目(ACE)的數量取決於交換機中可用的TCAM。
- 目的地連線埠超額訂閱精細的流量識別可減少要轉送到目的地連線埠的訊框數量，從而最大程度降低其超訂用的可能性。
- 效能VACL在硬體中實施；將VACL套用到Cisco Catalyst 6500系列交換器上的VLAN不會導致效能下降

設定

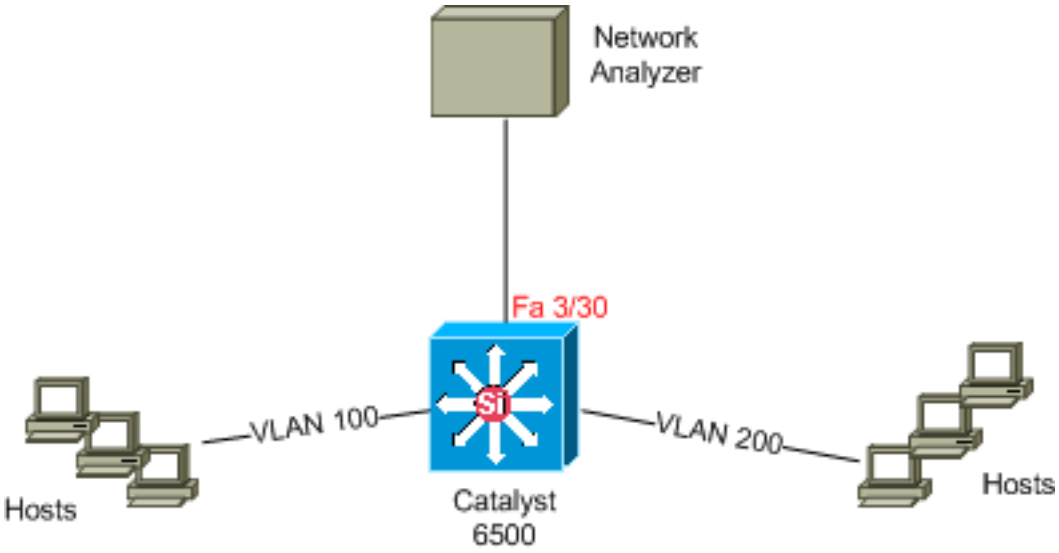
本節提供用於設定本文件中所述功能的資訊。

- 使用基於VLAN的SPAN設定
- 使用VACL配置

註：使用Command Lookup Tool(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

網路圖表

本檔案會使用以下網路設定：



使用基於VLAN的SPAN的組態

此組態範例列出擷取VLAN 100和VLAN 200中流動的所有第2層流量並將其傳送到網路分析器裝置所需的步驟。

1. 指定感興趣的流量。在我們的示例中，流量流入VLAN 100和VLAN 200。

```
Cat6K-IOS#conf t
Cat6K-IOS(config)#monitor session 50 source vlan 100 , 200 ?
  ,     Specify another range of VLANs
  -     Specify a range of VLANs
  both  Monitor received and transmitted traffic
  rx    Monitor received traffic only
  tx    Monitor transmitted traffic only
  <cr>

 !--- Default is to monitor both received and transmitted traffic

Cat6K-IOS(config)#monitor session 50 source vlan 100 , 200
Cat6K-IOS(config)#
```

2. 為捕獲的流量指定目標埠。

```
Cat6K-IOS(config)#monitor session 50 destination interface Fa3/30
Cat6K-IOS(config)#
```

這樣，所有屬於VLAN 100和VLAN 200的第2層流量都會被複製並傳送到埠Fa3/30。如果目的地埠是流量受監控的同一VLAN的一部分，則不會捕獲流出目的地埠的流量。

使用**show monitor**命令驗證您的SPAN設定。

```
Cat6K-IOS#show monitor detail
Session 50
----------
Type               : Local Session
Source Ports       :
    RX Only        : None
    TX Only        : None
    Both           : None
Source VLANs       :
    RX Only        : None
    TX Only        : None
    Both           : 100,200
```

```
Source RSPAN VLAN : None
Destination Ports : Fa3/30
Filter VLANs      : None
Dest RSPAN VLAN   : None
```

使用VACL的配置

在此配置示例中，網路管理員提出了多項要求：

- 需要擷取VLAN 200中從VLAN 100中的主機(10.20.20.128/25)範圍到VLAN 100中的特定伺服器(10.10.10.101)的HTTP流量。
- 需要從VLAN 100捕獲傳輸方向中目的地為組地址239.0.0.100的組播使用者資料包協定(UDP)流量。

1. 定義要捕獲並傳送到分析的相關流量。
```
Cat6K-IOS(config)#ip access-list extended HTTP_UDP_TRAFFIC
Cat6K-IOS(config-ext-nacl)#permit tcp 10.20.20.128 0.0.0.127 host 10.10.10.101 eq www
Cat6K-IOS(config-ext-nacl)#permit udp any host 239.0.0.100
Cat6K-IOS(config-ext-nacl)#exit
```
2. 定義一個umberlla ACL以對映所有其他流量。
```
Cat6K-IOS(config)#ip access-list extended ALL_TRAFFIC
Cat6K-IOS(config-ext-nacl)#permit ip any any
Cat6K-IOS(config-ext-nacl)#exit
```

3. 定義VLAN訪問對映。
```
Cat6K-IOS(config)#vlan access-map HTTP_UDP_MAP 10
Cat6K-IOS(config-access-map)#match ip address HTTP_UDP_TRAFFIC
Cat6K-IOS(config-access-map)#action forward capture
Cat6K-IOS(config)#vlan access-map HTTP_UDP_MAP 20
Cat6K-IOS(config-access-map)#match ip address ALL_TRAFFIC
Cat6K-IOS(config-access-map)#action forward
Cat6K-IOS(config-access-map)#exit
```
4. 將VLAN訪問對映應用到適當的VLAN。
```
Cat6K-IOS(config)#vlan filter HTTP_UDP_MAP vlan-list 100
!--- Here 100 is the ID of VLAN on which the VACL is applied.
```
5. 配置捕獲埠。
```
Cat6K-IOS(config)#int fa3/30
Cat6K-IOS(config-if)#switchport capture allowed vlan ?
  WORD    VLAN IDs of the allowed VLANs when this po
  add     add VLANs to the current list
  all     all VLANs
  except  all VLANs except the following
  remove  remove VLANs from the current list

Cat6K-IOS(config-if)#switchport capture allowed vlan 100
Cat6K-IOS(config-if)#switchport capture
Cat6K-IOS(config-if)#exit
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

- **show vlan access-map** — 顯示VLAN訪問對映的內容。
```
Cat6K-IOS#show vlan access-map HTTP_UDP_MAP
```

```
Vlan access-map "HTTP_UDP_MAP"  10
        match: ip address HTTP_UDP_TRAFFIC
        action: forward capture
Vlan access-map "HTTP_UDP_MAP"  20
        match: ip address ALL_TRAFFIC
        action: forward
```

- **show vlan filter** — 顯示有關VLAN過濾器的資訊。

```
Cat6K-IOS#show vlan filter
VLAN Map HTTP_UDP_MAP:
        Configured on VLANs:  100
            Active on VLANs:  100
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 使用執行CatOS軟體的Cisco Catalyst 6000/6500進行VACL擷取，以進行詳細流量分析
- Cisco Catalyst 6500系列交換器支援
- LAN 產品支援
- LAN 交換技術支援
- 技術支援與文件 - Cisco Systems