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

目錄

簡介

本檔案將提供使用VLAN存取控制清單(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擷取連線埠使用方式與基於VLAN的交換連線埠分析器(SPAN)(VSPAN)使用方式不同的優點。

要在執行Cisco IOS®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Cisco IOS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：

- 虛擬LAN — 請參閱虛擬LAN/VLAN主幹協定(VLAN/VTP) — 簡介以瞭解詳細資訊。
- 訪問清單 — 有關詳細資訊，請參閱配置訪問控制。

採用元件

本檔案中的資訊是根據執行Catalyst OS版本8.1(2)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

此組態也可用於執行Catalyst OS 6.3版及更新版本的Cisco Catalyst 6000/6500系列交換器。

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會將流量從任何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。

來源連線埠是受監控以用於網路流量分析的連線埠。來源VLAN是受監控以用於網路流量分析的VLAN。VLAN型SPAN(VSPAN)分析一個或多個VLAN中的網路流量。您可以將VSPAN設定為輸入SPAN、輸出SPAN或兩者。來源VLAN中的所有連線埠都會成為VSPAN作業階段的可用來源連線埠。目的地連線埠（如果屬於任何管理來源VLAN）會排除在作業來源之外。如果在管理來源VLAN中新增或刪除連線埠，則會相應地修改操作來源。

VSPAN作業階段准則：

- 主干連線埠作為VSPAN作業階段的來源連線埠包括在內，但只有管理員來源清單中的VLAN會在主幹這些VLAN處於作用中時受到監控。
- 對於已設定輸入和輸出SPAN的VSPAN作業階段，系統根據您擁有的Supervisor Engine型別來執行：WS-X6K-SUP1A-PFC、WS-X6K-SUP1A-MSFC、WS-X6K-S1A-MSFC2、WS-X6K-S2-PFC2、WS-X6K-S1A-MSFC2、WS-SUP720、WS-SUP32-GE-3B — 如果兩個資料包在相同埠上得到交換，則由SPAN目的地埠轉發VLAN。WS-X6K-SUP1-2GE、WS-X6K-SUP1A-2GE — 僅一個資料包由SPAN目的地埠轉發。
- 帶內連線埠不作為VSPAN作業階段的作業來源包括在內。
- 清除VLAN時，會將其從VSPAN作業階段的來源清單中移除。
- 如果管理來源VLAN清單為空，則VSPAN作業階段會停用。
- VSPAN設定不允許非作用中VLAN。
- 如果任何來源VLAN成為RSPAN VLAN，VSPAN作業階段就會處於非作用中狀態。

如需來源VLAN的詳細資訊，請參閱來源VLAN的特性。

VLAN ACL

VACL可以訪問控制所有流量。您可以在交換機上配置VACL，使其適用於路由入或出自VLAN或在

VLAN內橋接的所有資料包。VACL嚴格用於安全封包過濾，並將流量重新導向到特定實體交換器連線埠。與Cisco IOS ACL不同，VACL不是由方向（輸入或輸出）定義的。

您可以在第3層地址上為IP和IPX配置VACL。所有其他協定均通過MAC地址和EtherType使用MAC VACL進行訪問控制。IP流量和IPX流量不受MAC VACL的訪問控制。所有其他流量型別（AppleTalk、DECnet等）都歸類為MAC流量。MAC VACL用於訪問控制此流量。

VACL支援的ACE

VACL包含存取控制專案(ACE)的有序清單。 每個VACL只能包含一種型別的ACE。每個ACE包含許多欄位，這些欄位與資料包的內容相匹配。每個欄位可以具有相關的位掩碼來指示哪些位相關。操作與每個ACE相關聯，說明發生匹配時系統應對資料包做什麼。該操作取決於功能。Catalyst 6500系列交換機在硬體中支援三種型別的ACE:

- IP ACE
- IPX ACE
- 乙太網ACE

此表列出了與每個ACE型別關聯的引數：

ACE型別	TCP或UDP	ICMP	其他IP	IPX	乙太網路
第4層引數	來源連線埠	-	-	-	-
	來源連線埠接線員	-	-	-	-
	目的地連線埠	-	-	-	-
	目的地連線埠接線員	ICMP代碼	-	-	-
	不適用	ICMP類型	不適用	-	-
第3層引數	IP ToS位元組	IP ToS位元組	IP ToS位元組	-	-
	IP來源位址	IP來源位址	IP來源位址	IPX來源網路	-
	IP目的地位址	IP目的地位址	IP目的地位址	IP目的地網路	-
	-	-	-	IP目的地節點	-
	TCP或UDP	ICMP	其他通訊協定	IPX封包型別	-
第2層引數	-	-	-	-	EtherType
	-	-	-	-	乙太網路來源位址
	-	-	-	-	乙太網目的地址

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，請參閱功能摘要和限制。
- 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，由於具有分類流量的廣泛功能，引入了捕獲埠功能，因此網路流量分析可以變得更為簡單。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。可建立的ACE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應用到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。

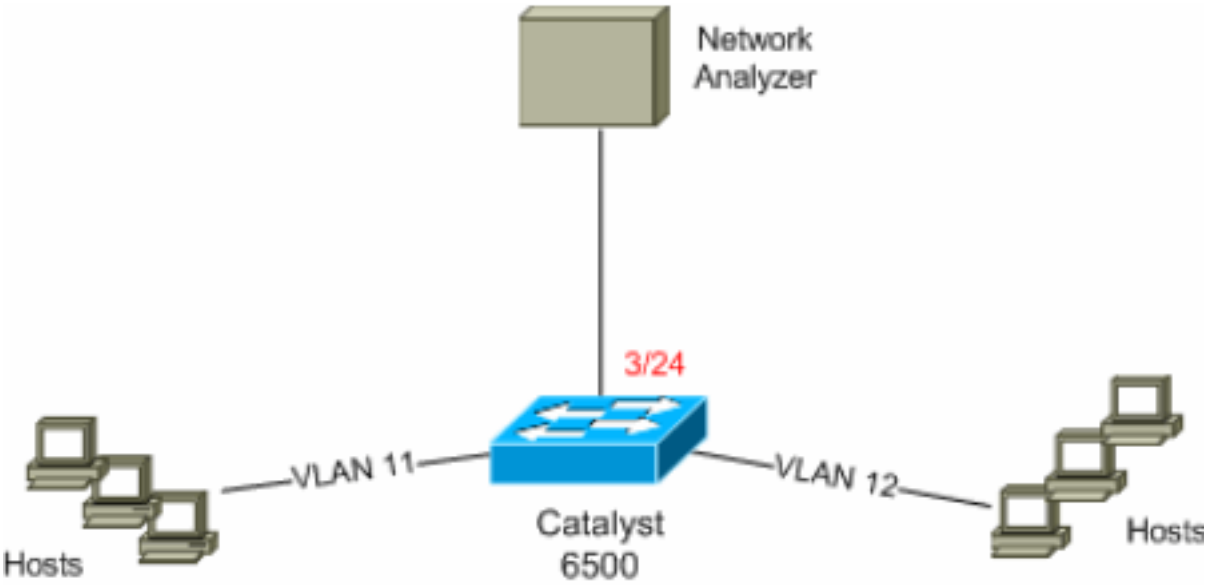
本檔案會使用以下設定：

- 使用基於VLAN的SPAN的組態
- 使用VACL的配置

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

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 11和VLAN 12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。在本範例中，流量流入VLAN 100和VLAN 200。

```
6K-CatOS> (enable) set span 11-12 3/24
!--- where 11-12 specifies the range of source VLANs and 3/24 specify the destination port.

2007 Jul 12 21:45:43 %SYS-5-SPAN_CFGSTATECHG:local span session inactive for des
tination port 3/24

Destination      : Port 3/24
Admin Source     : VLAN 11-12
Oper Source      : Port 3/11-12,16/1
Direction        : transmit/receive
Incoming Packets: disabled
Learning         : enabled
Multicast        : enabled
Filter           : -
Status           : active

6K-CatOS> (enable) 2007 Jul 12 21:45:43 %SYS-5-SPAN_CFGSTATECHG:local span sessi
on active for destination port 3/24
```

   這樣，所有屬於VLAN 11和VLAN 12的第2層流量都會被複製並傳送到埠3/24。
2. 使用**show span all**命令驗證您的SPAN設定。

```
6K-CatOS> (enable) show span all

Destination      : Port 3/24
Admin Source     : VLAN 11-12
Oper Source      : Port 3/11-12,16/1
Direction        : transmit/receive
Incoming Packets: disabled
Learning         : enabled
Multicast        : enabled
Filter           : -
Status           : active


Total local span sessions:  1

No remote span session configured
6K-CatOS> (enable)
```

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：

- 需要擷取從VLAN 12中的一系列主機(10.12.12.128/25)到VLAN 11中的特定伺服器(10.11.11.100)的HTTP流量。
- 需要從VLAN 11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. 使用安全ACL定義相關流量。請記住為定義的所有ACE提及關鍵字**capture**。

```
6K-CatOS> (enable) set security acl ip HttpUdp_Acl permit tcp 10.12.12.128 0.0.0.127 host
10.11.11.100 eq www capture
!--- Command wrapped to the second line. HttpUdp_Acl editbuffer modified. Use 'commit'
command to apply changes. 6K-CatOS> (enable) set security acl ip HttpUdp_Acl permit udp any
```

```
host 239.0.0.100 capture
HttpUdp_Acl editbuffer modified. Use 'commit' command to apply changes.
```

2. 驗證ACE配置是否正確且順序正確。

```
6K-CatOS> (enable) show security acl info HttpUdp_Acl editbuffer
set security acl ip HttpUdp_Acl
-------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
ACL HttpUdp_Acl Status: Not Committed
6K-CatOS> (enable)
```

3. 將ACL提交給硬體。

```
6K-CatOS> (enable) commit security acl HttpUdp_Acl
ACL commit in progress.

ACL 'HttpUdp_Acl' successfully committed.
6K-CatOS> (enable)
```

4. 驗證ACL的狀態。

```
6K-CatOS> (enable) show security acl info HttpUdp_Acl editbuffer
set security acl ip HttpUdp_Acl
-------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
ACL HttpUdp_Acl Status: Committed
6K-CatOS> (enable)
```

5. 將VLAN訪問對映應用到適當的VLAN。

```
6K-CatOS> (enable) set security acl map HttpUdp_Acl ?
  <vlans>                    Vlan(s) to be mapped to ACL
6K-CatOS> (enable) set security acl map HttpUdp_Acl 11
Mapping in progress.

ACL HttpUdp_Acl successfully mapped to VLAN 11.
6K-CatOS> (enable)
```

6. 檢驗ACL到VLAN的對映。

```
6K-CatOS> (enable) show security acl map HttpUdp_Acl
ACL HttpUdp_Acl is mapped to VLANs:
11
6K-CatOS> (enable)
```

7. 配置捕獲埠。

```
6K-CatOS> (enable) set vlan 11 3/24
VLAN  Mod/Ports
---- ----------------------
11    3/11,3/24
6K-CatOS> (enable)


6K-CatOS> (enable) set security acl capture-ports 3/24
Successfully set 3/24 to capture ACL traffic.
6K-CatOS> (enable)
```

注意：如果ACL對映到多個VLAN，則捕獲埠必須配置為所有這些VLAN。若要使擷取連線埠允許多個VLAN，請將連線埠設定為中繼線，並僅允許對應到ACL的VLAN。例如，如果ACL對映到VLAN 11和12，則完成配置。

```
6K-CatOS> (enable) clear trunk 3/24 1-10,13-1005,1025-4094
6K-CatOS> (enable) set trunk 3/24 on dot1q 11-12
6K-CatOS> (enable) set security acl capture-ports 3/24
```

8. 驗證捕獲埠配置。

```
6K-CatOS> (enable) show security acl capture-ports
ACL Capture Ports: 3/24
6K-CatOS> (enable)
```

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 security acl info** — 顯示當前配置或最後提交到NVRAM和硬體的VACL內容。
```
6K-CatOS> (enable) show security acl info HttpUdp_Acl
set security acl ip HttpUdp_Acl
---------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
6K-CatOS> (enable)
```
- **show security acl map** — 顯示特定ACL、埠或VLAN的ACL到VLAN或ACL到埠對映。
```
6K-CatOS> (enable) show security acl map all
ACL Name                         Type Vlans
-------------------------------- ---- -----
HttpUdp_Acl                         IP   11
6K-CatOS> (enable)
```
- **show security acl capture-ports** — 顯示捕獲埠清單。
```
6K-CatOS> (enable) show security acl capture-ports
ACL Capture Ports: 3/24
6K-CatOS> (enable)
```

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Cisco IOS軟體的Cisco Catalyst 6000/6500進行VACL擷取，以進行詳細流量分析
- 配置訪問控制 — Catalyst 6500系列軟體配置指南8.6
- LAN 產品支援頁面
- LAN 交換支援頁面
- 技術支援與文件 - Cisco Systems