CatOS ソフトウェアが稼働する Cisco Catalyst 6000/6500 を使った、詳細トラフィック分析用 VACL キャプチャ

内容

概要
前提条件
要件
使用するコンポーネント
関連製品
表記法
背景説明
VLANベースのSPAN
VLAN ACL
VSPAN ではなく VACL を使用する利点
設定
ネットワーク図
VLAN-based SPAN を使用する場合の設定
VACL を使用する場合の設定
確認
トラブルシュート
関連情報

概要

このドキュメントでは、より細かくネットワーク トラフィックを分析するために VLAN アクセス コントロール リスト（ACL）（VACL）キャプチャ ポート機能を使用する設定例を紹介します。このドキュメントでは、VLAN ベースのスイッチド ポート アナライザ（SPAN）（VSPAN）と比較した場合の VACL キャプチャ ポートを使用する利点についても説明します。

Cisco IOS®ソフトウェアが稼働するCisco Catalyst 6000/6500でVACLキャプチャポート機能を設定するには、『Cisco IOSソフトウェアが稼働するCisco Catalyst 6000/6500での詳細なトラフィック分析』を参照してください。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- 仮想LAN：詳細は、『仮想LAN/VLANトランキングプロトコル(VLAN/VTP)：概要』を参照してください。
- アクセスリスト：詳細は、『アクセスコントロールの設定』を参照してください。

使用するコンポーネント

このドキュメントの情報は、Catalyst OS(CatOS)リリース8.1(2)が稼働するCisco Catalyst 6506シリーズスイッチに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

関連製品

この設定は、Catalyst OSリリース6.3以降が稼働するCisco Catalyst 6000/6500シリーズスイッチでも使用できます。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

VLANベースのSPAN

SPANは、任意のVLAN内の1つ以上の送信元ポート、または1つ以上のVLANからのトラフィックを分析のために宛先ポートにコピーします。ローカル SPAN は、同じ Catalyst 6500 シリーズ スイッチ上の送信元ポート、送信元 VLAN、および宛先ポートをサポートします。

送信元ポートは、ネットワーク トラフィック分析のためにモニタ対象になるポートです。送信元 VLAN は、ネットワーク トラフィック分析のためにモニタ対象になる VLAN です。VLANベースのSPAN(VSPAN)は、1つ以上のVLANのネットワークトラフィックを分析します。VSPANは、入力SPAN、出力SPAN、またはその両方として設定できます。ソースVLANのすべてのポートが、VSPANセッションの動作可能な送信元ポートになります。宛先ポートが管理ソースVLANのいずれかに属している場合、そのポートは運用ソースから除外されます。管理ソースVLANのポートを追加または削除すると、それに応じて運用ソースが変更されます。

VSPANセッションのガイドライン：

- トランクポートはVSPANセッションの送信元ポートとして含まれますが、これらのVLANがトランクに対してアクティブな場合、Admin送信元リストにあるVLANだけがモニタされます。
- 入力SPANと出力SPANの両方が設定されたVSPANセッションでは、次のスーパーバイザエンジンのタイプに基づいてシステムが動作します。WS-X6K-SUP1A-PFC、WS-X6K-SUP1A-MSFC、WS-X6K-S1A-MSFC2、WS-X6K-S2-PFC2、WS-X6K-S1A-MSFC WS-SUP720、WS-SUP32-GE-3B：パケットが同じVLANでスイッチングされる場合、SPAN宛先ポートによって2つのパケットが転送されます。WS-X6K-SUP1-2GE、WS-X6K-SUP1A-2GE:SPAN宛

先ポートによって転送されるパケットは1つだけです。
- インバンドポートは、VSPANセッションの運用送信元として含まれません。
- VLANがクリアされると、VSPANセッションのソースリストから削除されます。
- 管理ソースVLANリストが空の場合、VSPANセッションは無効になります。
- 非アクティブなVLANは、VSPAN設定では許可されません。
- 送信元VLANのいずれかがRSPAN VLANになると、VSPANセッションは非アクティブになります。

ソースVLANの詳細については、「ソースVLANの特性」を参照してください。

VLAN ACL

VACLはすべてのトラフィックを制御できます。スイッチ上のVACLを設定して、VLANにルーティングされるか、VLAN内でブリッジされるすべてのパケットに適用できます。VACLは、セキュリティパケットフィルタリングおよび特定の物理スイッチポートへのトラフィックのリダイレクト専用です。Cisco IOS ACLとは異なり、VACLは方向（入力または出力）によって定義されません。

IPおよびIPXのレイヤ3アドレスにVACLを設定できます。他のすべてのプロトコルは、MACアドレスとEtherTypeを通じてMAC VACLを使用してアクセス制御されます。IPトラフィックとIPXトラフィックは、MAC VACLによって制御されたアクセスではありません。他のすべてのトラフィックタイプ（AppleTalk、DECnetなど）は、MACトラフィックとして分類されます。MAC VACLは、このトラフィックのアクセスコントロールに使用されます。

VACLでサポートされるACE

VACLには、アクセスコントロールエントリ(ACE)の順序リストが含まれています。 各VACLには、1つのタイプのACEのみを含めることができます。各ACEには、パケットの内容に一致する多数のフィールドが含まれています。各フィールドには、関連するビットを示す関連ビットマスクを設定できます。アクションは、一致が発生したときにシステムがパケットに対して行うべき処理を記述する各ACEに関連付けられます。動作は機能によって異なります。Catalyst 6500シリーズスイッチは、ハードウェアで次の3種類のACEをサポートします。

- IP ACE
- IPX ACE
- イーサネットACE

次の表に、各ACEタイプに関連付けられているパラメータを示します。

ACEタイプ	TCPまたはUDP	ICMP	その他のIP	IPX	イーサネット
レイヤ4パラメータ	送信元ポート	-	-	-	-
	送信元ポートオペレータ	-	-	-	-
	宛先ポート	-	-	-	-
	宛先ポートオペレータ	ICMPコード	-	-	-
	N/A	ICMP	N/A	-	-

		タイプ			
レイヤ3パラメータ	IP ToSバイト	IP ToSバイト	IP ToSバイト	-	-
	IP送信元アドレス	IP送信元アドレス	IP送信元アドレス	IPXソースネットワーク	-
	IP宛先アドレス	IP宛先アドレス	IP宛先アドレス	IP宛先ネットワーク	-
	-	-	-	IP宛先ノード	-
	TCPまたはUDP	ICMP	その他のプロトコル	IPXパケットタイプ	-
レイヤ2パラメータ	-	-	-	-	EtherType
	-	-	-	-	イーサネット送信元アドレス
	-	-	-	-	イーサネット宛先アドレス

VSPAN ではなく VACL を使用する利点

トラフィックの分析に VSPAN を使用する場合は、いくつかの制約があります。

- 対象の VLAN 内を流れるすべてのレイヤ 2 トラフィックがキャプチャされます。そのため、分析するデータ量が増大します。
- Catalyst 6500 シリーズ スイッチに設定できる SPAN セッション数に制限があります。詳細は、「機能の概要と制限」を参照してください。
- 宛先ポートは、モニタ対象になっているすべての送信元ポートの送受信トラフィックのコピーを受け取ります。宛先ポートがオーバーサブスクライブされている場合、輻輳状態になる可能性があります。この輻輳により、1 つ以上の送信元ポートのトラフィックの転送が影響を受ける可能性があります。

VACL キャプチャ ポート機能は、これらの制限の克服に役立ちます。VACLは、主にトラフィックをモニタするように設計されていません。ただし、トラフィックを分類する広範な機能を備えたキャプチャポート機能が導入され、ネットワークトラフィックの分析がより簡単になりました。VSPAN ではなく VACL キャプチャ ポートを使用する利点は、次のとおりです。

- きめ細かなトラフィック分析VACL では、送信元 IP アドレス、宛先 IP アドレス、レイヤ 4 プロトコル タイプ、送信元と宛先のレイヤ 4 ポートなどの情報に基づいて照合できます。この機能により、VACL はきめ細かなトラフィックの識別とフィルタリングに効果を発揮します。
- セッションの数VACLはハードウェアで適用されます。作成できるACEの数は、スイッチで使

用可能なTCAMによって異なります。
- 宛先ポートのオーバーサブスクリプションきめ細かなトラフィックの識別によって宛先ポートに転送されるフレームの数が減少するため、オーバーサブスクリプションの可能性が軽減されます。
- パフォーマンスVACLはハードウェアで適用されます。Cisco Catalyst 6500シリーズスイッチのVLANにVACLを適用しても、パフォーマンスに悪影響はありません。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

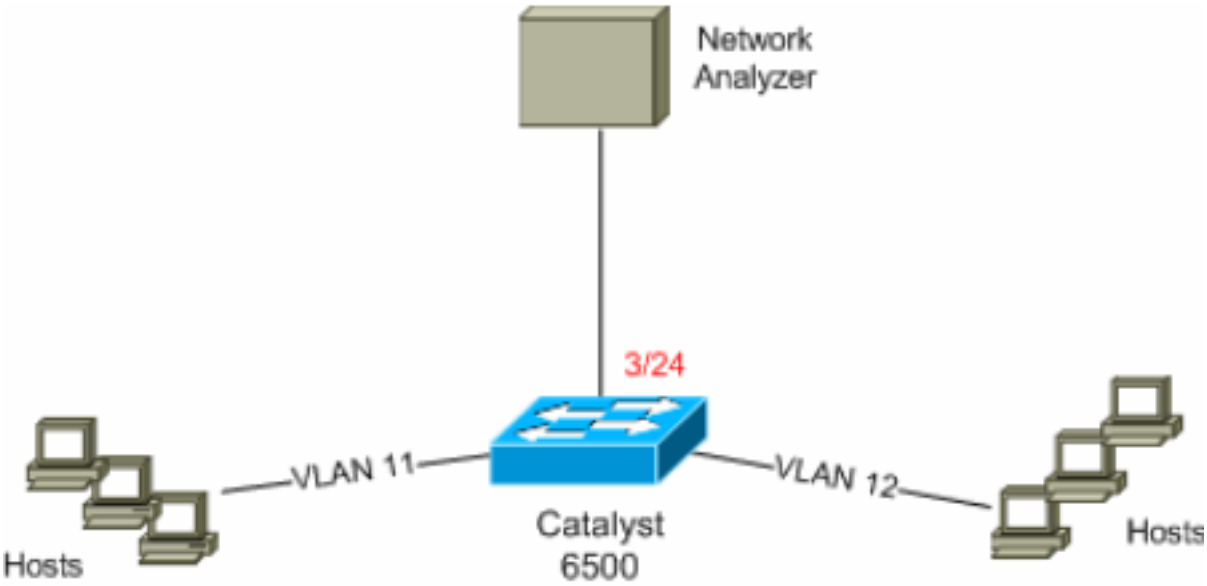
このドキュメントでは、次の構成を使用します。

- VLAN-based SPAN を使用する場合の設定
- VACL を使用する場合の設定

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



VLAN-based SPAN を使用する場合の設定

この設定例では、VLAN 11 と VLAN 12 のすべてのレイヤ 2 トラフィック フローをキャプチャし、これをネットワーク アナライザ デバイスに送信するために必要な手順を説明します。

1. 対象トラフィックを指定します。この例では、VLAN 100およびVLAN 200を流れるトラフィックです。

```
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
```

これにより、VLAN 11およびVLAN 12に属するすべてのレイヤ2トラフィックがコピーされ、ポート3/24に送信されます。

2. **show span all**コマンドを使用して、SPANの設定**を確認**します。

```
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)
```

VACL を使用する場合の設定

この設定例では、ネットワーク管理者から次のような要件が提示されています。

- VLAN 12のホスト(10.12.12.128/25)の範囲からVLAN 11の特定のサーバ(10.11.11.100)へのHTTPトラフィックをキャプチャする必要があります。
- グループ アドレス 239.0.0.100 を宛先とする送信方向のマルチキャスト ユーザ データグラム プロトコル (UDP) トラフィックを VLAN 11 からキャプチャする必要がある

1. セキュリティACLを使用して対象トラフィックを定義します。定義されているすべてのACEに対してキーワードcaptureを記述してください。

```
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. ACE設定が正しく、正しい順序で行われていることを確認します。

```
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. ACLをハードウェアにコミットします。

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

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

4. ACLのステータスを確認します。

```
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. VLAN アクセス マップを適切な VLAN にマッピングします。

```
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. ACLとVLANのマッピングを確認します。

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

7. キャプチャ ポートを設定します。

```
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：ACLが複数のVLANにマッピングされている場合は、キャプチャポートを、これらのVLANすべてに設定する必要があります。キャプチャポートで複数のVLANを許可するには、ポートをトランクとして設定し、ACLにマッピングされたVLANだけを許可します。たとえば、ACLがVLAN 11とVLAN 12にマッピングされている場合は、設定を完了します。

```
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. キャプチャポートの設定を確認します。

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

確認

ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサ

ポートします。 OIT を使用して、show コマンドの出力の分析を表示します。

- **show security acl info**：現在NVRAMおよびハードウェアに対して設定されている、または最後にコミットされたVACLの内容を表示します。

```
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**：特定のACL、ポート、またはVLANのACLからVLANへのマッピングまたはACLからポートへのマッピングを表示します。

```
6K-CatOS> (enable) show security acl map all
ACL Name                         Type Vlans
-------------------------------- ---- -----
HttpUdp_Acl                         IP   11
6K-CatOS> (enable)
```

- **show security acl capture-ports**：キャプチャポートのリストを表示します。

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

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco IOS ソフトウェアが稼働する Cisco Catalyst 6000/6500 による詳細なトラフィック分析用 VACL キャプチャ
- アクセスコントロールの設定 – Catalyst 6500シリーズソフトウェアコンフィギュレーションガイド8.6
- LAN 製品に関するサポート ページ
- LAN スイッチングに関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems