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

目次

はじめに

このドキュメントでは、ネットワーク トラフィック分析に VLAN ACL（VACL）キャプチャ ポート機能を使用するための設定例についてさらに詳しく説明します。 また、VLAN ベース SPAN（VSPAN）を使用するのではなく、VACL キャプチャ ポートを使用する利点も示します。

Catalyst OS ソフトウェアが稼働する Cisco Catalyst 6000/6500 での VACL キャプチャ ポート機能の設定については、『CatOS ソフトウェアが稼働する Cisco Catalyst 6000/6500 を使用した VACL キャプチャのきめ細か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。

- IP アクセス リスト： 詳細は、『IP アクセス リストの設定』を参照してください。

- 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。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。
Cisco IOS® ソフトウェア リリース 12.2(18)SXF8 が稼働する Cisco Catalyst 6506 シリーズ スイッチ

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

関連製品

このドキュメントで取り上げる設定は、Cisco IOS ソフトウェア リリース 12.1(13)E 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-based SPAN

SPAN (スイッチド ポート アナライザ) は、任意の VLAN 上の 1 つまたは複数の送信元ポートからのトラフィック、あるいは 1 つまたは複数の VLAN からのトラフィックを分析するために宛先ポートへコピーします。 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 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-based SPAN (VSPAN) は、VLAN を SPAN 送信元として使用します。 送信元 VLAN にあるすべてのポートが、送信元ポートになります。 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。 トランク ポートを、送信元ポートとして設定したり、非トランク送信元ポートと混在させたりすることができますが、SPAN は、送信元トランク ポートからのカプセル化をコピーしません。

入力および出力の両方が設定されている VSPAN セッションについては、2 つのパケットが同じ VLAN でスイッチングされている場合、それらは宛先ポートから (1 つは入力ポートからの入力トラフィックとして、もう 1 つは出力ポートからの出力トラフィックとして) 転送されます。

VSPAN は、VLAN 中のレイヤ 2 ポートから出入りするトラフィックだけをモニタします。

- ある VLAN を入力送信元として設定し、トラフィックがそのモニタ対象の VLAN にルーティングされる場合、ルーティングされたトラフィックは、その VLAN 内のレイヤ 2 ポートに着信した入力トラフィックと見なされないため、モニタされません。
- ある VLAN を出力送信元として設定し、トラフィックがそのモニタ対象の VLAN からルーテ

ィングされる場合、ルーティングされたトラフィックは、その VLAN 内のレイヤ 2 ポートから発信された出力トラフィックと見なされないため、モニタされません。

送信元 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、VLAN 内でブリッジされるか、VLAN または VACL キャプチャの WAN インターフェイスとの間でルーティングされているすべてのパケットのアクセス コントロールを行います。 ルータ インターフェイスでのみ設定され、ルーティング対象パケットだけに適用される通常の Cisco IOS 標準または拡張 ACL と異なり、VACL はすべてのパケットに適用され、どの VLAN または WAN インターフェイスにも適用できます。 VACL は、ハードウェアで処理されます。 VACL は Cisco IOS ACL を使用します。 VACL は、ハードウェアでサポートされていないすべての Cisco IOS ACL フィールドを無視します。

IP、IPX、および MAC レイヤ トラフィックの場合は、VACL を設定できます。 WAN インターフェイスに適用される VACL は、VACL キャプチャの IP トラフィックだけをサポートします。

VACL を設定して VLAN に適用すると、その VLAN に着信するすべてのパケットが、この VACL と照合されます。 VACL を VLAN に適用し、その VLAN 内のルーテッド インターフェイスに ACL を適用すると、その VLAN に着信したパケットは最初に VACL と照合されます。そこで許可されると、次に入力 ACL と照合され、その後ルーテッド インターフェイスで処理されます。 別の VLAN にルーティングされるパケットは、最初に、ルーテッド インターフェイスに適用されている出力 ACL と照合されます。そこで許可されると、宛先 VLAN 用に設定された VACL が適用されます。 VACL があるパケット タイプ用に設定されていて、VACL と該当タイプのパケットとが一致しない場合、デフォルト動作ではパケットが拒否されます。 VACL のキャプチャ オプションを使用する際は、次のガイドラインに留意してください。

- キャプチャ ポートは、非同期転送モード（ATM）ポートとして使用できません。
- キャプチャ ポートは、VLAN のスパニングツリー フォワーディング ステートに設定する必要があります。
- スイッチのキャプチャ ポート数に制限はありません。
- キャプチャ ポートでキャプチャされるのは、設定されている ACL で許可されたパケットだけです。
- キャプチャ ポートから送出されるのは、そのキャプチャ ポートの VLAN に属しているトラフィックだけです。 多数の VLAN へのトラフィックをキャプチャするために、必要な VLAN のトラフィックを伝送できるトランクとしてキャプチャ ポートを設定してください。

注意： ACL の不正確な組み合せはトラフィックフローを破壊する場合があります。 デバイスで ACL を設定する場合は、細心の注意を払う必要があります。

注: Catalyst 6000 シリーズ スイッチで IPv6 を使用する場合、VACL はサポートされません。 VLAN ACL リダイレクトと IPv6 の両方を同時に使用することはできないため、IPv6 トラフィックの照合に ACL は使用されません。

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

については、『ローカル SPAN および RSPAN セッションの制限』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 はトラフィックのモニタを主目的として設計された訳ではありませんが、トラフィックを分類する広範な機能とともにキャプチャ ポート機能が導入されているため、これを使用することで、ネットワーク トラフィックの分析がシンプルになります。 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 はハードウェアで処理されます。 作成できるアクセス コントロール エントリ（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 はハードウェアで処理されます。 Cisco Catalyst 6500 シリーズ スイッチの VLAN に VACL を適用しても、パフォーマンスが低下することはありません。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

- 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: このドキュメント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）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

VLAN-based SPAN を使用する場合の設定

この設定例では、VLAN 100 と VLAN 200 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 と VLAN 200 のトラフィックです。

```
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. キャプチャしたトラフィックの宛先ポートを指定します。

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

この例では、VLAN 100 と VLAN 200 に属しているすべてのレイヤ 2 トラフィックがコピーされ、ポート Fa3/30 に送信されます。 宛先ポートがモニタ対象のトラフィックと同じ VLAN に属している場合、宛先ポートから送出されるトラフィックはキャプチャされません。

show monitor コマンドを使用して SPAN の設定を確認します。

```
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
```

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 200 の一定範囲のホスト（10.20.20.128/25）からの HTTP トラフィックをキャプチャする必要がある
- 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 100 からキャプチャする必要がある

1. 分析対象としてキャプチャおよび送信するトラフィックを定義します。

```
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. 他のすべてのトラフィックをマッピングする包括的な ACL を定義します。

```
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. VLAN アクセス マップを定義します。

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

```
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. キャプチャ ポートを設定します。

```
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
```

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show vlan access-map** — VLAN アクセス マップの内容を表示します。

```
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** — VLAN フィルタについての情報を表示します。

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

トラブルシューティング

現在のところ、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

- 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
- Cisco Catalyst 6500 シリーズ スイッチに関するサポート ページ
- 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