Catalyst 4500 スイッチでの ACL および QoS TCAM 枯渇の防止

目次

概要

Cisco Catalyst 4500 および Catalyst 4948 シリーズ スイッチは、TCAM（Ternary Content Addressable Memory）を使用して、ワイヤ速度のアクセス コントロール リスト（ACL）および QoS 機能をサポートします。 ACL とポリシーをイネーブルにしても、ACL 全体が TCAM にロードされていれば、スイッチのスイッチングとルーティングのパーフォーマンスが低下することはありません。 TCAM が使い果たされている場合、パケットは CPU パスで転送される場合がありますが、これらのパケットのパフォーマンスが低下する可能性があります。 このドキュメントでは、次の項目についての詳細情報を提供します。

- Catalyst 4500 と Catalyst 4948 で使用されているさまざまな種類の TCAM
- Catalyst 4500 での TCAM のプログラム方法
- スイッチで ACL と TCAM を最適に設定して TCAM の枯渇を防止する方法

前提条件

要件

このドキュメントに関する固有の要件はありません。

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。

- Catalyst 4500 シリーズ スイッチ
- Catalyst 4948 シリーズ スイッチ

注: このドキュメントが対象とするのは Cisco IOS(R) ソフトウェア ベースのスイッチだけで、Catalyst OS（CatOS）ベースのスイッチは対象外です。

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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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

さまざまな種類の ACL および QoS ポリシーをハードウェアで実装するために、Catalyst 4500 は、ハードウェア ルックアップ テーブル（TCAM）とさまざまなハードウェア レジスタをスーパーバイザ エンジンでプログラムします。 パケットが到着すると、スイッチでハードウェア テーブル ルックアップ（TCAM ルックアップ）が行われ、そのパケットを許可するか、拒否するかが決定されます。

Catalyst 4500 ではさまざまな種類の ACL がサポートされています。 表 1 は、これらの種類の ACL の概要を示します。

表 1：Catalyst 4500 スイッチでサポートされている ACL の種類

ACL タイプ	適用箇所	制御されるトラフィック	方向
RACL[1]	L3[2] ポート、L3 チャネル、または SVI[3]（VLAN）	ルーティング対象 IP トラフィック	着信または発信
VACL[4]	VLAN（**vlan filter** コマンドによる）	VLAN へ、または VLAN からルーティングされるか、または VLAN 内でブリッジされるすべてのパケット	方向性なし
PACL[5]	L2[6] ポートか L2 チャネル	すべての IP トラフィックおよび non-IPv4[7] トラフィック（MAC ACL によって）	着信または発信

1 RACL = ルータ ACL

2 L3 = レイヤ 3

[3] SVI = switched virtual interface（スイッチ仮想インターフェイス）

[4] VACL = VLAN ACL

5 PACL = ポート ACL

[6] L2 = レイヤ 2

[7] IPv4 = IP バージョン 4

Catalyst 4500 ACL および QoS ハードウェアのプログラミング アーキテクチャ

Catalyst 4500 TCAM のエントリ数は次のようになります。

- セキュリティ ACL（機能 ACL）に 32,000 エントリ
- QoS ACL に 32,000 エントリ

セキュリティ ACL および QoS ACL の両方では、次のように専用エントリとなっています。

- 入力方向に 16,000 エントリ
- 出力方向に 16,000 エントリ

図 3 は、専用 TCAM エントリを示します。 TCAM の詳細については、「TCAM の種類」セクションを参照してください。

表 2 に、さまざまな Catalyst 4500 スーパーバイザ エンジンおよびスイッチで使用可能な ACL リソースを示します。

表 2：さまざまなスーパーバイザ エンジンとスイッチの Catalyst 4500 ACL リソース

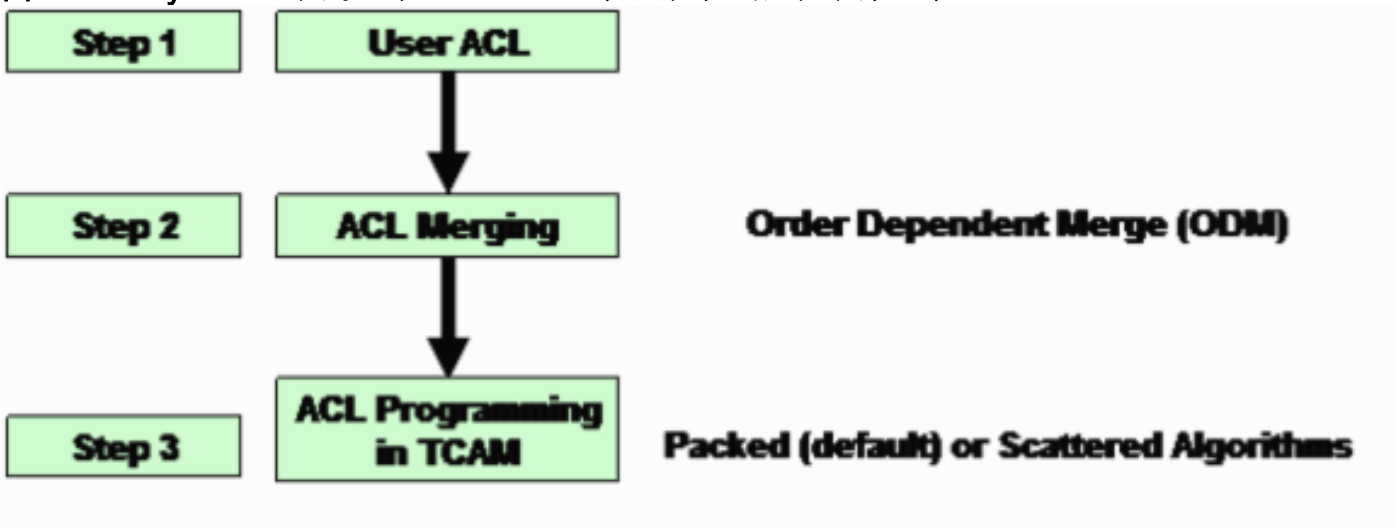
製品	TCAM バージョン	Feature TCAM（方向ごと）	QoS TCAM（方向ごと）
スーパーバイザ エンジン II+	2	8000 エントリ、1000 マスク	8000 エントリ、1000 マスク
スーパーバイザ エンジン II+TS/III/IV/V および WS-C4948	2	16,000 エントリ、2000 マスク	16,000 エントリ、2000 マスク
スーパーバイザ エンジン V-10GE と WS-C4948-10GE	3	16,000 エントリ、16,000 マスク	16,000 エントリ、16,000 マスク

Catalyst 4500 では、IP ユニキャストとマルチキャスト ルーティングに別々の専用 TCAM が使用されます。 Catalyst 4500 では、ユニキャストとマルチキャストのルートが共用するルート エントリを最大 128,000 まで持つことができます。 ただし、これらの詳細については、このドキュメントでは取り上げていません。 このドキュメントでは、セキュリティおよび QoS の TCAM 枯渇

の問題だけを取り上げます。

図 1 は、Catalyst 4500 のハードウェア テーブルに ACL をプログラムするステップを示します。

図 1：Catalyst 4500 スイッチでの ACL のプログラミング ステップ



ステップ 1

このステップでは次の作業のいずれかが必要です。

- インターフェイスまたは VLAN への ACL または QoS ポリシーの設定および適用ACL の作成は動的に発生する可能性があります。 その一例は、IP ソース ガード（IPSG）機能の場合です。 この機能では、ポートに関連付けられた IP アドレスのための PACL が、スイッチにより自動的に作成されます。
- 既存の ACL の変更

注: ACL を設定しただけでは、TCAM のプログラミングにはなりません。 TCAM に ACL をプログラムするには、ACL（QoS ポリシー）をインターフェイスに適用する必要があります。

ステップ 2

ACL はハードウェア テーブル（TCAM）にマージされて初めて、プログラム可能となります。 このマージにより、ハードウェア内に複数の ACL（PACL、VACL、または RACL）が結合してプログラムされます。 この方法では、パケットの論理転送パスで該当するすべての ACL に対してチェックするために必要なのは、1 つのハードウェア ルックアップだけです。

たとえば、図 2 では、PC-A から PC-C にルーティングされた可能性のあるパケットには、次の ACL を使用できます。

- PC-A のポートの入力 PACL
- VLAN 1 の VACL
- 入力方向の VLAN 1 インターフェイス上の入力 RACL

これらの 3 つの ACL がマージされると、許可か拒否の転送決定を行うのに、入力 TCAM での単一のルックアップしか必要ありません。 同様に、TCAM は次の 3 つの ACL のマージ結果でプログラムされるので、単一の出力ルックアップしか必要ありません。

- VLAN 2 インターフェイス上の出力 RACL
- VLAN 2 VACL

- PC-C ポート上の出力 PACL

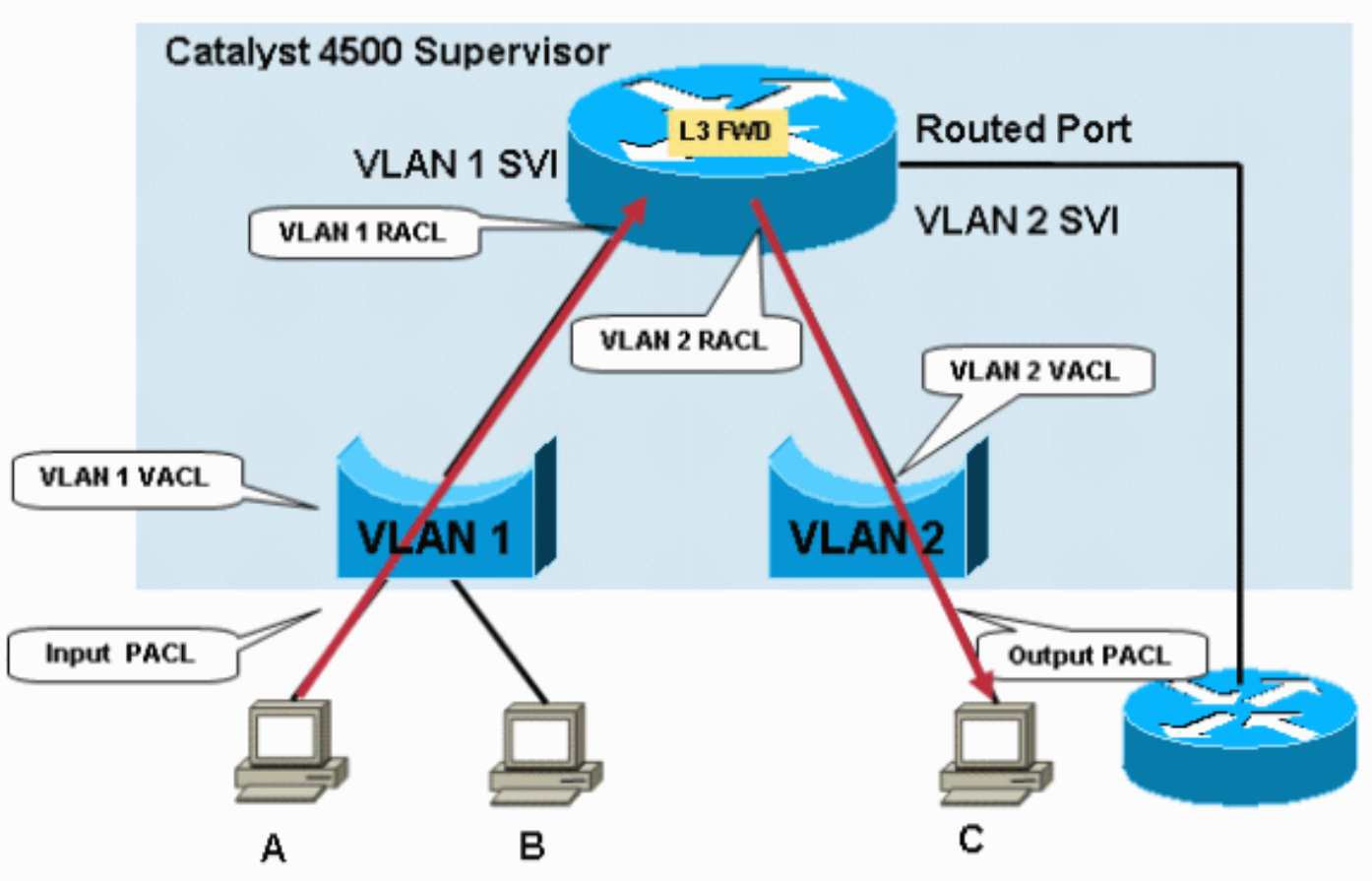
入力用の単一のルックアップと出力用の単一のルックアップを使用すると、これらの ACL のいずれかまたはすべてがパケット転送パスにある場合、パケットのペナルティ ハードウェア転送は発生しません。

注: 入力と出力の TCAM ルックアップは、ハードウェア上で同時に行われます。 よくある誤解は、論理パケット フローから考えられるように、出力 TCAM ルックアップが入力 TCAM ルックアップ後に発生するということです。 Catalyst 4500 の出力ポリシーは入力ポリシーが変更された QoS パラメータを照合できないので、これを理解しておくことは重要です。 セキュリティ ACL の場合は、最も深刻な動作が発生します。 次のいずれかの状態でパケットが廃棄されます。

- 入力ルックアップの結果がドロップで、出力ルックアップの結果が許可の場合
- 入力ルックアップの結果が許可で、出力ルックアップの結果がドロップの場合

注: 入力および出力の両方のルックアップ結果が許可の場合、パケットは許可されます。

図 2：Catalyst 4500 スイッチでのセキュリティ ACL によるフィルタリング



Catalyst 4500 での ACL のマージは順序に依存します。 このプロセスは Order Dependent Merge（ODM）としても知られています。 ODM を使用する場合は、ACL エントリが、ACL での表示順序でプログラムされます。 たとえば、ACL に 2 つのアクセス コントロール エントリ（ACE）がある場合は、スイッチが最初に ACE 1 を、次に ACE 2 をプログラムします。 ただし、順序の依存関係は、指定した ACL 内の ACE の間でのみ保持されます。 たとえば、ACL 120 の ACE は、TCAM の ACL 100 で ACE より先に開始できます。

ステップ 3

マージされた ACL は TCAM 内にプログラムされます。 ACL または QoS の入力や出力の TCAM は、さらに PortAndVlan と PortOrVlan の 2 つの領域に分割されます。 同じパケット パスに次の

*両方*の ACL が設定されている場合、マージされた ACL は TCAM の PortAndVlan 領域にプログラムされます。

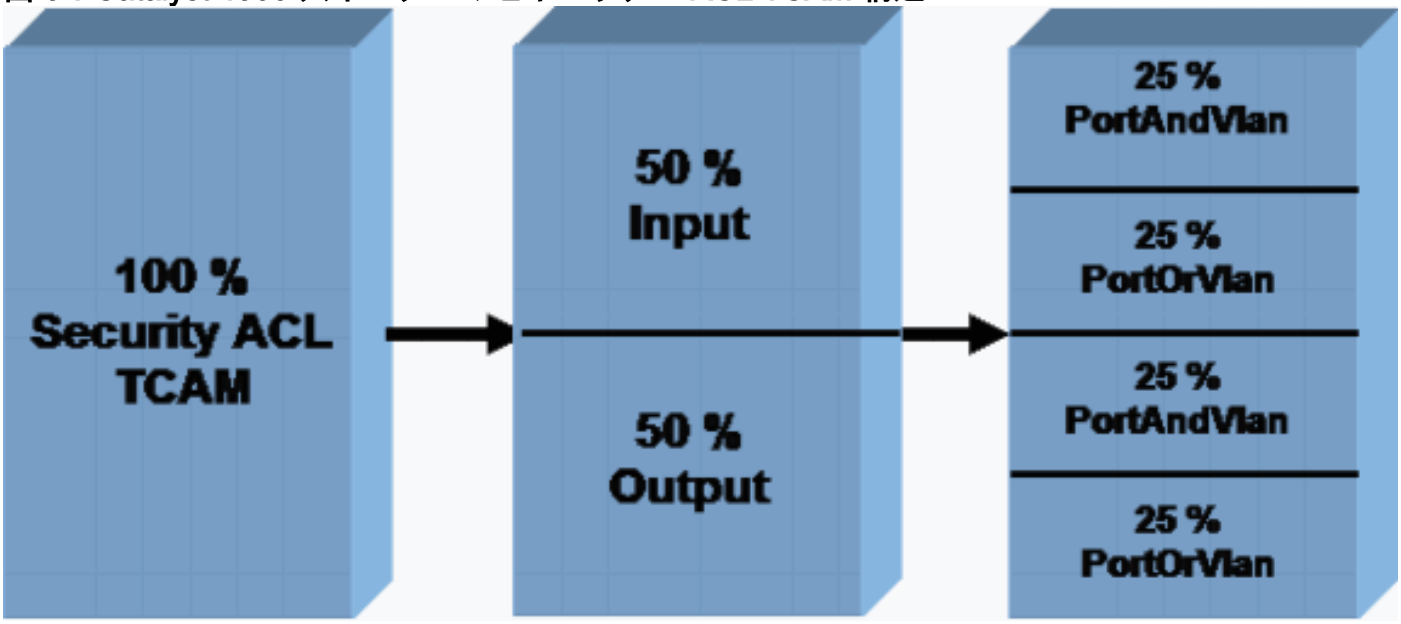
- PACL**注:** PACL は通常のフィルタリング ACL あるいは IPSG によって作成されたダイナミック ACL です。
- VACL または RACL

パケットの特定のパスに PACL、VACL、または RACL だけがある場合は、ACL が TCAM の PortOrVlan 領域にプログラムされます。 図 3 は、さまざまなタイプの ACL のセキュリティ ACL TCAM の切り分けを示します。 Qos も、同様に切り分けられた別々の専用 TCAM を持ちます。

現時点では、TCAM のデフォルトの割り当ては変更できません。 ただし、将来のソフトウェア リリースでは、PortAndVlan および PortOrVlan 領域で使用できる TCAM 割り当て変更機能を提供する計画があります。 この変更により、入力 TCAM または出力 TCAM のいずれかで、PortAndVlan と PortOrVlan の領域を増やしたり減らしたりすることが可能になります。

注: PortAndVlan 領域の割り当てを増加すると、必ず、入力または出力 TCAM の PortOrVlan 領域で同等の減少が発生します。

図 3：Catalyst 4500 スイッチ上のセキュリティ ACL TCAM 構造



show platform hardware ACL statistics utilization brief コマンドにより、ACL と QoS 両方の TCAM について、領域ごとの TCAM 使用率が表示されます。 このコマンドの出力では、利用可能なマスクとエントリが、図 3 で示したように領域ごとに表示されます。 次の出力例は Catalyst 4500 スーパーバイザ エンジン II+ によるものです。

注: マスクとエントリの詳細については、このドキュメントの「TCAM の種類」セクションを参照してください。

```
Switch#show platform hardware acl statistics utilization brief Entries/Total(%) Masks/Total(%) -
---------------- --------------- Input Acl(PortAndVlan) 2016 / 4096 ( 49) 252 / 512 ( 49) Input
Acl(PortOrVlan) 6 / 4096 ( 0) 5 / 512 ( 0) Input Qos(PortAndVlan) 0 / 4096 ( 0) 0 / 512 ( 0)
Input Qos(PortOrVlan) 0 / 4096 ( 0) 0 / 512 ( 0) Output Acl(PortAndVlan) 0 / 4096 ( 0) 0 / 512 (
0) Output Acl(PortOrVlan) 0 / 4096 ( 0) 0 / 512 ( 0) Output Qos(PortAndVlan) 0 / 4096 ( 0) 0 /
512 ( 0) Output Qos(PortOrVlan) 0 / 4096 ( 0) 0 / 512 ( 0) L4Ops: used 2 out of 64
```

TCAM の種類

Catalyst 4500 は、表 2 に示すように、2 種類の TCAM を使用します。 このセクションでは、2

つの TCAM の違いを説明して、ご使用のネットワークと設定に適切な製品を選択できるようにします。

TCAM 2 では、8 つのエントリが 1 つのマスクを共有する構造が使用されています。 ACE 内の 8 個の IP アドレスは、その一例です。 複数のエントリが共有マスクとして同一のマスクを使用する必要があります。 各 ACE に異なるマスクがある場合は、エントリが、必要に応じて異なるマスクを使用する必要があります。 別々のマスクの使用は、マスクの枯渇につながる可能性があります。 TCAM でのマスクの枯渇は、TCAM 枯渇の一般的な原因の 1 つです。

TCAM 3 では、このような制限はありません。 各エントリには、TCAM で一意のマスクを指定できます。 ハードウェアで使用できるすべてのエントリを完全に使用することは、そのエントリのマスクに関係なく、可能です。

このハードウェア アーキテクチャを示すために、このセクションの例で、TCAM 2 と TCAM 3 がハードウェアで ACL をプログラムする方法を示します。

```
access-list 101 permit ip host 8.1.1.1 any
access-list 101 deny ip 8.1.1.0 0.0.0.255 any
```

この ACL の例には 2 つの別々のマスクを持つ 2 つのエントリがあります。 ACE 1 はホスト エントリであるため、/32 マスクがあります。 ACE 2 は、/24 マスクを持つサブネット エントリです。 2 番目のエントリはマスクが異なるため、マスク 1 では空のエントリを使用できず、TCAM 2.の場合には、異なるマスクが使用されます。

次の表は TCAM 2 で ACL がプログラムされるしくみを示しています。

マスク	Entries
マスク 1 の照合： 発信元の IP アドレスの 32 ビットすべてには「影響なし」： 残りの全ビット	送信元 IP = 8.1.1.1
	空のエントリ 2
	空のエントリ 3
	空のエントリ 4
	空のエントリ 5
	空のエントリ 6
	空のエントリ 7
	空のエントリ 8
マスク 2 の照合： 発信元の IP アドレスの最も重要な 24 ビットには「影響なし」： 残りの全ビット	送信元 IP = 8.1.1.0
	空のエントリ 2
	空のエントリ 3
	空のエントリ 4

	空のエントリ 5
	空のエントリ 6
	空のエントリ 7
	空のエントリ 8

マスク 1 の一部として使用できる空きエントリがあっても、TCAM 2 構造により、マスク 1 の空のエントリ 2 には ACE 2 が入力されません。 このマスクの使用は、ACE 2 のマスクが ACE 1 の /32 マスクに一致しないため、許可されません。TCAM 2 は、異なるマスク、つまり、/24 マスクを使用して、ACE 2 をプログラムする必要があります。

表 2 が示すように、別々のマスクを使用すると、結果的に使用可能なリソースの枯渇が早まる可能性があります。 他の ACL は引き続き、マスク 1 の残りのエントリを使用できます。 ただし、ほとんどの場合、TCAM 2 は非常に効率的ですが、100% ではありません。 この効率は、各設定のシナリオによって変わります。

次の表は、TCAM 3 でプログラムされた同じ ACL を示しています。TCAM 3 では、次のように各エントリにマスクが割り当てられます。

マスク	**Entries**
IP アドレス 1 のマスク 32 ビット	送信元 IP = 8.1.1.1
IP アドレス 2 のマスク 24 ビット	送信元 IP = 8.1.1.0
空のマスク 3	空のエントリ 3
空のマスク 4	空のエントリ 4
空のマスク 5	空のエントリ 5
空のマスク 6	空のエントリ 6
空のマスク 7	空のエントリ 7
空のマスク 8	空のエントリ 8
空のマスク 9	空のエントリ 9
空のマスク 10	空のエントリ 10
空のマスク 11	空のエントリ 11
空のマスク 12	空のエントリ 12
空のマスク 13	空のエントリ 13
空のマスク 14	空のエントリ 14
空のマスク 15	空のエントリ 15
空のマスク 16	空のエントリ 16

この例では、残りの 14 個のエントリはそれぞれ、無制限で、マスクの異なる複数のエントリを持つことができます。 そのため、TCAM 3 は TCAM 2 より、はるかに効率的です。 この例は、TCAM の各バージョンの違いを説明するために非常に簡素化されています。 Catalyst 4500 ソフトウェアでは、実際の設定シナリオに対して TCAM 2 でプログラミングの効率を上げる多くの最適化が使用されます。 このドキュメントの「TCAM 2 での最適ではない TCAM プログラミング アルゴリズム」セクションでは、これらの最適化について説明しています。

Catalyst 4500 の TCAM 2 と TCAM 3 の両方で、異なるインターフェイスに同じ ACL が適用される場合は、TCAM エントリが共有されます。 この最適化により、TCAM の領域が節約されます。

TCAM 枯渇のトラブルシューティング

Catalyst 4500 スイッチでセキュリティ ACL のプログラミング中に TCAM の枯渇が生じると、ACL の一部がソフトウェア パス経由で適用されます。 TCAM に適用されない ACE に一致するパケットは、ソフトウェアで処理されます。 ソフトウェアによるこの処理の実行は、CPU の使用率が高くなる原因となります。 Catalyst 4500 ACL のプログラミングは順序に依存しているため、ACL は常に上から下へとプログラムされます。 特定の ACL が TCAM に完全には収まらない場合、ACL の最下部の ACE は、TCAM でプログラムされない可能性が高くなります。

TCAM オーバーフローが発生すると、次の警告メッセージが表示されます。 次に例を示します。

```
%C4K_HWACLMAN-4-ACLHWPROGERRREASON: (Suppressed 1times) Input(null, 12/Normal)
Security: 140 - insufficient hardware TCAM masks.
%C4K_HWACLMAN-4-ACLHWPROGERR: (Suppressed 4 times) Input Security: 140 - hardware TCAM
limit, some packet processing will be software switched.
```

syslog をイネーブルにしている場合は、**show logging** コマンドの出力でも、このエラー メッセージが見つかります。 このメッセージがあるということはつまり、ソフトウェア処理が行われるということです。 その結果、CPU 使用率が高くなる可能性があります。 新規 ACL の適用中に TCAM 容量の枯渇が発生しても、TCAM にプログラム済みの ACL はプログラムされたままで TCAM に残ります。 プログラム済みの ACL に一致するパケットは、継続してハードウェアで処理され、転送されます。

注: サイズの大きい ACL に変更を加えると、TCAM 超過メッセージが表示される場合があります。 スイッチは、ACL を TCAM で再プログラムしようとします。 ほとんどの場合、新しい、変更された ACL は、ハードウェアで完全に再プログラムできます。 スイッチが TCAM へと正常に ACL 全体を再プログラムできる場合は、次のメッセージが表示されます。

```
*Apr 12 08:50:21: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All configured ACLs
now fully loaded in hardware TCAM - hardware switching / QoS restored
```

ACL が完全にハードウェアで再プログラムされたことを確認するには、**show platform software acl input summary interface interface-id** コマンドを使用します。

次の出力では、VLAN 1 に対する ACL 101 の設定および、ACL が完全にハードウェアにプログラムされたことの確認が示されています。

注: ACL が完全にはプログラムされてなかった場合は、TCAM 枯渇のエラー メッセージが表示されることがあります。

```
Switch#configure terminal Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1 Switch(config-if)#ip access-group 101 in Switch(config-if)#end
Switch# Switch#show platform software acl input summary interface vlan 1 Interface
Name                 : Vl1   Path(dir:port, vlan)         : (in :null, 1)     Current
TagPair(port, vlan) : (null, 0/Normal)     Current Signature          : {FeatureCam:(Security:
101)}   Type                          : Current     Direction                 : In
TagPair(port, vlan)        : (null, 0/Normal)     FeatureFlatAclId(state)    :
0(FullyLoadedWithToCpuAces)     QosFlatAclId(state)        : (null)
Flags                      : L3DenyToCpu
```

Flags フィールド（L3DenyToCpu）は、ACL のためにパケットが拒否された場合、そのパケットが CPU にパントされることを示します。 すると、スイッチからは「Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）-unreachable」メッセージが送信されます。 これはデフォルトの動作です。 複数のパケットが CPU にパントされると、スイッチ

で CPU の使用率が高くなる可能性があります。 ただし、Cisco IOS ソフトウェア リリース 12.1(13)EW 以降では、これらのパケットが CPU にレート制限されます。 ほとんどの場合、シスコでは、ICMP 到達不能メッセージを送信する機能をオフにすることを推奨しています。

次の出力では、「ICMP-unreachable」メッセージを送信しないようにするスイッチの設定と、この変更後の TCAM プログラミングの確認が示されています。 このコマンド出力が示すように、ACL 101 の状態は FullyLoaded になります。 拒否されたトラフィックは CPU には向かいません。

```
Switch#configure terminal Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1 Switch(config-if)#no ip unreachables Switch(config-if)#end
Switch#show platform software acl input summary interface vlan 1 Interface Name
: Vl1   Path(dir:port, vlan)         : (in :null, 1)     Current TagPair(port, vlan) : (null,
1/Normal)     Current Signature          : {FeatureCam:(Security: 101)}
Type                          : Current     Direction                 : In     TagPair(port,
vlan)        : (null, 1/Normal)     FeatureFlatAclId(state)    : 0(FullyLoaded)
QosFlatAclId(state)        : (null)     Flags                       : None
```

注: 特定の QoS ポリシーの適用中に QoS TCAM を超過すると、そのポリシーは、インターフェイスにも VLAN にも*適用されません*。 Catalyst 4500 では、その QoS ポリシーがソフトウェア パスで実装されることはありません。 そのため、Qos TCAM の超過時に CPU 使用率が急上昇することはありません。

```
*May 13 08:01:28: %C4K_HWACLMAN-4-ACLHWPROGERR: Input Policy Map: 10Mbps - hardware TCAM
limit, qos being disabled on relevant interface.

*May 13 08:01:28: %C4K_HWACLMAN-4-ACLHWPROGERRREASON: Input Policy Map: 10Mbps - no
available hardware TCAM entries.
```

show platform cpu packet statistics コマンドを実行します。 ACL sw processing キューが多数のパケットを受け取っているかどうかを判断します。 パケットの数は多いことは、セキュリティ TCAM の枯渇を示しています。 この TCAM 枯渇により、パケットがソフトウェア転送のために CPU に送られることになります。

```
Switch#show platform cpu packet statistics !--- Output suppressed. Packets Received by Packet
Queue  Queue                  Total           5 sec avg 1 min avg 5 min avg 1 hour avg ---------
------------ -------------- --------- --------- --------- ----------
Control                      57902635        22        16        12          3 Host
Learning                       464678         0         0         0          0 L3 Fwd
Low                            623229         0         0         0          0 L2 Fwd
Low                          11267182         7         4         6          1 L3 Rx
High                             508         0         0         0          0 L3 Rx
Low                            1275695        10         1         0          0 ACL
fwd(snooping)                  2645752         0         0         0          0 ACL log,
unreach                     51443268         9         4         5          5 ACL sw
processing                  842889240      1453      1532      1267       1179  Packets Dropped by
Packet Queue  Queue                  Total           5 sec avg 1 min avg 5 min avg 1 hour avg --
------------------- -------------- --------- --------- --------- ---------- L2 Fwd
Low                            3270         0         0         0          0 ACL sw
processing                    12636         0         0         0          0
```

ACL sw processing キューで、過大な量のトラフィックが受信されていないことがわかった場合は、「Cisco IOS ソフトウェアベースの Catalyst 4500 スイッチでの高い CPU 使用率」を参照して、他に考えられる原因を調べてください。 このドキュメントでは、CPU の使用率が高くなる他のシナリオをトラブルシューティングする方法についての情報を提供しています。

Catalyst 4500 での TCAM のオーバーフローは次の理由で発生する可能性があります。

- TCAM 2 での最適ではない TCAM プログラミング アルゴリズム
- ACL でのレイヤ 4 操作（L4Op）の過剰な使用

- スーパーバイザ エンジンまたはスイッチ タイプの過剰な ACL

TCAM 2 での最適ではない TCAM プログラミング アルゴリズム

「TCAM の種類」セクションで説明しているように、TCAM 2 効率は、8 個のエントリが 1 個のマスクを共有するという事実のために、より低くなります。 Catalyst 4500 ソフトウェアでは、次の 2 種類の TCAM プログラミング アルゴリズムを TCAM 2 に対して使用できるため、TCAM 2 の効率が向上します。

- Packed：ほとんどのセキュリティ ACL のシナリオに適しています。**注:** これはデフォルトです。
- Scattered：IPSG のシナリオで使用されます。

Scattered アルゴリズムへの変更は可能ですが、RACL のように、セキュリティ ACL だけを設定している場合には、通常これによる改善はありません。 Scattered アルゴリズムの効果があるのは、同一の、または類似した小さな ACL が多数のポートに繰り返し適用されるようなシナリオでだけです。 このようなシナリオとは、複数のインターフェイスで IPSG がイネーブルにされているような場合です。 IPSG のシナリオでは、各ダイナミック ACL が以下に該当します。

- エントリの数が少ない。これには、承認済 IP アドレスの許可、不正な IP アドレスによるポートのアクセスを防ぐための末尾での拒否が含まれています。
- 設定済みのすべてのアクセス ポートに繰り返し適用されます。Catalyst 4507R では、ACL は最大で 240 ポートに繰り返し適用されます。

注: TCAM 3 ではデフォルトの Packed アルゴリズムが使用されます。 TCAM 構造では、エントリごとに 1 個のマスクがあるため、最適なアルゴリズムは Packed アルゴリズムです。 このため、これらのスイッチでは Scattered アルゴリズム オプションがイネーブルにされることはありません。

次の例は、IPSG 機能に設定されたスーパーバイザ エンジン II+ によるものです。 出力には、49 % のエントリしか使用されていないにもかかわらず、89 % のマスクが消費されていることが示されています。

```
Switch#show platform hardware acl statistics utilization brief
                                     Entries/Total(%)  Masks/Total(%)
                                     ----------------  --------------
                                                                  Input
Acl(PortAndVlan)  2016 / 4096 ( 49)   460 /  512 ( 89)             Input  Acl(PortOrVlan)      6
/ 4096 (  0)     4 /  512 (  0)             Input  Qos(PortAndVlan)     0 / 4096 (  0)     0 /
512 (  0)             Input  Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
Output Acl(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)             Output
Acl(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)             Output Qos(PortAndVlan)     0
/ 4096 (  0)     0 /  512 (  0)             Output Qos(PortOrVlan)      0 / 4096 (  0)     0 /
512 (  0)             L4Ops: used 2 out of 64
```

この場合は、プログラミング アルゴリズムを、デフォルト アルゴリズムの Packed アルゴリズムから Scattered アルゴリズムに変更すると、効果があります。 Scattered アルゴリズムでは、マスクの使用率が 89 % から 49 % に削減されます。

```
Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#access-list hardware entries scattered Switch(config)#end Switch#show platform
hardware acl statistics utilization brief Entries/Total(%) Masks/Total(%) ----------------- ----
----------- Input Acl(PortAndVlan) 2016 / 4096 ( 49) 252 / 512 ( 49) Input Acl(PortOrVlan) 6 /
4096 ( 0) 5 / 512 ( 0) Input Qos(PortAndVlan) 0 / 4096 ( 0) 0 / 512 ( 0) Input Qos(PortOrVlan) 0
/ 4096 ( 0) 0 / 512 ( 0) Output Acl(PortAndVlan) 0 / 4096 ( 0) 0 / 512 ( 0) Output
Acl(PortOrVlan) 0 / 4096 ( 0) 0 / 512 ( 0) Output Qos(PortAndVlan) 0 / 4096 ( 0) 0 / 512 ( 0)
Output Qos(PortOrVlan) 0 / 4096 ( 0) 0 / 512 ( 0) L4Ops: used 2 out of 64
```

Catalyst 4500 スイッチのセキュリティ機能のベスト プラクティスについては、「スーパーバイ

ザ用 Catalyst 4500 セキュリティ機能のベスト プラクティス」を参照してください。

ACL での L4Op の過剰な使用

L4Op という用語は、ACL 設定での **gt**、**lt**、**neq**、**range** キーワードの使用を意味します。 Catalyst 4500 では 1 つの ACL で使用できるこれらのキーワード数に制限があります。 この制限は、スーパーバイザ エンジンとスイッチにより変わりますが、ACL ごとに 6 または 8 の L4Op が使用できます。 表 3 に、スーパーバイザ エンジンごと、および ACL ごとの制限を示します。

表 3：さまざまな Catalyst 4500 スーパーバイザ エンジンおよびスイッチでの ACL ごとの L4Op の制限

製品	L4Op
Supervisor Engine II+/II+TS	32（ACL ごとに 6）
スーパーバイザ エンジン III/IV/V および WS-C4948	32（ACL ごとに 6）
スーパーバイザ エンジン V-10GE と WS-C4948-10GE	64（ACL ごとに 8）

ACL ごとの L4Op の制限を超えた場合は、警告メッセージがコンソールに表示されます。 次のようなメッセージです。

```
%C4K_HWACLMAN-4-ACLHWPROGERR: Input Security: severn - hardware TCAM limit, some
packet processing will be software switched.
19:55:55: %C4K_HWACLMAN-4-ACLHWPROGERRREASON: Input Security: severn - hardware TCAM L4
operators/TCP flags usage capability exceeded.
```

また、L4Op の制限を超えた場合は、特定の ACE が TCAM で拡張されます。 その結果、追加の TCAM が使用されます。 次の ACE がその一例です。

```
access-list 101 permit tcp host 8.1.1.1 range 10 20 any
```

ACL 内のこの ACE でスイッチが使用できるのは 1 つのエントリと 1 つの L4Op だけです。 ただし、この ACL で 6 個の L4Op がすでに使用されている場合、この ACE はハードウェアで 10 個のエントリに拡張されます。 このような拡張により、TCAM でエントリを使い切ってしまう可能性があります。 これらの L4Op を慎重に使用すると、TCAM のオーバーフローを防止できます。

注: この例でスーパーバイザ エンジン V-10GE と WS-C4948-10GE を使用している場合は、ACL で以前に 8 個の L4Op を使用していると、ACE が拡張されます。

Catalyst 4500 スイッチで L4Op を使用するときは、次の点に注意してください。

- L4 操作は、演算子またはオペランドが異なる場合は、異なると見なされます。たとえば、次の ACL には、3 つの異なる L4 操作が含まれます。これは、**gt 10** と **gt 11** が、2 つの異なる L4 操作と見なされるためです。`access-list 101 **permit** tcp host 8.1.1.1 any **gt 10** access-list 101 **deny** tcp host 8.1.1.2 any **lt 9** access-list 101 **deny** tcp host 8.1.1.3 any **gt 11**`
- L4 操作は、同じ演算子/オペランドの組み合わせが送信元ポートに 1 度、宛先ポートに 1 度適用される場合は、異なると見なされます。次に例を示します。`access-list 101 permit tcp host 8.1.1.1 **gt 10** any access-list 101 permit tcp host 8.1.1.2 any **gt 10**`
- Catalyst 4500 では、可能な場合には L4Op が共用されます。次の例では、***太字斜体***の行が、このシナリオを示します。ACL 101 = 5 への L4Op の使用ACL 102 = 4 への L4Op の使用 **注 : eq** キーワードでは、L4Op ハードウェア リソースは消費されません。L4Op 使用総数 = **8注** : ACL 101 および 102 は 1 つの L4Op を共有します。**注:** L4Op は、TCP または User

Datagram Protocol（UDP;ユーザ データグラム プロトコル）などのプロトコルが一致しない場合や、許可/拒否の動作が一致しない場合でも共有されます。

スーパーバイザ エンジンまたはスイッチ タイプの過剰な ACL

表 2 が示すように、TCAM は制限付きリソースです。 多数の IPSG エントリのある IPSG のような機能や過剰な ACL を設定すると、スーパーバイザ エンジンの TCAM リソースを超過する可能性があります。

スーパーバイザ エンジン用の TCAM スペースを超過した場合は、次の手順を実行します。

- スーパーバイザ エンジン II+ があり、Cisco IOS ソフトウェア リリース 12.2(18)EW *より前*の Cisco IOS ソフトウェア リリースを実行している場合は、最新の Cisco IOS ソフトウェア リリース 12.2(25)EWA メンテナンス リリースにアップグレードします。これ以降のリリースでは、TCAM の容量が増加されています。
- DHCP スヌーピングおよび IPSG を使用しており、TCAM を使い果たしそうな場合は、最新の Cisco IOS ソフトウェア リリース 12.2(25)EWA メンテナンス リリースを使用します。また、TCAM 製品が 2 台の場合は、Scattered アルゴリズムを使用します。**注:** Scattered アルゴリズムは、Cisco IOS ソフトウェア リリース 12.2(20)EW 以降で使用可能です。さらに、最新のリリースでは、DCHP スヌーピングと Dynamic Address Resolution Protocol(ARP; アドレス レゾリューション プロトコル）Inspection（DAI; ダイナミック ARP インスペクション）の機能に関して、TCAM の使用率を改善する改良が加えられています。
- L4Op の制限を超えたために TCAM を使い果たしそうな場合は、TCAM オーバーフローを防ぐために ACL での L4Op の使用を減らしてください。
- 同じ VLAN のさまざまなポートで多くの ACL またはポリシーを使用する場合は、VLAN のインターフェイスで 1 つの ACL またはポリシーに集約します。この集約により、TCAM 領域が節約されます。 たとえば、音声ベースのポリシーを適用する場合は、デフォルト ポートベースの QoS が分類に使用されます。 このデフォルトの QoS により TCAM の容量が超過する可能性があります。 QoS を VLAN ベースに切り替えると、TCAM の使用量が削減されます。
- 引き続き、TCAM に問題がある場合は、スーパーバイザ エンジン V-10GE または Catalyst 4948-10GE などのハイエンド スーパーバイザ エンジンの導入を検討してください。これらの製品では、最も効率的な TCAM 3 のハードウェアが使用されています。

要約

Catalyst 4500 では設定された ACL が TCAM を使用してプログラムされます。 TCAM により、スイッチのパーフォーマンスに影響を与えることなく、ハードウェア転送パスでの ACL の適用が可能となります。 パフォーマンスは、ACL ルックアップのパフォーマンスがライン レートで行われるので、ACL のサイズに関係なく一定です。 ただし、TCAM は有限のリソースです。 そのため、ACL エントリの数が過剰に設定されると、TCAM の容量を超えることになります。 Catalyst 4500 では最大の効率を実現するために、多くの最適化が実装され、さらに TCAM のプログラミング アルゴリズムを変更するコマンドが提供されています。 スーパーバイザ エンジン V-10GE や Catalyst 4948-10GE などの TCAM 3 製品では、セキュリティ ACL と QoS ポリシーのために最大の TCAM リソースが提供されています。

関連情報

- 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