



タップアグリゲーションおよびMPLSストリップングの設定

この章は、次の項で構成されています。

- [タップアグリゲーションに関する情報](#) (1 ページ)
- [MPLS ストリッピングに関する情報](#) (4 ページ)
- [タップアグリゲーションの設定](#) (5 ページ)
- [タップアグリゲーションの設定の確認](#) (9 ページ)
- [MPLS ストリッピングの設定](#) (10 ページ)
- [MPLS ラベルの設定の確認](#) (14 ページ)

タップアグリゲーションに関する情報

ネットワーク タップ

さまざまなメソッドを使用して、パケットをモニタできます。1つのメソッドでは、物理ハードウェア タップが使用されます。

ネットワーク タップは、ネットワークを通過するデータへの直接インライン アクセスが可能なので、トラフィックのモニタリングに非常に役立ちます。多くの場合、サードパーティがネットワーク内の2ポイント間のトラフィックをモニタするのに適しています。ポイント A と B の間のネットワークが物理ケーブルで構成されている場合、ネットワーク タップがこのモニタリングを実現する最良の方法になります。ネットワーク タップには、少なくとも3つのポート (A ポート、B ポート、およびモニタ ポート) があります。A ポートと B ポートの間に挿入されるタップは、すべてのトラフィックをスムーズに通過させますが、同じデータをそのモニタ ポートにもコピーするため、サードパーティがリッスンできるようになります。

タップには次の利点があります。

- 全二重データ伝送を処理可能
- 目立たず、ネットワークによって検出されることがなく、物理または論理アドレッシングが不要

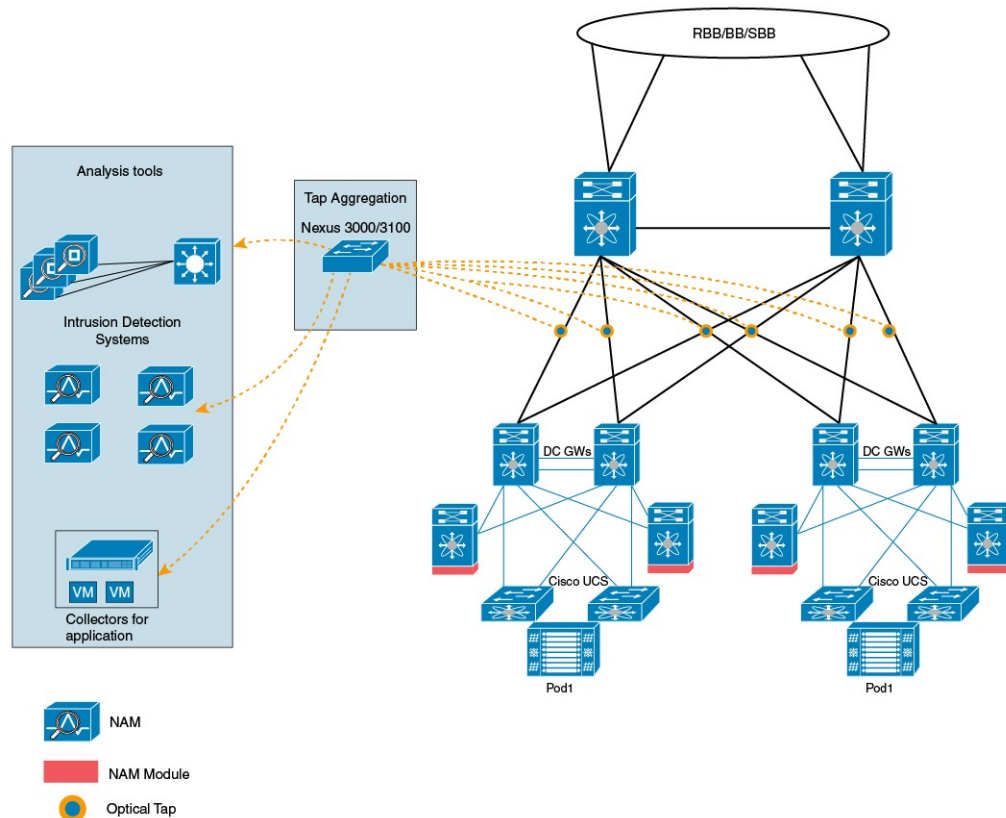
- 一部のタップは、分散タップを構築する機能のあるフル インライン パワーをサポート

ネットワークのエッジまたは仮想エッジにおけるサーバ間データ通信に対する可視性を確保しようとする場合、またはネットワークのインターネット エッジで侵入防御システム (IPS) アプリアランスにトラフィックのコピーを提供する場合でも、ネットワークタップは、環境内のほぼすべての場所で使用できます。ただし、大規模環境にネットワーク タップを導入する場合、多くのコストがかかり、運用の複雑さが増し、ケーブル配線の問題が生じます。

タップアグリゲーション

データセンターにおけるモニタリングおよびトラブルシューティング タスクに役立つ代替ソリューションは、複数タップの集約を可能にし、複数のモニタリングシステムに接続するためだけに指定されているデバイスを使用するソリューションです。このソリューションは、タップアグリゲーションと呼ばれます。タップアグリゲーション スイッチは、監視する必要があるパケットを処理するネットワーク ファブリック内の特定のポイントにすべてのモニタリング デバイスを直接リンクします。

図 1: タップアグリゲーションスイッチ ソリューション



タップアグリゲーション スイッチ ソリューションでは、Cisco Nexus 3000 または Cisco Nexus 3100 シリーズ スイッチは、パケットのモニタリングに都合の良い、ネットワーク内のさまざまなポイントに接続されます。各ネットワーク要素から、スイッチド ポート アナライザ

(SPAN) または光タップを使用して、このタップアグリゲーションスイッチにトラフィックフローを直接送信できます。タップアグリゲーションスイッチ自体は、ネットワークファブリック内のイベントをモニタするために使用されるすべての分析ツールに直接接続されます。これらのモニタリングデバイスには、リモートモニタリング (RMON) プロンプト、アプリケーションファイアウォール、IPS デバイス、およびパケットスニファツールが含まれます。

ネットワーク要素に接続されている特定のポートのセットを介して、トラフィックのスイッチへの到達を許可する設定を指定して、タップアグリゲーションスイッチを動的にプログラミングできます。特定のトラフィックをフィルタ処理して、1 つ以上のツールにリダイレクトする、複数の一致条件とアクションも設定できます。

タップアグリゲーションの注意事項と制約事項

タップアグリゲーションに関する注意事項と制約事項は次のとおりです。

- Cisco Nexus 3000 シリーズスイッチでは、MPLS タグでの TAP アグリゲーションフィルタはサポートされていません。
- タップアグリゲーションポリシーとともに適用されるインターフェイスは、レイヤ 2 にある必要があります。レイヤ 3 インターフェイスはポリシーを指定して設定できますが、そのポリシーは機能しなくなります。
- 各ルールは、1 つの固有の一致基準とのみ関連付ける必要があります。
- すべてのタップアグリゲーションインターフェイスが、同じ ACL を共有する必要があります。一致基準には入力インターフェイスが含まれているため、複数のインターフェイス間に複数の ACL は必要ありません。
- アクション **vlan-set** と **vlan-strip** は必ず **redirect** アクションの後に指定する必要があります。そうしないと、エントリが無効であるとして拒否されます。
- 拒否ルールでは、**redirect**、**vlan-set**、および **vlan-strip** などのアクションはサポートされません。
- ポリシー用インターフェイスのリストなどの入力リストを入力する場合は、スペースではなくカンマでエントリを区切る必要があります。例：
`port-channel50,ethernet1/12,port-channel20`。
- ポリシーにターゲットインターフェイスを指定する場合、短縮形ではなく、完全なインターフェイスタイプを入力する必要があります。例、`eth1/1` ではなく `ethernet1/1`、`po50` ではなく `port-channel 50` と入力します。

MPLS ストリッピングに関する情報

MPLS の概要

マルチプロトコルラベルスイッチング (MPLS) では、レイヤ2スイッチングのパフォーマンスおよびトラフィック管理機能と、レイヤ3ルーティングの拡張性、柔軟性、およびパフォーマンスが統合されています。

MPLS アーキテクチャには、次の利点があります。

- データは、レイヤ2テクノロジーの任意の組み合わせを使用して転送できます。
- サポートは、すべてのレイヤ3プロトコルに対して提供されています。
- 今日のネットワークで提供される最も優れた拡張性を備えています。

MPLS ヘッダー ストリッピング

Cisco Nexus 3172 の入力ポートは、さまざまな MPLS パケット タイプを受信します。MPLS ネットワークの各データ パケットには、1 つ以上のラベルヘッダーがあります。これらのパケットはリダイレクト ACL に基づいてリダイレクトされます。

ラベルは、Forwarding Equivalence Class (FEC) を特定するために使用される短い4バイトの固定長のローカルで有効な識別子です。特定のパケットに設定されているラベルは、そのパケットが割り当てられている FEC を表します。次のコンポーネントがあります。

- Label : ラベルの値 (非構造化) 、20 ビット
- Exp : 試験的使用、3 ビット、現在、サービス クラス (CoS) フィールドとして使用
- S : スタックの一番下、1 ビット
- TTL : 存続可能時間、8 ビット

MPLS ラベルはレイヤ2ヘッダーとレイヤ3ヘッダーの間に適用されるため、そのヘッダーとデータは、標準のバイトオフセットには含まれません。標準のネットワークモニタリングツールでは、このトラフィックのモニタリングと分析はできません。標準のネットワークモニタリングツールでこのトラフィックをモニタリングできるようにするには、単一ラベルのパケットから MPLS ラベルヘッダーを削除して、T キャッシュ デバイスにリダイレクトします。

複数のラベルヘッダーがある MPLS パケットは、MPLS ヘッダーが削除されずに、ディープパケットインスペクション (DPI) デバイスに送信されます。

MPLS ストリッピングに関する注意事項と制限事項

MPLS ストリッピングに関する注意事項と制約事項は次のとおりです。

- MPLS ストリッピングを有効にする前に、すべてのレイヤ 3 および vPC 機能を無効にします。
- グローバル タップ アグリゲーション モードが有効であることを確認します。
- MPLS ストリッピングに関係する入力および出力インターフェイスで、**mode tap-aggregation** が有効になっている必要があります。
- 目的の宛先にパケットを転送するためには、入力インターフェイスのリダイレクトアクションを使用してタップ アグリゲーション ACL を設定する必要があります。
- システムでは 1 つのタップ ACL のみサポートされます。
- 削除されたパケットが出力される出力インターフェイスは、許可 VLAN としての VLAN 1 が存在するインターフェイスである必要があります。出力インターフェイスは、デフォルトですべての VLAN が許可されるトランクとして設定することを推奨します。
- MPLS ストリッピングを有効にするには、MPLS のコントロールプレーン ポリシング (CoPP) クラス (copp-s-mpls) を設定する必要があります。
- MPLS ストリッピング パケットの場合、port-channel ロード バランシングがサポートされます。
- レイヤ 3 ヘッダー ベースのハッシュおよびレイヤ 4 ヘッダー ベースのハッシュはサポートされていますが、レイヤ 2 ヘッダー ベースのハッシュはサポートされていません。
- MPLS ストリッピング時、VLAN では MPLS ラベルも削除されます。
- MPLS ストリッピングは、Cisco Nexus 3100 シリーズ スイッチでのみサポートされています。

タップ アグリゲーションの設定

タップ アグリゲーションの有効化

タップ アグリゲーションを有効にしたら、**copy running-config startup-config** コマンドを実行して、スイッチをリロードしてください。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch (config)# [no] hardware profile tap-aggregation [l2drop]	タップ アグリゲーションを有効にし、VLAN タギングに必要なエントリをインターフェイス テーブルに予約します。

	コマンドまたはアクション	目的
		l2drop オプションは、タップ インターフェイス上で IP 以外のトラフィック入力をドロップします。 このコマンドの no 形式を使用すると、この機能が無効化されます。
ステップ 3	switch (config)# copy running-config startup-config	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。
ステップ 4	switch (config)# reload	Cisco NX-OS ソフトウェアをリロードします。

例

次に、スイッチ上でタップアグリゲーションをグローバルに設定する例を示します。

```
switch# configure terminal
switch(config)# hardware profile tap-aggregation
switch(config)# copy running-config startup-config
switch(config)# reload
```

タップアグリゲーションポリシーの設定

IP アクセス コントロール リスト (ACL) または MAC ACL で、TAP アグリゲーション ポリシーを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	- switch(config)# ip access-list <i>access-list-name</i> - switch(config)# mac access-list <i>access-list-name</i>	IP ACL を作成して IP アクセス リスト コンフィギュレーション モードを開始するか、あるいは MAC ACL を作成して MAC アクセス リスト コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
		(注) リリース 7.0(3)I5(1) 以降の Cisco Nexus 3000 シリーズ スイッチでは、IPv6 ACL のサポートが追加されます。IPv6 ACL ではリダイレクトアクションがサポートされます。リダイレクトアクションでは、現在 IPv6 PACL でサポートされているすべての <i>match</i> オプションがサポートされています。
ステップ 3	<code>switch(config-acl)# statistics per-entry</code>	各エントリで許可または拒否されるパケット数の統計情報の記録を開始します。
ステップ 4	<code>switch(config-acl)# [no] permit protocol source destination match-criteria action</code>	条件に一致するトラフィックを許可する、IP アクセス コントロール リスト (ACL) のルールを作成します。 このコマンドの no バージョンは、ポリシーから許可ルールを削除します。 <i>match-criteria</i> は、次のいずれかになります。 • ingress-intf (注) 入力インターフェイスはレイヤ 2 のみの一致基準 (EtherType またはポートチャネル) になります。 • vlan • vlan-priority (注) 各ポリシーには、一意の一致条件と関連付けられた 1 つのルールのみ設定できます。 <i>action</i> は、次のいずれかになります。 • redirect • priority • set-vlan

	コマンドまたはアクション	目的
		IP 以外の Ethertype で一致するタップ ACL には、0 よりも大きい優先度を指定する必要があります。
ステップ 5	<code>switch(config-acl)# [no] deny protocol source destination match-criteria action</code>	条件に一致するトラフィックを拒否する、IP アクセス コントロール リスト (ACL) のルールを作成します。 このコマンドの no バージョンは、ポリシーから拒否ルールを削除します。 redirect、および vlan-set アクションはサポートしていません。

例

次に、タップアグリゲーションポリシーを設定する例を示します。

```
switch# configure terminal
switch(config)# ip access-list test
switch(config-acl)# statistics per-entry
switch(config-acl)# permit ip any any ingress-intf Ethernet1/4 redirect Ethernet1/8
switch(config-acl)# permit ip any any ingress-intf Ethernet1/6 redirect
Ethernet1/1,Ethernet1/2,port-channel7,port-channel8,Ethernet1/12,Ethernet1/13
switch(config-acl)# permit tcp any eq www any ingress-intf Ethernet1/10 redirect
port-channel4
switch(config-acl)# deny ip any any
```

タップアグリゲーションポリシーのインターフェイスへのアタッチ

タップアグリゲーションポリシーをインターフェイスにアタッチするには、タップアグリゲーションモードを開始し、タップアグリゲーションが設定された ACL をインターフェイスに適用します。ポリシーをアタッチするインターフェイスがレイヤ2インターフェイスであることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	<code>switch# configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>switch(config)# interface type slot/port</code>	指定したインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switch (config-if)# [no] mode tap-aggregation</code>	ACL と一致基準とアクション基準のアタッチメントを許可します。

	コマンドまたはアクション	目的
		このコマンドの no 形式は、タップアグリゲーション ポリシーを設定した ACL のインターフェイスへのアタッチメントを禁止します。インターフェイスから ACL を削除するには、 no ip port access-group コマンドを使用します。
ステップ 4	switch(config-if)# [no] ip port access-group access-list-name in	IPv4 アクセス コントロール リスト (ACL) をポート ACL としてインターフェイスに適用します。 このコマンドの no 形式は、インターフェイスから ACL を削除します。

例

次に、タップアグリゲーションポリシーをインターフェイスにアタッチする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet1/2
switch (config-if)# mode tap-aggregation
switch(config-if)# ip port access-group test in
```

タップアグリゲーションの設定の確認

コマンド	目的
show ip access-list access-list-name	すべての IPv4 アクセス コントロール リスト (ACL) または特定の IPv4 ACL を表示します。

例

次に、IPv4 ACL を表示する例を示します。

```
switch(config)# show ip access-list test
IPV4 ACL test
    10 permit ip any any ethertype 0x800 ingress-intf Ethernet1/4 redirect Ethernet1/8
    20 permit ip any any ingress-intf Ethernet1/6 redirect Ethernet1/1,Ethernet1/2,port-channel7,port-channel8,Ethernet1/12,Ethernet1/13
    30 permit tcp any eq www any ethertype 0x800 ingress-intf Ethernet1/10 redirect port-channel4
    40 deny ip any any
```

MPLS ストリッピングの設定

MPLS ストリッピングの有効化

MPLS ストリッピングをグローバルに有効にできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [no] mpls strip	MPLS ストリッピングをグローバルに有効にします。 このコマンドの no 形式を使用すると、MPLS ストリッピングが無効化されます。

例

次に、MPLS ストリッピングを有効にする例を示します。

```
switch# configure terminal
switch(config)# mpls strip
```

MPLS ラベルの追加と削除

デバイスは、フレームがモード タップ インターフェイスで不明なラベルを受信するたびにラベルを動的に学習できます。また、次のコマンドを使用して、スタティック MPLS ラベルを追加または削除できます。

始める前に

- タップ アグリゲーションの有効化
- タップ アグリゲーション ポリシーの設定
- タップ アグリゲーション ポリシーのインターフェイスへのアタッチ

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# mpls strip label label	指定したスタティック MPLS ラベルを追加します。 ラベルの値の範囲は1～1048575 です。
ステップ 3	switch(config)# no mpls strip label label all	指定したスタティック MPLS ラベルを削除します。 all オプションは、すべてのスタティック MPLS ラベルを削除します。

例

次に、スタティック MPLS ラベルを追加する例を示します。

```
switch# configure terminal
switch(config)# mpls strip label 100
switch(config)# mpls strip label 200
switch(config)# mpls strip label 300
```

次に、スタティック MPLS ラベルを削除する例を示します。

```
switch# configure terminal
switch(config)# no mpls strip label 200
```

次に、すべてのスタティック MPLS ラベルを削除する例を示します。

```
switch# configure terminal
switch(config)# no mpls strip label all
```

ラベル エントリのクリア

次のコマンドを使用して、MPLS ラベル テーブルからダイナミック ラベル エントリをクリアできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# clear mpls strip label dynamic	MPLS ラベル テーブルからダイナミック ラベル エントリをクリアします。

例

次に、ダイナミック ラベル エントリをクリアする例を示します。

```
switch# clear mpls strip label dynamic
```

MPLS ストリッピング カウンタのクリア

すべてのソフトウェアおよびハードウェア MPLS ストリッピング カウンタをクリアできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# clear counters mpls strip	すべての MPLS ストリッピング カウンタをクリアします。

例

次に、すべての MPLS ストリッピング カウンタをクリアする例を示します。

```
switch# clear counters mpls strip
switch# show mpls strip labels
MPLS Strip Labels:
  Total      : 15000
  Static     : 2
Legend:      * - Static Label
Interface - where label was first learned
Idle-Age   - Seconds since last use
SW-Counter- Packets received in Software
HW-Counter- Packets switched in Hardware
```

Label	Interface	Idle-Age	SW-Counter	HW-Counter
4096	Eth1/44	15	0	0
8192	Eth1/44	17	0	0
12288	Eth1/44	15	0	0
16384	Eth1/44	39	0	0
20480	Eth1/44	47	0	0
24576	Eth1/44	7	0	0
28672	Eth1/44	5	0	0
36864	Eth1/44	7	0	0
40960	Eth1/44	19	0	0
45056	Eth1/44	9	0	0
49152	Eth1/44	45	0	0
53248	Eth1/44	9	0	0

MPLS ラベル エージングの設定

使用されていないダイナミック MPLS ラベルがエージアウトする時間を定義できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# mpls strip label-age age	ダイナミック MPLS ラベルがエージアウトする時間を指定します。

例

次に、ダイナミック MPLS ラベルのラベル エージを設定する例を示します。

```
switch# configure terminal
switch(config)# mpls strip label-age 300
```

宛先 MAC アドレスの設定

削除された出力フレームの宛先 MAC アドレスを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# mpls strip dest-mac mac-address	ヘッダーが削除された出力フレームの宛先 MAC アドレスを指定します。 MAC アドレスは、次の 4 つのいずれかの形式で指定できます。 • E.E.E • EE-EE-EE-EE-EE-EE • EE:EE:EE:EE:EE:EE • EEEE.EEEE.EEEE

例

次に、出力フレームの宛先 MAC アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# mpls strip dest-mac 1.1.1
```

MPLS ラベルの設定の確認

次のコマンドを使用して、MPLS ラベルの設定を表示します。

コマンド	目的
show mpls strip labels [<i>label</i> all dynamic static]	MPLS ラベルに関する情報を表示します。次のオプションを指定できます。 • label : 表示するラベル • all : すべてのラベルを表示することを指定します。これがデフォルトのオプションです。 • dynamic : ダイナミック ラベルのみ表示することを指定します。 • static : スタティック ラベルのみ表示することを指定します。

例

次に、すべての MPLS ラベルを表示する例を示します。

```
switch# show mpls strip labels
MPLS Strip Labels:
  Total      : 3005
  Static     : 5
Legend:      * - Static Label
Interface - where label was first learned
Idle-Age   - Seconds since last use
SW-Counter- Packets received in Software
HW-Counter- Packets switched in Hardware
-----
```

Label	Interface	Idle-Age	SW-Counter	HW-Counter
4096	Eth1/53/1	15	1	210
4097	Eth1/53/1	15	1	210
4098	Eth1/53/1	15	1	210
4099	Eth1/53/1	7	2	219
4100	Eth1/53/1	7	2	219
4101	Eth1/53/1	7	2	219
4102	Eth1/53/1	39	1	206
4103	Eth1/53/1	39	1	206
4104	Eth1/53/1	39	1	206
4105	Eth1/53/1	1	1	217
4106	Eth1/53/1	1	1	217
4107	Eth1/53/1	1	1	217
4108	Eth1/53/1	15	1	210
* 25000	None <User>	39	1	206
* 20000	None <User>	39	1	206
* 21000	None <User>	1	1	217

次に、スタティック MPLS ラベルのみ表示する例を示します。

```
switch(config)# show mpls strip labels static
```

```
MPLS Strip Labels:
```

```
Total      : 3005
```

```
Static      : 5
```

```
Legend:      * - Static Label
```

```
Interface - where label was first learned
```

```
Idle-Age   - Seconds since last use
```

```
SW-Counter- Packets received in Software
```

```
HW-Counter- Packets switched in Hardware
```

	Label	Interface	Idle-Age	SW-Counter	HW-Counter
*	300	None <User>	403	0	0
*	100	None <User>	416	0	0
*	25000	None <User>	869	0	0
*	20000	None <User>	869	0	0
*	21000	None <User>	869	0	0

