TAP アグリゲーション

この章では、Cisco NX-OS デバイスで TAP アグリゲーションおよび MPLS ストリッピングを設定する方法について説明します。

この章は、次の項で構成されています。

TAP アグリゲーションについて

ネットワーク TAP

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 テスト アクセス ポイント（TAP）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ー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します。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 TAP 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 TAP 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 TAP 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。

TAP 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 TAP は、分散 TAP 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ー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）アプライア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 TAP 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。

TAP アグリゲーション

TAP アグリゲーションは、データ センターのタスクのモニタリングとトラブルシューティングに役立つ代替ソリューションです。複数のテスト アクセス ポイント（TAP）の集約を許可し、複数のモニタリング システムに接続するようにデバイスを指定することで機能します。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ーリング デバイスをリンクします。

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 9000 シリーズ スイッチは、パケットのモニター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 TAP を使用して、この TAP]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。TAP 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）プローブ、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。

特定のトラフィックをフィルタリングして 1 つ以上のツールにリダイレクトするように TAPアグリゲーション スイッチを設定できます。トラフィックを複数のインターフェイスにリダイレクトするために、マルチキャスト グループがスイッチの内部で作成され、リダイレクト リストの一部であるインターフェイスがメンバー ポートとして追加されます。リダイレクト アクションを持つアクセス コントロール リスト（ACL）ポリシーがインターフェイスに適用されると、作成された内部マルチキャスト グループに ACL ルールに一致するトラフィックがリダイレクトされます。

TAP 集約の注意事項と制約事項

（注） スケールの情報については、リリース特定の『*Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*』を参照してください。

TAP 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。

- TAP アグリゲーション：
  - すべての Cisco Nexus 9300 シリーズ スイッチおよび 3164Q、31128PQ、3232C と 3264Q スイッチでサポートされます。
  - 100G ポートでサポートされます。
  - スイッチ ポートおよび入力方向でのみサポートされます。
  - Cisco Nexus 9200、9300、および 9300-EX シリーズ スイッチの UDF ベースの一致で IPv4 ACL をサポートします。
  - Cisco Nexus 9300-FX、9300-FX2、9300-FX3、9300-GX、9300-GX2、9300-HX、9500-EX、および 9500-FX プラットフォーム スイッチでサポートされます。
  - サポートされるリダイレクト ポートの最大数は 32 インターフェイスです。
- Cisco NX-OS リリース 9.2(1) 以降、MPLS タグに基づく TAP アグリゲーション フィルタは、次の Cisco Nexus プラットフォーム スイッチでサポートされています。
  - 9700-EX および 9700-FX ライン カードを搭載した Cisco Nexus 9000 プラットフォーム スイッチ。
  - Cisco Nexus 9200 プラットフォーム スイッチ。
  - Cisco Nexus 9300 プラットフォーム スイッチ。
  - Cisco Nexus 9500 スイッチ。
- 次の Cisco Nexus シリーズ スイッチ、ライン カードおよびファブリック モジュールでは、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。

表 *1 : Cisco Nexus 9000* シリーズ スイッチ

Cisco Nexus 3164Q-40GE	Cisco Nexus 9372PX	Cisco Nexus 9372PX-E
Cisco Nexus 9372TX	Cisco Nexus 9372TX-E	Cisco Nexus 9332PQ
Cisco Nexus 3232C	Cisco Nexus 93120TX	Cisco Nexus 31128PQ
Cisco Nexus 3264Q-S	—	—

表 *2 : Cisco Nexus 9500* シリーズ ラインカードおよびファブリック モジュール

N9K-M6PQ	N9K-X9632PC-QSFP100	N9K-X9536PQ
N9K-S X9432C	N9K-C93128TX	N9K-C9396PX
N9K-X9432PQ	N9K-X9464TX	—

- Cisco Nexus 9700-EX および 9700-FX ライン カードは、IPv4、IPv6、および MAC ACL による TAP アグリゲーションをサポートします。
- レイヤ 2 インターフェイスのみが TAP アグリゲーション ポリシーをサポートします。レイヤ 3 インターフェイスにポリシーを設定できますが、そのポリシーは機能しなくなります。
- リダイレクト ポートは、送信元（TAP）ポートと同じ VLAN の一部である必要があります。
- 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。
- TAP アグリゲーション ポリシー用インターフェイスの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。たとえば、port-channel50、ethernet1/12、port-channel20 などです。
- 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、簡略版ではなく、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。たとえば、**eth1/1** の代わりに **ethernet1/1** を入力し、**po50** の代わりに **port-channel50** を入力します。
- *tcp-option-length* と *VLAN ID* フィルタを同時に使用する HTTP 要求はサポートされていません。両方のフィルタを同時に設定すると、ACE に対するトラフィック照合が機能しない場合があります。
- Cisco NX-OS リリース 10.2(1)F 以降では、TAP アグリゲーション機能はライセンスによるもので、関連する CLI を構成する前に、機能の TAP アグリゲーションを構成する必要があります。ただし、TAP アグリゲーションに依存する CLI の使用が以前の設定で見つかった場合、この機能は sysmgr の ISSU インフラ変換フェーズ中に自動生成されます。この機能は、すべての Cisco Nexus 9000 シリーズ スイッチでサポートされています。ライセンスの詳細については、『ポリシー ガイドを使用する *Cisco Nexus 9000 NX-OS* スマート ライセンシング』を参照してください。
- Cisco NX-OS リリース 10.2(2)F 以降では、L2 インターフェイスに TapAgg ACL をアタッチする前に、**mode tap-aggregation** コマンドを設定するようにしてください。
- まだ設定されていないポート チャネルへのリダイレクトを使用して ACL エントリを設定する場合、ユーザーは指定されたポート チャネルを後で設定するように注意する必要があります。
- Cisco NX-OS リリース 10.3(1)F 以降、選択的な Q-in-Q トランク モードのインターフェイスでは、プロバイダー VLAN タギングが Cisco Nexus 9300-GX、N9K-C9504-FM-G、および N9K- C9508-FM-G スイッチおよび N9K-X9716D-GX ライン カードでサポートされていますが、以下の制限があります。
  - VXLAN が有効になっている場合、この機能はサポートされません。
  - システム レベル全体で最大 7000 の外部 VXLAN レイト エントリ、およびポートごとに 4000 のエントリを持つことができます。
- 入力インターフェイスで二重 VLAN タグを許可するには、次のように **switchport trunk allow-multi-tag** コマンドを正しく構成する必要があります。

- Cisco Nexus 9300-FX2 スイッチでは、NDB が構成されている場合に限りこのコマンドを使用する必要があります。
- Cisco Nexus 9300-GX/GX2 スイッチでは、NDB が構成されている場合でもこのコマンドは必要ありません。

MPLS ストリッピングについて

Cisco Nexus 9000 シリーズ スイッチの入力ポートは、さまざまなマルチプロトコル ラベル スイッチング（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 アクセス コントロール リスト（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

標準のネットワーク モニタリング ツールでは、MPLS 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監視ツールでMPLSトラフィックを監視できるようにするには、MPLS ストリップ機能を有効にする必要があります。この機能は、トラフィックの MPLS ラベル ヘッダーを取り除き、トラフィックをモニタリング デバイスにリダイレクトします。

MPLS ストリッピングに関する注意事項と制限事項

（注） スケールの情報については、リリース特定の『*Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*』を参照してください。

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。

- Cisco Nexus 9700-EX および 9700-FX ライン カードは、MPLS ストリッピングをサポートしていません。
- Cisco NX-OS リリース 10.2(1)F 以降、すべてのタップ アグリゲーションおよびストリッピング機能に対して**機能タップ アグリゲーション**を有効にする必要があります。
- 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。

- スタティック MPLS、MPLS セグメント ルーティング、および MPLS ストリッピングを同時に有効にすることはできません。
- MPLS ストリッピングに関係する入力インターフェイスで、TAP 集約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。
- MPLS ストリップ後、SMAC はスイッチ mac (**show vdc**) に変更され、DMAC は **00:00:00:ab:cd:ef** に設定されます。
- 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。
- ストリッピングは IP PACL に基づいており、ストリッピングに MAC-ACL を使用することはできません。
- MPLS ストリッピングは、IPv4 トラフィックに対してのみサポートされます。
- MPLS ストリッピング パケットの場合、ポートチャネル 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 ストリッピング中、着信 VLAN は維持されません。
- Cisco Nexus 9200、9300-EX、および9300-FX プラットフォーム スイッチは、リダイレクト ポートから送信されるパケットへの VLAN のタギングをサポートします。入力/出力ポートは、イーサネットまたはポート チャネルのいずれかです。VLAN タグは、着信ポート設定から取得されます。入力インターフェイスの新しい ACL を、インターフェイス VLAN 値とは異なる VLAN 値に関連付けないでください。
- 一意のリダイレクト ポート リストを持つすべての ACE（特定の VLAN に関連付けられた ACL の下で）に対して、ハードウェア エントリを割り当てます。現在の ACE 数のハードウェア制限は 50 で、50 を超える ACE を設定することはできません。
- MPLS ストリップは、MPLS ラベル スタックのレイヤ 3 パケットでのみサポートされます。
- Cisco NX-OS Release 10.2(2)F 以降では、IPv6 は Cisco Nexus 9300-EX プラットフォーム スイッチでのみサポートされます。ただし、VPLS ストリップおよび制御ワードパケット ストリップはサポートされていません。
- Cisco NX-OS リリース 10.2(3)F 以降、OFM ベースの MPLS ストリッピングが追加されています。新しい OFM ベースの MPLS ストリッピングと従来の実装は共存できません。詳細については、Nexus Data Broker のヘッダ ストリッピング機能の構成 の OFM ベースの MPLS ヘッダー ストリップのセクションを参照してください。

- 新しい OFM ベースの MPLS ストリッピング機能は、展開で MPLS ストリッピングと、VXLAN、iVXLAN、GRE、ERSPAN ヘッダーなどの他のタイプのヘッダー ストリッピングとの共存が必要な場合にのみ使用します。

  他のストリッピング機能との共存が必要ない場合、既存の MPLS ストリッピング機能は、MPLS ストリッピングを引き続きサポートします。

- Cisco NX-OS Release 10.3（2）F 以降では、EoMPLS ラベル ストリッピングは Cisco Nexus 9300-FX ToR スイッチでもサポートされます。

TAP アグリゲーションの設定

ライン カードの TAP 集約のイネーブル化

Cisco NX-OS リリース 7.0(3)I7(2) 以降では、9700-EX および 9700-FX ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチの TAP 集約を有効にできます。

手順の概要

1. **configure terminal**
2. [**no**] **hardware acl tap-agg**
3. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	[**no**] **hardware acl tap-agg** 例： `switch(config)# hardware acl tap-agg`	Cisco Nexus 9700-EX および 9700-FX ライン カードの TAP 集約を有効にします。 このコマンドは、Cisco Nexus 9300-GX、9300-HX, 9300-FX3、および 9300-GX2 プラットフォーム スイッチでも必要であり、リロードが必要になる場合があります。
ステップ 3	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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ます。

TAP 集約ポリシーの設定

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。

始める前に

IPv4 ポート ACL または MAC ポート ACL 用の ACL TCAM のリージョン サイズは、**hardware access-list tcam region** {*ifacl* | *mac-ifacl*} コマンドを使用して設定する必要があります。**hardware access-list team region ipv6-ifcal** コマンドを使用して、IPv6 ポート ACL の ACL TCAM リージョン サイズを設定します。

詳細については、『Cisco Nexus 9000 シリーズ NX-OS セキュリティの設定ガイド』の「ACL TCAM リージョン サイズの設定」を参照してください。

（注） デフォルトでは、ifacl と mac-ifacl の両方の領域サイズはゼロです。TAP 集約をサポートするには、ifacl または mac-ifacl リージョンに十分なエントリを割り当てる必要があります。

手順の概要

1. **configure terminal**
2. **feature tap-aggregation**
3. 次のいずれかのコマンドを入力します。
   - **ip access-list** *access-list-name*
   - **mac access-list** *access-list-name*
4. （任意） **statistics per-entry**
5. [**no**] **permit** *protocol source destination* **redirect** *interfaces*
6. （任意） 次のいずれかのコマンドを入力します。
   - **show ip access-lists** [*access-list-name*]
   - **show mac access-lists** [*access-list-name*]
7. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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

	コマンドまたはアクション	目的

ステップ 2	**feature tap-aggregation**
	例：
	`switch(config)# feature tap-aggregation`
	`switch(config)#`
		タップ集約に関連する CLI を設定できます。
		（注）
		Cisco NX-OSリリース10.2(1)F 以降、以前のリリースからこの機能を備えた新しい NX-OS リリースへのソフトウェア アップグレードでは、サポートされているマトリックスで ISSU が完了した場合、機能タップアグリゲーション設定が自動的に生成されます。

ステップ 3	次のいずれかのコマンドを入力します。
	• **ip access-list** *access-list-name*
	• **mac access-list** *access-list-name*
	例：
	`switch(config)# ip access-list test`
	`switch(config-acl)#`
	`switch(config)# mac access-list mactap1`
	`switch(config-mac-acl)#`
		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。

ステップ 4	（任意） **statistics per-entry** 例： `switch(config-acl)# statistics per-entry`	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 5	[**no**] **permit** *protocol source destination* **redirect** *interfaces* 例： `switch(config-acl)# permit ip any any redirect ethernet1/8`	条件ごとにトラフィックのリダイレクトを許可する IP または MAC AC Lルールを作成します。このコマンドの**いずれの**バージョンも、ポリシーからのパーミッションを削除することはありません。 （注） TAP集約ポリシーのインターフェイスを入力するときは、それを省略しないでください。インターフェイスのリストを入力するときは、コンマで区切り、スペースを入れないでください。

ステップ 6	（任意） 次のいずれかのコマンドを入力します。
	• **show ip access-lists** [*access-list-name*]
	• **show mac access-lists** [*access-list-name*]
	例：
	`switch(config-acl)# show ip access-lists test`
	`switch(config-mac-acl)# show mac access-lists mactap1`
		すべての IPv4 または MAC ACL、あるいは特定の IPv4 または MAC ACL を表示します。

	コマンドまたはアクション	目的
ステップ 7	（任意） **copy running-config startup-config** 例： `switch(config-acl)# copy running-config startup-config`	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ます。

TAP 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

TAP アグリゲーションで設定された ACL をレイヤ 2 インターフェイスに適用できます。

手順の概要

1. **configure terminal**
2. **interface** *type slot/port*
3. **switchport**
4. 次のいずれかのコマンドを入力します。
   - [**no**] **ip port access-group** *access-list-name* **in**
   - [**no**] **mac port access-group** *access-list-name* **in**
5. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**interface** *type slot/port*
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		指定したインターフェイスに対してインターフェイス 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	**switchport** 例： `switch(config-if)# switchport`	レイヤ 3 インターフェイスをレイヤ 2 インターフェイスに変更します。 （注） 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。

	コマンドまたはアクション	目的

ステップ 4	次のいずれかのコマンドを入力します。
	• [**no**] **ip port access-group** *access-list-name* **in**
	• [**no**] **mac port access-group** *access-list-name* **in**
	例：
	`switch(config-if)# ip port access-group test in`
	`switch(config-if)# mac port access-group test in`
		TAP 集約で設定された IPv4 または MAC ACL をインターフェイスに適用します。このコマンドの **no** 形式を使用すると、インターフェイスから ACL を削除します。

ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	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ます。

プロバイダー VLAN で選択的 Q-in-Q を構成する

始める前に

プロバイダー VLAN を設定する必要があります。

手順の概要

1. **configure terminal**
2. **interface** *[インターフェイス id（interface-id）]*
3. **switchport**
4. **switchport mode trunk**
5. 次のいずれかのコマンドを入力します。
   - **switchport vlan mapping** *[vlan-id 範囲（vlan-id-range）]***dot1q-tunnel** *[外部 vlan-id（outer vlan-id）]*
   - **switchport vlan mapping all dot1q-tunnel** *[外部 vlan-id（outer vlan-id）]*
6. **switchport trunk allowed vlan** *vlan_list*
7. 次のいずれかのコマンドを入力します。
   - [**no**] **ip port access-group** *access-list-name* **in**
   - [**no**] **mac port access-group** *access-list-name* **in**
8. （任意） **mode tap-aggregation**
9. （任意） **copy running-config startup-config**
10. switch(config-if)# **exit**
11. （任意） switch(config-if)# **show interfaces** *interface-id* **vlan mapping**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**interface** *[インターフェイス id（interface-id）]* 例： `switch(config)# interface Ethernet1/1`	サービス プロバイダ ネットワークに接続される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。物理インターフェイスまたは EtherChannel ポート チャネルを入力できます。
ステップ 3	**switchport** 例： `switch(config if)# switchport`	インターフェイスをレイヤ 2 スイッチング ポートとして設定します。
ステップ 4	**switchport mode trunk** 例： `switch(config-if)# switchport mode trunk`	インターフェイスをレイヤ 2 トランク ポートとして設定します。
ステップ 5	次のいずれかのコマンドを入力します。 • **switchport vlan mapping** *[vlan-id 範囲（vlan-id-range）]***dot1q-tunnel** *[外部 vlan-id（outer vlan-id）]* • **switchport vlan mapping all dot1q-tunnel** *[外部 vlan-id（outer vlan-id）]* 例： `switch(config-if)# switchport vlan mapping all dot1q-tunnel 300`	マッピングする VLAN ID を入力します。 • vlan-id-range1：カスタマー ネットワークからスイッチに入るカスタマー VLAN ID（C-VLAN）の範囲。指定できる範囲は 1 ～ 4094 です。VLAN-ID のストリングを入力できます。 • outer vlan-id：サービス プロバイダー ネットワークの外部 VLAN ID（S-VLAN）を入力します。指定できる範囲は 1 ～ 4094 です。
ステップ 6	**switchport trunk allowed vlan** *vlan_list* 例： `switch(config-if)# switchport trunk allowed vlan 300`	トランク インターフェイスの許可 VLAN を設定します。
ステップ 7	次のいずれかのコマンドを入力します。 • [**no**] **ip port access-group** *access-list-name* **in** • [**no**] **mac port access-group** *access-list-name* **in** 例：	TAP 集約で設定された IPv4 または MAC ACL をインターフェイスに適用します。このコマンドの **no** 形式を使用すると、インターフェイスから ACL を削除します。

	コマンドまたはアクション	目的

	`switch(config-if)# ip port access-group test in`
	
	`switch(config-if)# mac port access-group test in`	

ステップ 8	（任意） **mode tap-aggregation**
	例：
	`switch(config-if)# mode tap-aggregation`
	`switch(config-if)# no shutdown`
		TAP 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。

ステップ 9	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	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ます。
ステップ 10	switch(config-if)# **exit**	コンフィギュレーション モードを終了します。
ステップ 11	（任意） switch(config-if)# **show interfaces** *interface-id* **vlan mapping**	マッピングの設定の確認

TAP アグリゲーションの設定の確認

TAP アグリゲーションの設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ip access-lists [*access-list-name*]	すべての IPv4 ACL または特定の IPv4 ACL を表示します。
show ip access-lists [*access-list-name*]	すべての MAC ACL または特定の MAC ACL を表示します。

TAP アグリゲーションの設定例

次に、IPv4 ACL で TAP 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)# feature tap-aggregation
switch(config)# ip access-list test
switch(config-acl)# 10 deny ip 100.1.1/24 any
switch(config-acl)# 20 permit tcp any eq www any redirect port-channel4
switch(config-acl)# 30 permit ip any any redirect
Ethernet1/1,Ethernet1/2,port-channel7,port-channel8,Ethernet1/12,Ethernet1/13
switch(config-acl)# show ip access-lists test
IP access list test
        10 deny ip 100.1.1/24 any
        20 permit tcp any eq www any redirect port-channel4
        30 permit ip any any redirect
```

```
Ethernet1/1,Ethernet1/2,port-channel7,port-channel8,Ethernet1/12,Ethernet1/13
```

次に、MAC ACL で TAP 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)# feature tap-aggregation
switch(config)# mac access-list mactap1
switch(config-mac-acl)# 10 permit any any 0x86dd redirect port-channel1
switch(config-mac-acl)# show mac access-lists mactap1
MAC access list mactap1
        10 permit any any 0x86dd redirect port-channel1
```

次に、TAP アグリゲーション ポリシーをレイヤ 2 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 ethernet 1/2
switch(config-if)# ip port access-group test in
switch(config-if)#
```

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。

始める前に

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。

mode tap-aggregation コマンドを使用して、TAP アグリゲーション ポリシーを含む ACL をレイヤ 2 インターフェイスまたはポート チャネルにアタッチします。詳細については、TAP 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 （10 ページ）を参照してください。

手順の概要

1. **configure terminal**
2. [**no**] **mpls strip**
3. [**no**] **mpls strip mode dot1q**
4. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	[**no**] **mpls strip** 例： `switch(config)# 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。
ステップ 3	[**no**] **mpls strip mode dot1q** 例： `switch(config)# mpls strip mode dot1q`	リダイレクト ポートからのパケットの VLAN タギングを有効にします。タグ付けする必要がある VLAN は、入力ポートで指定する必要があります。
ステップ 4	必須: **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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ます。

VLAN タグの着信ポートの設定

VLAN タグは、着信ポート設定から取得されます。入力/出力ポートは、イーサネットまたはポート チャネルのいずれかです。

手順の概要

1. **configure terminal**
2. **interface** *type slot/port*
3. **switchport**
4. 次のいずれかのコマンドを入力します。
   - [**no**] **ip port access-group** *access-list-name* **in**
   - [**no**] **mac port access-group** *access-list-name* **in**
5. 次のいずれかのコマンドを入力します。
   - [**no**] **ip port access-group** *access-list-name* **in**
   - [**no**] **mac port access-group** *access-list-name* **in**
6. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**interface** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/26`
	`switch(config-if)#`
		指定したインターフェイスに対してインターフェイス 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	**switchport** 例： `switch(config-if)# switchport`	レイヤ 3 インターフェイスをレイヤ 2 インターフェイスに変更します。 （注） 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。

ステップ 4	次のいずれかのコマンドを入力します。
	• [**no**] **ip port access-group** *access-list-name* **in**
	• [**no**] **mac port access-group** *access-list-name* **in**
	例：
	`switch(config-if)# ip port access-group test in`
	`switch(config-if)# mac port access-group test in`
		TAP 集約で設定された IPv4 または MAC ACL をインターフェイスに適用します。このコマンドの **no** 形式を使用すると、インターフェイスから ACL を削除します。

ステップ 5	次のいずれかのコマンドを入力します。
	• [**no**] **ip port access-group** *access-list-name* **in**
	• [**no**] **mac port access-group** *access-list-name* **in**
	例：
	`switch(config-if)# ip port access-group test in`
	`switch(config-if)# mac port access-group test in`
		TAP 集約で設定された IPv4 または MAC ACL をインターフェイスに適用します。このコマンドの **no** 形式を使用すると、インターフェイスから ACL を削除します。

ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	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ます。

MPLS ラベルの追加と削除

デバイスは、フレームが TAP 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、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

TAPアグリゲーションポリシーを設定してインターフェイスへアタッチする詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

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。

手順の概要

1. **configure terminal**
2. **mpls strip label** ラベル
3. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**mpls strip label** ラベル 例： `switch(config)# mpls strip label 100`	指定したスタティック MPLS ラベルを追加します。ラベルの 20 ビット値の範囲は 1 ～ 1048575 です。 （注） このCLIは、次のクラウドスケールプラットフォーム スイッチを除き、「注意事項と制限事項」の項でMPLSストリッピング機能に指定されたすべてのプラットフォーム スイッチで使用できます。 • N9K-C93180YC-EX • N9K-C93180YC-FX • N9K-C93240YC-FX2 • N9K-C93180YC-FX3 • N9K-C93600CD-GX

	コマンドまたはアクション	目的
		[**no**] **mpls strip label** {*label* | **all**} コマンドは、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。
ステップ 3	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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ます。

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。

手順の概要

1. **configure terminal**
2. **mpls strip dest-mac** *mac-address*
3. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**mpls strip dest-mac** *mac-address* 例： `switch(config)# mpls strip dest-mac 1.1.1`	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
ステップ 3	（任意） **copy running-config startup-config** 例：	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ます。

	コマンドまたはアクション	目的
	`switch(config)# copy running-config startup-config`	

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。

手順の概要

1. **configure terminal**
2. **mpls strip label-age** 経過期間
3. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**mpls strip label-age** 経過期間 例： `switch(config)# mpls strip label-age 300`	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（秒）。範囲は 61ー 31622400 です。
ステップ 3	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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ます。

MPLS ストリッピング設定の確認

MPLS ストリッピングの設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show mpls strip labels [*label* | **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。

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
```

MPLS ストリッピング カウンタおよびラベル エントリのクリア

MPLS ストリッピング カウンタとラベル エントリをクリアするには、次の作業を行います。

コマンド	目的
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。
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。

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 ストリッピングの設定例

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
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IP ACL	『*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*』
MAC ACL	『*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*』
ポートチャネル対称ハッシュ	『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』
リモート モニタリング（RMON）	RMON の設定
スイッチド ポート アナライザ（SPAN）	SPAN の設定
トラブルシューティング	『*Cisco Nexus 9000 Series NX-OS Troubleshooting Guide*』

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。