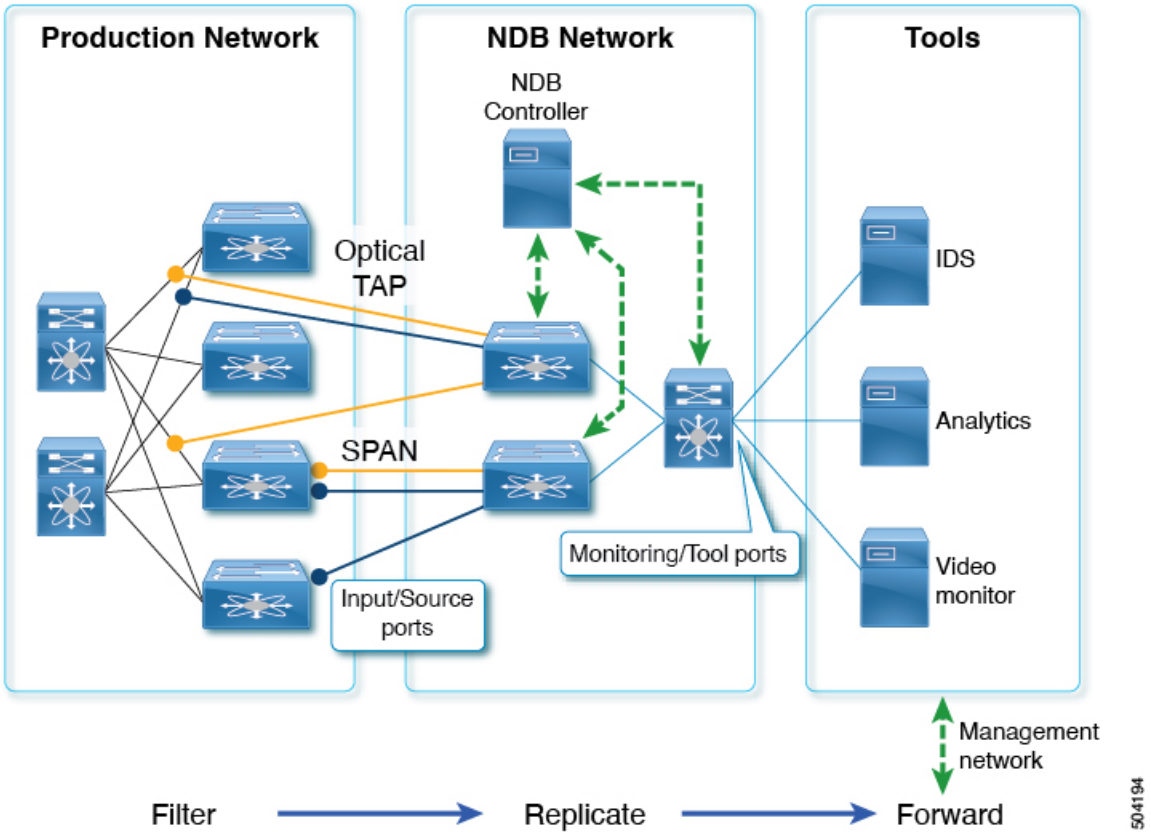
Nexus Data Broker のヘッダ ストリッピング機能の構成

Nexus Data Broker の ヘッダー ストリッピングの紹介

Cisco Nexus Data Broker（NDB）は、操作が簡単なスケーラブルなパケット ブローカー ネットワーク ソリューションを構築します。Cisco Nexus Dashboard Data Broker コントローラ ソフトウェアと Cisco Nexus スイッチは、アウトオブバンドとインライン ネットワーク トラフィックの両方をモニタするための新たなソフトウェア定義アプローチを可能にします。

図 *1 : NBD* 集中型展開モデル



NDB スイッチは、パケットの監視に使用されます。パフォーマンス監視、侵入検知、コンプライアンスチェックなどには、パケット監視が必要です。

ヘッダーストリップの場合、アウトオブバンド監視が実行されます。非侵入型であり、パケットのコピーが TAP または SPAN を使用して監視されます。したがって、トラフィックに対しフィルタ処理、本番ネットワークからの複製、NDB スイッチのヘッダーの除去が行われて、監視のためにツールに転送されます。ここで言及されている入力/送信元ポートは、ヘッダーストリッピングが行われるポートです。モニタリング/ツール ポートは、ツールに直接接続するポートです。

ヘッダーを削除する理由は次のとおりです。

- 一部の監視ツールは、カプセル化されたパケットを認識しません。
- 追加のヘッダーが存在すると、分析データに間違いが生じます。
- ヘッダーを追加すると、パケット サイズが増加するため、ツールに送信されて処理されるデータ量が最適化されません。

Cisco Nexus Data Broker スイッチのパケット ヘッダーまたはラベル ストリッピング機能の利点は次のとおりです。

- マルチプロトコル ラベル スイッチング（MPLS）ラベル ストリッピング

- コピー トラフィックからの VXLAN ヘッダー ストリッピングのネイティブ サポート
- Generic Route Encapsulation（GRE）ヘッダー ストリッピングのサポート
- 出力での Q-in-Q VLAN ヘッダー ストリッピング

これらにより、NDB は、従来の VXLAN、IVXLAN、ERSPAN、GRE、および MPLS ストリッピング機能をオーバーレイ フォワーディング マネージャー（OFM）ベースのモデルに整合させることができます。OFM は、ヘッダー ストリッピング機能のためのコマンド ライン インターフェイス（CLI）をホストします。

この章は、次の内容で構成されています。

ヘッダー ストリッピングに関する注意事項と制限事項

すべてのヘッダー ストリッピング機能に適用される注意事項と制限事項は次のとおりです。

- VxLAN、iVxLAN、GRE、MPLS などのさまざまなカプセル化タイプを持つすべてのトンネル プロファイルで、最大 500 のフロー終端インターフェイスがサポートされます。ERSPAN の場合、サポートされるフロー終端インターフェイスの最大数は 31 です。
- Cisco NX-OS リリース 10.2(3)F 以降、OFM モデルを使用した MPLS ストリッピングが、他のストリッピング機能と共存するようになります。しかし、他の種類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が、MPLS ストリッピングを引き続きサポートします。
- 同じインターフェイスまたは異なるインターフェイス上で共存させることができます。

（注） Cisco NX-OS リリース 10.2(3)F 以降、同じインターフェイスでの ERSPAN の共存がサポートされています。ただし、これは 9300-FX2 以降のプラットフォームでのみサポートされます。

- 従来の MPLS ストリッピング機能と OFM ストリッピング機能は相互に排他的です。
- Cisco NX-OS リリース 10.2(3)F 以降、IPv6 内部パケットのトラフィックは、すべてのストリッピング機能でサポートされます。
- 以前のリリースから Cisco NX-OS リリース 10.2(3)F への中断のない ISSU を実行し、ヘッダー ストリッピング機能を実行した後、dot1q トンネル VLAN_tag が見つからないか、

vlan_id=1 に設定されている場合は、その特定のストリッピング対応インターフェイスの L2 インターフェイスからポート ACL を削除して追加します。

- インターフェイスに VLAN が設定されていないものの、switchport mode dot1q-tunnel コマンドがそのインターフェイスに設定されている場合、ストリップされたパケットはデフォルトで VLAN=1 になります。
- 互換性のない OFM コマンドが show running コマンドの出力に存在し、Cisco NX-OS リリース 10.2(3)F から以前のリリースへの中断を伴う ISSU が実行されるシナリオで、その以前の NX-OS バージョンで OFM コマンドがサポートされていなかった場合、適切なエラーが表示されます。ただし、show incompatibility コマンドは、OFM 関連の非互換性コマンドのそのようなエラーにフラグを立てません。
- OFM ベースの GRE、ERSPAN、および MPLS ストリッピング機能は、ライン カードではなく TOR でのみサポートされます。
- カプセル化（iVXLAN、VXLAN、GRE、MPLS、ERSPAN）の一部として、次の制限が一般的です。
  - 2 つ以上のトンネル プロファイルが同じカプセル化タイプを持つことはできません。
  - 機能トンネルが有効になっている場合、OFM ベースのヘッダー ストリッピング機能はサポートされません。

Nexus Data Broker の VXLAN および iVXLAN ヘッダー ストリッピング

このsubchapterでは、Nexus Data Broker（NDB）の VXLAN および IVXLAN ヘッダー ストリッピング手順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。

Nexus Data Broker – VXLAN および iVXLAN ヘッダ ストリッピングについて

Nexus Data Broker（NDB）VXLAN および iVXLAN 終端により、スイッチは VXLAN および iVXLAN パケットの受信時にヘッダーを削除できます。

NDB スイッチは、以下のシナリオでパケットを受信します。

- スパインとリーフ間のテスト アクセス ポイント（TAP）ポートは、ACI ファブリックのファブリック リンクに配置されます。
- スイッチド ポート アナライザ（SPAN）セッションが設定されるか、TAP が VXLAN オーバーレイ ネットワークに配置されます。

ストリップ VXLAN および iVXLAN をサポートされている PID

Cisco NX-OS リリース 10.2(2)F 以降、VXLAN ストリッピング機能は Cisco Nexus 9364C および 9300-EX、9300-FX、9300-FX2、9300-FX3、9300-GX、9300-GX2、9500-EX、および 9500-FX ラインカードでサポートされています。

Cisco NX-OS リリース 10.2(2)F 以降、iVXLAN ストリッピング機能は Cisco Nexus 9364C および 9300-EX、9300-FX、9300-FX2、9300-GX、9300-GX2、9500- EX および 9500-FX ラインカードでサポートされています。

VXLAN および IVXLAN ヘッダー ストリップに関する注意事項と制限事項

- VXLAN アンダーレイが V4 の場合、VXLAN ヘッダ ストリップがサポートされます。
- PTEP / VTEP を使用せずに VXLAN および iVXLAN ヘッダを削除できる必要があります。
- VXLAN ヘッダ ストリップはポートごとに有効になります。
- VXLAN および iVXLAN ストリッピングは、次の機能が有効になっている場合はサポートされません。
  - NV オーバーレイ
  - VN-segment-vlan
  - レガシー MPLS ストリップおよび tap-aggregation
- VXLAN ストリッピングは、デフォルトの UDP 値が使用されている場合にサポートされます。
- ポートは、トンネリングされたパケットとトンネリングされていないパケットの両方を管理できる必要があります。
- レイヤ 2 スイッチポート モード トランクまたはレイヤ 2 PO インターフェイスは、VXLAN ヘッダを削除できる必要があります。
- リダイレクト インターフェイスが出力ポートまたはアナライザ ポートを指している場合、Tap-ACL に redirect キーワードを含む適切な ACE が含まれていることを確認します。そうでない場合、パケットは同じ入力ポートにフラッディングされます。
- OFM は、標準 ISSU および LXC-ISSUの VXLAN ストリッピング機能を有効にします。
- Cisco NX-OS リリース 10.2(1)F 以降、VXLAN および iVXLAN ストリッピング機能は、Cisco Nexus 9364C および 9300-EX、9300-FX、9300-FX2、9500-EX、および 9500-FX ラインカードでサポートされています。
- Cisco NX-OS リリース 10.2（2）F 以降、VXLAN と iVXLAN ストリッピング機能は Cisco Nexus 9300-GX と 9300-GX2 プラットフォーム スイッチでサポートされます。

- カプセル化のタイプごとに 1 つずつ、最大 4 つのトンネル プロファイルをスイッチ上に作成できます。 ただし、Cisco NX-OS リリース 10.2(3)F 以降では、最大 5 つのトンネル プロファイルがサポートされます。
- 最大 12 のリダイレクト インターフェイス (リリース 10.2(1) より前) および 32 のリダイレクト インターフェイス (リリース 10.2(1) 以降) は、TAP アグリゲーション ポリシーの単一の ACE でのみ構成できます。
- Cisco Nexus 9300-GX プラットフォーム スイッチの場合、VXLAN ストリップ後、L2 ヘッダー アドレスの送信元 MAC は VDC MAC アドレス、宛先 MAC は 000000abcdef に書き換えられます。
- Cisco NX-OS リリース 10.2(3)F 以降、VXLAN ストリップは Cisco N9K-C93180YC-FX3 と N9K-C93108TC-FX3P プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.2(4)M 以降、iVXLAN ストリッピング機能は Cisco N9K-C93180YC-FX3 と N9K-C93108TC-FX3P プラットフォーム スイッチでサポートされます。
- 次のスイッチは、上記のリリースからの VXLAN および iVXLAN ヘッダー ストリッピング機能をサポートしています。
  - N9K-C9348GC-FX3 – 10.4(1)F
  - N9K-C9332D-H2R – 10.4(1)F
  - N9K-C93108TC-FX3 – 10.4(2)F
  - N9K-C93400LD-H1 – 10.4(2)F
  - N9K-C9364C-H1 – 10.4(3)F
  - N9K-C92348GC-FX3 – 10.5(2)F
  - N9K-X9736C-FX3 line card - 10.5(2)F

VXLAN および iVXLAN ヘッダ ストリップでは、以下のステートメントが当てはまります。

- インターフェイスは、内部パケットで Q-in-Q VLAN のスラップを許可します。
- パケット CRC が正しく実行されます。
- 内部パケットは、入力ポート ACL を使用してフィルタリングできます。

Nexus Data Broker 終了の構成

次の手順は、NDB for VXLAN の終了の概要を示しています。iVXLAN ヘッダ ストリップについても同じ手順に従います。

（注） カプセル化トンネル タイプを VXLAN から iVXLAN に、またはその逆に変更するには、構成されたトンネルを no encapsulation CLI を使用して削除する必要があります。

（注） 次の CLI が、インターフェイスで VXLAN または iVXLAN のストリッピングを有効にするように構成されていることを確認します。

- 宛先
- encapsulation vxlan
- flow terminate interface add Ethernet 1/1

上記の CLI のいずれかが存在しない場合、CLI で指定されたポートでVXLAN または iVXLAN の除去は行われません。

手順の概要

1. **configure terminal**
2. **feature ofm**
3. **tunnel-profile profile-name**
4. **encapsulation vxlan**
5. **destination any**
6. **flow terminate interface ethernet 1/1**
7. **flow terminate interface remove ethernet 1/1**
8. **flow terminate interface add ethernet 1/2-5**
9. **flow terminate interface add port-channel 100-110**
10. **no flow terminate interface**
11. **feature tap-aggregation**
12. **ip access-list** <access-list name>
13. **[no] permit** protocol source destination redirect interfaces
14. **ip port access-group** <access-group name> **in**

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

	コマンドまたはアクション	目的
ステップ 2	**feature ofm** 例： `switch (config)# feature ofm`	機能 ofm を有効にします。

ステップ 3	**tunnel-profile profile-name**
	例：
	`switch(config)# tunnel-profile vtep_vxlan_term`
	`switch(config-tnl-profile)#`
		スタティック VXLANトンネルを有効にします。

ステップ 4	**encapsulation vxlan**
	例：
	`switch(config-tnl-profile)# encapsulation vxlan`
	`switch(config-tnl-profile)#`
		トンネル プロファイルの適切なカプセル化タイプを設定します。

ステップ 5	**destination any** 例： `switch(config-tnl-profile)# destination any`	トンネルプロファイルに必要な宛先を設定します。
ステップ 6	**flow terminate interface ethernet 1/1** 例： `switch(config-tnl-profile)# flow terminate interface ethernet 1/1`	フロー条件リストに ethernet1/1 を追加します（**no flow terminate interface**コマンドは、構成されていた場合）。
ステップ 7	**flow terminate interface remove ethernet 1/1** 例： `switch(config-tnl-profile)# flow terminate interface remove ethernet 1/1`	イーサネット 1/1 ポートのみを削除します。
ステップ 8	**flow terminate interface add ethernet 1/2-5** 例： `switch(config-tnl-profile)# flow terminate interface add ethernet 1/2-5`	e1/2、e1/3、e1/4、e1/5 をフロー終端インターフェイスの既存のリストに追加します。 （注） フロー終了インターフェイスを追加する際、CLI は L2 ポート インターフェイスが存在するか、または有効になっているかを確認しません。たとえば、e1/10 は非ブレークアウト モードです。CLI では、インターフェイス e1/10/1-4 でフロー終了リストを追加できます。e1/10 がブレークアウトの場合、VXLAN ヘッダー ストリップ機能が機能します。
ステップ 9	**flow terminate interface add port-channel 100-110** 例： `switch(config-tnl-profile)# flow terminate interface add po100-110`	ポート チャネル 100-110 を古いリストに追加します。新しいリストは e1/10-11 と po100-110 です。

	コマンドまたはアクション	目的
ステップ 10	**no flow terminate interface** 例： `switch(config-tnl-profile)# no flow terminate interface`	プロファイルからすべてのフローを削除し、インターフェイスを終了するには。
ステップ 11	**feature tap-aggregation** 例： `switch(config)# feature tap-aggregation`	機能のタップ集約を有効にします。

ステップ 12	**ip access-list** <access-list name>
	例：
	`switch(config)# ip access-list test`
	`switch(config-acl)#`
		IPACL を作成し、IP アクセス リスト コンフィギュレーション モードを開始します。

ステップ 13	**[no] permit** protocol source destination redirect interfaces 例： permit ip any any redirect interface ethernet 1/1, ethernet 1/19	条件ごとにトラフィックのリダイレクトを許可する IP AC L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 フォームを削除します。 （注） TAP アグリゲーション 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 14	**ip port access-group** <access-group name> **in** 例： configure terminal interface Ethernet 1/32 ip port access-group test in	ERSPAN ストリップ/終端ポートにポート アクセス リストを適用します。

VXLAN および iVXLAN ヘッダー ストリップの構成例

次に、VXLAN および iVXLAN ヘッダー ストリッピングの例を示します。手順は iVXLAN でも同じです：

```
switch(config-tnl-profile)# show run ofm
show running-config ofm
feature ofm
tunnel-profile vxlan1
encapsulation vxlan
destination any
flow terminate interface add port-channel101
flow terminate interface add Ethernet1/1
```

```
tunnel-profile vxlan2
encapsulation ivxlan
destination any
flow terminate interface add port-channel101
flow terminate interface add Ethernet1/1
switch(config-tnl-profile)#
switch(config-tnl-profile)# show tunnel-profile
Profile : vxlan1
Encapsulation : Vxlan
State : UP
Destination : Any
Terminate Interfaces : 2
Terminate List : port-channel101 Ethernet1/1
Profile : vxlan2
Encapsulation : iVxlan
State : UP
Destination : Any
Terminate Interfaces : 2
Terminate List : port-channel101 Ethernet1/1
switch(config-tnl-profile)#
```

Nexus Data Broker の ERSPAN ヘッダー ストリッピング

この節では、Cisco Nexus プラットフォーム スイッチの ERSPAN ヘッダ ストリッピング手順について説明します。これの主な使用例は、Nexus Data Broker（NDB）スイッチです。

この章は、次の項で構成されています。

ERSPAN ヘッダ ストリッピングについて

この機能は、NX-OS スイッチまたは Nexus Data Broker（NDB）スイッチの着信 ERSPAN パケットからのインライン ERSPAN ヘッダ ストリッピングを実装します。

ERSPAN パケットが着信すると、この機能によって ERSPAN ヘッダが削除され、インラインで外部ボックスに転送されます。つまり、パケットは終端ポートに着信し、ACL 設定に基づいて、外部サーバに接続されているポートにリダイレクトされます。

この機能は、単一パスの ERSPAN ヘッダ ストリッピングと PACL リダイレクトを実行します。

ERSPAN ヘッダをストリッピングするためにサポートされる PID

Cisco NX-OS リリース 10.2(1)F 以降では、Cisco Nexus 9300-FX2、9300-FX3、9300-GX、および 9300-GX2 プラットフォーム スイッチで ERSPAN ヘッダー ストリッピングがサポートされています。ただし、この機能は TOR スイッチでのみサポートされます。

ERSPAN ヘッダ ストリッピングに関する注意事項と制限事項

- 着信ポートはレイヤ 2 ポートである必要がありますが、レイヤ 3 への接続は SVI 経由である必要があります。
- ERSPAN 接続先セッションと ERSPAN ストリッピングは共存できません。

- ポート チャネル メンバーを含む終端ポートの総数は、31 を超えることはできません。
- この機能にはモード タップアグを設定しないでください。
- すべての ERSPAN ID のトンネル プロファイルがサポートされます。特定の ERSPAN セッション ID の終了はサポートされていません。ERSPAN セッション ID を持つトラフィックは、終端ノードで終端されます。
- ノードごとに 1 つのトンネル プロファイルのみがサポートされます。
- 最大 31 のフロー終端インターフェイスが、encap タイプ：ERSPAN のトンネル プロファイルでサポートされます。
- Cisco Nexus 9300-FX2、9300-FX3、9300-GX、および 9300-GX2 プラットフォーム スイッチで ERSPAN ヘッダ ストリッピング機能がサポートされます。この機能は TOR スイッチでのみサポートされます。
- ERSPAN 削除/リダイレクトが正しく動作するように、ポートで ERSPAN 削除を有効にする必要があります。他のストリップが有効になっているポートでは、ERSPAN トラフィックを送信しないでください。
- 終端ポートのすべての着信 ERSPAN ヘッダを削除します。
- この機能は、OFM トンネル プロファイル および ACL リダイレクトが構成されている場合にのみ機能します。
- この機能は、ポート ACL がレイヤ 2 終端ポートに適用されている場合にのみ機能します。
- スイッチ上の ERSPAN カプセル化のトンネル プロファイルは 1 つだけです。
- ポート ACL を使用するには、適切な tcam をカービングする必要があります。たとえば、カービングに **tcam region ing-ifacl** を使用します。

ERSPAN ヘッダ ストリッピングの設定

次の手順では、ERSPAN ヘッダ ストリッピングの設定の概要を示します。

（注） 次の CLI がインターフェイスで ERSPAN のストリッピングを有効にするように設定されていることを確認します。

- encapsulation erspan
- erspan セッション id すべて
- flow terminate interface add e1 / 16

上記の CLI のいずれかが欠落している場合、ERSPAN の除去は、CLI で指定されたポートでは発生しません。

手順の概要

1. **configure terminal**
2. **feature ofm**
3. **tunnel-profile** <profile-name>
4. **encapsulation erspan**
5. **erspan session-id all**
6. **flow terminate interface add ethernet1/16**
7. **ip access-list** <access-list-name>
8. [**no**] **permit** protocol source destination **redirect** interfaces
9. **ip port access-group** <access-group name>**_redir in**

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	**feature ofm** 例： `switch (config)# feature ofm`	機能 ofm を有効にします。

ステップ 3	**tunnel-profile** <profile-name>
	例：
	`switch(config)# tunnel-profile foo`
	`switch(config-tnl-profile)#`
		スタティック ERSPANトンネルを有効にします。

ステップ 4	**encapsulation erspan**
	例：
	`switch(config-tnl-profile)# encapsulation erspan`
	`switch(config-tnl-profile)#`
		トンネルプロファイルの適切なカプセル化タイプを設定します。

ステップ 5	**erspan session-id all** 例： `switch(config-tnl-profile)# erspan session-id all`	ERSPAN セッション ID は、関連する ERSPAN パケットが送信元スイッチで関連付けられているモニタ対象セッションを示します。
ステップ 6	**flow terminate interface add ethernet1/16** 例： `switch(config-tnl-profile)# flow terminate interface add ethernet1/16`	フロー条件リストに ethernet1/16 を追加します（フロー CLI が設定されていない場合）。

	コマンドまたはアクション	目的

ステップ 7	**ip access-list** <access-list-name>
	例：
	`switch(config)# ip access-list test`
	`switch(config-acl)#`
		IPACL を作成し、IP アクセス リスト コンフィギュレーション モードを開始します。

ステップ 8	[**no**] **permit** protocol source destination **redirect** interfaces 例： `permit ip any any redirect ethernet1/1,ethernet1/19`	条件ごとにトラフィックのリダイレクトを許可する IP 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 アグリゲーション 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 9	**ip port access-group** <access-group name>**_redir in** 例： `interface e1/16 (config-if)# ip port access-group test in`	ERSPAN ストリップ/終端ポートにポート アクセス リストを適用します。

ERSPAN ヘッダ ストリッピングの設定例

次に、ERSPAN ヘッダ ストリッピングの例を示します。

```
switch(config)# feature ofm
switch(config)# tunnel-profile foo
switch(config-tnl-profile)# encapsulation erspan
switch(config-tnl-profile)# erspan session-id all
switch(config-tnl-profile)# flowterminate interface add ethernet1/16
switch(config)# ip access-list test
permit ip any any redirect ethernet1/1,ethernet1/19
interfacee1/16 (config-if)# ip port access-group test in
```

ERSPAN ヘッダ ストリッピングの設定の確認

ERSPAN ヘッダ ストリッピング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 run ofm	トンネル プロファイルを表示します。
show run aclmgr	インターフェイス上のすべての ACL とそれらの ACL のアプリケーションを表示します。

コマンド	目的
show ip access-list acl_nam	ACL のヒット数とリダイレクトされたパケット数を表示します。
show tunnel-profile	全てのトンネル プロファイルの状態を表示します。

Nexus Data Broker の GRE ヘッダ ストリッピング

この節では、Cisco Nexus プラットフォーム スイッチの GRE ヘッダ ストリッピング手順について説明します。これの主な使用例は、Nexus Data Broker（NDB）スイッチです。

この章は、次の項で構成されています。

NDB GRE ヘッダー ストリッピングについて

この機能を使用すると、GRE カプセル化されて着信するパケットから GRE ヘッダーを取り除くことができます。GRE カプセル化パケットの内部パケットには、イーサネット ヘッダーが含まれていません。したがって、GRE ストリップの後、イーサネット ヘッダーが次のカスタム フィールドとともに内部パケットに追加されます：

1. 802.1q ヘッダーには、着信ポートで構成された VLAN が設定されます。
2. 接続先 MAC アドレスは に設定されます。 00:00:00:ab:cd:ef または 000.000.abc.def。
3. 送信元 MAC アドレスは、スイッチの VDC MAC アドレスに設定されます。

NDB GRE ヘッダー ストリッピングに関する注意事項と制限事項

- トンネルプロファイルからフローインターフェイスを削除するには、**no** の代わりに **remove** を使用します。**no** コマンドを使用すると、フロー終了リストからすべてのインターフェースが削除されます。

  次に例を示します。

  ```
  switch(config)# tunnel-profile gre_strip
  switch(config-tnl-profile)# flow terminate interface remove Ethernet 1/48
  ```

- フロー終了インターフェイスは、ESPRAN および GRE/VXLAN/IVXLAN プロファイルを共有できません。
- GRE ストリップ対応インターフェイスが ERSPAN トラフィックを受信した場合、ストリップは成功しますが、トラフィックはリダイレクト ポートに転送されません。
- 機能 OFM と機能トンネルは、同じスイッチ上に共存できません。

- Cisco Nexus 9300-EX、9300-FX、9300-FX2、9300-FX3、9300-GX、および N9K-C9332D-GX2B TOR上でサポートされている NBD GRE ヘッダー ストリッピング機能。ただし、この機能はラインカードではサポートされていません。
- **mode tap-aggregation** の構成は、GRE ヘッダー ストリッピング機能が有効になっているインターフェイスに存在しないようにする必要があります。
- トンネル カプセル化タイプの変更は許可されていません。

```
QP-CF-1(config-tnl-profile)# encapsulation gre
Error: encap-type modify not allowed, delete and add again
```

- 最大 500 のフロー終端インターフェイスが、encap タイプ iVXLAN/VXLAN/GRE のトンネル プロファイルでサポートされます。
- 最大 31 のフロー終端インターフェイスが、encap タイプ ERSPAN のトンネル プロファイルでサポートされます。
- フロー終了インターフェイス CLI が **add** キーワードなしで設定されている場合、それは **replace** として機能します。つまり、以前に追加されたフロー終了インターフェイスが削除され、新しいインターフェイスだけがフロー終了インターフェイスとして機能します。
- 以前の NX-OS バージョンから 10.2(3)F への中断のないアップグレード後、特定のインターフェイスの GRE ヘッダー ストリップ機能を有効にする前に、ポート ACL をすべてのインターフェイスから削除して追加する必要があります。
- dot1q トンネル伝搬を許可するには、9300-GX で **hardware acl tap-agg redirect disable-dot1q-sharing** コマンドが必要です。このコマンドを有効にした後、スイッチをリロードする必要があります。

GRE ヘッダー ストリップ機能の CLI

インターフェイスで GRE ヘッダーを有効にするために構成する CLI は次のとおりです：

```
feature ofm
tunnel-profile gre_strip
    encapsulation gre
    destination any
    flow terminate interface add Ethernet1/1-10
```

次に、トンネル プロファイルの show コマンドを示します：

```
switch# show tunnel-profile gre_strip
  Profile               : gre_strip
  Encapsulation         : GRE
  State                 : UP
  Destination           : Any
  Terminate Interfaces  : 10
  Terminate List        : Ethernet1/1 Ethernet1/2 Ethernet1/3 Ethernet1/4 Ethernet1/5
Ethernet1/6 Ethernet1/7 Ethernet1/8 Ethernet1/9 Ethernet1/10
```

出力ポートと入力ポートの構成

入力ポートの構成は次のとおりです。

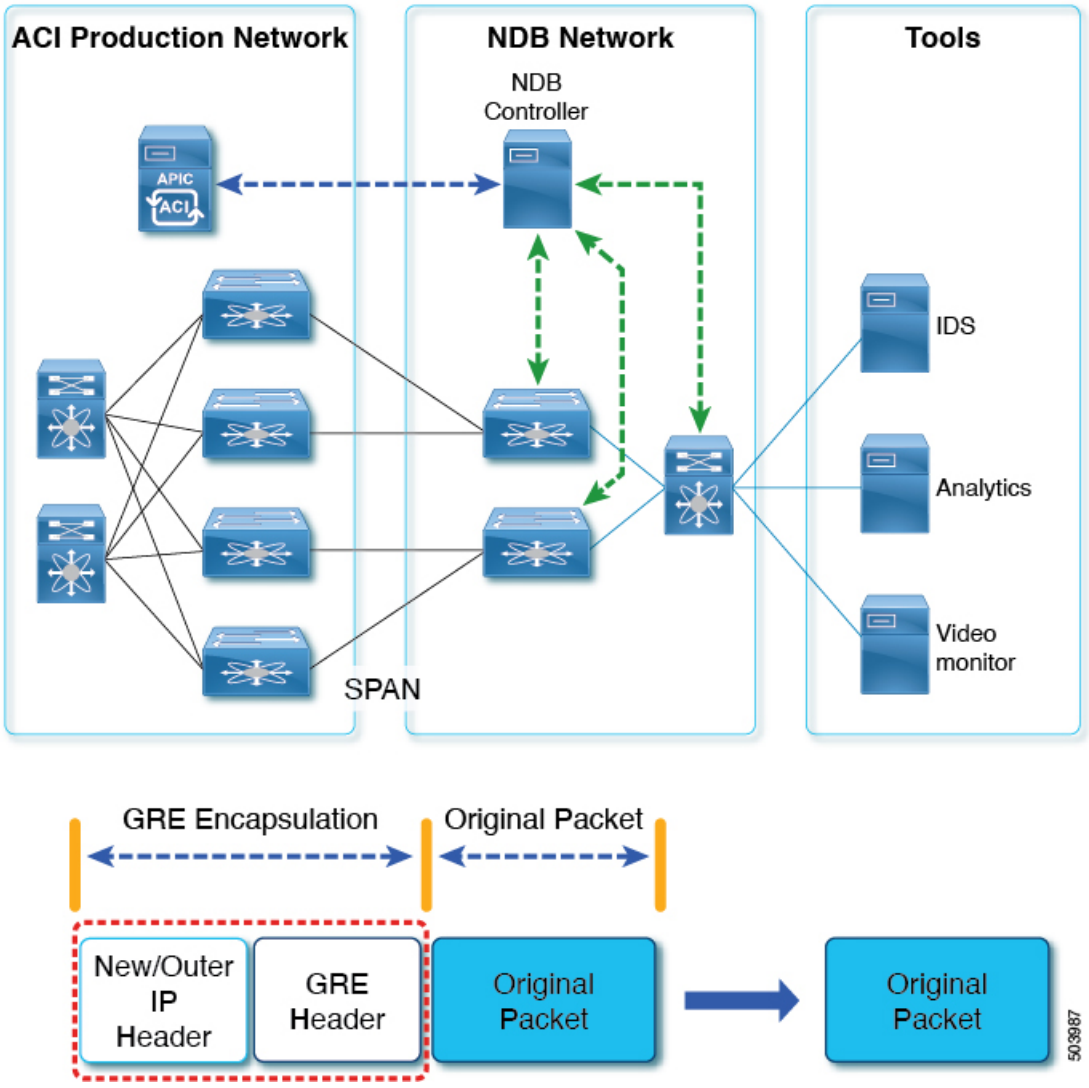
```
interface eth1/1
    switchport access vlan 101
    switchport mode dot1q-tunnel
    ip port access-group ndb_acl in <<<
    no shutdown
```

出力ポートの構成は次のとおりです。

```
interface Ethernet1/7
    switchport mode trunk
    no shutdown

IP access list ndb_acl
    statistics per-entry
    10 permit udp any any eq 4789 redirect Ethernet1/7
    15 permit ip any any redirect Ethernet1/7
```

図 *2 : NDB GRE* ヘッダー ストリップ ソリューション



Nexus Data Broker の MPLS ヘッダ ストリッピング

このの節では、Cisco Nexus プラットフォーム スイッチの MPLS ヘッダ ストリッピング手順について説明します。これの主な使用例は、Nexus Data Broker（NDB）スイッチです。

この章は、次の項で構成されています。

NDB MPLS ヘッダー ストリッピングについて

この機能を使用すると、MPLS カプセル化されて着信したパケットから MPLS ヘッダーを取り除くことができます。MPLS ラベル ストリッピングは、IPoMPLS および EoMPLS パケット フォーマットの両方でサポートされています。MPLS ラベル ストリップの後、イーサネット ヘッダーが次のカスタム フィールドを使用して内部パケットに追加されます。

1. 着信ポートに 802.1q ヘッダー と vlan が構成されます。
2. 接続先 MAC アドレスは 00:00:00:ab:cd:ef または 000.000.abc.def に設定されます。

（注） EoMPLS ヘッダー ストリッピングの場合、これは Cisco Nexus 9300-EX、9300-FX、および 9300-GX プラットフォームにのみ適用されます。

3. 送信元 MAC アドレスは、スイッチの VDC MAC アドレスに設定されます。

（注） EoMPLS ヘッダー ストリッピングの場合、これは Cisco Nexus 9300-EX、9300-FX、および 9300-GX プラットフォームにのみ適用されます。

NDB MPLS ヘッダー ストリッピングに関する注意事項と制限事項

レガシー MPLS ヘッダー ストリッピングから OFM ベースの構成に移行する場合は、次の注意事項と制限事項が適用されます。

- レガシー MPLS ストリッピング導入は OFM ベースのストリッピングと共存できません。
- 機能 OFM と機能トンネルは、同じスイッチ上に共存できません。
- レガシー MPLS ストリッピング機能から移行するには、OFM ベースの MPLS ストリッピングを有効にする前に、次のクリーンアップが必要です。
  - インターフェース レベルでの **mode tap-aggregation** の削除
  - グローバル レベルでの**mpls strip; mpls strip dot1q** の除去
  - 構成を保存して、上記の構成でスイッチをリロードします。

- Cisco NX-OS リリース 10.2（3）F 以降、NDM MPLS ヘッダー ストリッピング機能がサポートされています。
  - IPoMPLS（パケット フォーマット）ヘッダー ストリッピングは、Cisco Nexus 9300-EX、9300-FX、9300-FX2、9300-FX3、9300-GX、および C9332D-GX2B プラットフォームでサポートされています。
  - EoMPLS（パケット形式）ヘッダー ストリッピングは、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ています。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。

（注） OFM MPLS ストリッピング機能は、TOR でのみサポートされます。ラインカードではサポートされていません。

- 以前の NX-OS バージョンから 10.2(3)F への中断のないアップグレード後、特定のインターフェイスの MPLS ヘッダー ストリッピング機能を有効にする前に、ポート ACL をすべてのインターフェイスから削除して追加する必要があります。
- dot1q トンネル伝搬を許可するには、Cisco Nexus 9300-GX プラットフォーム スイッチで **hardware acl tap-agg redirect disable-dot1q-sharing** コマンドが必要です。このコマンドを有効にした後、スイッチをリロードする必要があります。
- トンネル カプセル化タイプの変更は許可されていません。

```
QP-CF-1(config-tnl-profile)# encapsulation mpls
Error: encap-type modify not allowed, delete and add again
```

- ERSPAN ACL リダイレクト トンネル プロファイルが構成されておらず、インターフェイスが ERSPAN パケットを受信している場合、ERSPAN パケットは TapAgg ポリシーの ERSPAN ACL リダイレクト エントリにヒットし、削除されません。
- MPLS ヘッド ストリップが有効になっているインターフェイスでは、モード タップ アグリゲーションが存在しないようにする必要があります。
- MPLS 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 を使用しないでください。
- MPLS ストリッピング中、オリジナル パケットの着信 VLAN は維持されません。
- ERSPAN トンネル プロファイルでは、入力インターフェイスが dot1q-tunnel からトランクモードに変換されると、出力パケットに VLAN=1 の dot1q タグが付けられます。このタグ付けは、ストリップされたパケットとリダイレクトされる通常の IP パケットの両方に対して行われます。
- MPLS ストリップ対応インターフェイスが ERSPAN トラフィックを受信すると、ストリップは成功しますが、トラフィックはリダイレクト ポートに転送されません。

- トンネルプロファイルからフローインターフェイスを削除するには、**no** の代わりに **remove** を使用します。**no** コマンドを使用すると、フロー終了リストからすべてのインターフェースが削除されます。

  次に例を示します。

  ```
  switch(config)# tunnel-profile mpls_strip
  switch(config-tnl-profile)# flow terminate interface remove Ethernet 1/48
  ```

- **add** キーワードなしでフロー 終端 インターフェイス コマンドを構成すると、**replace** として動作します。このことは、以前追加したフロー終了インターフェイスは削除され、新しいものだけがフロー 終端 インターフェイスとして動作することを意味します。

- 入力インターフェイスは、トランク モードまたはアクセス モードのいずれかです。どちらのモードでも、タグ付きパケットとタグなしパケットのリダイレクトが可能です。access-mode が dot1q-tunnel モードで使用される場合、ヘッダー ストリッピングの後に、access-mode で指定された方法で VLAN_tag が追加されます。

- Cisco NX-OS リリース 10.3（1）F までは、EoMPLS ヘッダー ストリッピングは 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ていました（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でした）。Cisco NX-OS リリース 10.3（2）F 以降、EoMPLS ヘッダー ストリッピング機能は、Cisco Nexus 9300-FX、9300-FX2、9300-FX3、9300-GX、および 9300-GX2 ToR でもサポートされています。ラインカードではサポートされていません。次の注意事項と制限事項が適用されます。

  - EoMPLS ストリッピングは、同じまたは異なるインターフェイス上で他のすべてのヘッダー ストリッピング機能と共存できます。

  - Cisco Nexus 9300-EX、9300-FX、および 9300-GX プラットフォーム スイッチの場合、EoMPLS ヘッダー ストリップの後、L2 ヘッダー アドレスは次のように書き換えられます。送信元 MAC は VDC MAC アドレス、接続先 MAC は 000000abcdef です。

  - 疑似ワイヤー コントロール ワードはサポートされていません。

  - Cisco Nexus 9300-GX プラットフォーム スイッチでは、dot1q vlan 設定が同じでない限り、2 つの入力ポートは ACL を共有できません。そうでない場合、タグ付けは機能しません。

MPLS ヘッダー ストリップ機能のコマンド

インターフェイスで MPLS ヘッダーを有効にするには、次のコマンドを構成する必要があります：

```
feature ofm
tunnel-profile
mpls_strip encapsulation mpls destination any
flow terminate interface add Ethernet1/1-10
```

トンネル プロファイルの show コマンドは次のとおりです。

```
switch# show tunnel-profile mpls_strip
  Profile               : mpls_strip
  Encapsulation         : MPLS
```

```
  State                 : UP
  Destination           : Any
  Terminate Interfaces  : 10
  Terminate List        : Ethernet1/1 Ethernet1/2 Ethernet1/3 Ethernet1/4 Ethernet1/5
Ethernet1/6 Ethernet1/7 Ethernet1/8 Ethernet1/9 Ethernet1/10
```

出力ポートと入力ポートの構成

入力ポートの構成は次のとおりです。

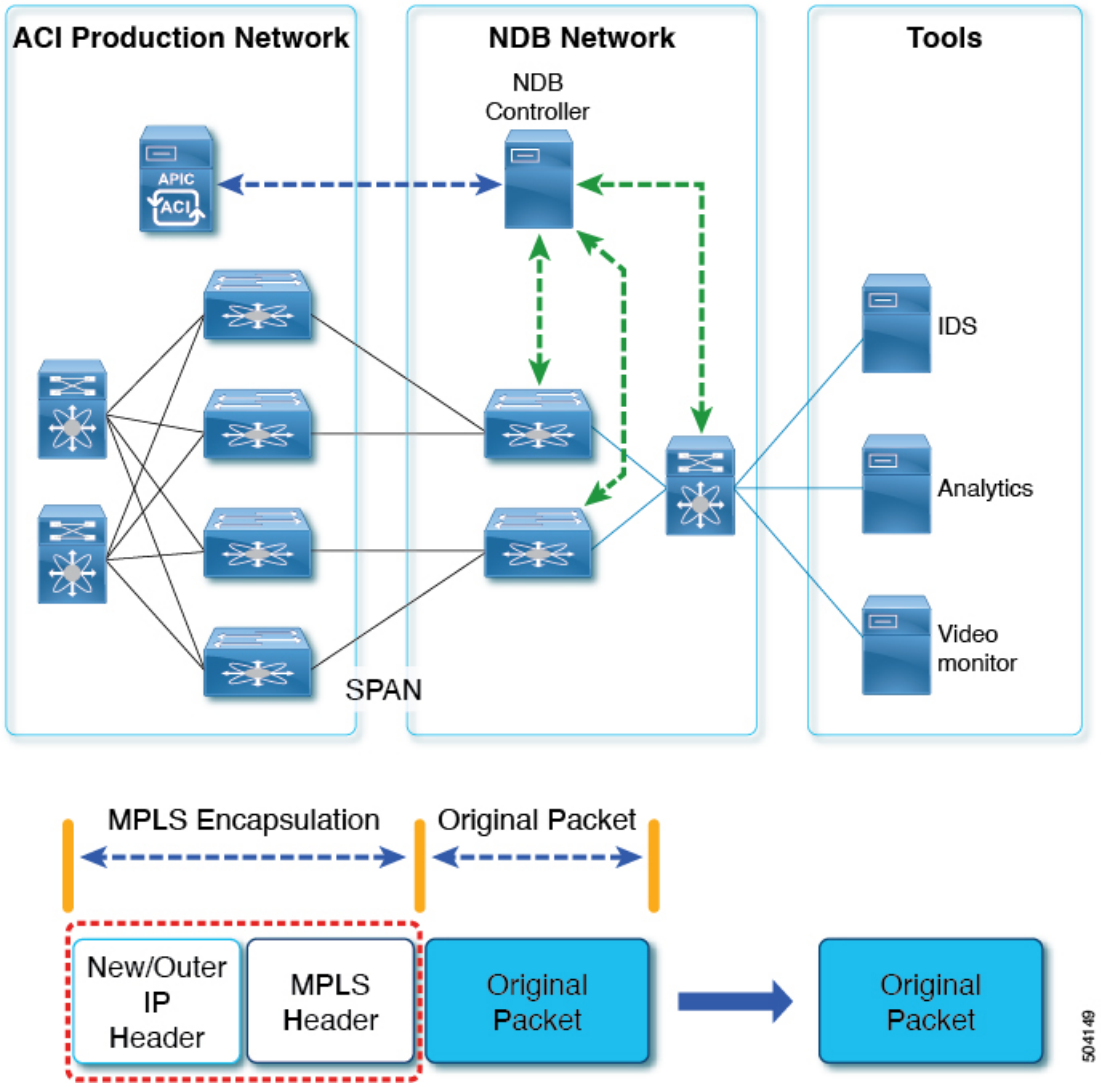
```
interface eth1/1
    switchport access vlan 101
    switchport mode dot1q-tunnel
    ip port access-group ndb_acl in
    no shutdown
```

出力ポートの構成は次のとおりです。

```
interface Ethernet1/7
    switchport mode trunk
    no shutdown

IP access list ndb_acl
    statistics per-entry
    10 permit udp any any eq 4789 redirect Ethernet1/7
    15 permit ip any any redirect Ethernet1/7
```

図 *3 : NDB MPLS* ヘッダー ストリップ ソリューション



（注） MPLS などのカプセル化解除されたパケットの場合、NDB スイッチはイーサネット/VLAN ヘッダーを**オリジナルのパケット**に追加するため、出力パケットはイーサネット/VLAN を持つオリジナルのパケットになります。

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。