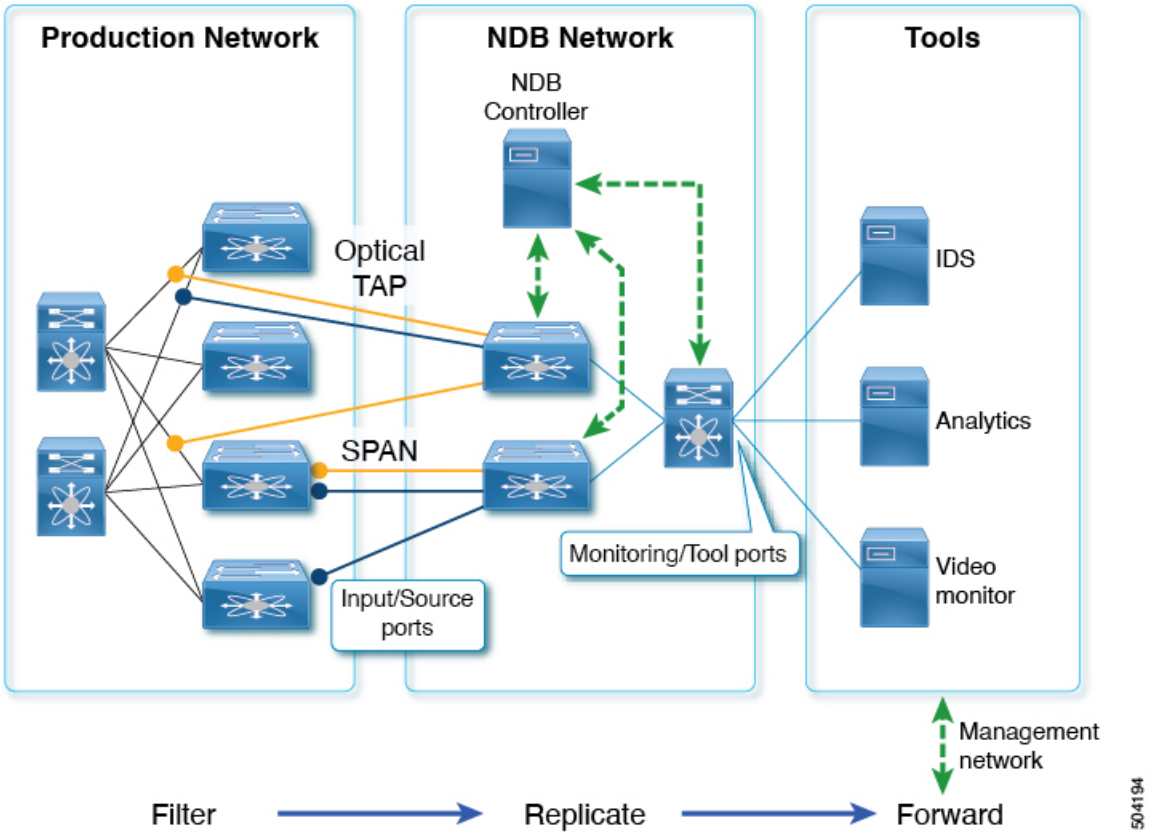
Nexus Data Broker のヘッダ ストリッピング機能の構成

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 – 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。

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。
- カプセル化のタイプごとに 1 つずつ、最大 2 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。
- 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。
-

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

	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 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。

	コマンドまたはアクション	目的
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。
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。

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)#
```

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。
- 終端ポートが同じ場合、VXLAN ストリッピングと ERSPAN ストリッピングは共存できません。
- 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。
- 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。
- この機能は IPv6 をサポートしていません。

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
- 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

	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 acl mgr	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。

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。