CHAPTER 30

Flexible NetFlow の設定

フローは、パケット フィールドを含む場合があるキー フィールド アトリビュート、パケット ルーティング アトリビュート、および入出力インターフェイス情報の一意のセットとして定義されます。NetFlow 機能は、フローを、機能キー フィールドの値が同じ一連のパケットとして定義します。Flexible Netflow（FNF）を使用すれば、さまざまなフロー アトリビュートが指定されたフロー レコードを収集して、オプションで転送することができます。Netflow 収集は、IP、IPv6、およびレイヤ 2 トラフィックをサポートします。

（注） この章では、Catalyst 4500 スイッチ固有の情報について説明します。プラットフォーム固有の設定やコマンド情報については、次のリンクを参照してください。

Flexible NetFlow コンフィギュレーション ガイド：

http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/12_4t/fnf_12_4t_book.html

Flexible NetFlow コマンド リファレンス：

http://www.cisco.com/en/US/docs/ios/fnetflow/command/reference/fnf_book.html

次の項目は、Catalyst 4500 シリーズ スイッチに適用されます。

1. Supervisor Engine 7-E は、スイッチ上のすべてのポートと VLAN で共有された 100,000 エントリのハードウェア フロー テーブルをサポートします。特定のインターフェイスまたは VLAN 上のテーブル エントリ数を制限するには、**cache entries** *number* コマンドを入力します。

   次に、1,000 エントリを保持するようにフロー モニタ *m1* キャッシュを設定する例を示します。この設定では、インターフェイス gig 3/1 で最大 1,000 個のフローを、インターフェイス gig 3/2 で最大 1,000 個のフローを作成することができます。

```
flow exporter e1
    ! exporter specifies where the flow records are send to
    destination 20.1.20.4
!
flow record r1
    ! record specifies packet fields to collect
    match ipv4 source address
    match ipv4 destination address
    collect counter bytes long
    collect counter packets long
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last
```

```
!
flow monitor m1
    ! monitor refers record configuration and optionally exporter
    ! configuration. It specifies the cache size i.e. how many unique flow
    ! records to collect
    record r1
    exporter e1
    cache timeout active 60
    cache timeout inactive 30
    cache entries 1000

!interface GigabitEthernet 3/1
    ! layer2-switched allows collection of flow records even when the packet is
    ! bridged
     ip flow monitor m1 layer2-switched input
!
interface GigabitEthernet 3/2
    ip flow monitor m1 input
!
```

2. フロー収集は、複数のターゲット（ポート、VLAN、ポート単位/VLAN 単位（特定のポートの VLAN 上で FNF をイネーブルにできる））と 1 つのポートチャネル（FNF が個々のメンバー ポートではなく、ポートチャネル インターフェイス上で設定される）上でサポートされます。
3. 64 個の一意のフロー レコード設定がサポートされます。
4. フロー QoS/UBRL と FNF は同じターゲット上で設定できません（フロー ベースの QoS については、「フローベース QoS」（P.31-11）を参照してください）。
5. 14,000 個の一意の IPv6 アドレスをモニタすることができます。
6. 特定のターゲット上で、トラフィック タイプごとに 1 つずつのモニタを使用することができます。ただし、同じターゲット上の複数のモニタを複数のトラフィック タイプ用に設定することができます。

   たとえば、次の設定が使用できます。

```
 ! vlan config 10
       ip flow monitor <name> input
       ipv6 flow monitor <name> input
 !
```

   次の設定は使用できません。

```
!
interface GigabitEthernet 3/1
       ip flow monitor m1 input
       ip flow monitor m2 input
```

7. レイヤ 2 とレイヤ 3 をモニタしている特定のターゲット上で、同時トラフィックはサポートされません。

```
 interface channel-group 1
       datalink flow monitor m1 input
        ip flow monitor m2 input
!
```

8. 1 つのフロー レコード定義でレイヤ 2 パケット フィールドとレイヤ 3 パケット フィールドを選択することはできません。ただし、パケット COS とレイヤ 3 パケット フィールドを選択することはできます。
9. 永続的と通常のフロー キャッシュ タイプしかサポートされません。
10. フロー キャッシュ内でのフローの有効期限は、アクティブと非アクティブのタイマー設定を通して制御されます。アクティブと非アクティブのエージング タイマーの最小値は 5 秒です。このタイマーは、5 秒単位にする必要があります。

（注）　ハードウェア テーブル内のフローは、アクティブまたは非アクティブ タイマーの設定値に関係なく、5 秒間の無活動期間後に削除されます。これにより、新しいハードウェア フローをすばやく作成することができます。

11. First-seen および Last-seen フローのタイムスタンプの精度は 3 秒以内です。

- TTL がフロー フィールドとして設定されている場合は、次の値が特定のパケット TTL 値として報告されます。表 30-1 に、パケット TTL と報告される値を示します。

表 30-1　TTL マップ

パケット TTL 長	報告される値
0	0
1	1
2 ～ 10	10
11 ～ 25	25
26 ～ 50	50
51 ～ 100	100
100 ～ 150	150
150 ～ 255	255

- パケット長がフロー フィールドとして設定されている場合は、次の値が特定のパケット長として報告されます。表 30-2 に、パケット TTL と報告される値を示します。

表 30-2　パケット長マップ

パケット長	報告される値
0 ～ 64	64
65 ～ 128	128
129 ～ 256	256
257 ～ 512	512
513 ～ 756	756
757 ～ 1500	1500
1500 ～ 4000	4000
4000+	8192

次の表に、FNF 経由で使用可能なオプションとサポートされているフィールドを示します。

表 30-3　FNF 経由で使用可能なオプションとサポートされているフィールド

フィールド	説明	説明
データ リンク フィールド（レイヤ 2 フロー ラベル + A94）		
dot1q priority	802 1Q ユーザ	
dot1q vid	802.1Q VLAN ID	出力 VLAN は収集オプションとしてのみサポートされます。
mac destination-address	アップストリーム宛先 MAC アドレス	
mac source-address	ダウンストリーム送信元 MAC アドレス	
IPv4 フィールド		
destination address	IPv4 宛先アドレス	可
DSCP	IPv4 DSCP（TOS の一部）	
fragmentation flags	IPv4 フラグメンテーション フラグ	非キーとしてサポートされます。DF フラグはサポートされません。
is-multicast	IPv4 マルチキャスト パケットかどうか（0：マルチパケットでない場合、1：マルチパケットの場合）	非キーとしてサポートされます。
Precedence	IPv4 precedence	
Protocol	IPv4 プロトコル	
source address	IPv4 送信元アドレス	
total length	IPv4 データグラム	値は表 30-2 に基づいて報告されます。
Total length minimum	検出された最小パケット サイズ	
Total length maximum	検出された最大パケット サイズ	
Tos	IPv4 Type Of Service（TOS; タイプ オブ サービス）	
ttl	Pv4 Time to Live（TTL）	値は表 30-1 に基づいて報告されます。
ttl minimum	FNF は mon-key モードでのみこのフィールドをサポートします。	
ttl maximum	FNF は mon-key モードでのみこのフィールドをサポートします。	

表 30-3　FNF 経由で使用可能なオプションとサポートされているフィールド（続き）

フィールド	説明	説明
IPv6 フィールド		
destination address	IPv6 宛先アドレス	
dscp	IPv6 DSCP（IPv6 トラフィック クラスの一部）	
flow-label	IPv6 フロー ラベル	
is-multicast	IPv6 マルチキャスト パケットかどうか（0：マルチパケットでない場合、1：マルチパケットの場合）	非キー フィールドとしてサポートされます。
hop-limit	IPv6 ホップ制限（従来の IPv4 ttl）	値は表 30-1 に基づいて報告されます。
hop-limit minimum	フロー内で検出された IPv6 最小ホップ制限値。非キー フィールドとしてしか使用することができません。	
hop-limit maximum	フロー内で検出された IPv6 最大ホップ制限値。非キー フィールドとしてしか使用することができません。	
next-header	IPv5 ネクスト ヘッダー タイプ	最初のネクスト ヘッダーのみが報告されます。
total length	IPv6 総パケット長	値は表 30-2 に基づきます。
Total length minimum	検出された最小パケット サイズ	
Total length maximim	検出された最大パケット サイズ	
protocol	最後の IPv6 拡張ヘッダー内の IPv6 ネクスト ヘッダー タイプ	
source address	IPv6 送信元アドレス	
traffic-class	IPv6 トラフィック クラス	可
ルーティング アトリビュート		
forwarding-status	パケットの転送ステータス（転送済み、ルータ内で終端、ACL、RPF、または CAR によってドロップ）	非キー フィールドとしてサポートされます。
レイヤ 4 ヘッダー フィールド		

表 30-3　FNF 経由で使用可能なオプションとサポートされているフィールド（続き）

フィールド	説明	説明
TCP ヘッダー フィールド		
destination-port TCP destination number	TCP 宛先ポート	
flags [ack] [fin] [psh] [rst] [syn] [urg]	TCP フラグ	非キー フィールドとしてサポートされます。
source-port	TCP 送信元ポート	
UDP ヘッダー フィールド		
destination-port	UDP 宛先ポート	
source-port	UDP 送信元ポート	
ICMP ヘッダー フィールド		
code	ICMP コード	
type	ICMP タイプ	
IGMP ヘッダー フィールド		
type	IGMP	
インターフェイス フィールド		
input	入力インターフェイス索引	
output	入力インターフェイス索引	出力インターフェイスは非キーとしてのみサポートすることができます。
Flexible NetFlow 機能関連フィールド		
direction: input		
カウンタ フィールド		
bytes	32 ビット カウンタ	
bytes long	64 ビット カウンタ	
packets	32 ビット カウンタ	
packets long	フロー内のパケットの 64 ビット カウンタ	
タイムスタンプ		
first seen	フロー内でアカウントされた最初のパケットのタイムスタンプ（ミリ秒単位、ルータ起動後に開始）	3 sec accuracy
last seen	フロー内でアカウントされた最後のパケットのタイムスタンプ（ミリ秒単位、ルータ起動後に開始）	3 sec accuracy

フロー モニタ キャッシュ値の設定

アクティブ キャッシュ タイムアウト値を小さくすると、より頻繁にフローがリモート コレクタに転送されます。また、ソフトウェアによって、転送されたフローがローカル キャッシュから削除されます。そのため、スイッチから報告されるキャッシュ統計情報に実際のモニタ対象フローが表示されない場合があります。