CHAPTER 61

NetFlow の設定

（注） NetFlow は、Catalyst 4900M、Catalyst 4948E、Supervisor Engine 6-E、Supervisor Engine 6L-E、Supervisor Engine 7-E、Supervisor Engine 7L-E、および Catalyst 4500X ではサポートされません。これは、Supervisor Engine V および Supervisor Engine V-10GE だけでサポートされます。

この章では、Catalyst 4500 シリーズ スイッチ上で、NetFlow 統計情報を設定する方法について説明します。設定上の注意事項、設定手順、および設定例についても示します。

次のトピックについて説明します。

（注） この章で使用するスイッチ コマンドの構文および使用方法の詳細については、次の URL で『*Cisco Catalyst 4500 Series Switch Command Reference*』と関連資料を参照してください。

http://www.cisco.com/en/US/products//hw/switches/ps4324/index.html

『Catalyst 4500 Series Switch Command Reference』に掲載されていないコマンドについては、より詳細な Cisco IOS ライブラリを参照してください。次の URL で『*Cisco IOS Command Reference*』と関連資料を参照してください。

http://www.cisco.com/en/US/products/ps6350/index.html

（注） NetFlow の使用および管理の詳細については、『*NetFlow Solutions Guide*』を参照してください。

NetFlow 統計情報収集について

ネットワーク フローは、特定の送信元と宛先（両方ともネットワーク層 IP アドレスおよびトランスポートレイヤ ポート番号で定義）の間における、パケットの単方向ストリームとして定義されます。具体的にフローは、送信元 IP アドレス、宛先 IP アドレス、送信元ポート番号、宛先ポート番号、プロトコル タイプ、Type of Service（ToS; タイプ オブ サービス）、入力インターフェイスというフィールドの組み合わせとして識別されます。

NetFlow 統計情報は、グローバル トラフィックのモニタ機能であり、これにより、NetFlow Data Export（NDE; NetFlow データ エクスポート）を使用して、スイッチを通過するすべての IPv4 ルーテッド トラフィックをフローレベルで監視できるようになります。収集された統計情報は、外部デバイス（NetFlow Collector/Analyzer）にエクスポートしてさらに処理できます。ネットワーク プランナーは、NetFlow 統計情報（および NDE）をデバイス単位で選択的にイネーブルにして、特定のネットワーク領域のトラフィック パフォーマンス、制御、または課金情報を得ることができます。

NetFlow は、2 つのフォーマットのうちどちらかにより、UDP データグラムでフロー情報をエクスポートします。バージョン 1 フォーマットは最初にリリースされたバージョンであり、バージョン 5 は、Border Gateway Protocol（BGP）自律システム（AS）情報およびフロー シーケンス番号を追加した強化機能です。バージョン 1 フォーマットおよびバージョン 5 フォーマットでは、ヘッダーおよび 1 つ以上のフロー レコードからデータグラムが構成されます。ヘッダーの最初のフィールドに、エクスポート データグラムのバージョン番号が指定されます。

ここでは、次の内容について説明します。

NDE バージョン

Catalyst 4500 シリーズ スイッチでは、収集された統計情報用に NDE バージョン 1 および 5 がサポートされます。NetFlow 集計では NDE バージョン 8 が必要です。

現在のフロー マスクによっては、フロー レコードの一部のフィールドに値が入らない場合があります。サポートされないフィールドには、ゼロ（0）が充填されます。

次の表では、NDE バージョン 5 でサポートされているフィールドについて説明します。

- 表 61-1：バージョン 5 ヘッダー形式
- 表 61-2：バージョン 5 フロー レコード形式

表 61-1　NDE バージョン 5 ヘッダー形式

バイト	内容	説明
0 ～ 1	version	NetFlow がエクスポートする形式のバージョン番号
2 ～ 3	count	このパケットにエクスポートされたフロー数（1 ～ 30）
4 ～ 7	sysUpTime	スイッチを起動してから経過したミリ秒単位の時間
8 ～ 11	unix_secs	0000 UTC 1970 から現在までの秒数
12 ～ 15	unix_nsecs	0000 UTC 1970 からの残り時間（ナノ秒）
16 ～ 19	flow_sequence	表示される合計フローのシーケンス カウンタ
20 ～ 21	engine_type	フロー スイッチング エンジンのタイプ
21 ～ 23	engine_id	フロー スイッチング エンジンのスロット番号

表 61-2　NDE バージョン 5 フロー レコード形式

バイト	内容	説明	フロー マスク • X = 読み込まれる • A = 追加のフィールド 送信元	宛先	宛先 送信元	宛先 送信元 インターフェイス	フル	フル インターフェイス
0 ～ 3	srcaddr	送信元 IP アドレス	X		X	X	X	X
4 ～ 7	dstaddr	宛先 IP アドレス		X	X	X	X	X
8 ～ 11	nexthop	ネクスト ホップ スイッチの IP アドレス		A[1]	A	A	A	A
12 ～ 13	input	入力インターフェイス SNMP ifIndex				X		X
14 ～ 15	output	出力インターフェイス SNMP ifIndex		A[1]	A	A	A	A
16 ～ 19	dPkts	フロー内のパケット数	X	X	X	X	X	X
20 ～ 23	dOctets	フロー内のオクテット数（バイト）	X	X	X	X	X	X
24 ～ 27	first	フロー開始時の sysUptime	X	X	X	X	X	X
28 ～ 31	last	フローの最終パケット受信時の sysUptime	X	X	X	X	X	X
32 ～ 33	srcport	レイヤ 4 送信元ポート番号またはそれと同等のもの					X[2]	X[2]
34 ～ 35	dstport	レイヤ 4 宛先ポート番号またはそれと同等のもの					X	X
36	pad1	未使用（ゼロ）バイト						
37	tcp_flags	TCP フラグの累積 OR						
38	prot	レイヤ 4 プロトコル（たとえば、6=TCP、17=UDP）					X	X
39	tos	IP タイプ オブ サービス バイト						
40 ～ 41	src_as	送信元の自律システム番号（オリジンまたはピア）	X		X	X	X	X
42 ～ 43	dst_as	宛先の自律システム番号（オリジンまたはピア）		X	X	X	X	X
44 ～ 45	src_mask	送信元アドレス プレフィックス マスク ビット	X		X	X	X	X
46 ～ 47	dst_mask	宛先アドレス プレフィックス マスク ビット		X	X	X	X	X
48	pad2	使用しない（0 の）バイト						

1. 宛先フロー マスクの場合、「ネクスト ホップ スイッチの IP アドレス」フィールドおよび「出力インターフェイスの SNMP ifIndex」フィールドには、すべてのフローで正確な情報が含まれないことがあります。
2. PFC3BXL モードまたは PFC3B モードでは、ICMP トラフィックに ICMP コードとタイプの値が含まれます。

ハードウェアから取得する情報

ハードウェアからの一般的な NetFlow レコードで入手できる情報には、次の内容が含まれます。

- パケット数とバイト数
- 開始タイムスタンプおよび終了タイムスタンプ
- 送信元 IP アドレスおよび宛先 IP アドレス
- IP プロトコル
- 送信元ポート番号および宛先ポート番号

ソフトウェアから取得する情報

ソフトウェアからの一般的な NetFlow レコードで入手できる情報には、次の内容が含まれます。

- 入力識別子および出力識別子
- ネクストホップ アドレス、始点およびピア AS、送信元および宛先プレフィックス マスクを含むルーティング情報

入力および出力インターフェイス番号と AS 番号の割り当て

ここでは、次の内容について説明します。

- 「予測フィールドの割り当て」（P.61-4）
- 「出力インターフェイスおよび出力関連予測フィールドの割り当て」（P.61-4）
- 「入力インターフェイスおよび入力関連予測フィールドの割り当て」（P.61-5）

予測フィールドの割り当て

Catalyst 4500 シリーズ スイッチでは、ハードウェアで NetFlow フローが収集されます。ハードウェアでは、すべての NetFlow フロー フィールドのサブセットが収集されます。残りのフィールドは、ソフトウェアによってルーティング状態が調査されたとき、ソフトウェアによって入力されます。

Netflow Services Card には、NetFlow Flows に関連する入力インターフェイス、出力インターフェイス、その他のルーティング情報を正確にかつ一貫して判別する情報が十分にありません。Catalyst 4500 シリーズ スイッチには、これを補うソフトウェア メカニズムがあります。このメカニズムについて、次の段落で説明します。

出力インターフェイスおよび出力関連予測フィールドの割り当て

ソフトウェアは、（宛先 IP アドレスに基づいた）デフォルトの Forwarding Information Base（FIB; 転送情報ベース）テーブルの FIB エントリを検索して出力インターフェイス情報を判別します。この FIB エントリから、ソフトウェアはこの宛先 IP アドレスの宛先 AS 番号およびインターフェイス情報を格納する適切な隣接装置へのアクセスができるようになります。出力インターフェイスは単に宛先

IP アドレスに基づいています。スイッチ上でロード バランシングがイネーブルにされている場合、FIB エントリで隣接装置を検索する代わりに、ロード バランシング ハッシュが適切な FIB パスにアクセスするように適用され、適切な隣接装置にアクセスします。このプロセスは、通常、正しい結果を生成しますが、デフォルトの FIB テーブルで IP アドレスを共有する PBR が使用されている場合、正しい結果が得られない場合があります。このような環境では、同一の宛先 IP アドレスに FIB テーブル エントリおよび関連付けられた隣接装置が複数存在するようになります。

入力インターフェイスおよび入力関連予測フィールドの割り当て

同様に、入力インターフェイスと送信元 IP アドレスの送信元 AS 番号は、送信元 IP アドレスに基づいたデフォルトの FIB テーブルの FIB エントリを検索することによって判別されます。入力インターフェイスは単に送信元 IP アドレスに基づいており、逆ルックアップが行われて、この IP 宛先アドレスを持つパケットがルーティングされる必要があるインターフェイスが判別されます。このプロセスは、転送パスが対称であると仮定します。ただし、このプロセスが複数の入力インターフェイスを生成する場合、最小の IP アドレスを持つインターフェイスを 1 つ選択するように決定論的なアルゴリズムが適用されます。このプロセスは通常正しい値を生成しますが、値が正確でない場合もあります。

- ロード バランシングがアップストリーム隣接スイッチによって適用されている場合、使用可能な複数の入力インターフェイスから任意の 1 つの入力インターフェイスが選択される必要があります。このアクションが必要とされるのは、使用される入力インターフェイスが、隣接アップストリーム スイッチによって適用されるロードバランシング アルゴリズムのタイプに左右されるためです。そのアルゴリズムを常に知ることができるとはかぎりません。すべてのフロー統計情報は、1 つの入力インターフェイスによるものとなります。ソフトウェアは、最小の IP サブネット番号を持つインターフェイスを選択します。
- 非対称ルーティング方式では、IP サブネットのトラフィックが、この IP サブネットにパケットを送信するインターフェイスとは別のインターフェイスで受信されることがありますが、逆ルックアップに基づいて入力インターフェイスを選択した予測が、不正確で確認できない可能性があります。
- スイッチ上で PBR または VRF がイネーブルに設定されており、フローが PBR 範囲または VRF 範囲にあるアドレスに送られる場合、または PBR 範囲または VRF 範囲にあるアドレスから送信される場合、この情報は正しくありません。入力および出力インターフェイスは、デフォルトのルート（設定されている場合）を指定する可能性が高く、そうでない場合は値が得られずヌルの状態となります。
- 一部のインターフェイスのスイッチで VRF がイネーブルになっており、フローが VRF インターフェイスから送信される場合、情報は正しくありません。入力および出力インターフェイスは、デフォルトのルート（設定されている場合）を指定する可能性が高く、そうでない場合は値が得られずヌルの状態となります。

UBRL およびマイクロフロー ポリシングと Netflow 統計情報の機能の相互作用

Supervisor Engine V-10GE を含むシステムでは、Netflow 統計情報および User Based Rate Limiting（UBRL）の間に機能の相互作用があります。特定インターフェイスで正しく設定している UBRL の一部として、クラスマップではフローマスクを指定する必要があります。このフローマスクは、フローのハードウェアベース NetFlow 統計情報の作成に使用されます。デフォルトの場合、従来の full flow NetFlow 統計情報には、full flow マスクが使用されます。しかし UBRL では、マスクが異なることがあります。特定インターフェイスで UBRL を設定している場合、統計情報は、UBRL 用に設定したマスクに基づいて収集されます。その結果、UBRL で設定されたインターフェイスを通過するトラフィックの full flow 統計情報がシステムで収集されません。詳細については、第 41 章「Quality of Service の設定」を参照してください。

VLAN の統計情報

NetFlow がサポートされている場合は、レイヤ 2 出力 VLAN 統計、および VLAN を出入りするルーティング済みトラフィックの VLAN 統計をレポートできます。

次の例は、特定 VLAN の CLI 出力を示しています。

```
Switch# show vlan counters or show vlan id 22 count
* Multicast counters include broadcast packets
Vlan Id                                          :22
L2 Unicast Packets                               :38
L2 Unicast Octets                                :2432
L3 Input Unicast Packets                         :14344621
L3 Input Unicast Octets                          :659852566
L3 Output Unicast Packets                        :8983050
L3 Output Unicast Octets                         :413220300
L3 Output Multicast Packets                      :0
L3 Output Multicast Octets                       :0
L3 Input Multicast Packets                       :0
L3 Input Multicast Octets                        :0
L2 Multicast Packets                             :340
L2 Multicast Octets                              :21760
```

（注）　NetFlow のサポートには、プラットフォームのサポートをすべての NetFlow フィールドのサブセットに限定するハードウェア制限があります。具体的には、TCP フラグおよび ToS バイト（DSCP）がサポートされません。

NetFlow 統計情報収集機能の設定

NetFlow スイッチングを設定するには、次の作業を行います。

- 「必要なハードウェアの確認」（P.61-6）
- 「NetFlow 統計情報収集機能のイネーブル化」（P.61-7）
- 「スイッチド/ブリッジド IP フローの設定」（P.61-8）
- 「NetFlow 統計情報のエクスポート」（P.61-9）
- 「NetFlow 統計情報収集機能の管理」（P.61-10）
- 「集約キャッシュの設定」（P.61-10）
- 「ルータベース集約の NetFlow 最小プレフィックス マスクの設定」（P.61-11）
- 「NetFlow エージング パラメータの設定」（P.61-12）

必要なハードウェアの確認

必要なハードウェアがイネーブルであることを確認するためには、次のように **show module** コマンドを入力します。

```
Switch# show module all
Chassis Type : WS-C4507R

Power consumed by backplane : 40 Watts

Mod Ports Card Type                              Model
Serial No.
```

```
---+-----+---------------------------------------+------------------+-----------
1     2  1000BaseX (GBIC) Supervisor(active)    WS-X4515
JAB062604KB
2     2  1000BaseX (GBIC) Supervisor(standby)   WS-X4515
JAB062408CB
6    48  10/100BaseTX (RJ45)                    WS-X4148
JAB032305UH

M MAC addresses                    Hw  Fw           Sw               Status
--+--------------------------------+---+------------+----------------+---------
1 0001.6442.2c00 to 0001.6442.2c01 0.4 12.1(14r)EW( 12.1(20030513:00 Ok
2 0001.6442.2c02 to 0001.6442.2c03 0.4 12.1(14r)EW( 12.1(20030513:00 Ok
6 0050.3ed8.6780 to 0050.3ed8.67af 1.6 12.1(14r)EW( 12.1(20030513:00 Ok

Mod  Submodule               Model             Serial No.   Hw   Status
----+----------------------+-----------------+------------+----+---------
1   Netflow Services Card   WS-F4531          JAB062209CG  0.2  Ok
2   Netflow Services Card   WS-F4531          JAB062209AG  0.2  Ok

Switch#
```

（注） この機能をイネーブルにしても、スイッチのハードウェア転送パフォーマンスには影響しません。

ハードウェアのフロー キャッシュ テーブルの有効サイズは 65,000 フローです。Supervisor Engine V-10GE のハードウェア フロー キャッシュは、85,000 フローです。85,000 フローより多いフローが同時にアクティブになると、一部のフローの統計情報が失われます。

ソフトウェアのフロー テーブルの有効サイズは 256,000 フローです。NetFlow ソフトウェアは、ハードウェア テーブルとソフトウェア テーブル間の一貫性を管理します。ソフトウェア テーブルへの非アクティブのハードウェア フローを削除することで、ハードウェア テーブルをオープンのままにします。

ユーザが設定するタイムアウト設定は、フローが削除され、ソフトウェア キャッシュから NDE を通じてエクスポートされる時間を指定します。ハードウェア フロー管理は、ハードウェア フロー削除とユーザが設定するタイムアウト設定との一貫性を保ちます。

また、ソフトウェア転送フローも監視されます。さらに、いずれかのフローが 2 Gbps を超える平均速度でトラフィックを受信すると統計情報がオーバーフローになります。ただし、一般的にポートは 1 Gbps を超える速度で伝送できないため、このような状態は発生しません。

（注） 設計上、タイムアウト設定が高い場合でも、統計情報の制限に近づくとフローは自動的に「期限切れ」となります。

（注） First-seen および Last-seen（開始および終了時間）フローのタイムスタンプの精度は 3 秒以内です。

NetFlow 統計情報収集機能のイネーブル化

（注） デフォルトでは、NetFlow 統計情報はディセーブルです。

NetFlow スイッチングをイネーブルにするには、最初に『*Cisco IOS IP and IP Routing Configuration Guide*』の「IP configuration」にある IP ルーティング用のスイッチ設定を実行してください。IP ルーティングを設定したあと、次のいずれかの作業を行ってください。

コマンド	目的
`Switch(config)# ip flow ingress`	IP ルーティング用の NetFlow をイネーブルにします。
`Switch(config)# ip flow ingress infer-fields`	情報として予測入力/出力インターフェイスおよび送信元/宛先 BGP を持つ NetFlow をイネーブルにします。 AS 情報が判別されるようにするには、**inter-fields** オプションを設定する必要があります。

スイッチド/ブリッジド IP フローの設定

Netflow は、すべてのルーテッド IP トラフィック用に作成および追跡されるルーテッド IP フローの収集として定義されます。スイッチング環境では、多量の IP トラフィックが VLAN 内でスイッチングされ、ルーティングはされません。このトラフィックは、*スイッチド/ブリッジド IP トラフィック*といいます。これに関連するフローを*スイッチド/ブリッジド IP フロー*といいます。NetFlow ハードウェアには、このタイプのフローを作成および追跡する機能があります。NetFlow スイッチド IP フロー機能により、スイッチド IP フローを作成、追跡、およびエクスポートできます（つまり、スイッチングされ、ルーティングされない IP トラフィックのフローを作成および追跡します）。

次の点に注意してください。

- Catalyst 4500 シリーズ スイッチでは、スイッチド IP フロー収集を単独でイネーブルにできません。スイッチド IP フローの収集を開始するには、ルーテッド フロー収集およびスイッチド フロー収集の両方をイネーブルにする必要があります。
- 一般的に、入力および出力インターフェイスの情報はヌルになります。トラフィックが SVI に関連付けられた VLAN 上でスイッチングされる場合、入力および出力インターフェイス情報は同じレイヤ 3 インターフェイスをポイントします。
- スイッチド フローは通常のエクスポート設定に従ってエクスポートされます。個別のエクスポート CLI は存在しません。
- メイン キャッシュでは、ハードウェアの制限により、IP フローおよびルーテッド IP フローは区別できません。

（注） すべてのインターフェイス上でスイッチド IP フロー収集をイネーブルにするには、**ip flow ingress** および **ip flow ingress layer2-switched** コマンドの両方を入力する必要があります。

（注） スイッチド IP フロー トラフィック上で User Based Rate Limiting ポリシーをイネーブルにするには、**ip flow ingress** コマンドではなく **ip flow ingress layer2-switched** コマンドを入力する必要があります。第 41 章「Quality of Service の設定」を参照してください。

NetFlow キャッシュを設定し、スイッチド IP フロー収集をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# conf terminal`	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 flow ingress`	ルーテッド フロー収集をイネーブルにします。
ステップ 3	`Switch(config)# ip flow ingress layer2-switched`	スイッチド フロー収集をイネーブルにします。

次に、スイッチ IP フローを含む IP フロー キャッシュの内容を表示する例を示します。

```
Switch# show ip cache flow
IP Flow Switching Cache, 17826816 bytes
 2 active, 262142 inactive, 2 added
 6 ager polls, 0 flow alloc failures
 Active flows timeout in 30 minutes
 Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 1081480 bytes
 2 active, 65534 inactive, 2 added, 2 added to flow
 0 alloc failures, 0 force free
 1 chunk, 1 chunk added
 last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa1           150.1.1.1       Fa1           13.1.1.1        11 003F 003F   425K
Fa1           13.1.1.1        Fa1           150.1.1.1       11 003F 003F   425K
Switch#
```

NetFlow 統計情報のエクスポート

フローの有効期限が切れたときに NetFlow 統計情報をワークステーションにエクスポートするようにスイッチを設定するには、次のいずれかの作業を行います。

コマンド	目的
`Switch(config)# ip flow-export destination {hostname | ip-address} udp-port`	（必須）NetFlow キャッシュ エントリを特定の宛先（ワークステーションなど）にエクスポートするようにスイッチを設定します。 **（注）**　複数の宛先を指定できます。
`Switch(config)# ip flow-export version {1 | {5 [origin-as | peer-as]}}`	（任意）バージョン 1 または 5 が必要な受信ソフトウェアを使用している場合に、ワークステーションに NetFlow キャッシュ エントリをエクスポートするようにスイッチを設定します。デフォルトはバージョン 1 です。 **origin-as** によって、NetFlow は、フローの送信元と宛先ホスト両方の始点 BGP 自律システムを判別します。 **peer-as** によって、NetFlow は、フローの入力および出力インターフェイス両方のピア BGP 自律システムを判別します。
`Switch(config)# ip flow-export source interface`	（任意）IP アドレスが NetFlow Data Export（NDE; NetFlow データ エクスポート）パケットの IP ヘッダー内で送信元 IP アドレスとして使用されるインターフェイスを指定します。デフォルトは、NDE 出力インターフェイスです。

NetFlow 統計情報収集機能の管理

IP フロー スイッチング キャッシュ情報やフロー情報（プロトコル、フロー合計、秒あたりのフローなど）などの NetFlow 統計情報を表示し、クリアできます。また、結果情報を使用してスイッチ トラフィックの情報を得ることもできます。

NetFlow スイッチング統計情報を管理するには、次のいずれかの作業、または両方の作業を行います。

コマンド	目的
`Switch# show ip cache flow`	NetFlow スイッチング統計情報を表示します。
`Switch# clear ip flow stats`	NetFlow スイッチング統計情報をクリアします。

集約キャッシュの設定

NetFlow 統計情報の集約は、通常、管理ワークステーション上の NetFlow 収集ツールによって実行されます。このサポートを Catalyst 4500 シリーズ スイッチに拡張することによって、次のことが可能になります。

- エクスポートされる NDE パケットが少なくなるため、スイッチとワークステーション間で必要な帯域幅が削減されます。
- 必要な収集ワークステーション数が削減されます。
- CLI で集約されたフローの統計情報を表示できます。

集約キャッシュを設定するには、集約キャッシュ コンフィギュレーション モードを開始し、設定する集約方式のタイプ（autonomous system、destination prefix、protocol prefix、または source prefix aggregation cache）を決定する必要があります。集約方式を定義したら、その方式の動作パラメータを定義します。同時に複数の集約キャッシュを設定できます。

集約キャッシュを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# ip flow-aggregation cache as`	集約キャッシュ コンフィギュレーション モードを開始し、集約キャッシュ方式（autonomous system、destination-prefix、prefix、protocol-port、または source-prefix）をイネーブルにします。
ステップ 2	`Switch(config-flow-cache)# cache timeout inactive 199`	非アクティブのエントリが削除されるまで集約キャッシュに保持される秒数（ここでは、199）を指定します。
ステップ 3	`Switch(config-flow-cache)# cache timeout active 45`	アクティブ エントリがアクティブの状態である分数（ここでは、45）を指定します。
ステップ 4	`Switch(config-flow-cache)# export destination 10.42.41.1 9991`	データ エクスポートをイネーブルにします。
ステップ 5	`Switch(config-flow-cache)# enabled`	集約キャッシュの作成をイネーブルにします。

集約キャッシュ設定およびデータ エクスポートの確認

集約キャッシュ情報を確認するには、次の作業を行います。

コマンド	目的
Switch# **show ip cache flow aggregation destination-prefix**	指定された集約キャッシュ情報を表示します。

データ エクスポートを確認するには、次の作業を行います。

コマンド	目的
Switch# **show ip flow export**	メイン キャッシュおよびその他のすべてのイネーブルに設定されたキャッシュを含むデータ エクスポートの統計情報を表示します。

ルータベース集約の NetFlow 最小プレフィックス マスクの設定

最小プレフィックス マスクは、1 つの IP アドレス ベースの集約キャッシュ（source-prefix、destination-prefix、prefix）内の集約フローに使用される最短のサブネット マスクを指定します。このようなキャッシュでは、フローは IP アドレス（送信元、宛先、またはその両方のそれぞれ）に基づいて集約され、最小プレフィックス マスク、およびスイッチのルーティング テーブルで見つかったフローの送信元/宛先ホストへのルートのサブネット マスクのうち長い方によってマスクされます。

（注） 最小マスクのデフォルト値は 0 です。最小マスクの設定可能範囲は、1 ～ 32 です。トラフィックに応じて適切な値を選択する必要があります。最小マスクの値が高いと、より詳細なネットワーク アドレスが提供できますが、集約キャッシュのフローの数が増加する可能性もあります。

ルータベース集約機能の最小プレフィックス マスクを設定するには、次の項で説明する作業を行います。これらの作業は任意です。

- 「prefix 集約方式の最小マスクの設定」（P.61-11）
- 「destination-prefix 集約方式の最小マスクの設定」（P.61-11）
- 「source-prefix 集約方式の最小マスクの設定」（P.61-12）
- 「集約方式の最小マスクのモニタおよび保守」（P.61-12）

prefix 集約方式の最小マスクの設定

prefix 集約方式の最小マスクを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# **ip flow-aggregation cache prefix**	prefix 集約キャッシュを設定します。
ステップ 2	Switch(config-flow-cache)# **mask source minimum** *value*	送信元マスクの最小値を指定します。
ステップ 3	Switch(config-flow-cache)# **mask destination minimum** *value*	宛先マスクの最小値を指定します。

destination-prefix 集約方式の最小マスクの設定

destination-prefix 集約方式の最小マスクを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# ip flow-aggregation cache destination-prefix`	宛先集約キャッシュを設定します。
ステップ 2	`Switch(config-flow-cache)# mask destination minimum value`	宛先マスクの最小値を指定します。

source-prefix 集約方式の最小マスクの設定

source-prefix 集約方式の最小マスクを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# ip flow-aggregation cache source-prefix`	source-prefix 集約キャッシュを設定します。
ステップ 2	`Switch(config-flow-cache)# mask source minimum value`	送信元マスクの最小値を指定します。

集約方式の最小マスクのモニタおよび保守

設定された最小マスクの値を表示するには、必要に応じて各集約方式に対して次のコマンドを使用します。

コマンド	目的
`Switch# show ip cache flow aggregation prefix`	prefix 集約方式の設定された最小マスクの値を表示します。
`Switch# show ip cache flow aggregation destination-prefix`	destination-prefix 集約方式の設定された最小マスクの値を表示します。
`Switch# show ip cache flow aggregation source-prefix`	source-prefix 集約方式の設定された最小マスクの値を表示します。

NetFlow エージング パラメータの設定

フローをソフトウェア フロー キャッシュから削除する（また、設定されている場合、NDE を通じてレポートする）時期を、**ip flow-cache timeout** コマンドの設定エージング パラメータ **Active** および **Inactive** を使用して制御できます。

アクティブ エージングは、フローが作成されたあとにフローがソフトウェア フロー キャッシュから削除される時間を指定します。一般的に、このパラメータは外部収集デバイスへアクティブ フローについて定期的に通知するために使用します。このパラメータは、フローの既存のトラフィックから独立して動作します。アクティブ タイムアウト設定は通常、分単位で計測されます（デフォルトは 30 分）。

非アクティブ エージングは、最後のパケットが確認されてからフローを削除するまでの時間を指定します。非アクティブ パラメータは、古いフローのフロー キャッシュをクリアして、（リソース不足により）新しいフローが長時間停止しないようにします。非アクティブ タイムアウト設定は通常、秒単位です（デフォルトは 15 秒）。

NetFlow 統計情報収集機能の設定例

次に、設定を変更して NetFlow スイッチングをイネーブルにする例を示します。また、フロー統計情報をエクスポートして、IP アドレスが 40.0.0.2 のワークステーションの UDP ポート 9991 で処理する例を示します。この例では、既存の NetFlow 統計情報がクリアされるため、**show ip cache flow** コマンドで NetFlow スイッチング統計情報の正確なサマリーが確実に表示されます。

```
Switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip route-cache flow
Switch(config)# ip flow-export destination 40.0.0.2 9991
Switch(config)# ip flow-export version 5
Switch(config)# end
Switch# show ip flow export
Flow export is enabled
  Exporting flows to 40.0.0.2 (9991)
  Exporting using source IP address 40.0.0.1
  Version 5 flow records
  2 flows exported in 1 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
Switch#

Switch# show ip cache flow

IP Flow Switching Cache, 17826816 bytes
  69 active, 262075 inactive, 15087 added
  4293455 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 1081480 bytes
  0 active, 65536 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet          28      0.0       167    40      0.0      20.9      11.9
TCP-other          185      0.0         2    48      0.0       6.2      15.4
UDP-DNS              4      0.0         1    61      0.0       0.0      15.5
UDP-other        13466      0.0   3396586    46  91831.3     139.3      15.9
ICMP                97      0.0         2    95      0.0       2.3      15.4
IGMP                 1      0.0         2    40      0.0       0.9      15.1
IP-other          1120      0.0  38890838    46  87453.0    1354.5      24.0
Total:           14901      0.0   5992629    46 179284.3     227.8      16.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi6/2         30.20.1.18      Gi6/1         30.10.1.18      11 4001 4001   537K
Gi6/2         30.20.1.19      Gi6/1         30.10.1.19      11 4001 4001   537K
Gi6/2         30.20.1.16      Gi6/1         30.10.1.16      11 4001 4001   537K
Gi6/2         30.20.1.17      Gi6/1         30.10.1.17      11 4001 4001   537K
Gi6/2         30.20.1.20      Gi6/1         30.10.1.20      11 4001 4001   537K
Gi6/2         30.20.1.10      Gi6/1         30.10.1.10      11 4001 4001   539K
```

```
Gi6/2          30.20.1.11      Gi6/1          30.10.1.11      11 4001 4001   539K
Gi6/2          30.20.1.14      Gi6/1          30.10.1.14      11 4001 4001   539K
Gi6/2          30.20.1.15      Gi6/1          30.10.1.15      11 4001 4001   539K
Gi6/2          30.20.1.12      Gi6/1          30.10.1.12      11 4001 4001   539K
Gi6/2          30.20.1.13      Gi6/1          30.10.1.13      11 4001 4001   539K
Gi5/48         171.69.23.149   Local          172.20.64.200   06 8214 0017   759
Gi6/1          30.10.1.12      Gi6/2          30.20.1.12      11 4001 4001   539K
Gi6/1          30.10.1.13      Gi6/2          30.20.1.13      11 4001 4001   539K
Gi6/1          30.10.1.14      Gi6/2          30.20.1.14      11 4001 4001   539K
Gi6/1          30.10.1.15      Gi6/2          30.20.1.15      11 4001 4001   539K
Gi6/1          30.10.1.10      Gi6/2          30.20.1.10      11 4001 4001   539K
Gi6/1          30.10.1.11      Gi6/2          30.20.1.11      11 4001 4001   539K
Gi6/1          30.10.1.20      Gi6/2          30.20.1.20      11 4001 4001   537K
Gi6/1          30.10.1.16      Gi6/2          30.20.1.16      11 4001 4001   537K
Gi6/1          30.10.1.17      Gi6/2          30.20.1.17      11 4001 4001   537K
Gi6/1          30.10.1.18      Gi6/2          30.20.1.18      11 4001 4001   537K
Gi6/1          30.10.1.19      Gi6/2          30.20.1.19      11 4001 4001   537K
Switch#
```

NetFlow の設定例

ここでは、次の基本的な設定例を提供します。

- 「NetFlow イネーブル化方式の例」（P.61-14）
- 「NetFlow 集約の設定例」（P.61-14）
- 「ルータベース集約方式の NetFlow 最小プレフィックス マスクのサンプル」（P.61-16）

NetFlow イネーブル化方式の例

（注）　Catalyst 4500 スイッチ上では、インターフェイス単位の NetFlow のイネーブル化がサポートされていません。

次に、NetFlow をグローバルにイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# ip flow ingress
```

次に、予測フィールドをサポートする NetFlow をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# ip flow ingress infer-fields
```

NetFlow 集約の設定例

ここでは、次の集約キャッシュ設定例を示します。

- 「自律システムの設定」（P.61-15）
- 「宛先プレフィックスの設定」（P.61-15）
- 「プレフィックスの設定」（P.61-15）
- 「プロトコル ポートの設定」（P.61-15）
- 「送信元プレフィックスの設定」（P.61-16）

自律システムの設定

次に、自律システムの集約キャッシュに、200 秒の非アクティブ タイムアウト、45 分のキャッシュ アクティブ タイムアウト、エクスポート宛先 IP アドレス 10.42.42.1、および宛先ポート 9992 を設定する例を示します。

```
Switch(config)# ip flow-aggregation cache as
Switch(config-flow-cache)# cache timeout inactive 200
Switch(config-flow-cache)# cache timeout active 45
Switch(config-flow-cache)# export destination 10.42.42.1 9992
Switch(config-flow-cache)# enabled
```

宛先プレフィックスの設定

次に、宛先プレフィックスの集約キャッシュに、200 秒の非アクティブ タイムアウト、45 分のキャッシュ アクティブ タイムアウト、エクスポート宛先 IP アドレス 10.42.42.1、および宛先ポート 9992 を設定する例を示します。

```
Switch(config)# ip flow-aggregation cache destination-prefix
Switch(config-flow-cache)# cache timeout inactive 200
Switch(config-flow-cache)# cache timeout active 45
Switch(config-flow-cache)# export destination 10.42.42.1 9992
Switch(config-flow-cache)# enabled
```

プレフィックスの設定

次に、プレフィックスの集約キャッシュに、200 秒の非アクティブ タイムアウト、45 分のキャッシュ アクティブ タイムアウト、エクスポート宛先 IP アドレス 10.42.42.1、および宛先ポート 9992 を設定する例を示します。

```
Switch(config)# ip flow-aggregation cache prefix
Switch(config-flow-cache)# cache timeout inactive 200
Switch(config-flow-cache)# cache timeout active 45
Switch(config-flow-cache)# export destination 10.42.42.1 9992
Switch(config-flow-cache)# enabled
```

プロトコル ポートの設定

次に、プロトコル ポートの集約キャッシュに、200 秒の非アクティブ タイムアウト、45 分のキャッシュ アクティブ タイムアウト、エクスポート宛先 IP アドレス 10.42.42.1、および宛先ポート 9992 を設定する例を示します。

```
Switch(config)# ip flow-aggregation cache protocol-port
Switch(config-flow-cache)# cache timeout inactive 200
Switch(config-flow-cache)# cache timeout active 45
Switch(config-flow-cache)# export destination 10.42.42.1 9992
Switch(config-flow-cache)# enabled
```

送信元プレフィックスの設定

次に、送信元プレフィックスの集約キャッシュに、200 秒の非アクティブ タイムアウト、45 分のキャッシュ アクティブ タイムアウト、エクスポート宛先 IP アドレス 10.42.42.1、および宛先ポート 9992 を設定する例を示します。

```
Switch(config)# ip flow-aggregation cache source-prefix
Switch(config-flow-cache)# cache timeout inactive 200
Switch(config-flow-cache)# cache timeout active 45
Switch(config-flow-cache)# export destination 10.42.42.1 9992
Switch(config-flow-cache)# enabled
```

ルータベース集約方式の NetFlow 最小プレフィックス マスクのサンプル

ここでは、NetFlow 最小プレフィックス マスク集約キャッシュの設定例を示します。

- 「prefix 集約方式」（P.61-16）
- 「destination-prefix 集約方式」（P.61-16）
- 「source-prefix 集約方式」（P.61-16）

prefix 集約方式

次に、prefix 集約キャッシュの設定例を示します。

```
!
ip flow-aggregation cache prefix
mask source minimum 24
mask destination minimum 28
```

この例では、次の設定が前提になっています。

```
ip route 118.42.20.160 255.255.255.224 110.42.13.2
ip route 122.16.93.160 255.255.255.224 111.22.21.2
```

両方のルートがスイッチ上のルーティング テーブルに 27 ビットのサブネット マスクを持ちます。

118.42.20.160 サブネットから、送信元 IP アドレスが 27 ビットのマスクに一致し、宛先 IP アドレスが 28 ビットのマスクに一致する 122.16.93.160 サブネットに移動するフローは、キャッシュ統計情報で一緒に集約されます。

destination-prefix 集約方式

次に、destination-prefix 集約キャッシュの設定例を示します。

```
!
ip flow-aggregation cache destination-prefix
mask destination minimum 32
!
```

source-prefix 集約方式

次に、source-prefix 集約キャッシュの設定例を示します。

```
ip flow-aggregation cache source-prefix
mask source minimum 30
```