フロー パラメータとポート マッピング パラメータの設定

この章では、CSS のフロー パラメータとポート マッピング パラメータを設定する方法について説明します。この章の内容は、特に指定のない限り、すべての CSS モデルに共通です。

この章の主な内容は次のとおりです。

- フロー パラメータの設定
- コンテンツ ルールとソース グループでのフロー無活動タイムアウトの設定
- 断片化 IP パケットのフロー処理の設定
- VIP を利用できないときに CSS に TCP Reset を送信させる設定
- フロー状態テーブルの設定
- CSS ポート マッピングの設定

CSS でのフローの処理方法については、第 1 章「コンテンツ ロード バランシングの概要」を参照してください。

フロー パラメータの設定

CSS のフロー パラメータを設定するには、**flow** コマンドを使用します。このグローバル設定モード コマンドには、次のオプションがあります。

- **flow permanent** :再要求されない固定 TCP（または UDP）ポートを作成する。
- **flow tcp-mss** ：転送デバイスから CSS が受信する TCP の最大セグメント サイズを設定する。
- **flow persist-span-ooo** ：固定スパニング パケットの再配列を有効にする。
- **flow set-port-zero** ：CSS が TCP（または UDP）の送信元ポート 0 または宛先ポート 0 へトラフィックを送信できるようにする。
- **flow tcp-del-ack** ：レイヤ 5 のスパニング パケットに対し、TCP の遅延確認応答を有効にする。
- **flow statistics** ：現在割り当てられているフローに関する統計情報を表示する。

（注） CSS がフロー パラメータを設定できるのは、次の TCP または UDP ポートに限られます。67 （BOOTP サーバ）、68 （BOOTP クライアント）、137 （NETBIOS ネーム サービス）、138 （NETBIOS データグラム サービス）、161 （SNMP）、162 （SNMP トラップ）、520 （RIP）、および 8089 （制限付き UDP のみ）。デフォルトでは、CSS は、送信元または送信先のポートが 0 の TCP（または UDP）トラフィックを通しません。このトラフィックを通過させるように CSS を設定する方法については、「送信元ポートまたは宛先ポートが 0 の TCP または UDP トラフィックの通過」を参照してください。

ここでは、次の内容について説明します。

TCP または UDP ポートの固定接続の設定

CSS では、TCP または UDP ポートを 20 まで設定できます。これらのポートは固定接続であり、フローがアクティブでなくても CSS は再要求しません。TCP または UDP ポートを固定接続として設定するには、**flow permanent port1** *portnumber*（～ **flow permanent port 20** *portnumber*）コマンドを使用します。0 ～ 65535 の値を入力します。デフォルト値は 0 です。

CSS は、約 15 秒間 ACK またはコンテンツ要求を受信しないと、フローを再要求する場合があります。特定の送信元ポートまたは宛先ポートへの TCP/UDP フローの再要求が行われないようにするには、いずれかの **flow permanent port** コマンドを使用し、再要求しない TCP または UDP ポート番号を指定します。

たとえば、ポート 80 を固定接続として設定するには、次のように入力します。

```
(config) flow permanent port1 80
```

port1 のポート番号を 0 にリセットするには、次のように入力します。

```
(config) no flow permanent port1
```

flow permanent port コマンドを設定する場合は、**cmd-sched** コマンドも有効にして定期的に固定ポートを削除し、消去できるようにすることをお勧めします。**cmd-sched** コマンドによる CLI コマンドの実行スケジュールの設定の詳細については、『*Cisco Content Services Switch Administration Guide*』を参照してください。

TCP の最大セグメント サイズの設定

maximum segment size （MSS; 最大セグメント サイズ）は、1 つのセグメントで転送可能な TCP データの最大量です。デバイス間の MSS を削減する必要があるのは、非常にまれで、デバイス間にネットワークの制限がある場合です。転送デバイスから CSS が受信する TCP MSS のサイズを調整するには、**flow tcp-mss** コマンドを使用します。**flow tcp-mss** コマンドは、SYN セグメントの TCP ヘッダーの OPTIONS フィールドにある MSS の値を変更して、MSS をデフォルトの 1460 バイトよりも小さい値に設定します。

flow tcp-mss コマンドを適用できるのは、クライアントがレイヤ 5 のコンテンツルールにアクセスする場合だけです。CSS では、レイヤ 3 またはレイヤ 4 のコンテンツ ルールの TCP 最大セグメント サイズを変更することはできません。

最大セグメント サイズ（バイト単位）として 1 ～ 1460 を入力します。デフォルト値は 1460 バイトです。TCP 最大セグメント サイズをデフォルト値の 1460 バイトに戻すには、このコマンドの **no** 形式を使用します。

注意　**flow tcp-mss** コマンドで TCP 最大セグメント サイズを必要以上に小さい値に設定しないでください。ペイロードを減らすと、オーバーヘッドが増加し、効率が低下します。

1400 バイトの TCP 最大セグメント サイズを設定するには、次のように入力します。

```
(config)# flow tcp-mss 1400
```

TCP 最大セグメント サイズをデフォルト値の 1460 バイトに戻すには、次のように入力します。

```
(config)# no flow tcp-mss
```

固定スパニング パケットの再配列の有効化

デフォルトでは、固定スパニング パケットの再配列は無効に設定されています。パケットを正しい順序で再配列させるには、グローバル設定モードで **flow persist-span-ooo** コマンドを使用します。

たとえば、次のように入力します。

```
(config)# flow persist-span-ooo
```

固定スパニング パケットの再配列をデフォルトの動作に戻して無効にするには、**no flow persist-span-ooo** コマンドを使用します。たとえば、次のように入力します。

```
(config)# no flow persist-span-ooo
```

（注） arrowpoint クッキーをサーバからの応答に挿入するように設定した場合、その設定 は、正しい順序で到着したパケットに対して適用されます。FIN パケットを受信している CSS にパケットが誤った順序で到着した場合、サーバ データ パケットの受信が完了すると、CSS は arrowpoint クッキーを挿入せずにそのパケットを転送します。**flow persist-span-ooo** コマンドを有効にすると、CSS は、誤った順序で到着した FIN パケットを検出した場合に、これを廃棄します。その後、サーバがパケットを再送信すると、CSS は正しい順序のパケットを処理し、arrowpoint クッキーをサーバのデータ パケットに挿入します。

送信元ポートまたは宛先ポートが 0 の TCP または UDP トラフィックの通過

デフォルトでは、TCP（または UDP）の送信元ポート 0 または宛先ポート 0 を使用するトラフィックの通過は無効に設定されています。CSS は通常、DoS 攻撃時に、送信元ポート 0 または宛先ポート 0 を使用してトラフィックをロギングします。ポート 0 のトラフィックを有効にした場合、CSS は DoS 攻撃時にフローをロギングしません。

CSS でポート 0 を使用したトラフィックの通過を有効または無効にするには、**flow set-port-zero** コマンドを使用します。このコマンドのシンタックスは次のとおりです。

flow set-port-zero enable | disable

TCP/UDP の送信元ポート 0 または宛先ポート 0 を使用したトラフィックの通過を有効にするには、**enable** キーワードを使用します。たとえば、次のように入力します。

```
(config)# flow set-port-zero enable
```

CSS をデフォルトの動作に戻して TCP/UDP の送信元ポート 0 または宛先ポート 0 を使用したトラフィックの通過を無効にするには、**disable** キーワードを使用します。たとえば、次のように入力します。

```
(config)# flow set-port-zero disable
```

TCP のレイヤー 5 スパニング パケットに対する遅延確認応答の有効化

デフォルトでは、CSS では、TCP のレイヤー 5 スパニング パケットの遅延確認応答（ACK）は無効です。TCP のレイヤー 5 スパニング パケットに対する遅延確認応答を有効にするには、**flow tcp-del-ack** コマンドを使用します。たとえば、次のように入力します。

```
(config)# flow tcp-del-ack
```

デフォルトの動作に戻すには、**no flow tcp-del-ack** コマンドを使用します。たとえば、次のように入力します。

```
(config)# no flow tcp-del-ack
```

フロー統計情報の表示

CSS インターフェイス上のアクティブなフローや FCB の統計情報を表示するには、**flow statistics** コマンドを使用します。

（注） 冗長休止フローの要約情報を表示するには、**flow statistics dormant** コマンドを使用します。詳細については、『*Cisco Content Services Switch Redundancy Configuration Guide*』を参照してください。

表 2-1 に、**flow statistics** コマンドで表示されるフィールドについて説明します。

表 2-1　flow statistics コマンドのフィールド

フィールド	説明
Flow Manager Statistics - Slot *n*, Subslot *n*	CSS シャーシ内の指定されたスロットおよびサブスロット内のモジュールに関するフロー マネージャの統計情報。FCB の作成とフロー マッピングは、フロー マネージャによって実行されます。
UDP Flows per Second	CSS が 1 秒間に受信した UDP フローの数（現在値、最大値、平均値）

表 2-1　flow statistics コマンドのフィールド（続き）

フィールド	説明
TCP Flows per Second	CSS が 1 秒間に受信した TCP フローの数（現在値、最大値、平均値）
Total Flows Per Second	CSS が 1 秒間に受信した TCP フローと UDP フローの合計数（現在値、最大値、平均値）
Hits Per Second	設定済みの各コンテンツ ルールの合計ヒット カウント（現在値、最大値、平均値）。レイヤ 3 とレイヤ 4 のルールの場合、この値はセッションのヒットごとに 1 だけ増加します。一方、レイヤ 5 ルールでは HTTP メソッドのヒットごとに 1 だけ増加します。
Number of Allocated Flows (non-purged)	このモジュールのフローマネージャに割り当てられている FCB の数。フロー マネージャは CSS の起動時に、割り当て可能なフロー数を指定します。このフローが不足すると、フロー マネージャは FCB を 200 ブロックずつ、最大値まで割り当てることができます。起動時に指定するフロー数と、割り当て可能な最大値は、モジュールで利用可能なメモリの容量に基づいて決定されます。割り当てられるフローの数は、当該モジュールの各ポートのアクティブ フローの合計数に等しくなります。
Number of Free Flows	フロー マネージャが CSS の初期化時、およびシステムの実行中にメモリから割り当てる FCB の合計数。この値は、**show system-resources** コマンドで表示されるメモリから取得されます。
Number of Allocated Fast-Path FCBs	CSS 内の fastpath ソフトウェアで使用されている FCB の合計数。FCB は TCP フローでは 2 つ、UDP フローでは通常 1 つ使用されます。
Number of Free Fast-Path FCBs	CSS 内の fastpath ソフトウェアで使用できる FCB の合計数
Aggregate Flow Statistics Per Port	TCP フローと UDP フローのアクティブ ポート別サマリー

表 2-1　flow statistics コマンドのフィールド（続き）

フィールド	説明
Port	CSS 11503 または CSS 11506 のスロットとサブスロットの入力ポート（例：2/1）
Active	TCP および UDP のアクティブ フローの合計数
Total	フロー数の累計
TCP	現在アクティブな TCP フローの数
UDP	現在アクティブな UDP フローの数

コンテンツ ルールとソース グループでのフロー無活動タイムアウトの設定

この機能は 1 台の CSS を対象として使用され、TCP フローと UDP フローの無活動タイムアウトを、コンテンツ ルールとソース グループごとに設定します。タイムアウトの値は、CSS がフロー リソースを再要求する*頻度ではなく*、CSS がアイドル状態のフローに消去のマークをつけるまでに待機しなければならない時間の長さを意味します。

タイムアウト値の優先順位

CSS では、フロー リソースの再要求時に、次の指針が上から順に適用されます。

1. フローがコンテンツ ルールに一致すると、CSS でユーザ設定のタイムアウト値が検査され、検出されたタイムアウト値が使用されます。
2. フローがソース グループに一致すると、CSS でユーザ設定のタイムアウト値が検査され、検出されたタイムアウト値が使用されます。
3. **flow permanent port** コマンドを使用して固定ポートを設定した場合（「TCP または UDP ポートの固定接続の設定」を参照）は、CSS でフロー タイムアウト値が 0 に設定され、フローがタイムアウトしません。
4. 前述の条件に当てはまらない場合は、プロトコルの種類に応じてデフォルトのタイムアウト値が使用されます。詳細については、「フロー タイムアウト統計情報の表示」を参照してください。

フロー タイムアウトの設定

CSS でアイドル状態のフローを切断するまでの待機時間（秒数）を指定するには、**flow-timeout-multiplier** コマンドを使用します。このコマンドは、所有者コンテンツ設定モードまたはグループ設定モードで指定します。このコマンドのシンタックスは次のとおりです。

flow-timeout-multiplier *number*

（注） ソース グループを、クライアントのソース NAT 用の宛先サービスで設定する場合は、**flow-timeout multiplier** コマンドはコンテンツ ルールだけに使用します。CSS は、どちらの方向のフローにも同じタイムアウトを設定します。コンテンツ ルールとソース グループに、互いに異なるタイムアウトを設定した場合、どちらの方向のフローにもコンテンツ ルールに設定したタイムアウトが使用されます。

0 ～ 65534 の整数値を *number* に入力します。CSS は、フローのタイムアウト（秒）を計算するために、その値に 16 を掛けます。デフォルト値は、TCP または UDP のポート番号によって異なります（「フロー タイムアウト統計情報の表示」を参照）。デフォルト値は、コンテンツ ルールまたはソース グループに基づいて作成されたフローだけに適用されます。

値 0（タイムアウトなし）を指定すると、フローが破棄されないので、リソースは常に使用されている状態となります。値 0 の指定は、**flow permanent port** コマンドの入力と同じ効果を持ちます（「TCP または UDP ポートの固定接続の設定」を参照）。

（注） レイヤ 3 とレイヤ 4 のコンテンツ ルールで、UDP フローへの **flow-timeout multiplier** コマンドで 0 を指定することは推奨できません。値を 0 に設定すると、UDP フローのリソースのクリーンアップが実行されません。

（注） FTP 制御チャネルは、無活動状態のまま 10 分間経過すると CSS によって切断されます。ファイルの転送中にアイドル状態になり、そのまま 10 分が経過した場合も、チャネルは切断されます。関連するコンテンツ ルールを対象に **flow-timeout-multiplier** コマンドを実行すれば、予想される FTP ファイル転送時間に合わせて、タイムアウトの長さを設定できます。

次の 2 つの例では、フロー タイムアウト期間を 80 秒に設定します。

```
(config-owner-content[cisco-rule1])# flow-timeout-multiplier 5
(config-group[group1])# flow-timeout-multiplier 5
```

設定済みの **flow-timeout-multiplier** 値を無効にし、ポートの種類に応じてデフォルトのタイムアウト値を復元するには、次のように入力します。

```
(config-owner-content[cisco-rule1])# no flow-timeout
(config-group[group1])# no flow-timeout
```

フロー タイムアウト統計情報の表示

TCP および UDP ポートとアプリケーションのデフォルトのタイムアウト値を表示するには、**show flow-timeout default** コマンドを使用します。デフォルト値を変更することはできません。表 2-2 に、**show flow-timeout default** コマンドの出力に含まれる各フィールドと、その説明を示します。

表 2-2　show flow-timeout default コマンドのフィールド

フィールド	説明
TCP/IP Port	デフォルトの TCP または UDP ポート番号
Application	デフォルトの TCP または UDP アプリケーションの名前
Inactivity Timeout Seconds	TCP または UDP ポートに対するデフォルトのフローの無活動タイムアウト値（秒単位）。フローがアイドル状態になったままで、指定したタイムアウト値の時間が経過すると、フローが破棄され、フローのリソースが回収されます。

設定済みのフロー タイムアウト値を表示する場合は、**show flow-timeout configured** コマンドを使用します。コマンド出力には、フローのタイムアウト値を設定したコンテンツ ルールまたはソース グループも表示されます。

表 2-3 に、**show flow-timeout configured** コマンドの出力に含まれる各フィールドと、その説明を示します。

表 2-3　show flow-timeout configured コマンドのフィールド

フィールド	説明
Port	TCP または UDP ポート番号
Content Rule	フローのタイムアウト値を設定したコンテンツ ルールの名前
Source Group	フローのタイムアウト値を設定したソース グループの名前
Timeout	TCP または UDP ポートの設定済み無活動タイムアウト値（16 秒単位）。フローがアイドル状態のままこの時間が経過すると、接続が破棄され、FCB が回収されます。

コンテンツ ルールとソース グループの情報の表示

コンテンツ ルールまたはソース グループでフローのタイムアウト値を設定すると、**show rule** コマンドまたは **show group** コマンドの実行結果として表示される画面には **Flow Timeout Multiplier** というフィールドが表示されます。このフィールドには、そのルールやグループに一致するフローに割り当てられた設定済みタイムアウト値が表示されます。

断片化 IP パケットのフロー処理の設定

デフォルトでは、CSS は フロー パス上で断片化している TCP や UDP の IP パケット（IP フラグメント）を処理しません。標準の IP ルーティング方式に基づいてルーティングするだけです。その結果、IP フラグメントはコンテンツ ルールやソース グループなどの設定項目と照合されないため、CSS は NAT もロードバランシングも行うことはありません。

IP フラグメントのフロー処理を有効にすると、CSS は IP ヘッダーと TCP（または UDP）ヘッダー内にある IP アドレスと TCP （または UDP）のポート情報を使用して、フロー パス上の IP フラグメントを処理します。次に、設定済みのコンテンツ ルールと、フラグメントによって照合されたソース グループに基づいて、パケットの各フラグメントに対して転送と NAT を実行します。

この機能を使用できるのは、レイヤ 3 とレイヤ 4 のコンテンツ ルールだけです。レイヤ 5 コンテンツ ルールには、**flow tcp-mss** コマンドを使用してください。**flow-tcp-mss** コマンドの詳細については、「フロー パラメータの設定」を参照してください。

この機能によって、次の各項目がサポートされます。

- Microsoft Media Server UDP（MMSU）プロトコルを使用する Microsoft Media Server など、UDP IP パケットを断片化するアプリケーション
- TCP IP パケットを断片化するアプリケーション（E メールなど）
- MTU 経路検出に対応していないアプリケーションやデバイス
- ネットワーク経由のために TCP や UDP の IP パケット断片化が必要になるネットワーク構成

（注） 可能な限り、IP フラグメントを作成するアプリケーションやネットワーク設定は避けてください。この機能によって、IP 断片化が不可避な状況がサポートされます。

ここでは、断片化された IP パケットのフロー処理を設定する方法について説明します。内容は次のとおりです。

- 断片化 IP パケットのフロー処理の有効化
- 最大組み立てサイズの設定
- 最小フラグメント サイズの設定
- IP フラグメント統計情報のリセット
- IP フラグメント統計情報の表示

IP パケット断片化の概要

IP フラグメントとは、完全な IP パケットの一部分のことです。ネクストホップ ネットワークの Maximum Transmission Unit（MTU; 最大伝送ユニット）が着信パケット サイズより小さい場合は、IP パケットを断片化する必要があります。伝送装置は、ネットワーク メディアが収容できる小片にパケットを分割し、各フラグメントにパケットの IP ヘッダーをコピーします。パケットは発信元ホスト、経路上のルータ、およびその他のネットワーク装置で断片化されることがあります。

IP パケットの断片化は通常、望ましくない状況と考えられます。パケットの断片化とその後の再組み立てによって、CPU とネットワークに余計なオーバーヘッドが生じるためです。ただし、ネットワーク設計者がいかに努力しても、断片化が不可避なこともあります。ネットワーク メディアの種類によって、IP プロトコルをサポートする MTU が異なるためです。

IP パケットの断片化と再組み立ての詳細については、RFC 791 と RFC 815 を参照してください。

設定の制約

CSS が断片化パケットを受信し、TCP IP フラグメントのフロー処理が有効な環境では、次に挙げる TCP アプリケーションは使用できません。

- レイヤ 5 コンテンツ ルール（クライアント要求が断片化している場合）。レイヤ 3 または 4 のルールが設定されていても、これらのルールに戻ることはありません。
- フロントエンド SSL 終了用の SSL モジュールを備えた HTTPS クライアント（SSL）

- SSL モジュールなしの HTTPS クライアント（**advanced-balance-ssl** コマンドで設定済み）
- FTP 制御チャネル
- ArrowPoint クッキー

（注）　CSS は負荷分散の決定で、断片化した IP パケットの UDP/TCP ペイロードを考慮することはできません。

断片化 IP パケットのフロー処理の有効化

CSS で IP フラグメントのフロー処理を可能にするには、グローバル設定モードで **udp-ip-fragment-enabled**（または **tcp-ip-fragment-enabled**）コマンドを使用します。デフォルトでは、この機能は無効に設定されています。

（注）　**ip-fragment-enabled** コマンドは使用できなくなりました。**ip-fragment-enabled** コマンドは、自動的に **udp-ip-fragment-enabled** コマンドに変換されます。

CSS のデフォルトの動作をリセットして IP フラグメントを転送するには、このコマンドに **no** を付けて実行します。

たとえば、次のように入力します。

```
(config)# no udp-ip-fragment-enabled
(config)# no tcp-ip-fragment-enabled
```

（注）　この機能は、IP ヘッダーおよび TCP/UDP ヘッダーにあるレイヤ 3 （IP アドレス）とレイヤ 4 （TCP/UDP ポート）情報を使用して、コンテンツ ルールに基づく転送を実行します。パケットのペイロード（データ部）に基づくレイヤ 5 の IP フラグメント転送はサポートされていません。

最大組み立てサイズの設定

最大組み立てサイズとは、すべての IP フラグメントが元のパケットに組み立てられた場合の IP パケットの合計サイズのことです。組み立てられた IP パケットは、64KB 以内にする必要があります。CSS は IP フラグメントを受け取ると、最大組み立てサイズに対してフラグメントをチェックします。フラグメント IP オフセットに IP ペイロード（データ）を加えたサイズが設定済みの最大組み立てサイズより大きい場合、CSS は **show ip-fragment-stats** コマンド出力の **Max Assembled Size error** フィールドの値をインクリメントし、パケットを破棄します。「IP フラグメント統計情報の表示」を参照してください。

（注） 不必要な処理によるオーバーヘッドを回避するため、CSS では断片化した IP パケットの再組み立ては行いません。

最大組み立てサイズを指定するには、**ip-fragment max-assembled-size** コマンドを使用します。このグローバル設定モードのコマンドのシンタックスは次のとおりです。

ip-fragment max-assembled-size *number*

変数 *number* には、組み立てられるパケットの最大サイズ（バイト）を指定します。2048 ～ 65535 の整数を入力します。デフォルトは 5120 バイトです。

たとえば、次のように入力します。

```
(config)# ip-fragment max-assembled-size 4096
```

最大 IP フラグメント組み立てサイズをデフォルトの 5120 バイトに戻すには、このコマンドに **no** を付けて実行します。

たとえば、次のように入力します。

```
(config)# no ip-fragment max-assembled-size
```

最小フラグメント サイズの設定

最小フラグメント サイズは、CSS が受け付ける IP フラグメントの最小 IP ペイロードです。CSS は IP フラグメントを受け取ると、最小フラグメント サイズに対してフラグメントをチェックします。フラグメントの IP ペイロードのサイズが設定済みの最小フラグメント サイズより小さい場合は、CSS は **show ip-fragment-stats** コマンド出力の **Less Than Min Size error** フィールドの値をインクリメントし、パケットを破棄します。「IP フラグメント統計情報の表示」を参照してください。

TCP や UDP の IP フラグメントの最小 IP フラグメント ペイロードを用途に応じて指定するには、**ip-fragment min-fragment-size** コマンドを使用します。このコマンドは、フラグメント攻撃からの保護も行います。フラグメント攻撃は、有効に見える非常に小さい一連のフラグメント チェーンです。

このグローバル設定モードのコマンドのシンタックスは次のとおりです。

ip-fragment min-fragment-size *number*

変数 *number* には、CSS がサポートする IP フラグメント ペイロードの最小サイズ（バイト）を指定します。64 ～ 1024 の整数を入力します。デフォルトは 1024 バイトです。

たとえば、次のように入力します。

```
(config)# ip-fragment min-fragment-size 256
```

（注） 最小フラグメント サイズを最小 64 バイトとすることで、IP と TCP または UDP のヘッダー情報が最初のフラグメントに存在することが保証されます。

デフォルトの最小 IP フラグメント ペイロード サイズを 1024 バイトに戻すには、このコマンドに **no** を付けて実行します。

たとえば、次のように入力します。

```
(config)# no ip-fragment min-fragment-size
```

IP フラグメント統計情報の表示

TCP と UDP の IP フラグメント処理に関連する状態、統計情報、およびエラー数を表示するには、任意のモードで **show ip-fragment-stats** コマンドを使用します。

表 2-4 に、**show ip-fragment-stats** コマンドの出力に含まれる各フィールドと、その説明を示します。

表 2-4　show ip-fragment-stats コマンドのフィールド

フィールド	説明
IP Fragment Status	
UDP State	UDP IP フラグメント機能の設定状態（Enabled または Disabled）
TCP State	TCP IP フラグメント機能の設定状態（Enabled または Disabled）
Min Fragment Size	設定されているフラグメント IP ペイロードの最小サイズ
Max Assembled Size	設定されている組み立て IP パケットの最大サイズ
IP Fragment Statistics	
Packets Tracked	CSS で追跡された断片 IP パケットの現在の数、最大数、および合計数。このフィールドに格納されているのは追跡された実際のパケット数で、フラグメントの数ではありません。
Fragments Buffered	CSS で追跡されたすべての IP パケットのうち、バッファに格納された IP フラグメントの現在数、最大数、および合計数
Packets Completed	正常に処理された断片化 IP パケット数
Longest Frag Chain	断片化 IP パケットを構成する最長の IP フラグメント チェーン。IP フラグメント チェーンとは、元のパケットを構成する一連のフラグメントのことです。
Largest Asm Packet	CSS が受信した IP 断片化パケットの最大 IP 長

表 2-4　show ip-fragment-stats コマンドのフィールド（続き）

フィールド	説明
Smallest Fragment	CSS が受信した最小 IP ペイロード長。このフィールドには、どの IP フラグメントについても最後のフラグメントは含まれません。ペイロードのサイズは決まっていないからです。
IP Fragment Errors	
No Tracking Entry	新しいパケットのフラグメントの受信時に、CSS はフラグメント追跡エントリを取得できなかった。このエラーは、CSS メモリが少ないか残りがない場合に発生することがあります。
Could Not Buffer	CSS はフラグメントを受信したが、CSS のバッファが少なかったためバッファリングできなかった。
Duplicate Fragment	CSS は重なったオフセットまたは最後のフラグメントを検出した。
Validating Fragments	CSS は、IP フラグメントをすべて受信した後、フラグメントの検証中に、重なったオフセット、短かすぎるオフセットなどの、Denial of Service （DoS; サービスの拒絶）フラグメント攻撃状態を検出した。
Inserting Fragment	CSS は、追跡エントリ上のフラグメント チェーンにフラグメントを挿入しているときに、重なったフラグメント、設定された最小フラグメント サイズより小さいフラグメント、設定された最大組み立てサイズより大きな合計組み立てサイズを検出した。
Less Than Min Size	CSS は、IP ペイロードが設定された最小フラグメント サイズより小さい、（最後のフラグメントではない）IP フラグメントを受信した。
Max Assembled Size	フラグメントを受信後、組み立てられた IP パケットの合計サイズを計算したところ、設定された最大組み立てサイズを超えていた。
Collection Timeout	CSS が IP フラグメントの受信待ちをしている時間が長すぎた。

表 2-4　show ip-fragment-stats コマンドのフィールド（続き）

フィールド	説明
Flow Timeout	CSS が IP パケットの全フラグメントを受信し、1 つのフラグメントがフロー処理のため送信された後、フラグメントが返ってくる前にエントリがタイムアウトになった。
IPv4 Header	CSS が、合計の IP フラグメント サイズと比較して、無効な IPv4 ヘッダー長を持つフラグメントを受信した。
RxQueue Full	IP フラグメントの CSS フロー処理受信キューが一杯になった。この IP フラグメントは、CSS によって廃棄されています。

IP フラグメント統計情報のリセット

TCP と UDP の IP フラグメントの統計情報をリセットするには、任意のモードで **zero ip-fragment-stats** コマンドを使用します。このコマンドは、**show ip-fragment-stats** コマンド出力の IP Fragment Statistics および IP Fragment Errors セクションにある統計情報の値を 0 に戻します。

show ip-fragment-stats コマンドの詳細については、「IP フラグメント統計情報の表示」を参照してください。

VIP を利用できないときに CSS に TCP Reset を送信させる設定

レイヤ 3 またはレイヤ 4 のコンテンツ ルールに設定されている VIP が利用できない場合、その VIP を提供している CSS は、デフォルトで次のように動作します。

- クライアントから当該 VIP 宛てに送信された TCP パケットを拒否する。
- その TCP パケットをドロップする。

この動作は、パケットが次の条件を満たす場合に実行されます。

- アクティブなサービスを持たないレイヤ 3 またはレイヤ 4 のコンテンツ ルールに一致する。
- サービスが最大接続数に達したレイヤ 3 またはレイヤ 4 のコンテンツ ルールに一致する。

TCP パケットが CSS で拒否されると、クライアントはそのパケットを再送信することがあります。ただし、レイヤ 3 またはレイヤ 4 の合致するコンテンツ ルールのサービスが利用可能にならなければ、クライアント アプリケーションは応答しなくなり、接続やアプリケーションは最終的にタイムアウトになります。その結果、アプリケーションはタイムアウトになるまでの時間を浪費することになり、用途によっては重大な問題になります。

ここで説明する機能を使用すれば、VIP が利用できないときに TCP パケットへの応答として、TCP RST を送信するように CSS を設定できます。TCP RST を受信したアプリケーションは、パケットの再送信を停止します。さらに、通常は接続失敗を示すエラー メッセージを表示します。

（注） レイヤ 5 のスプーフィング接続では、CSS はコンテンツ要求を拒否すると、常に TCP RST をクライアントに送信します。この動作には変更はありません。

この機能は、次のようなアプリケーションで役立ちます。

- Web ブラウザ
- Telnet

- FTP

VIP が利用できないときにクライアントに TCP RST を送信するように CSS を設定するには、グローバル設定モードで **flow tcp-reset-vip-unavailable** コマンドを使用します。CSS は、自分が提供している VIP を利用できない場合にのみ、その VIP 宛てに送信された TCP パケットへの応答として TCP RST を送信します。

次に設定例を示します。

```
(config)# flow tcp-reset-vip-unavailable
```

CSS の動作をデフォルト（VIP が利用できないときに TCP パケットをドロップする）に戻すには、次のコマンドを実行します。

```
(config)# no flow tcp-reset-vip-unavailable
```

VIP が利用できなかったために CSS が送信した TCP RST の数は、**show ip statistics** コマンドで表示できます。**show ip statistics** コマンドの詳細については、『*Cisco Content Services Switch Routing and Bridging Configuration Guide*』を参照してください。

フロー状態テーブルの設定

CSS では、ほとんどすべての TCP トラフィックと UDP トラフィックのフローを設定します。ただし、CSS は、特定のポートを使用するパケットにはフローを設定しません。デフォルトでは、表 2-5 に示している各ポートのフローは設定されません。

表 2-5　デフォルトで CSS がフローを無効にするポート

ポート	アプリケーション
67	Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）サーバ
68	BOOTP クライアント
137	NETBIOS ネーム サービス
138	NETBIOS データグラム サービス
161	Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）
162	SNMP トラップ
520	Routing Information Protocol （RIP; ルーティング情報プロトコル）
8089	Inktomi-UDP

TCP ポートと UDP ポートのフロー状態を追跡するために、CSS ではフロー状態テーブルを管理します。表 2-6 は、CSS によってフロー状態テーブル内に事前設定される、10 個のデフォルトの TCP ポートと UDP ポートを示しています。これらの 10 個のポートのうち、DNS （ポート 53、TCP と UDP）および SIP （ポート 5060、UDP だけ) だけがデフォルトでフローが有効になります。表 2-6 に示す他のポートのフローを設定するには、**flow-state** コマンドでフローを設定する必要があります。ここに示す 10 個のデフォルト ポート以外のすべてのポートでは、デフォルトでフローが有効になります。

表 2-6　フロー状態テーブルのデフォルト値

ポート	プロトコル	NAT の状態	フローの状態	ヒット カウント
53	TCP	----------	フローは有効	0
53	UDP	----------	フローは有効	0

表 2-6　フロー状態テーブルのデフォルト値（続き）

ポート	プロトコル	NAT の状態	フローの状態	ヒット カウント
67	TCP	----------	フローは無効	0
67	UDP	NAT は無効	フローは無効	0
68	TCP	----------	フローは無効	0
68	UDP	NAT は無効	フローは無効	0
137	TCP	----------	フローは無効	0
137	UDP	NAT は無効	フローは無効	0
138	TCP	----------	フローは無効	0
138	UDP	NAT は無効	フローは無効	0
161	TCP	----------	フローは無効	0
161	UDP	NAT は無効	フローは無効	0
162	TCP	----------	フローは無効	0
162	UDP	NAT は無効	フローは無効	0
520	UDP	NAT は無効	フローは無効	0
5060	UDP	----------	フローは有効	0
8089	UDP	NAT は無効	フローは無効	0

事前設定されているポートのフロー状態は変更することができます。また、一意の TCP ポートまたは UDP ポートを 16 個まで追加でき、それぞれのフロー状態を設定することもできます。フローが無効になっている UDP ポートの場合だけ、Network Address Translation (NAT; ネットワーク アドレス変換）状態を設定できます。

CSS が、自身の IP アドレスまたは VIP アドレス宛のトラフィックを受信し、受信したトラフィックにより指定されたポートがフローも NAT も無効化されている場合、CSS はクライアントに ICMP ポート到達不能メッセージを送信します。

CSS が、フローが無効化されているポートで TCP パケットを受信すると、CSS はこれらのパケットを NAT 変換しません。この場合、CSS は単にパケットを転送します。自身の VIP 宛のパケットを受信すると、CSS はそのパケットを廃棄します。

（注）　CSS は、Real-Time Streaming Protocol （RTSP）に必要なペイロード データなどは NAT 変換しません。

次の場合には、フロー状態テーブルを使用してください。

- 任意のクライアント　ポートを使用しないアプリケーションの場合。たとえば、連続する要求で送信元ポート 1024 と宛先ポート 53 を繰り返して使用する当事者間の DNS トラフィックのフローを CSS が設定する場合、すべてのトラフィックのフローは同一の接続で行われ、負荷は分散されません。
- 一時的な UDP パケットのフローの設定によるオーバーヘッドを回避する場合。
- 既知の NAT 変換されていないパケットのフローの設定によるオーバーヘッドを回避する場合。

NAT の詳細については、第 5 章「サービスのソース グループの設定」を参照してください。DNS の詳細については、『*Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*』を参照してください。

サーバがソース グループの背後にある場合（CSS がサーバから送信されたトラフィックのサーバ IP アドレスを NAT 変換する場合）に限り、フローが有効になっているポートでだけ Trivial File Transfer Protocol （TFTP; トリビアル ファイル転送プロトコル）および TFTP に似たプロトコル（サーバが応答でポートをランダムに選択）をサポートします。クライアントがソース グループの背後にある場合（CSS がクライアントから送信されたトラフィックのクライアント IP アドレスを NAT 変換する場合）、またはフローが無効になっているポートでは、これらのプロトコルはサポートされません。

以降では、フロー状態の設定とフロー状態テーブルの表示について説明します。

- ポートのフロー状態の設定
- フローが無効な接続でのサーバ応答タイムアウトの設定
- フロー状態テーブルのヒット カウンタのリセット
- フロー状態テーブルの表示

ポートのフロー状態の設定

TCP ポートまたは UDP ポートのフロー状態を設定するには、**flow-state** コマンドを使用します。ポートのフロー状態を **flow-enable** に設定すると、CSS はコンテンツ ルールとソース グループの照合を行います。フローが無効になっている UDP ポートでは、フロー状態に関係なく NAT の状態を有効にできます。これにより、CSS は NAT 変換とポート マッピングを行います。フロー状態テーブルで事前設定されているデフォルトのポートに加え、一意の TCP ポートまたは UDP ポートを最大 16 個まで設定できます。

このグローバル設定モードのコマンドのシンタックスは次のとおりです。

flow-state *number* **tcp** [**flow-enable**|**flow-disable**]

flow-state *number* **udp** [**flow-enable**|**flow-disable** {**nat-enable**|**nat-disable**}]

このグローバル設定モード コマンドには、次のオプションと変数があります。

- *number* ：フロー状態を設定する TCP または UDP ポートの番号。1 ～ 65535 の整数を入力します。
- **tcp** ：トラフィックの送信に TCP を使用する。
- **udp** ：トラフィックの送信に UDP を使用する。
- **flow-enable** ：指定した TCP ポートまたは UDP ポートのフローを有効にする。このオプションを指定すると、CSS は、レイヤ 5 （URL 文字列）コンテンツベースのロード バランシングとスティッキを含め、コンテンツ ルールとソース グループの完全な照合を行います。
- **flow-disable** ：指定した TCP ポートまたは UDP ポートのフローを無効にする。ポートのフローを無効にすると、CSS はコンテンツ ルールとソース グループの照合を行いません。フローの設定によるオーバーヘッドが発生しないことがこのオプションの利点です。
- **nat-enable** ：フローが無効にされた UDP ポートの場合だけ、NAT 変換のためのコンテンツ ルールとソース グループの検索が有効になる。このオプションを指定すると、レイヤ 3 （IP アドレス）とレイヤ 4 （IP アドレスと宛先ポート）コンテンツ ルールおよびスティッキ テーブル（たとえば、**sticky-srcip**）を使用できます。ただし、フローが無効になっていると、レイヤ 5 コンテンツベースの決定に必要なバックエンド接続はスプーフできません。
- **nat-disable** ：フローが無効にされた UDP ポートの場合だけ、NAT 変換のためのコンテンツ ルールとソース グループの検索を行わない。

注意　特定のポートで **flow-disable** オプションと **nat-disable** オプションを同時に設定すると、ポートでのコンテンツ ルールとソース グループの検索はできなくなります。この場合、ポートに関連付けられた VIP アドレス宛の TCP パケットは廃棄されます。UDP の場合、CSS はクライアントに ICMP ポート到達不能メッセージを送信します。パケットは他の IP アドレスに転送されます。

例 1

SNMP TCP ポート 161 のフローを有効にするには、次のように入力します。

```
(config)# flow-state 161 tcp flow-enable
```

SNMP TCP ポート 161 の設定をデフォルト値の **flow-disable** に戻すには、次のように入力します。

```
(config)# no flow-state 161 tcp
```

例 2

SIP UDP ポート 5060 のフローを無効にするには、次のように入力します。

```
(config)# flow-state 5060 udp flow-disable
```

SIP UDP ポート 5060 の設定をデフォルト値の **flow-enable** に戻すには、次のように入力します。

```
(config)# no flow-state 5060 udp
```

例 3

SNMP UDP ポート 162 （SNMP トラップ）のフローを無効にし、NAT を有効にするには、次のように入力します。

```
(config)# flow-state 162 udp flow-disable nat-enable
```

SNMP UDP ポート 162 の設定をデフォルト値の **flow-disable** と **nat-disable** に戻すには、次のように入力します。

```
(config)# no flow-state 162 udp
```

フローが無効な接続でのサーバ応答タイムアウトの設定

デフォルトでは、フローが無効にされた（フローなし）接続は、サーバからの応答を受信しない場合、5 秒でタイムアウトになります。DNS 応答の場合は、応答が 5 秒を超えることがあり、接続が失敗する原因になります。グローバル設定モードで **flow-state flow-disable timeout** コマンドを使用すると、フローが無効にされたポートへのサーバ応答を待機する時間を長く設定することができます。このコマンドのシンタックスは次のとおりです。

flow-state flow-disable timeout *seconds*

変数 *seconds* に時間を秒単位で指定します。5 ～ 20 の整数を入力します。デフォルトは 5 です。

たとえば、応答を待機する時間を 10 秒に設定するには、次のように入力します。

```
(config)# flow-state flow-disable 10
```

待機時間をデフォルトの 5 秒にリセットするには、次のように入力します。

```
(config)# no flow-state flow-disable
```

フロー状態テーブルのヒット カウンタのリセット

フロー状態テーブルには、各ポートの合計ヒット数をそれぞれ表すヒット カウンタがあります。テーブル内のヒット カウンタをすべてゼロにリセットするには、**zero flow-state-counters** コマンドを使用します。たとえば、次のように入力します。

```
(config)# zero flow-state-counters
```

フロー状態テーブルの表示

フロー状態テーブルのエントリを表示するには、**show flow-state-table** コマンドを使用します。フロー状態テーブルのデフォルト設定については、表 2-6 を参照してください。

表 2-7 に、**show flow-state-table** コマンドの出力に含まれる各フィールドと、その説明を示します。

表 2-7　show flow-state-table コマンドのフィールド

フィールド	説明
Flow-Disable Timeout	フローが無効にされているポートへのサーバからの応答を待機する秒数
Port	フロー状態データを表示するポートの番号
Protocol	ポート番号に関連付けられた IP プロトコル（TCP または UDP）
NAT-State	ポートの NAT の状態。状態は、nat-enable、nat-disable、または ---------（状態が変更できないか、Flow-State フィールドの値との組み合わせでフィールドが該当しない）のいずれかです。フローが無効になっている UDP ポートでだけ、nat-enable と nat-disable の状態になります。
Flow-State	特定ポートのフローの状態。状態は、flow-enable または flow-disable のどちらかです。
Hit-Count	特定ポートのヒット数
*	フロー状態テーブル内の該当する行の値がデフォルト値であることを示します。

CSS ポート マッピングの設定

ここでは、クライアントから送信されたパケットに指定されている TCP および UDP 送信元ポート番号の port address translation （PAT; ポート アドレス変換）を実行するとき、CSS が使用するポート番号の範囲をグローバルに制御する方法を説明します。CSS は、パケットに指定された送信元ポート番号に対して設定可能な範囲で一意のポート番号を割り当て、このパケットを正しいサーバ ポートに送信します。サーバからリターン フローが送信されると、これらのパケットは CSS を通過します。CSS は、変換されたポート番号と要求を開始したクライアントを照合し、サーバ パケットを正しいクライアントに送信します。

ソース グループとポート マッピングの詳細については、第 5 章「サービスのソース グループの設定」の「ソース グループとポート マッピングの概要」を参照してください。

グローバル ポート マッピングの概要

CSS の各モジュール（SSL モジュールを除く）は、いずれもフロー管理用の session processor （SP; セッション プロセッサ）を 1 基内蔵しています。

- CSS 11501 は 1 基の SP をサポートしています。
- CSS11503 は最大 3 基の SP をサポートしています。
- CSS 11506 は最大 6 基の SP をサポートしています。

CSS のグローバル ポート マッパーは、メガ ポート マッパーと呼ばれます。各 SP にはポートマップ番号のバンク（メガマップ バンク）16 個から構成されるメガ ポート マッパーのデータベースがあり、各バンクには 63488 個のポート マップ番号があります。CSS は送信元アドレスのハッシュ アルゴリズムを使用して、特定の SP 内のメガマップ バンクを 1 つ選択します。

クライアント側のフローについては、CSS はフロー処理のために複数の SP にパケットを送信し、その SP の送信元ポートにフローが着信します。CSS は TCP または UDP の送信元ポート番号と宛先ポート番号に単純な XOR ハッシュを実行して、このフローを管理するマスター SP を特定します。送信元ポート番号と宛先ポート番号が同じ場合（DNS UDP ポート 53 など）、CSS はソースと宛先の IP アドレスの下位ビットを使用してハッシュ値を計算し、このハッシュ値を使用して SP の加重テーブル内にインデックスを付け、適切な SP を選択します。

CSS が PAT を実行するとき、処理対象フローのマスター SP は、グローバル ポートマッパーまたはソース グループ（設定に依存）から得られた送信元ポートを使用します（ソース グループの詳細については、第 5 章「サービスのソース グループの設定」を参照してください）。CSS は、送信元ポートのハッシュ値と宛先ポートによって、クライアント側フローのマスターと同じ SP がサーバ側フローでも選択されるように、送信元ポートを選択します。

指定の宛先ポートからのサーバ側フローでは、クライアント側フローで使用されたのと同じ SP にハッシュされるのは、一部の送信元ポート番号だけです。そのため、バックエンド接続の確立時に、特定の SP で*利用可能*なポートが*適切*でないことがあります。したがって、ハッシュ アルゴリズムで選択されるのは、SP で利用可能なポートの一部です。

各 CSS では、使用されたポートマップ番号と使用可能なポートマップ番号のデータベースが維持されます。CSS で送信元ポートの PAT が必要になると、データベース内で次に位置する未使用ポートが使用されます。

ここでは、次の内容について説明します。

- グローバル ポート マッピングの設定
- グローバル ポート マッピング統計情報の表示
- フローなしポート マッピングの設定
- フローなしポート マッピング統計情報の表示

グローバル ポート マッピングの設定

CSS で TCP フローのグローバル PAT を制御するには、**global-portmap** コマンドを使用します。このコマンドは常に有効です。

このコマンドを使用して、次に示す CSS で送信元ポート マッピングの範囲を指定できます。

- デフォルト以外の宛先ポート番号を使用するサービスを設定する CSS。要求がコンテンツ ルールに一致すると、このコンテンツ ルール内のサービスで設定された TCP 宛先ポート番号が CSS により変更され、選択されたサーバにパケットが送信されます。CSS は、**global portmap** コマンド パラメータを使って、対応するクライアントの送信元ポート番号を変換し、同じサービスを要求している他のクライアントと区別します。

- Cisco 11500 リーズ CSS の冗長ピア（ASR 設定の場合）。詳細については、『*Cisco Content Services Switch Redundancy Configuration Guide*』を参照してください。
- バックエンド サーバの再マッピングを有効にしている CSS（第 10 章「コンテンツ ルールの設定」を参照）。

ソース グループを設定する場合は、**portmap** コマンド パラメータの値が **global-portmap** コマンド パラメータの値より優先されます。**portmap disable** コマンドは TCP フローには影響しません。

このグローバル設定モードのコマンドのシンタックスは次のとおりです。

global-portmap base-port *number1* **range** *number2*

このコマンドのオプションと変数は次のとおりです。

- **base-port** *number1* ：CSS でグローバル ポート マッピングに使用する最初のポート番号。2016 ～ 63456 の整数を入力します。デフォルトは 2016 です。

注意　変数 *number1* の値を変更すると、既存フローでポートの競合が発生する可能性があります。

- **range** *number2* ：CSS が各 SP 内の 16 個のメガマップ バンクに個別に割り当てるポートマップ範囲内のポートの合計数。SP 内の各メガマップ バンクは、設定されているポートの範囲全体を使用できます。CSS では一意の送信元アドレス ハッシュを使用して SP 内のメガバンクが選択されるため、同じポート番号を使用しても複数の SP のタプルの競合を起こすことはありません。

注意　変数 *number2* の値を変更すると、既存フローでポートの競合が発生する可能性があります。

2048 ～ 63488 の整数を入力します。デフォルトは 63488 です。32 の倍数以外の値を入力すると、次の 32 の倍数に切り上げられます。

（注）　使用可能なポートの数を超えるポートマップ範囲を入力すると、エラーが返されます。使用可能なポートの数を知るには、65504 からポート範囲の最初のポート番号の値を減算します。

たとえば、次のように入力します。

```
(config)# global-portmap base-port 3096 range 42308
```

global-portmap コマンド パラメータをデフォルト値に戻すには、次のように入力します。

```
(config)# no global-portmap
```

グローバル ポート マッピング統計情報の表示

CSS　のグローバル　ポートマッピング統計情報を表示するには、**show global-portmap** コマンドを使用します。このコマンドは、RMON、URQL、VLAN 設定モード以外のすべてのモードで使用できます。

このコマンドのシンタックスは次のとおりです。

show global-portmap [**all-banks** [**all-sps**|**slot** *number1*]|*number2* [**all-sps**|**slot** *number1*]]

このコマンドのオプションと変数は次のとおりです。

- **all-banks** ：すべてのポート マップ バンク（0 ～ 15）に関するグローバル ポートマップ情報が表示される。
- **all-sps** ：CSS 内のすべての SP に関するグローバル ポートマップ情報が表示される。
- **slot** *number1* ：モジュールを装着しているシャーシ スロットを指定する。CSS 11503 では、1 ～ 3 の整数を入力します。CSS 11506 では、1 ～ 6 の整数を入力します。

  CSS で使用可能なアクティブなスロットを表示するには、**show global-portmap all-banks slot ?** コマンドを入力します。無効なスロット番号を入力すると、CLI には表 2-8 に示す最初の 2 つのパラメータの値だけが表示されます。

- *number2* ：グローバル ポートマップ バンク番号を指定する。0 ～ 15 の整数を入力します。

CSS でアクティブな各 SP についてのすべてのメガマップ バンク（最大 16）のポート マッピング統計情報を表示するには、次のように入力します。

```
(config)# show global-portmap all-banks all-sps
```

スロット 3 にある SP のメガマップ バンク 12 に関するグローバル ポート マッピング統計情報を表示するには、次のように入力します。

```
(config)# show global-portmap 12 slot 3
```

表 2-8 に、**show global-portmap** コマンドの出力に含まれる各フィールドと、その説明を示します。

表 2-8　show global-portmap コマンドのフィールド

フィールド	説明
MegaMap Banks in Use Per SP	各 SP で使用中のグローバル ポート マッピング バンクの数。各 SP で使用可能なバンクは 16 です。CSS は、パケットに含まれる送信元アドレスのハッシュによりバンクを選択します。
Configured Base Port	**global-portmap** コマンドで指定した **base-port** （ポート範囲の最初のポート番号）またはデフォルトの 2016
Total Configured Ports	**global-portmap range** コマンドで指定したポート総数またはデフォルトの 63488
Slot	特定の SP が常駐する CSS 11503 または CSS 11506 のスロット番号
MegaMap Bank #	ポート マッピング バンクの数。指定可能な値は、各 SP に対して 0 ～ 15 （16 バンク）です。
Number Normal Avail Ports	送信元ポート番号が TCP パケット内の宛先ポート番号と異なる場合にネットワーク アドレス変換アルゴリズムで使用できるポートの数
Current Mapped Ports	現在使用中またはマップされているポートの総数

表 2-8　show global-portmap コマンドのフィールド（続き）

フィールド	説明
Last Normal Mapped Port	送信元ポート番号が TCP パケット内の宛先ポート番号と異なる場合にネットワーク アルゴリズムで最後に使用されたポート番号
Equal Port Base Port	送信元ポート番号と TCP パケット内の宛先ポート番号が同じ場合にネットワーク アドレス変換アルゴリズムで使用される最初のポート番号
Number Equal Avail Ports	送信元ポート番号と TCP パケット内の宛先ポート番号が同じ場合にネットワーク アドレス変換アルゴリズムで使用できるポートの数
High Water Mark	最後の CSS リブート後のある時点でマッピングされた、または使用中のポートの最大数
Last Equal Mapped Port	送信元ポート番号と TCP パケット内の宛先ポート番号が同じ場合にネットワーク アドレス変換アルゴリズムで使用された最後のポート番号
No Portmap Errors	ポートが使用できない（すべてのポートがマップされている）ために障害が発生した回数

フローなしポート マッピングの設定

CSS で 1023 を超える DNS UDP 送信元ポート番号の PAT 範囲を制御するには、**noflow-portmap** コマンドを使用します。このコマンドは常に有効です。ただし、CSS でこのコマンドを使用するには、あらかじめ flow-state コマンドを使用して、CSS で DNS フローを無効にしておく必要があります。「フロー状態テーブルの設定」を参照してください。

（注）　ソース グループで設定した **portmap** コマンドの値は、**noflow-portmap** コマンドの値より優先されます。ただし、**portmap disable** コマンドを設定した場合を除きます。ソース グループで **portmap** コマンドを設定する方法の詳細については、第 3 章「サービスの設定」を参照してください。

このグローバル設定モードのコマンドのシンタックスは次のとおりです。

noflow-portmap base-port *number1* **range** *number2*

このコマンドのオプションと変数は次のとおりです。

- **base-port** *number1* ：CSS で no-flow （DNS フローが無効）ポート マッピングに使用する最初のポート番号。2016 ～ 63456 の整数を入力します。デフォルトは 2016 です。

注意　変数 *number1* の値を変更すると、既存フローでポートの競合が発生する可能性があります。

- **range** *number2* :CSS が各 SP に割り当てるポートマップ範囲内のポートの合計数。各 SP は設定済みのポートの範囲全体を使用できます。

注意　変数 *number2* の値を変更すると、既存フローでポートの競合が発生する可能性があります。

2048 ～ 63488 の整数を入力します。デフォルトは 63488 です。32 の倍数以外の値を入力すると、次の 32 の倍数に切り上げられます。

（注）　使用可能なポートの数を超える値を **range** に入力すると、エラーが返されます。使用可能なポートの数を知るには、65504 からポート範囲の最初のポート番号の値を減算します。

たとえば、ポート 4317 から始めてポートマップ範囲を指定するには、次のように実行します。

```
(config)# noflow-portmap base-port 4317 range 35421
```

最初のポート番号とポートマップ範囲をデフォルト値に戻すには、次のように入力します。

```
(config)# no noflow-portmap
```

フローなしポート マッピング統計情報の表示

CSS の no-flow ポート マッピング統計情報を表示するには、**show noflow-portmap** コマンドを使用します。このコマンドは、RMON、URQL、VLAN 設定モード以外のすべてのモードで使用できます。

このコマンドのシンタックスは次のとおりです。

show noflow-portmap [**all-sps**|**slot** *number*]

このコマンドのオプションと変数は次のとおりです。

- **all-sps** ：CSS 内のすべての SP に関する noflow ポートマップ情報が表示される。
- **slot** *number* ：モジュールを装着しているシャーシ スロット番号。CSS 11503 では、1 ～ 3 の整数を入力します。CSS 11506 では、1 ～ 6 の整数を入力します。

（注） CSS で使用可能なアクティブなスロットを表示するには、**show noflow-portmap slot ?** コマンドを入力します。無効なスロット番号を入力すると、CLI には表 2-9 に示す最初の 2 つのパラメータの値だけが表示されます。

次に指定例を示します。

```
(config)# show noflow-portmap slot 3
```

表 2-9 に、**show noflow-portmap** コマンドの出力に含まれる各フィールドと、その説明を示します。

表 2-9　show noflow-portmap コマンドのフィールド

フィールド	説明
Configured Base Port	**noflow-portmap base-port** コマンドで指定したポート範囲の最初のポート番号またはデフォルトの 2016
Total Configured Ports	**noflow-portmap range** コマンドで指定したポート総数またはデフォルトの 63488
Slot	特定の SP が常駐する CSS 11503 や CSS 11506 のスロット番号
Number Normal Avail Ports	送信元ポート番号が UDP パケット内の宛先ポート番号と異なる場合にネットワーク アドレス変換アルゴリズムで使用できるポートの数
Current Mapped Ports	現在使用中またはマップされているポートの総数
Last Normal Mapped Port	送信元ポート番号が UDP パケット内の宛先ポート番号と異なる場合にネットワーク アドレス変換アルゴリズムで最後に使用されたポートの番号
Equal Port Base Port	送信元ポート番号と UDP パケット内の宛先ポート番号が同じ場合にネットワーク アドレス変換アルゴリズムで使用するポート範囲の最初のポート番号
Number Equal Avail Ports	送信元ポート番号と UDP パケット内の宛先ポート番号が同じ場合にネットワーク アドレス変換アルゴリズムで使用できるポートの数
High Water Mark	最後の CSS リブート後のある時点でマッピングされた、または使用中のポートの最大数
Last Equal Mapped Port	送信元ポート番号と UDP パケット内の宛先ポート番号が同じ場合にネットワーク アドレス変換アルゴリズムで使用された最後のポート番号
No Portmap Errors	ポートが使用できない（すべてのポートがマップされている）ために障害が発生した回数