



# Stream Control Transmission Protocol

---

Stream Control Transmission Protocol (SCTP; ストリーム制御通信プロトコル) は信頼性のあるデータグラム型 IP トラnsポート プロトコルで、RFC 2960 で仕様が規定されています。SCTP では、SCTP ユーザと IP のような信頼性のないエンドツーエンド データグラム サービスとの間にレイヤが用意されています。SCTP が提供する基本的なサービスは、SCTP ピア間での信頼性のあるユーザ データグラム 転送です。このサービスは、2 つのホストが連携する SCTP アソシエーションのコンテキスト内で行われます。SCTP はコネクション型ですが、SCTP アソシエーションは、たとえば Transmission Control Protocol (TCP; 伝送制御プロトコル) よりも範囲が広い概念です。

SCTP では、それぞれの SCTP エンドポイントはピアに対し、(たとえば、アドレス と UDP ポートの組み合わせなど) 転送アドレスのリストを提供できます。このリストはアソシエーションが開始される間に提供され、到達可能なエンドポイントの転送アドレスとメッセージの発信元となる転送アドレスを示します。SCTP アソシエーションには、2 つのエンドポイント リストから合成できるすべての発信元と送信先の組み合わせで示される転送 (マルチホーミングとも呼ばれます) が含まれます。

SCTP は、ルータでは明示的に構成されていませんが、一部の Cisco アプリケーションでは基盤として使用されます。このマニュアルに記載されているコマンドは、障害の原因が SCTP に関連する可能性がある問題のトラブルシューティングに役立ちます。

## 機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「[SCTP の機能情報](#)」(P.24) を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

## この章の構成

- 「[SCTP の前提条件](#)」(P.2)
- 「[SCTP に関する情報](#)」(P.2)



- 「SCTP の設定方法」 (P.4)
- 「SCTP の設定例」 (P.21)
- 「その他の参考資料」 (P.21)
- 「SCTP の機能情報」 (P.24)

## SCTP の前提条件

- Cisco IOS Release 12.2(2)MB、Cisco IOS Release 12.2(4)T、またはそれ以降のリリース。

## SCTP に関する情報

- 「SCTP の利点」 (P.2)
- 「SCTP リリース 2」 (P.2)
- 「SCTP Show および Clear の CLI 機能拡張」 (P.2)
- 「SCTP リリース 4」 (P.3)

## SCTP の利点

SCTP では、以下のサービスと機能が提供されます。

- 確認応答され高信頼性で非重複のユーザ データ転送
- Maximum Transmission Unit (MTU; 最大伝送ユニット) サイズに準拠するアプリケーション レベルのセグメント分割
- 多重ストリーム内でのユーザ データグラムの順列化された配送
- SCTP データグラムへのデータグラム多重化 (任意)
- アソシエーションの片側または両側の端点でのマルチホーミングのサポートを通じて強化された信頼性
- 輻輳回避およびフラッディングとマスカレード アタックに対する防御

## SCTP リリース 2

SCTP リリース 2 では、次の SCTP コマンドの出力が更新されています。

- **show ip sctp association parameters**
- **show ip sctp association statistics**

## SCTP Show および Clear の CLI 機能拡張

SCTP Show および Clear の CLI 機能拡張で、潜在的な問題のトラブルシューティングに役立つ SCTP の追加情報にアクセスできます。また、これらの機能拡張によって、更新された **SCTP show** と **clear** コマンドは他の転送プロトコルの CLI と一致するようになりました。

この機能により、次のコマンドが置き換えられました。

**clear ip sctp statistics、show ip sctp association list、show ip sctp association parameters、show ip sctp association statistics、show ip sctp errors、show ip sctp instances、show ip sctp statistics**

この機能により、次のコマンドが導入されました。

**clear sctp statistics、show sctp association、show sctp association list、show sctp association parameters、show sctp association statistics、show sctp errors、show sctp instance、show sctp instances、show sctp instances、show sctp statistics**

## SCTP リリース 4

SCTP リリース 4 により、SCTP ストリーム リセットと SCTP 認証機能が Cisco IOS リリース 12.4(11)T に、Add-IP 機能が Cisco IOS リリース 12.4(20)T に導入されました。

### SCTP ストリーム リセット

SCTP ストリーム リセット機能では、SCTP がストリーム転送シーケンス番号およびすべてのストリーム シーケンス番号をリセットできます。SCTP を使用するアプリケーションは、ストリームをリセットしてストリーム シーケンスの付番を 0 から再開できます。ストリーム シーケンスの付番が再送信されたという上位レイヤへの通知は、アプリケーションによって送信されます。SCTP ストリームのリセットで、アプリケーションがストリームを違う用途に再利用可能となり、メッセージの流れを追跡するためにストリーム シーケンス番号を保護できます。SCTP ストリームのリセット機能がない場合、ストリームを再利用すると、メッセージ番号が予想よりも大きくなります。SCTP ストリーム リセットを使用すると、次の操作を実行できます。

- ピアの発信ストリームを動的にリセットする
- ローカル ホストの発信ストリームを動的にリセットする
- 指定番号のストリームを動的にリセットする

ストリーム リセットは、上位レイヤのアプリケーションからの要求で発生します。この機能は、Cisco IOS Release 12.4(15)T とそれ以降のリリースでは、デフォルトでイネーブルです。

### SCTP 認証

SCTP 認証を使用すると、次の操作を実行できます。

- 共有秘密鍵なしでダイナミック共有アソシエーション鍵をセットアップする
- 共有秘密鍵をアソシエーション鍵と結合する
- 共有アソシエーション シークレットを使用してチャンクを認証する
- 認証する必要があるチャンク タイプをネゴシエートする

SCTP 認証機能では、アプリケーションはこれらのオプションの機能拡張を使用できます。クライアントに認証を要求するチャンクを定義するには、**ip sctp authenticate** コマンドを使用します。

SCTP 認証処理では、Message Digest 5 (MD5; メッセージ ダイジェスト 5) または Secure Hash Algorithm 1 (SHA-1) のどちらかを利用しますが、メモリと CPU を集中的に使用することがあります。DATA チャンクの SCTP 認証をイネーブルにした場合、認証されたチャンクが大量に送信されたときに CPU の利用に影響を与える可能性があります。

## SCTP Add-IP

SCTP Add-IP 機能では、既存の SCTP アソシエーションのエンドポイントに IP アドレスを追加または削除して、この変更をリモートの端点に伝えることができます。アソシエーションの冗長なサーバアドレスを追加または削除するときに、リモートの端点に ADD-IP チャンクが送信されます。ADD-IP チャンクでは、応答しなくなったホストのすべてのアドレスをアソシエーションから削除することもできます。

Cisco IOS ソフトウェアでは、アプリケーションでプログラムの、あるいはルータで IP アドレスの変更に応じて自動的に SCTP アソシエーションから IP アドレスを追加または削除できます。

SCTP Add-IP 機能で、アプリケーションからプログラムの SCTP アソシエーションへのプライマリアドレスを設定することもできます。

SCTP Add-IP 機能により、2 つの新しい SCTP チャンク タイプ、Address Configuration (ASCONF; アドレス設定) チャンク、および Address Acknowledgement (ASCONF-ACK; アドレス確認応答) チャンクが導入されました。ASCONF チャンクは、SCTP ストリームに確認応答が必要な設定変更の要求が含まれていることをリモートのエンドポイントに伝えるとき、SCTP ストリームの送信者によって使用されます。ASCONF チャンクを受信したエンドポイントは、ASCONF チャンク受信に対する確認応答のため ASCONF-ACK チャンクを使用します。

`ip asconf auto` コマンドで、アプリケーションがエンドポイントの IP アドレスの変更に応じて自動的に ASCONF チャンクを送信するように、また、SCTP が ASCONF チャンクを自動的に受け入れ、チャンネルの認証を要求するように設定できます。

# SCTP の設定方法

SCTP は、ルータでは明示的に構成されていませんが、一部の Cisco アプリケーションでは基盤として使用されます。ここでは、次の作業について説明します。

- 「SCTP 認証パラメータの設定」(P.4)
- 「SCTP アソシエーションとパラメータに関する情報の表示」(P.6)
- 「SCTP アソシエーションとパラメータのトラブルシューティング」(P.10)

## SCTP 認証パラメータの設定

SCTP 認証パラメータを設定するには、次のタスクを実行します。クライアントに認証を要求する SCTP チャンクのタイプを定義できます。任意で、`ip sctp asconf` コマンドを使用して、SCTP ストリームの中の IP アドレスの変更に応じて自動的に ASCONF チャンクを送信するように、また、ASCONF チャンクを送信する前にエンドポイントが認証をサポートしているかチェックするように、SCTP を設定できます。

表 1 にグローバル コンフィギュレーション モードで `ip sctp authenticate` コマンドを入力すると認証を要求できる SCTP チャンク タイプと番号のリストを示します。

表 1 SCTP 認証チャンネル タイプ

SCTP チャンク タイプ	SCTP チャンク番号	説明
abort association	0x06	ABORT チャンク。
asconf	0xc1	ASCONF。アドレス設定変更チャンネル。
asconf-ack	0x80	ASCONF-ACK。ASCONF 確認応答。

表 1 SCTP 認証チャンク タイプ (続き)

SCTP チャンク タイプ	SCTP チャンク番号	説明
cookie-ack	0x0b	COOKIE 確認応答チャンク。
cookie-echo	0x0a	COOKIE-ECHO チャンク。
data	0x00	DATA チャンク。
fwd-tsn	0xc0	FWD-CUM-TSN チャンク。転送された累積転送シーケンス番号チャンク。
heartbeat	0x04	HEARTBEAT 要求チャンク。
heartbeat-ack	0x05	HEARTBEAT 確認応答チャンク。
packet-drop	0x81	PACKET-DROP チャンク。
sack	0x03	選択的確認応答チャンク。
shutdown	0x07	SHUTDOWN チャンク。
shutdown-ack	0x08	SHUTDOWN 確認応答チャンク。
stream-reset	0x82	STREAM-RESET チャンク。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **ip sctp authenticate {*chunk-type* | *chunk-number*}**
4. **ip sctp asconf {**authenticate check** | **auto**}**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例: Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"><li>• プロンプトが表示されたら、パスワードを入力します。</li></ul>
ステップ 2	<b>configure terminal</b>  例: Router# 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 3	<b>ip sctp authenticate {<i>chunk-type</i>   <i>chunk-number</i>}</b>  例: Router(config)# ip sctp authenticate sack	クライアントに認証を要求する SCTP データ チャンクを定義します。
ステップ 4	<b>ip sctp asconf {<b>authenticate check</b>   <b>auto</b>}</b>  例: Router(config)# ip sctp asconf auto	(任意) ルータで IP アドレスの変更に応じて自動的に ASCONF チャンクを送信するように、また、ASCONF チャンクを送信する前にエンドポイントが認証をサポートしているかチェックするように、SCTP を設定します。

## SCTP アソシエーションとパラメータに関する情報の表示

SCTP アソシエーションとパラメータに関する情報を表示するには、次のコマンドを使用します。



(注)

統計情報を表示する SCTP コマンドは、最後に **clear sctp statistics** コマンドを実行した後に得られる情報しか表示できません。**clear sctp statistics** コマンドによって、すべての SCTP 統計情報（個別のアソシエーション向けにコンパイルされた情報および全体的にコンパイルされた情報）が消去されます。

### 手順の概要

1. **show sctp association list**
2. **show sctp association parameters**
3. **show sctp association statistics**
4. **show sctp errors**
5. **show sctp instance**
6. **show sctp instances**
7. **show sctp statistics**

### 手順の詳細

#### ステップ 1 show sctp association list

**show sctp association list** コマンドを使用すると、現在の SCTP アソシエーションとインスタンス識別子、現在の SCTP アソシエーションの状態、およびアソシエーションに使用されているローカルおよびリモートのポート番号とアドレスが表示されます。次に、確立した状態にある現在のアソシエーションを 3 つ表示する例を示します。インスタンス識別子からわかるとおり、それぞれのアソシエーションは同一のインスタンスに属しています。

```
Router# show sctp association list

*** Sctp Association List ***

AssocID:0, Instance ID:0
Current state:ESTABLISHED
Local port:8989, Addrs:10.1.0.2 10.2.0.2
Remote port:8989, Addrs:10.6.0.4 10.5.0.4

AssocID:1, Instance ID:0
Current state:ESTABLISHED
Local port:8989, Addrs:10.1.0.2 10.2.0.2
Remote port:8990, Addrs:10.6.0.4 10.5.0.4

AssocID:2, Instance ID:0
Current state:ESTABLISHED
Local port:8989, Addrs:10.1.0.2 10.2.0.2
Remote port:8991, Addrs:10.6.0.4 10.5.0.4
```

#### ステップ 2 show sctp association parameters

**show sctp association parameters** コマンドを使用すると、SCTP アソシエーションの安定性を測定する情報、動的に算出された接続先に関する統計情報、およびネットワーク輻輳を評価する値が表示されます。また、指定したアソシエーションのパラメータ値も表示されます。

アソシエーション設定セクションには、アソシエーション識別子、状態、ローカルおよびリモートのポート番号とアドレスなど、**show sctp association list** コマンドと同様の情報が表示されます。また、現在のプライマリ送信先も表示されます。

次の出力例は、アソシエーション 0 の IP SCTP アソシエーション パラメータを示します。

```
Router# show sctp association parameters 0

** SCTP Association Parameters **

AssocID: 0 Context: 0 InstanceID: 1
Assoc state: ESTABLISHED Uptime: 19:05:57.425
Local port: 8181
Local addresses: 10.1.0.3 10.2.0.3

Remote port: 8181
Primary dest addr: 10.5.0.4
Effective primary dest addr: 10.5.0.4
Destination addresses:

10.5.0.4: State: ACTIVE
Heartbeats: Enabled Timeout: 30000 ms
RTO/RTT/SRTT: 1000/16/38 ms TOS: 0 MTU: 1500
cwnd: 5364 ssthresh: 3000 outstand: 768
Num retrans: 0 Max retrans: 5 Num times failed: 0

10.6.0.4: State: ACTIVE
Heartbeats: Enabled Timeout: 30000 ms
RTO/RTT/SRTT: 1000/4/7 ms TOS: 0 MTU: 1500
cwnd: 3960 ssthresh: 3000 outstand: 0
Num retrans: 0 Max retrans: 5 Num times failed: 0

Local vertag: 9A245CD4 Remote vertag: 2A08D122
Num inbound streams: 10 outbound streams: 10
Max assoc retrans: 5 Max init retrans: 8
CumSack timeout: 200 ms Bundle timeout: 100 ms
Min RTO: 1000 ms Max RTO: 60000 ms
LocalRwnd: 18000 Low: 13455 RemoteRwnd: 15252 Low: 13161
Congest levels: 0 current level: 0 high mark: 325
```

### ステップ 3 show sctp association statistics

このコマンドを使用すると、最後に **clear sctp statistics** コマンドを SCTP アソシエーションに対して実行した以降に使用可能になった情報だけが表示されます。

次の出力例は、SCTP アソシエーション 0 の累積統計情報を示します。

```
Router# show sctp association statistics 0

** SCTP Association Statistics **

AssocID/InstanceID: 0/1
Current State: ESTABLISHED
Control Chunks
  Sent: 623874 Rcvd: 660227
Data Chunks Sent
  Total: 14235644 Retransmitted: 60487
  Ordered: 6369678 Unordered: 6371263
  Avg bundled: 18 Total Bytes: 640603980
Data Chunks Rcvd
  Total: 14496585 Discarded: 1755575
  Ordered: 6369741 Unordered: 6371269
  Avg bundled: 18 Total Bytes: 652346325
  Out of Seq TSN: 3069353
```

```
ULP Dgrams
Sent: 12740941 Ready: 12740961 Rcvd: 12740941
```

#### ステップ 4 show sctp errors

**show sctp errors** コマンドを使用すると、**clear sctp statistics** コマンドで最後に SCTP 統計情報がクリアされた時点からロギングされているすべてのアソシエーション間のすべてのエラーが表示されます。エラーがロギングされていないときは、出力にはそのように示されます。次の出力例は、SCTP エラーがあるセッションを示します。

```
Router# show sctp errors

** Sctp Error Statistics **

Invalid verification tag:      5
Communication Lost:           64
Destination Address Failed:   3
Unknown INIT params rcvd:    16
Invalid cookie signature:     5
Expired cookie:               1
Peer restarted:               1
No Listening instance:         2
```

#### ステップ 5 show sctp instance

**show sctp instance** コマンドを使用すると、コマンド構文で指定される ID のインスタンスについて現在設定されている情報が表示されます。インスタンス番号、ローカルポート、およびアドレスの情報が表示されます。インスタンスの状態は、*available* または *deletion pending* のいずれかです。インスタンスの削除要求があるにも関わらず、そのインスタンスに現在確立されているアソシエーションがある場合、インスタンスは *deletion pending* の状態に移行します。インスタンスを直ちに削除できないため、代わりに保留の状態に移行します。このインスタンスへの新たなアソシエーションは禁止され、最後のアソシエーションが終了したり失敗するとインスタンスが削除されます。

デフォルトの着信および発信ストリーム番号（次のセクションで出力例が示されます）は、着信アソシエーションを確立するために使用されます。このインスタンスに許される最大アソシエーション番号が表示され、もし存在していれば各アソシエーションのスナップショットが表示されます。

次の出力例は、SCTP インスタンス 0 の情報を表示しています。この例では、インスタンス 0 はローカルポート 1000 を使用し、現在のところ、3 つのアソシエーションがあります。

```
Router# show sctp instance 0

Instance ID:0 Local port:1000 State:available
Local addr:10.1.0.2 10.2.0.2
Default streams inbound:1 outbound:1
Current associations: (max allowed:200)
  AssocID:0 State:ESTABLISHED Remote port:8989
    Dest addr:10.6.0.4 10.5.0.4
  AssocID:1 State:ESTABLISHED Remote port:8990
    Dest addr:10.6.0.4 10.5.0.4
  AssocID:2 State:ESTABLISHED Remote port:8991
    Dest addr:10.6.0.4 10.5.0.4
```

#### ステップ 6 show sctp instances

**show sctp instances** コマンドを使用すると、現在設定されているインスタンスのそれぞれの情報が表示されます。インスタンス番号、ローカルポート、およびアドレスの情報が表示されます。インスタンスの状態は、*available* または *deletion pending* のいずれかです。インスタンスの削除要求があるにも関わらず、そのインスタンスに現在確立されているアソシエーションがある場合、インスタンスは *deletion pending* の状態に移行します。インスタンスを直ちに削除できないため、代わりに保留の状態に移行します。このインスタンスへの新たなアソシエーションは禁止され、最後のアソシエーションが終了したり失敗するとインスタンスが削除されます。



デフォルトの着信および発信ストリーム番号は、着信アソシエーションを確立するために使用されます。このインスタンスに許される最大アソシエーション番号が表示され、もし存在していれば各アソシエーションのスナップショットが表示されます。



(注)

**show sctp instances** コマンドを入力するときは、コマンド構文の中で、**instances** を完全な単語でタイプする必要があります。この単語を省略形で入力しようとすると、部分一致によって **show sctp instance instance-id** コマンドであると見なされます。

次の出力例は、有効な IP SCTP インスタンスを示します。この例では、2 つの現在のインスタンスがアクティブで有効です。初めのインスタンスはポート 8989、2 番目はポート 9191 を使っています。インスタンス識別子 0 には 3 つの現在のアソシエーションがあり、インスタンス識別子 1 には現在のアソシエーションはありません。

```
Router# show sctp instances

*** Sctp Instances ****

Instance ID:0 Local port:8989
Instance state:available
Local addrs:10.1.0.2 10.2.0.2
Default streams inbound:1 outbound:1
  Current associations: (max allowed:6)
  AssocID:0 State:ESTABLISHED Remote port:8989
    Dest addrs:10.6.0.4 10.5.0.4
  AssocID:1 State:ESTABLISHED Remote port:8990
    Dest addrs:10.6.0.4 10.5.0.4
  AssocID:2 State:ESTABLISHED Remote port:8991
    Dest addrs:10.6.0.4 10.5.0.4

Instance ID:1 Local port:9191
Instance state:available
Local addrs:10.1.0.2 10.2.0.2
Default streams inbound:1 outbound:1

No current associations established for this instance.
Max allowed:6
```

## ステップ 7 show sctp statistics

**show sctp statistics** コマンドを使用すると、最後の **clear sctp statistics** コマンド実行時から蓄積されたすべての SCTP 統計情報が表示されます。この情報には、現在確立されているすべてのアソシエーションの番号、および終了したアソシエーションの番号が含まれます。表示される統計情報は、個々のアソシエーションの表示と同様の内容です。次に、SCTP 統計情報の出力例を示します。

```
Router# show sctp statistics

*** Sctp Overall Statistics ****

Total Chunks Sent:          2097
Total Chunks Rcvd:         2766

Data Chunks Rcvd In Seq:   538
Data Chunks Rcvd Out of Seq: 0
Total Data Chunks Sent:    538
Total Data Chunks Rcvd:    538
Total Data Bytes Sent:     53800
Total Data Bytes Rcvd:     53800
Total Data Chunks Discarded: 0
Total Data Chunks Retrans: 0
```

Total SCTP Dgrams Sent:	1561
Total SCTP Dgrams Rcvd:	2228
Total ULP Dgrams Sent:	538
Total ULP Dgrams Ready:	538
Total ULP Dgrams Rcvd:	538

## SCTP アソシエーションとパラメータのトラブルシューティング

ここでは、SCTP アソシエーションとパラメータのトラブルシューティングに有効なデバッグ コマンドについて説明します。

動作中のシステムでは、パフォーマンス、状態、シグナル、および警告に関するデバッグ コマンドが便利です。これらのデバッグ コマンドは任意のアソシエーションや送信先アドレスの障害を表示し、確立されたアソシエーションの安定性を監視するために使用できます。

パフォーマンス、状態、シグナルや警告について以外のデバッグ コマンドは大量の出力を生成することがあるため、アソシエーションの障害を引き起こす可能性があります。これらのコマンドは、テスト環境、またはトラフィック量が非常に低いときに限定して使用してください。



**注意**

SCTP デバッグ コマンドの多くは、トラフィック量に依存しますが、必要以上に生成されるメッセージがアソシエーションに障害を起こすことがあるので、慎重に使用するか、または動作中のシステムでは使用しないでください。動作中のシステムが中断する可能性があるコマンドの説明で、この注記を繰り返し記載します。



**(注)**

SCTP デバッグ コマンドを使用すると、現在の SCTP アソシエーションすべてに関する情報が表示されます。特定のアソシエーションに限定することはできません。

### 手順の概要

1. `debug ip sctp api`
2. `debug ip sctp congestion`
3. `debug ip sctp init`
4. `debug ip sctp multihome`
5. `debug ip sctp performance`
6. `debug ip sctp rcvchunks`
7. `debug ip sctp rto`
8. `debug ip sctp segments`
9. `debug ip sctp segmentv`
10. `debug ip sctp signal`
11. `debug ip sctp state`
12. `debug ip sctp sndchunks`
13. `debug ip sctp timer`
14. `debug ip sctp warnings`

## 手順の詳細

## ステップ 1 debug ip sctp api

**debug ip sctp api** コマンドを使用すると、実行されているすべての Sctp Application Programming Interface (API; アプリケーションプログラミング インターフェイス) 呼び出しとそのパラメータが表示されます。



## 注意

**debug ip sctp api** コマンドは、大量のトラフィックを生成しアソシエーションの障害を起こす可能性があるため、トラフィック量が多い動作中のシステムでは使わないようにしてください。

次に、このコマンドのサンプル出力を示します。

```
Router# debug ip sctp api

*Mar 1 00:31:14.211: SCTP: sctp_send: Assoc ID: 1
*Mar 1 00:31:14.211: SCTP:                stream num: 10
*Mar 1 00:31:14.211: SCTP:                bptr: 62EE332C, dptr: 4F7B598
*Mar 1 00:31:14.211: SCTP:                datalen: 100
*Mar 1 00:31:14.211: SCTP:                context: 1
*Mar 1 00:31:14.211: SCTP:                lifetime: 0
*Mar 1 00:31:14.211: SCTP:                unorder flag: FALSE
*Mar 1 00:31:14.211: SCTP:                bundle flag: TRUE
*Mar 1 00:31:14.211: SCTP: sctp_send successful return
*Mar 1 00:31:14.211: SCTP: sctp_receive: Assoc ID: 1
*Mar 1 00:31:14.215: SCTP:                max data len: 100
.
.
.
```

## ステップ 2 debug ip sctp congestion

**debug ip sctp congestion** コマンドを使用すると、送信先アドレスごとの輻輳ウィンドウ (cwnd) 値、ローカルおよびリモートのレシーバーウィンドウ (rwnd) パラメータなど、現在の輻輳パラメータの評価に関係するさまざまなイベントが表示されます。データチャンクのハンドル時および送信時に情報が表示されます。現在の cwnd 値、rwnd 値、およびリモートの rwnd 値を示します。そのため、データを送信またはバンドルできたとき、またはできなかったときに表示されます。チャンクがリモートピアで確認応答されたとき、未処理バイト数およびリモート rwnd 値が更新されます。

情報は、新しいチャンクを受信してローカル rwnd スペースが減少したときや、Upper-Layer Protocol (ULP; 上位層プロトコル) が Sctp からデータグラムを受け取り、チャンクが解放されてローカル rwnd スペースを解放するときにも表示されます。次に、このコマンドのサンプル出力を示します。

```
Router# debug ip sctp congestion

SCTP: Assoc 0: Slow start 10.6.0.4, cwnd 3000
SCTP: Assoc 0: Data chunks rcvd, local rwnd 7800
SCTP: Assoc 0: Free chunks, local rwnd 9000
SCTP: Assoc 0: Data chunks rcvd, local rwnd 8200
SCTP: Assoc 0: Add Sack, local a_rwnd 8200
SCTP: Assoc 0: Free chunks, local rwnd 9000
SCTP: Assoc 0: Data chunks rcvd, local rwnd 7800
SCTP: Assoc 0: Data chunks rcvd, local rwnd 7000
SCTP: Assoc 0: Add Sack, local a_rwnd 7000
SCTP: Assoc 0: Free chunks, local rwnd 9000
SCTP: Assoc 0: Bundle for 10.5.0.4, rem rwnd 14000, cwnd 19500, outstand 0
SCTP: Assoc 0: Bundled 12 chunks, remote rwnd 12800, outstand 1200
SCTP: Assoc 0: Bundling data, next chunk dataLen (100) > remaining mtu size
SCTP: Assoc 0: Bundle for 10.5.0.4, rem rwnd 12800, cwnd 19500, outstand 1200
SCTP: Assoc 0: Bundled 12 chunks, remote rwnd 11600, outstand 2400
```

```

SCTP: Assoc 0: Bundling data, next chunk dataLen (100) > remaining mtu size
SCTP: Assoc 0: Bundle for 10.5.0.4, rem rwnd 11600, cwnd 19500, outstand 2400
SCTP: Assoc 0: Bundled 12 chunks, remote rwnd 10400, outstand 3600
SCTP: Assoc 0: Bundling data, next chunk dataLen (100) > remaining mtu size
SCTP: Assoc 0: Bundle for 10.5.0.4, rem rwnd 10400, cwnd 19500, outstand 3600
SCTP: Assoc 0: Bundled 4 chunks, remote rwnd 10000, outstand 4000
SCTP: Assoc 0: No additional chunks waiting.
SCTP: Assoc 0: Data chunks rcvd, local rwnd 7800
SCTP: Assoc 0: Data chunks rcvd, local rwnd 7000
SCTP: Assoc 0: Add Sack, local a_rwnd 7000
SCTP: Assoc 0: Chunk A22F3B45 ack'd, dest 10.5.0.4, outstanding 3900
SCTP: Assoc 0: Chunk A22F3B46 ack'd, dest 10.5.0.4, outstanding 3800
SCTP: Assoc 0: Chunk A22F3B47 ack'd, dest 10.5.0.4, outstanding 3700
SCTP: Assoc 0: Chunk A22F3B48 ack'd, dest 10.5.0.4, outstanding 3600
SCTP: Assoc 0: Chunk A22F3B49 ack'd, dest 10.5.0.4, outstanding 3500
SCTP: Assoc 0: Chunk A22F3B4A ack'd, dest 10.5.0.4, outstanding 3400
SCTP: Assoc 0: Chunk A22F3B4B ack'd, dest 10.5.0.4, outstanding 3300
SCTP: Assoc 0: Chunk A22F3B4C ack'd, dest 10.5.0.4, outstanding 3200
SCTP: Assoc 0: Chunk A22F3B4D ack'd, dest 10.5.0.4, outstanding 3100
SCTP: Assoc 0: Chunk A22F3B4E ack'd, dest 10.5.0.4, outstanding 3000
SCTP: Assoc 0: Chunk A22F3B4F ack'd, dest 10.5.0.4, outstanding 2900
SCTP: Assoc 0: Chunk A22F3B50 ack'd, dest 10.5.0.4, outstanding 2800
SCTP: Assoc 0: Chunk A22F3B51 ack'd, dest 10.5.0.4, outstanding 2700
SCTP: Assoc 0: Chunk A22F3B52 ack'd, dest 10.5.0.4, outstanding 2600
SCTP: Assoc 0: Chunk A22F3B53 ack'd, dest 10.5.0.4, outstanding 2500
SCTP: Assoc 0: Chunk A22F3B54 ack'd, dest 10.5.0.4, outstanding 2400
SCTP: Assoc 0: Chunk A22F3B55 ack'd, dest 10.5.0.4, outstanding 2300
SCTP: Assoc 0: Chunk A22F3B56 ack'd, dest 10.5.0.4, outstanding 2200

```

### ステップ 3 debug ip sctp init

**debug ip sctp init** コマンドを使用すると、新しいアソシエーションの初期化に関するデータグラムおよびその他の情報が表示されます。INIT、INIT\_ACK、COOKIE\_ECHO、および COOKIE\_ACK チャンクを含むすべての初期化チャンクが表示されます。このデバッグ コマンドは、初期化シーケンスと関係するチャンクを確認するために使用できますが、アソシエーションが確立すると、送信されたデータ チャンクは表示されません。そのため、アソシエーションが失敗して再確立が必要な問題があるときに、トラフィック フローがある動作中のシステムで使用しても安全です。

```
Router# debug ip sctp init
```

```

*Mar 1 00:53:07.279: SCTP Test: Attempting to open assoc to remote port 8787...assoc ID
is 0
*Mar 1 00:53:07.279: SCTP: Process Assoc Request
*Mar 1 00:53:07.279: SCTP: Assoc 0: dest addr list:
*Mar 1 00:53:07.279: SCTP:                addr 10.5.0.4
*Mar 1 00:53:07.279: SCTP:                addr 10.6.0.4
*Mar 1 00:53:07.279:
...
*Mar 1 00:53:13.279: SCTP: Assoc 0: Send Init
*Mar 1 00:53:13.279: SCTP:                INIT_CHUNK, len 42
*Mar 1 00:53:13.279: SCTP:                Initiate Tag: B4A10C4D, Initial TSN: B4A10C4D, rwnd
9000
*Mar 1 00:53:13.279: SCTP:                Streams Inbound: 13, Outbound: 13
*Mar 1 00:53:13.279: SCTP:                IP Addr: 10.1.0.2
*Mar 1 00:53:13.279: SCTP:                IP Addr: 10.2.0.2
*Mar 1 00:53:13.279: SCTP:                Supported addr types: 5
*Mar 1 00:53:13.307: SCTP: Process Init
*Mar 1 00:53:13.307: SCTP:                INIT_CHUNK, len 42
*Mar 1 00:53:13.307: SCTP:                Initiate Tag: 3C2D8327, Initial TSN: 3C2D8327, rwnd
18000
*Mar 1 00:53:13.307: SCTP:                Streams Inbound: 13, Outbound: 13
*Mar 1 00:53:13.307: SCTP:                IP Addr: 10.5.0.4
*Mar 1 00:53:13.307: SCTP:                IP Addr: 10.6.0.4

```

```

*Mar 1 00:53:13.307: SCTP: Supported addr types: 5
*Mar 1 00:53:13.307: SCTP: Assoc 0: Send InitAck
*Mar 1 00:53:13.307: SCTP: INIT_ACK_CHUNK, len 124
*Mar 1 00:53:13.307: SCTP: Initiate Tag: B4A10C4D, Initial TSN: B4A10C4D, rwnd
9000
*Mar 1 00:53:13.307: SCTP: Streams Inbound: 13, Outbound: 13
*Mar 1 00:53:13.307: SCTP: Responder cookie len 88
*Mar 1 00:53:13.307: SCTP: IP Addr: 10.1.0.2
*Mar 1 00:53:13.307: SCTP: IP Addr: 10.2.0.2
*Mar 1 00:53:13.311: SCTP: Assoc 0: Process Cookie
*Mar 1 00:53:13.311: SCTP: COOKIE_ECHO_CHUNK, len 88
*Mar 1 00:53:13.311: SCTP: Assoc 0: dest addr list:
*Mar 1 00:53:13.311: SCTP: addr 10.5.0.4
*Mar 1 00:53:13.311: SCTP: addr 10.6.0.4
*Mar 1 00:53:13.311:
*Mar 1 00:53:13.311: SCTP: Instance 0 dest addr list:
*Mar 1 00:53:13.311: SCTP: addr 10.5.0.4
*Mar 1 00:53:13.311: SCTP: addr 10.6.0.4
*Mar 1 00:53:13.311:
*Mar 1 00:53:13.311: SCTP: Assoc 0: Send CookieAck
*Mar 1 00:53:13.311: SCTP: COOKIE_ACK_CHUNK

```

#### ステップ 4 debug ip sctp multihome

**debug ip sctp multihome** コマンドを使用すると、マルチホーム アドレスの利用を監視するデータグラム  
の発信元と宛先が表示されます。INIT チャンクの送信者がマルチホーム化されているとき、2 つ以上  
の IP アドレス パラメータが INIT チャンクに含まれます。ネットワークに問題が発生していなければ、  
多くの場合、データグラムはプライマリの送信先アドレスに送信されますが、データグラムがセカンダ  
リ アドレスに送信されることもあります。



#### 注意

**debug ip sctp multihome** コマンドを使用すると、送信および受信したそれぞれのデータグラムに 1  
つのデバッグ行が生成されます。動作中のシステムでは慎重に使用してください。

次に、このコマンドのサンプル出力を示します。

```
Router# debug ip sctp multihome
```

```

SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 1404
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 476
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 28
SCTP: Assoc 0: Send Data to dest 10.5.0.4
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 1404
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 1404
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 1404
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 476
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 28
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 28
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 1404
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 1404
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 28
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 1404
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 476
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 28
SCTP: Assoc 0: Send Data to dest 10.5.0.4
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 1404
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 1404
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 1404
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 476
SCTP: Rcvd s=10.6.0.4 8787, d=10.2.0.2 8787, len 44
SCTP: Sent: Assoc 0: s=10.2.0.2 8787, d=10.6.0.4 8787, len 44
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 28

```

```

SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 28
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 1404
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 1404
SCTP: Sent: Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 28
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 1404
SCTP: Rcvd s=10.5.0.4 8787, d=10.1.0.2 8787, len 476

```

## ステップ 5 debug ip sctp performance

**debug ip sctp performance** コマンドを使用すると、チャンクと送受信データグラムの 1 秒あたりの平均値が表示されます。いったんイネーブルされると、**debug ip sctp performance** コマンドは 10 秒ごとにこの情報を表示します。平均値は最後に統計情報がクリアされてからの累積値であり、現在送受信されているデータグラムとチャンクの数値が正確には反映されていない可能性があることに注意してください。

次の例では、最初にパフォーマンス デバッグがイネーブルにされたとき、非常に低いトラフィック率が表示されています。ただし、これらの数値は正確ではないと考えられるので、**clear ip sctp** コマンドが実行されました。平均値はすぐに補正され、正確なトラフィック流量を反映しています。

```

Router# debug ip sctp performance

SCTP Sent: SCTP Dgrams 5, Chunks 28, Data Chunks 29, ULP Dgrams 29
SCTP Rcvd: SCTP Dgrams 7, Chunks 28, Data Chunks 29, ULP Dgrams 29
Chunks Discarded: 0, Retransmitted 0

SCTP Sent: SCTP Dgrams 6, Chunks 29, Data Chunks 30, ULP Dgrams 30
SCTP Rcvd: SCTP Dgrams 7, Chunks 29, Data Chunks 30, ULP Dgrams 30
Chunks Discarded: 0, Retransmitted 0

SCTP Sent: SCTP Dgrams 6, Chunks 29, Data Chunks 31, ULP Dgrams 31
SCTP Rcvd: SCTP Dgrams 7, Chunks 30, Data Chunks 31, ULP Dgrams 31
Chunks Discarded: 0, Retransmitted 0

SCTP Sent: SCTP Dgrams 6, Chunks 30, Data Chunks 31, ULP Dgrams 31
SCTP Rcvd: SCTP Dgrams 7, Chunks 31, Data Chunks 32, ULP Dgrams 31
Chunks Discarded: 0, Retransmitted 0

SCTP Sent: SCTP Dgrams 6, Chunks 31, Data Chunks 32, ULP Dgrams 32
SCTP Rcvd: SCTP Dgrams 7, Chunks 32, Data Chunks 32, ULP Dgrams 32
Chunks Discarded: 0, Retransmitted 0

Router# clear ip sctp statistics

SCTP Sent: SCTP Dgrams 30, Chunks 210, Data Chunks 199, ULP Dgrams 201
SCTP Rcvd: SCTP Dgrams 30, Chunks 208, Data Chunks 198, ULP Dgrams 198
Chunks Discarded: 0, Retransmitted 0

SCTP Sent: SCTP Dgrams 30, Chunks 210, Data Chunks 199, ULP Dgrams 200
SCTP Rcvd: SCTP Dgrams 30, Chunks 209, Data Chunks 199, ULP Dgrams 199
Chunks Discarded: 0, Retransmitted 0

SCTP Sent: SCTP Dgrams 30, Chunks 211, Data Chunks 200, ULP Dgrams 199
SCTP Rcvd: SCTP Dgrams 30, Chunks 209, Data Chunks 198, ULP Dgrams 198
Chunks Discarded: 0, Retransmitted 0

```

## ステップ 6 debug ip sctp rcvchunks

**debug ip sctp rcvchunks** コマンドを使用すると、受信されたチャンクに関する情報が表示されます。それぞれの受信されたチャンクに対するストリーム番号、シーケンス番号、チャンク長、チャンクの Transmission Sequence Number (TSN; 転送シーケンス番号)、およびチャンクが新しいデータグラムのものかあるいは既に再編成されたデータグラムの部分なのかが表示されます。コマンド出力では、データグラムがこのチャンク受信後に完成したのかそうでないか、および完成した場合は、指定したス

トリームの中のシーケンスにあるかどうか、ULP に配送できるのかが表示されます。リモートに送信された SACK が表示されます。確認応答された累積 TSN、含まれるフラグメントの数、およびデータグラムが ULP に受信されたことが示されます。



**注意**

**debug ip sctp rcvchunks** コマンドを使用すると、受信したそれぞれのデータグラムに複数のデバッグ行が生成されます。動作中のシステムでは慎重に使用してください。

次の例では、セグメント化されたデータグラムが、ストリーム 0、シーケンス番号 0 の 2 つのチャンクで受信されています。最初のチャンク長は 1452 で、2 番目は 1 バイトです。最初のチャンクは新しいデータグラム用のチャンクであることを示しますが、2 番目のチャンクはすでに再編成された既存データグラムの一部であることを示します。最初のチャンクを処理すると、順序どおりでも完了していないため、まだ配送できません。2 番目のチャンクを受信すると、データグラムは順序どおりに完了します。アプリケーションはデータグラムを受信し、両方のチャンクが損失なしに（つまり、フラグメントなしで）受信されたことが確認応答のために SACK に示されます。

```
Router# debug ip sctp rcvchunks

SCTP: Assoc 0: New chunk (0/0/1452/2C33D822) for new dgram (0)
SCTP: Assoc 0: dgram (0) is in seq
SCTP: Assoc 0: Add Sack Chunk, CumTSN=2C33D822, numFrgs=0
SCTP: Assoc 0: New chunk (0/0/1/2C33D823) for existing dgram (0)
SCTP: Assoc 0: dgram (0) is complete
SCTP: Assoc 0: ApplRecv chunk 0/0/1452/2C33D822
SCTP: Assoc 0: ApplRecv chunk 0/0/1/2C33D823
SCTP: Assoc 0: Add Sack Chunk, CumTSN=2C33D823, numFrgs=0
```

#### ステップ 7 debug ip sctp rto

**debug ip sctp rto** コマンドを使用すると、データチャンクの再送信や未応答のハートビートのために、再送信 (retrans) タイムアウト値に実行された調整が表示されます。



**注意**

**debug ip sctp rto** コマンドを使用すると、大量の出力が生成されることがあります。動作中のシステムでは慎重に使用してください。

次の例では、使用できる宛先アドレスは 1 つだけです。チャンクが再送信されるたびに、Retransmission Timeout (RTO; 再送信タイムアウト) 値が 2 倍になります。

```
Router# debug ip sctp rto

SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 942BAC55
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 2000 ms
SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 942BAC55
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 4000 ms
SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 942BAC55
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 8000 ms
SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 942BAC55
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 16000 ms
SCTP: Assoc 0: destaddr 10.5.0.4, retrans timeout on chunk 942BAC55
SCTP: Assoc 0: destaddr 10.5.0.4, rto backoff 32000 ms
```

#### ステップ 8 debug ip sctp segments

**debug ip sctp segments** 出力で、送受信されたすべてのデータグラムとそれぞれに含まれるチャンクが表示されます。セグメント デバッグ コマンドには、簡易および詳細の 2 つの形式があります。ここでは簡易形式でセグメント出力がされており、それぞれのチャンク タイプの基本的情報が表示されます。詳細形式での出力については、**debug ip sctp segmentv** コマンドを参照してください。



## 注意

**debug ip sctp segments** コマンドでは、送受信されたそれぞれのセグメントについていくつかの出力行が生成されます。動作中のシステムでは慎重に使用してください。

次の出力は、アソシエーションが確立され、いくつかのハートビートが送信され、リモートのエンドポイントに障害が発生してアソシエーションが再起動された例を示します。

```
Router# debug ip sctp segments

SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 56
SCTP:      INIT_CHUNK, Tag: 3C72A02A, TSN: 3C72A02A
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 56
SCTP:      INIT_CHUNK, Tag: 13E5AD6C, TSN: 13E5AD6C
SCTP: Sent:  Assoc NULL: s=10.1.0.2  8787, d=10.5.0.4  8787, len 136
SCTP:      INIT_ACK_CHUNK, Tag: 3C72A02A, TSN: 3C72A02A
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 100
SCTP:      COOKIE_ECHO_CHUNK, len 88
SCTP: Sent:  Assoc NULL: s=10.1.0.2  8787, d=10.5.0.4  8787, len 16
SCTP:      COOKIE_ACK_CHUNK
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 52
SCTP:      HEARTBEAT_CHUNK
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 52
SCTP:      HEARTBEAT_CHUNK
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 52
SCTP:      HEARTBEAT_CHUNK
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 56
SCTP:      INIT_CHUNK, Tag: 4F2D8235, TSN: 4F2D8235
SCTP: Sent:  Assoc NULL: s=10.1.0.2  8787, d=10.5.0.4  8787, len 136
SCTP:      INIT_ACK_CHUNK, Tag: 7DD7E424, TSN: 7DD7E424
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 100
SCTP:      COOKIE_ECHO_CHUNK, len 88
SCTP: Sent:  Assoc NULL: s=10.1.0.2  8787, d=10.5.0.4  8787, len 16
SCTP:      COOKIE_ACK_CHUNK
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 144
SCTP:      SACK_CHUNK, TSN ack: 7DD7E423, rwnd 18000, num frags 0
SCTP:      DATA_CHUNK, 4/0/100/4F2D8235
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 28
SCTP:      SACK_CHUNK, TSN ack: 4F2D8235, rwnd 8900, num frags 0
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 128
SCTP:      DATA_CHUNK, 4/0/100/7DD7E424
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 28
SCTP:      SACK_CHUNK, TSN ack: 7DD7E424, rwnd 17900, num frags 0
SCTP: Recv:  Assoc 0: s=10.6.0.4  8787, d=10.2.0.2  8787, len 44
SCTP:      HEARTBEAT_CHUNK
SCTP: Sent:  Assoc 0: s=10.2.0.2  8787, d=10.6.0.4  8787, len 44
SCTP:      HEARTBEAT_ACK_CHUNK
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 128
SCTP:      DATA_CHUNK, 7/0/100/4F2D8236
SCTP: Sent:  Assoc 0: s=10.1.0.2  8787, d=10.5.0.4  8787, len 144
SCTP:      SACK_CHUNK, TSN ack: 4F2D8236, rwnd 9000, num frags 0
SCTP:      DATA_CHUNK, 7/0/100/7DD7E425
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 28
SCTP:      SACK_CHUNK, TSN ack: 7DD7E424, rwnd 18000, num frags 0
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 28
SCTP:      SACK_CHUNK, TSN ack: 7DD7E425, rwnd 17900, num frags 0
SCTP: Recv:  Assoc 0: s=10.5.0.4  8787, d=10.1.0.2  8787, len 128
SCTP:      DATA_CHUNK, 4/1/100/4F2D8237
```

## ステップ 9 debug ip sctp segmentv



**debug ip sctp segmentv** コマンドでは、送受信されたそれぞれのセグメントについていくつかの出力行が生成されます。ここでは詳細形式でセグメントが出力されており、それぞれのチャンク タイプの詳細情報が表示されます（簡易形式での出力については、**debug ip sctp segments** コマンドを参照してください）。



**注意**

**debug ip sctp segmentv** コマンドでは、送受信されたそれぞれのセグメントについて複数の出力行が生成されます。動作中のシステムでは慎重に使用してください。

次の出力は、アソシエーションが確立され、いくつかのハートビートが送信され、リモートのエンドポイントに障害が発生してアソシエーションが再起動された例を示します。

```
Router# debug ip sctp segmentv

SCTP: Sent:  Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 56, ver tag 0
SCTP:  INIT_CHUNK, len 42
SCTP:  Initiate Tag: B131ED6A, Initial TSN: B131ED6A, rwnd 9000
SCTP:  Streams Inbound: 13, Outbound: 13
SCTP:  IP Addr: 10.1.0.2
SCTP:  IP Addr: 10.2.0.2
SCTP:  Supported addr types: 5
SCTP: Recv:  Assoc 0: s=10.5.0.4 8787, d=10.1.0.2 8787, len 56, ver tag 0
SCTP:  INIT_CHUNK, len 42
SCTP:  Initiate Tag: 5516B2F3, Initial TSN: 5516B2F3, rwnd 18000
SCTP:  Streams Inbound: 13, Outbound: 13
SCTP:  IP Addr: 10.5.0.4
SCTP:  IP Addr: 10.6.0.4
SCTP:  Supported addr types: 5
SCTP: Sent:  Assoc NULL: s=10.1.0.2 8787, d=10.5.0.4 8787, len 136, ver tag 5516B2F3
SCTP:  INIT_ACK_CHUNK, len 124
SCTP:  Initiate Tag: B131ED6A, Initial TSN: B131ED6A, rwnd 9000
SCTP:  Streams Inbound: 13, Outbound: 13
SCTP:  Responder cookie len 88
SCTP:  IP Addr: 10.1.0.2
SCTP:  IP Addr: 10.2.0.2
SCTP: Recv:  Assoc 0: s=10.5.0.4 8787, d=10.1.0.2 8787, len 100, ver tag B131ED6A
SCTP:  COOKIE_ECHO_CHUNK, len 88
SCTP: Sent:  Assoc NULL: s=10.1.0.2 8787, d=10.5.0.4 8787, len 16, ver tag 5516B2F3
SCTP:  COOKIE_ACK_CHUNK
SCTP: Recv:  Assoc 0: s=10.5.0.4 8787, d=10.1.0.2 8787, len 144, ver tag B131ED6A
SCTP:  SACK_CHUNK, len 16
SCTP:  TSN ack: (0xB131ED69)
SCTP:  Rcv win credit: 18000
SCTP:  Num frags: 0
SCTP:  DATA_CHUNK, flags 3, chunkLen 116
SCTP:  DATA_CHUNK, 0/0/100/5516B2F3
SCTP: Sent:  Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 28, ver tag 5516B2F3
SCTP:  SACK_CHUNK, len 16
SCTP:  TSN ack: (0x5516B2F3)
SCTP:  Rcv win credit: 8900
SCTP:  Num frags: 0
SCTP: Sent:  Assoc 0: s=10.1.0.2 8787, d=10.5.0.4 8787, len 128, ver tag 5516B2F3
SCTP:  DATA_CHUNK, flags 3, chunkLen 116
SCTP:  DATA_CHUNK, 0/0/100/B131ED6A
SCTP: Recv:  Assoc 0: s=10.6.0.4 8787, d=10.2.0.2 8787, len 44, ver tag B131ED6A
SCTP:  HEARTBEAT_CHUNK
SCTP: Sent:  Assoc 0: s=10.2.0.2 8787, d=10.6.0.4 8787, len 44, ver tag 5516B2F3
SCTP:  HEARTBEAT_ACK_CHUNK
SCTP: Recv:  Assoc 0: s=10.5.0.4 8787, d=10.1.0.2 8787, len 28, ver tag B131ED6A
SCTP:  SACK_CHUNK, len 16
```

## ステップ 10 debug ip sctp signal

**debug ip sctp signal** コマンドを使用すると、アプリケーションまたは ULP に向けて SCTP から送信されたシグナルが表示されます。これらのシグナルは、ULP にアソシエーションの状態遷移や送信先アドレスを通知します。そのほか、新規の受信データが利用可能になったとき ULP に送信されるシグナルもありますが、発生頻度が低いため、以下の出力例では示していません。現在のアソシエーションが安定している場合は、このデバッグ コマンドを使用できます。状態遷移以外に関する出力は生成されないため、動作中のシステムで使用しても安全です。ただし、システムで処理されるアソシエーション数やネットワークの安定性に依存するので、注意して使用してください。

### ステップ 11 debug ip sctp state

**debug ip sctp state** コマンドは、多くの場合、**debug ip sctp signal** コマンドと同時に使用されます。2 つのコマンドを一緒に使用すると、アソシエーションの安定性について詳細に確認できます。

次の例では、新しいアソシエーションが要求され確立されます。次に、ピアがアソシエーションを再起動し、アソシエーションが失敗し、再確立されていることを認識します。ローカルピアは、特定のチャンクの再送信が成功しないまま最大数を超過して試行しようとしたため、アソシエーションが失敗したことを示します。その結果、アソシエーションは（通信の損失のため）失敗し、終了します。ULP からアソシエーションを再び試行するよう要求され、この試みは成功します。リモートピアからのシャットダウン受信により、ローカルピアはシャットダウン確認応答送信状態に移行して、アソシエーションの終了がその後続きます。再び、別のアソシエーションが試行され成功します。

```
Router# debug ip sctp signal
Router# debug ip sctp state

<new assoc attempt>
00:20:08: SCTP: Assoc 0: state CLOSED -> COOKIE_WAIT
00:20:15: SCTP: Assoc 0: state COOKIE_WAIT -> ESTABLISHED
00:20:15: SCTP: Assoc 0: Sent ASSOC_UP signal for CONFIGD_ASSOC
00:21:03: SCTP: Assoc 0: Restart rcvd from peer
00:21:03: SCTP: Assoc 0: Sent ASSOC_RESTART signal
00:21:04: SCTP: Assoc 0: chunk 62EA7F40 retransmitted more than max times, failing assoc
00:21:04: SCTP: Assoc 0: Sent ASSOC_FAILED signal, reason: SCTP_COMM_LOST
00:21:04: SCTP: Assoc 0: Sent ASSOC_TERMINATE signal
00:21:04: SCTP: Assoc 0: state ESTABLISHED -> CLOSED
<new assoc attempt>
00:21:04: SCTP: Assoc 0: state CLOSED -> COOKIE_WAIT
00:21:04: SCTP: Assoc 0: state COOKIE_WAIT -> COOKIE_ECHOED
00:21:04: SCTP: Assoc 0: state COOKIE_ECHOED -> ESTABLISHED
00:21:04: SCTP: Assoc 0: Sent ASSOC_UP signal for CONFIGD_ASSOC
00:21:04: SCTP: Assoc 0: Sent TERMINATE_PENDING signal
00:21:04: SCTP: Assoc 0: state ESTABLISHED -> SHUTDOWN_ACKSENT
00:21:04: SCTP: Assoc 0: Sent ASSOC_TERMINATE signal
00:21:04: SCTP: Assoc 0: state SHUTDOWN_ACKSENT -> CLOSED
<new assoc attempt>
00:21:04: SCTP: Assoc 0: state CLOSED -> COOKIE_WAIT
00:21:04: SCTP: Assoc 0: state COOKIE_WAIT -> COOKIE_ECHOED
00:21:04: SCTP: Assoc 0: state COOKIE_ECHOED -> ESTABLISHED
00:21:04: SCTP: Assoc 0: Sent ASSOC_UP signal for CONFIGD_ASSOC
```

### ステップ 12 debug ip sctp sndchunks

**debug ip sctp sndchunks** コマンドを使用すると、リモートの SCTP ピアに送信されるすべてのチャンクについて次のような情報が表示されます。

- ローカルの SCTP ピアからのアプリケーション送信要求
- リモートピアにバンドルおよび送信されるチャンク
- 正常に受信したチャンクを示す、リモートピアからの SACK 処理
- 再送信向けにマークされたチャンク

**注意**

**debug ip sctp sndchunks** コマンドは、かなりのトラフィック流量がある場合、大量のデータを生成します。動作中のシステムでは慎重に使用してください。

```
Router# debug ip sctp sndchunks

SCTP: Assoc 0: ApplSend, chunk: 0/10412/100/A23134F8 to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 5/10443/100/A23134F9 to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 5/10448/100/A231355C to 10.5.0.4
SCTP: Assoc 0: Set oldest chunk for dest 10.5.0.4 to TSN A23134F8
SCTP: Assoc 0: Bundling data, added 0/10412/100/A23134F8, outstanding 100
SCTP: Assoc 0: Bundling data, added 5/10443/100/A23134F9, outstanding 200
SCTP: Assoc 0: Bundling data, added 4/10545/100/A23134FA, outstanding 300
SCTP: Assoc 0: Bundling data, added 10/10371/100/A23134FB, outstanding 400
SCTP: Assoc 0: Bundling data, added 11/10382/100/A23134FC, outstanding 500
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A231350F, numFrgs=0
SCTP: Assoc 0: Reset oldest chunk on addr 10.5.0.4 to A2313510
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A2313527, numFrgs=0
SCTP: Assoc 0: Reset oldest chunk on addr 10.5.0.4 to A2313528
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A231353F, numFrgs=0
SCTP: Assoc 0: Reset oldest chunk on addr 10.5.0.4 to A2313540
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A2313557, numFrgs=0
SCTP: Assoc 0: Reset oldest chunk on addr 10.5.0.4 to A2313558
SCTP: Assoc 0: ApplSend, chunk: 10/10385/100/A23135BE to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 8/10230/100/A23135BF to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 5/10459/100/A23135C0 to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 4/10558/100/A23135C1 to 10.5.0.4
SCTP: Assoc 0: Set oldest chunk for dest 10.5.0.4 to TSN A231355D
SCTP: Assoc 0: Bundling data, added 5/10449/100/A231355D, outstanding 100
SCTP: Assoc 0: Bundling data, added 3/10490/100/A231355E, outstanding 200
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A23135A4, numFrgs=0
SCTP: Assoc 0: Reset oldest chunk on addr 10.5.0.4 to A23135A5
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A23135BC, numFrgs=0
SCTP: Assoc 0: Reset oldest chunk on addr 10.5.0.4 to A23135BD
SCTP: Assoc 0: Process Sack Chunk, CumTSN=A23135C1, numFrgs=0
SCTP: Assoc 0: ApplSend, chunk: 5/10460/100/A23135C2 to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 5/10461/100/A23135C3 to 10.5.0.4
SCTP: Assoc 0: ApplSend, chunk: 11/10403/100/A2313626 to 10.5.0.4
SCTP: Assoc 0: Set oldest chunk for dest 10.5.0.4 to TSN A23135C2
SCTP: Assoc 0: Bundling data, added 5/10460/100/A23135C2, outstanding 100
SCTP: Assoc 0: Bundling data, added 5/10461/100/A23135C3, outstanding 200
SCTP: Assoc 0: Bundling data, added 5/10462/100/A23135C4, outstanding 300
SCTP: Assoc 0: Bundling data, added 4/10559/100/A23135C5, outstanding 400
SCTP: Assoc 0: Bundling data, added 4/10560/100/A23135C6, outstanding 500
SCTP: Assoc 0: Bundled 12 chunk(s) in next dgram to 10.5.0.4
SCTP: Assoc 0: Bundling data, added 1/10418/100/A2313622, outstanding 9700
SCTP: Assoc 0: Bundling data, added 3/10502/100/A2313623, outstanding 9800
SCTP: Assoc 0: Bundling data, added 7/10482/100/A2313624, outstanding 9900
SCTP: Assoc 0: Bundling data, added 3/10503/100/A2313625, outstanding 10000
SCTP: Assoc 0: Bundling data, added 11/10403/100/A2313626, outstanding 10100
SCTP: Assoc 0: Bundled 5 chunk(s) in next dgram to 10.5.0.4
SCTP: Assoc 0: Mark chunk A23135C2 for retrans
SCTP: Assoc 0: Mark chunk A23135C3 for retrans
SCTP: Assoc 0: Mark chunk A23135C4 for retrans
SCTP: Assoc 0: Mark chunk A23135C5 for retrans
SCTP: Assoc 0: Mark chunk A23135C6 for retrans
SCTP: Assoc 0: Mark chunk A23135C7 for retrans
SCTP: Assoc 0: Mark chunk A23135C8 for retrans
SCTP: Assoc 0: Mark chunk A23135C9 for retrans
SCTP: Assoc 0: Mark chunk A23135CA for retrans
SCTP: Assoc 0: Bundled 6 chunk(s) in next dgram to 10.6.0.4
SCTP: Assoc 0: Mark chunk A23135C2 for retrans
```

```
SCTP: Assoc 0: Mark chunk A23135C3 for retrans
SCTP: Assoc 0: Mark chunk A23135C4 for retrans
```

### ステップ 13 debug ip sctp timer

**debug ip sctp timer** コマンドは、すべての開始、停止およびトリガーされた SCTP タイマーについての情報を表示します。多くの SCTP タイマーは、開始した後に、期限切れや停止するまで再起動しません。これらのタイマーでは、タイマーを開始する最初の呼び出しが成功して、続く呼び出しではタイマーが期限切れになるか停止するまでは何もしません。たとえば、最初のチャンクが送信されたとき、再送信タイマーは開始しますが、それに続くチャンクで未処理データがあるときは、再び開始することはありません。



#### 注意

**debug ip sctp timer** コマンドはかなりの量の出力を生成します。動作中のシステムでは慎重に使用してください。

以下の例では、**debug ip sctp timer** コマンドからの出力を示します。

```
Router# debug ip sctp timer

SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Timer BUNDLE triggered
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Stopping RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Stopping RETRANS timer for destaddr 10.5.0.4
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Timer already started, not restarting
SCTP: Assoc 0: Stopping CUMSACK timer
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Assoc 0: Starting CUMSACK timer
SCTP: Timer already started, not restarting
```

### ステップ 14 debug ip sctp warnings

**debug ip sctp warnings** コマンドは、通常の状態における情報を表示します。これらの状態は、状況の詳細にも依存しますが、問題を示す場合も示さない場合もあります。以下は、警告としてフラグ設定されたイベントや状態の例です。

```
Router# debug ip sctp warnings

SCTP: Assoc 0: No cookie in InitAck, discarding
SCTP: Assoc 0: Incoming INIT_ACK: inbound streams req'd 15, allowed 13
SCTP: Assoc 0: Incoming INIT_ACK request: outbound streams req'd 13, allowed 1
SCTP: Assoc 0: Remote verification tag in init ack is zero, discarding
```

```
SCTP: Remote verification tag in init is zero, discarding
SCTP: Assoc 0: Rwnd less than min allowed (1500) in incoming INITACK, rcvd 0
SCTP: Assoc 0: Rwnd less than min allowed (1500) in incoming INITACK, rcvd 1499
SCTP: Rwnd in INIT too small (0), discarding
SCTP: Rwnd in INIT too small (1499), discarding
SCTP: Unknown INIT param 16537 (0x4099), length 8
SCTP: Assoc 0: Unknown INITACK param 153 (0x99), length 8
SCTP: Assoc 0: No cookie in InitAck, discarding
SCTP: Assoc 0: No cookie in InitAck, discarding
SCTP: Processing INIT, invalid param len 0, discarding...
SCTP: Assoc 0: Processing INITACK, invalid param len 0, discarding...
```

## SCTP の設定例

ここでは、次の設定例について説明します。

- [「SCTP 認証パラメータの定義：例」\(P.21\)](#)

## SCTP 認証パラメータの定義：例

以下の例では、クライアントに認証を要求する SCTP データ チャンクを定義し、ルータで IP アドレスの変更に応じて自動的に ASCONF チャンクを送信するように SCTP を設定する方法を示します。

```
configure terminal
ip sctp authenticate data
ip sctp asconf auto
```

## その他の参考資料

ここでは、SCTP 機能に関する関連資料について説明します。

## 関連資料

内容	参照先
SCTP を利用するアプリケーション	<ul style="list-style-type: none"> <li>『<i>PRI Backhaul Using the Stream Control Transmission Protocol and the ISDN Q.921 User Adaptation Layer</i>』</li> <li>『<i>Netflow Reliable Export with SCTP</i>』</li> </ul>
SCTP コマンド：コマンド構文、コマンドモード、コマンド履歴、デフォルト設定、使用に関する注意事項、および例	『 <i>Cisco IOS IP Application Services Command Reference</i> 』

## 規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

## MIB

MIB	MIB リンク
この機能がサポートする新しい MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	<p>選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFC

RFC	タイトル
RFC 2960	『 <i>Stream Control Transmission Protocol (SCTP)</i> 』

## シスコのテクニカル サポート

説明	リンク
<p>Cisco Support Web サイトには、豊富なオンライン リソースが提供されており、それらに含まれる資料やツールを利用して、トラブルシューティングやシスコ製品およびテクノロジーに関する技術上の問題の解決に役立てることができます。</p> <p>以下を含むさまざまな作業にこの Web サイトが役立ちます。</p> <ul style="list-style-type: none"><li>• テクニカル サポートを受ける</li><li>• ソフトウェアをダウンロードする</li><li>• セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける</li><li>• ツールおよびリソースへアクセスする</li><li>• Product Alert の受信登録</li><li>• Field Notice の受信登録</li><li>• Bug Toolkit を使用した既知の問題の検索</li><li>• Networking Professionals (NetPro) コミュニティで、技術関連のディスカッションに参加する</li><li>• トレーニング リソースへアクセスする</li><li>• TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する</li></ul> <p>Japan テクニカル サポート Web サイトでは、Technical Support Web サイト (<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>) の、利用頻度の高いドキュメントを日本語で提供しています。Japan テクニカル サポート Web サイトには、次の URL からアクセスしてください。 <a href="http://www.cisco.com/jp/go/tac">http://www.cisco.com/jp/go/tac</a></p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

## SCTP の機能情報

表 2 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。この表には、Cisco IOS リリース 12.2(1) 以降のリリースで導入または変更された機能だけを示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンドリファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator により、どの Cisco IOS および Catalyst OS ソフトウェア イメージが特定のソフトウェア リリース、フィチャセット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。



(注) 表 2 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 2 SCTP の機能情報

機能名	リリース	機能情報
SCTP リリース 1	12.2(4)T	<p>Stream Control Transmission Protocol (SCTP; ストリーム制御通信プロトコル) は信頼性のあるデータグラム型 IP トラフィックの転送プロトコルで、RFC 2960 で仕様が定められています。</p> <p>この機能は、12.2(4)T で初めて導入されました。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> <li>「SCTP の前提条件」(P.2)</li> <li>「SCTP に関する情報」(P.2)</li> <li>「SCTP の利点」(P.2)</li> <li>「SCTP アソシエーションとパラメータに関する情報の表示」(P.6)</li> <li>「SCTP アソシエーションとパラメータのトラブルシューティング」(P.10)</li> </ul> <p>この機能により、次のコマンドが導入または変更されました。clear ip sctp statistics、debug ip sctp api、debug ip sctp congestion、debug ip sctp init、debug ip sctp multihome、debug ip sctp performance、debug ip sctp rcvchunks、debug ip sctp rto、debug ip sctp segments、debug ip sctp segmentv、debug ip sctp signal、debug ip sctp sndchunks、debug ip sctp state、debug ip sctp timer、debug ip sctp warnings、show ip sctp association list、show ip sctp association parameters、show ip sctp association statistics、show ip sctp errors、show ip sctp instances、show ip sctp statistics</p>



表 2 SCTP の機能情報 (続き)

機能名	リリース	機能情報
SCTP リリース 2	12.2(8)T	<p>SCTP リリース 2 では、SCTP コマンドの出力が更新されています。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> <li>• 「SCTP リリース 2」 (P.2)</li> <li>• 「SCTP アソシエーションとパラメータのトラブルシューティング」 (P.10)</li> <li>• 「SCTP 認証パラメータの定義：例」 (P.21)</li> </ul> <p><b>show ip sctp association paramters</b> および <b>show ip sctp association statistics</b> の各コマンドがこの機能により変更されました。</p>
SCTP Show および Clear の CLI 機能拡張	12.4(11)T	<p>SCTP Show および Clear の CLI 機能拡張で、潜在的な問題のトラブルシューティングに役立つ SCTP の追加情報にアクセスできます。また、これらの機能拡張によって、更新された SCTP show と clear コマンドは他の転送プロトコルの CLI と一致するようになりました。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> <li>• 「SCTP Show および Clear の CLI 機能拡張」 (P.2)</li> </ul> <p>この機能により、次のコマンドが置き換えられました。  <b>clear ip sctp statistics</b>、<b>show ip sctp association list</b>、<b>show ip sctp association parameters</b>、<b>show ip sctp association statistics</b>、<b>show ip sctp errors</b>、<b>show ip sctp instances</b>、<b>show ip sctp statistics</b></p> <p>この機能により、次のコマンドが導入されました。  <b>clear sctp statistics</b>、<b>show sctp association</b>、<b>show sctp association list</b>、<b>show sctp association parameters</b>、<b>show sctp association statistics</b>、<b>show sctp errors</b>、<b>show sctp instance</b>、<b>show sctp instances</b>、<b>show sctp instances</b>、<b>show sctp statistics</b></p>

表 2 SCTP の機能情報 (続き)

機能名	リリース	機能情報
SCTP リリース 4、フェーズ 1	12.4(15)T	<p>SCTP リリース 4 で、SCTP ストリーム リセットと認証機能が導入されました。</p> <p>SCTP ストリーム リセット機能では、SCTP がストリーム転送シーケンス番号およびすべてのストリーム シーケンス番号をリセットできます。SCTP ストリーム リセットを使用すると、次の操作を実行できます。</p> <ul style="list-style-type: none"> <li>• ピアの発信ストリームを動的にリセットする</li> <li>• ローカル ホストの発信ストリームを動的にリセットする</li> <li>• 指定番号のストリームを動的にリセットする</li> </ul> <p>SCTP 認証を使用すると、次の操作を実行できます。</p> <ul style="list-style-type: none"> <li>• 共有秘密鍵なしでダイナミック共有アソシエーション鍵をセットアップする</li> <li>• 共有秘密鍵をアソシエーション鍵と結合する</li> <li>• 共有アソシエーション シークレットを使用してチャンクを認証する</li> <li>• 認証する必要があるチャンク タイプをネゴシエートする</li> </ul> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> <li>• 「SCTP リリース 4」 (P.3)</li> <li>• 「SCTP 認証パラメータの設定」 (P.4)</li> <li>• 「SCTP アソシエーションとパラメータに関する情報の表示」 (P.6)</li> <li>• 「SCTP アソシエーションとパラメータのトラブルシューティング」 (P.10)</li> <li>• 「SCTP 認証パラメータの定義：例」 (P.21)</li> </ul> <p>コマンド <code>ip sctp authenticate</code> がこの機能により導入されました。</p>

表 2 SCTP の機能情報 (続き)

機能名	リリース	機能情報
SCTP リリース 4、フェーズ 2	12.4(20)T	<p>Cisco IOS Release 12.4(20)T の時点で、SCTP リリース 4 にて SCTP Add-IP 機能が導入されました。</p> <p>SCTP Add-IP 機能では、既存の SCTP アソシエーションのエンドポイントに IP アドレスを追加または削除して、この変更をリモートの端点に伝えることができます。アソシエーションの冗長なサーバアドレスを追加または削除するときに、リモートの端点に ADD-IP チャンクが送信されます。ADD-IP チャンクでは、応答しなくなったホストのすべてのアドレスをアソシエーションから削除することもできます。SCTP Add-IP 機能で、アプリケーションからプログラマ的に SCTP アソシエーションへのプライマリ アドレスを設定することもできます。</p> <p>SCTP リリース 4 に対する強化に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> <li>• 「SCTP Add-IP」 (P.4)</li> <li>• 「SCTP 認証パラメータの設定」 (P.4)</li> <li>• 「SCTP 認証パラメータの定義：例」 (P.21)</li> </ul> <p><b>ip sctp authenticate</b> および <b>ip sctp asconf</b> の各コマンドがこのリリースで導入または修正されました。</p>

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2007-2008 Cisco Systems, Inc.  
All rights reserved.

Copyright © 2007-2010, シスコシステムズ合同会社.  
All rights reserved.

