



# Rate-Based Satellite Control Protocol (RBSCP)

---

Rate-Based Satellite Control Protocol (RBSCP) は、衛星リンクなどのエラー レートが高い無線または長距離の遅延リンクのために設計されました。RBSCP では、トンネルを使用して、エンドツーエンドモデルを中断することなく衛星リンクを介して TCP および IP Security (IPSec) などの特定の IP プロトコルのパフォーマンスを改善できます。

## 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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、“[Feature Information for AToM NSF](#)” [section on page 10](#) を参照してください。

プラットフォーム サポートと Cisco 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。

## 内容

- 「[Rate Based Satellite Control Protocol の制約事項](#)」 (P.2)
- 「[Rate-Based Satellite Control Protocol \(RBSCP\) について](#)」 (P.2)
- 「[Rate-Based Satellite Control Protocol \(RBSCP\) の設定方法](#)」 (P.5)
- 「[Rate-Based Satellite Control Protocol \(RBSCP\) の設定例](#)」 (P.9)
- 「[その他の参考資料](#)」 (P.11)
- 「[Rate Based Satellite Control Protocol の機能情報](#)」 (P.13)



## Rate Based Satellite Control Protocol の制約事項

- RBSCP は、衛星リンクなどの、エラー レートが高い無線または長距離の遅延リンクのために設計されました。エラー レートが高い長距離遅延リンクがない場合は、この機能を実装しないでください。
- RBSCP トンネルによって使用されるインターフェイス上に IP Access List (ACL; アクセス リスト) が設定されている場合、RBSCP IP プロトコル (199) では、動作しないインターフェイスまたはトンネルの開始および終了を行える必要があります。
- トンネルを介するトラフィックはプロセスで切り替えられるため、RBSCP には一部パフォーマンス上の制約事項があります。

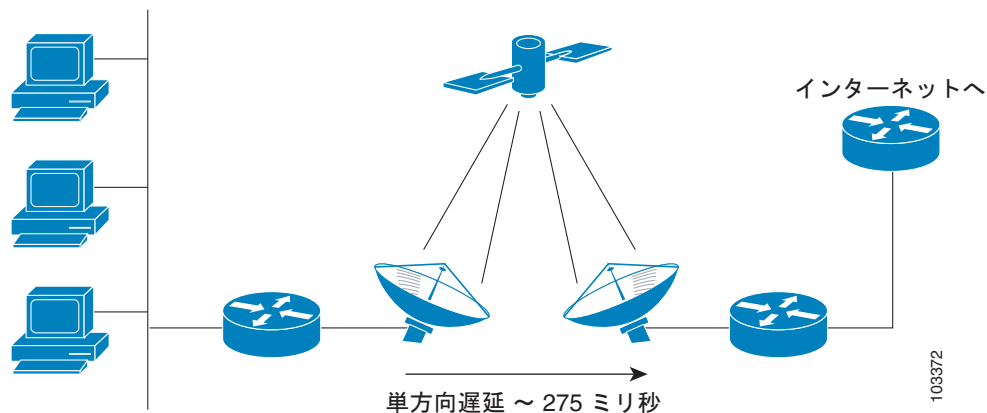
## Rate-Based Satellite Control Protocol (RBSCP) について

- 「衛星リンクを介した IP」(P.2)
- 「衛星リンクを介したプロキシを拡張するパフォーマンス」(P.3)
- 「衛星リンクを介した RBSCP」(P.4)

### 衛星リンクを介した IP

衛星リンクには、リンクを介する IP プロトコルに影響を及ぼすいくつかの特性があります。図 1 は、衛星リンクに 275 ミリ秒の単方向遅延が発生する可能性があることを示しています。550 ミリ秒の Round-Trip Time (RTT; ラウンドトリップ時間) は、TCP に対する非常に長時間の遅延です。別の問題は、LAN の無線リンクに比較して衛星リンクに通常発生する、エラー レート (パケット損失レート) が高いことです。天候さえ衛星リンクに影響を及ぼし、使用可能な帯域幅の減少、RTT およびパケット損失の増加を招きます。

図 1 通常の衛星リンク



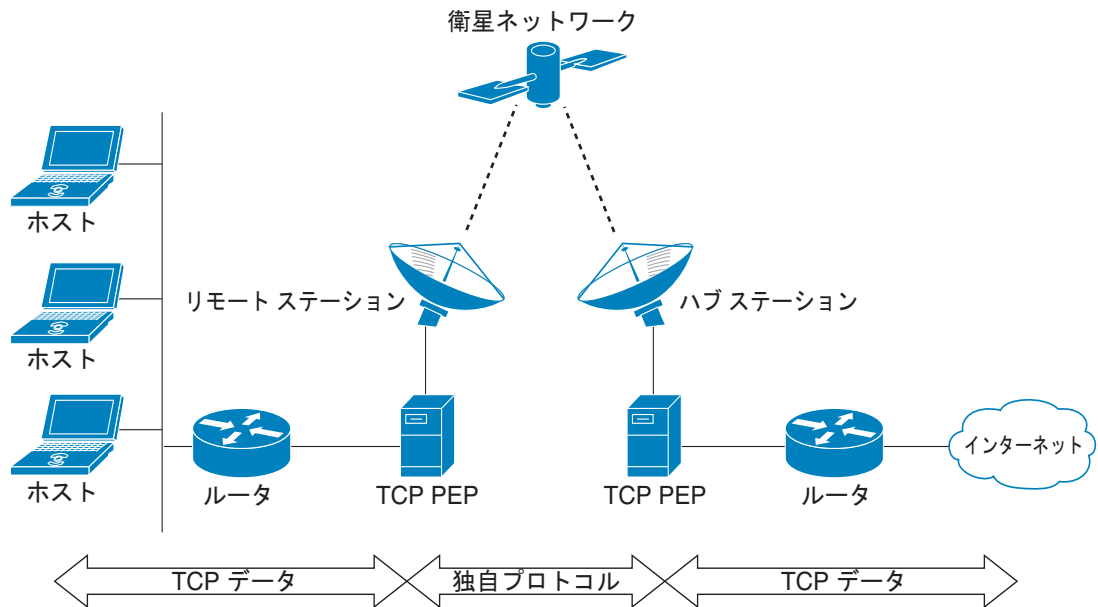
RTT が長時間の場合、TCP は低速開始モードのまま、衛星リンク帯域幅全体が使用される前の時間が長くなります。TCP および Stream Control Transmission Protocol (SCTP) では、パケット損失イベントがネットワークの輻輳状態と解釈され、輻輳リカバリ手順の実行が開始されます。これによって、リンクを介して送信されるトラフィックが少なくなります。

使用可能な衛星リンク帯域幅は大きくなりますが、衛星リンクを介した IP プロトコルで発生する長時間の RTT および高いエラー レートによって、高い Bandwidth-Delay Product (BDP; 帯域遅延積) が生成されます。

## 衛星リンクを介したプロキシを拡張するパフォーマンス

衛星リンクの使用時に、低速開始モードで継続される TCP の問題に対処するために、中断を伴う Performance Enhancing Proxy (PEP) ソリューションがネットワークに導入されます。図 2 は、転送接続が、そのデフォルト ルータを介してインターネットに接続しているリモート側のホストで、3 つのセクションに分かれることを示したものです。ルータによって、すべてのインターネット バインド型トラフィックが TCP PEP に送信されます。これによって、インターネットへの TCP 接続が中断されず、PEP によって、すべてのデータのローカル TCP ACK (TCP スプーフィング) が生成されます。トラフィックはバッファリングされ、衛星リンクを介して 1 つの PEP プロトコルを介して再送信されます。2 つ目の PEP では、衛星リンクからのデータを受信し、別の TCP 接続を介してインターネットにデータが再送信されます。TCP 送信が妨害され、ドロップされたパケットは、TCP の輻輳として解釈されず、バッファリングされたデータから再送信されます。最小限の TCP ACK と抑制された TCP 低速の開始では、より多くの帯域幅を使用できます。

図 2 中断を伴う TCP PEP のソリューション



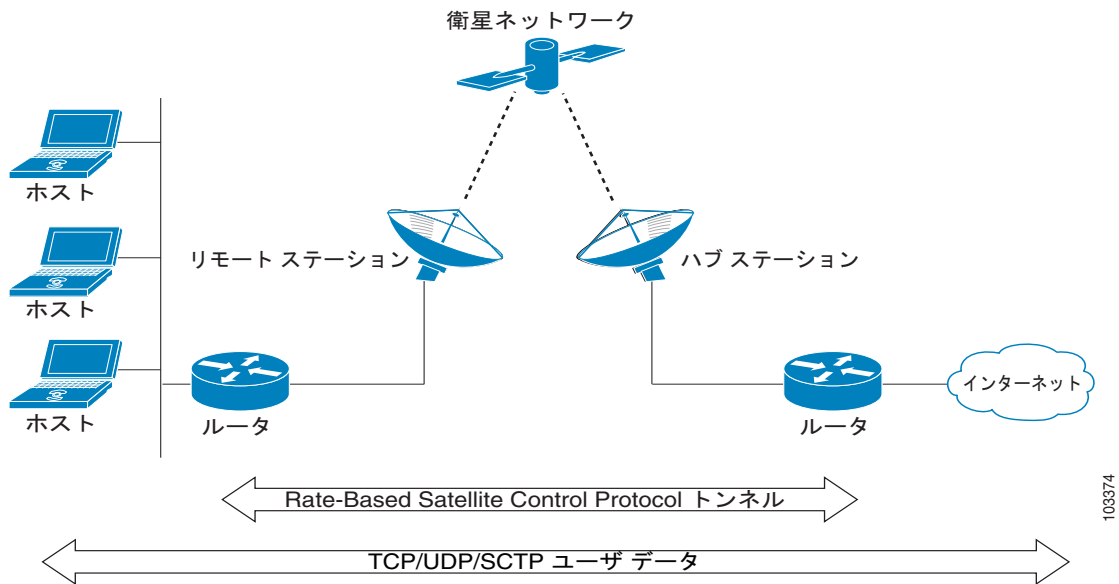
中断を伴う TCP PEP を使用する場合の欠陥の 1 つは、中断を伴う TCP PEP によって、エンドツーエンド モデルが中断されることです。トラフィックのフローが中断されると、一部のアプリケーションは動作できず、PEP では、暗号化トラフィック (IPSec) の処理の準備がありません。SCTP などの新しい転送プロトコルでは、中断を伴う TCP PEP で機能する場合に特別な処理または追加コードが必要です。各衛星ルータでは、追加の管理対象ネットワーク コンポーネントも必要です。

## 衛星リンクを介した RBSCP

RBSCP は、エンドツーエンド モデルを保持するために設計され、PEP ソリューションを使用して衛星リンクを介してパフォーマンスの改善がもたらされます。衛星リンク中でのクリア テキスト トラフィックの IPSec の暗号化（たとえば VPN サービス設定）はサポートされます。RBSCP を使用すると、2つのルータで、衛星リンクの送信レートを制御およびモニタリングでき、帯域利用率が高まります。損失パケットは、RBSCP によって衛星リンクを介して再送信され、エンドホスト TCP の送信側が低速開始モードになることが防止されます。

図 3 に示されているように、RBSCP はトンネル インターフェイスを使用して実装されます。トンネルは、衛星モデムまたは内部衛星モデム ネットワーク モジュールで使用可能な Cisco IOS ソフトウェアによってサポートされる任意のネットワーク インターフェイスを介して設定できます。IP トラフィックは、ルータ設定によって指定された適切な変更および機能拡張が使用される衛星リンクにまたがって送信されます。標準ルーティングまたはポリシーベース ルーティングを使用して、RBSCP トンネルを介して送信されるトラフィックを特定できます。

図 3 中断を伴わない RBSCP ソリューション



RBSCP トンネルでは、次のいずれかの機能を設定できます。

### 時間の遅延

RBSCP ルータの 1 つでは、RBSCP トンネルを介した転送のため、フレームを保持するよう設定できます。遅延時間は、エンドホストでの RTT が増え、RBSCP 時間によって、損失 TCP フレームまたはその他のプロトコルフレームを再送信できます。再送信が正常に実行されると、損失フレーム イベントが、輻輳手順がイネーブルのエンドホストに到達することが防止されます。一部の場、遅延なしで RBSCP によって再送信を完了できます。

### ACK の分割

受信した各 TCP ACK で生成された多数の追加の TCP ACK は、Acknowledgement (ACK) 分割を使用したクリア テキスト TCP トラフィックでパフォーマンスを改善できます。TCP では、受信した各 TCP ACK の 1 つの Maximum Transmission Unit (MTU; 最大伝送ユニット) によって、輻輳ウィンドウが開きます。輻輳ウィンドウが開くと、より大きな帯域幅が使用可能になります。衛星リンクで使用可能なすべての帯域幅が使用されていないときにのみ、この機能を設定します。暗号化トラフィックでは、ACK 分割は使用できません。

### ウィンドウ スタッフィング

クリア テキスト TCP トラフィックと SCTP トラフィックは、RBSCP ウィンドウ スタッフィング機能の利点を活用できます。RBSCP では、アドバタイジングされるウィンドウを、使用可能な衛星リンク帯域幅またはルータで使用可能なメモリまで増やすことができるよう、トラフィックをバッファリングできます。パケットを送信するエンドホストでは、より大きなウィンドウが受信側のエンドホストに存在し、より多くのトラフィックが送信されると、誤って見なされます。エンドホストによって、衛星リンクに処理するトラフィックを多く送りすぎることがあり、発生したパケットの損失および再送信によって、リンクに輻輳状態が発生する可能性があるため、この機能は注意して使用してください。

### SCTP ドロップ レポート

SCTP では、ACK 計算方式の代わりに適切なバイト計算方式を使用して送信ウィンドウのサイズが決定されるため、ACK 分割は、SCTP では動作しません。RBSCP トンネルでは、輻輳による損失の結果としてではなく、衛星全体でドロップされたパケットの SCTP パケット ドロップ レポートを生成できます。この SCTP ドロップ レポートはデフォルトでオンに設定されており、輻輳ウィンドウ サイズに影響を及ぼすことなくパケットを再送信する機会が提供されます。実際の輻輳損失は、引き続きレポートされますが、通常のリカバリ メカニズムがアクティブにされます。

## Rate-Based Satellite Control Protocol (RBSCP) の設定方法

- 「RBSCP トンネルの設定」(P.5) (必須)
- 「RBSCP トンネルがアクティブであるかの確認」(P.8) (任意)
- 「RBSCP トラフィックの確認」(P.8) (任意)

## RBSCP トンネルの設定

RBSCP トンネルを設定するには、この作業を実行します。必ずトンネルの両側にルータを設定するようにしてください。

### 前提条件

この作業でトンネル ソースとして使用される物理インターフェイスは、すでに設定済みであることを確認してください。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface *type number***
4. **ip unnumbered *interface-type interface-number***
5. **tunnel source {*ip-address* | *interface-type interface-number*}**
6. **tunnel destination {*hostname* | *ip-address*}**
7. **tunnel bandwidth {*receive* | *transmit*} *bandwidth***

8. `tunnel mode {aurp | cayman | dvmrp | eon | gre | gre multipoint | ipip [decapsulate-any] | iptalk | mpls | nos | rbscp}`
9. `tunnel rbscp ack_split split-size`
10. `tunnel rbscp delay`
11. `tunnel rbscp report`
12. `tunnel rbscp window_stuff step-size`
13. `exit`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>enable</code>  例： Router> enable	特権 EXEC モードをイネーブルにします。  • プロンプトが表示されたら、パスワードを入力します。
ステップ2	<code>configure terminal</code>  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	<code>interface type number</code>  例： Router(config)# interface tunnel 0	インターフェイスのタイプと番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ4	<code>ip unnumbered interface-type interface-number</code>  例： Router(config-if)# ip unnumbered Ethernet 1	明示的な IP アドレスを割り当てずに、インターフェイスで IP 処理をイネーブルにします。  • 番号なしインターフェイスでパケットが生成される（たとえば、ルーティング アップデート）たびに、指定されたインターフェイスのアドレスが IP パケットのソース アドレスとして使用されます。
ステップ5	<code>tunnel source {ip-address   interface-type interface-number}</code>  例： Router(config-if)# tunnel source Ethernet 1	トンネル送信元を設定します。  • サービス プロバイダーの IP アドレスを指定する場合は、 <i>ip-address</i> 引数を使用します。  • 使用するインターフェイスを指定する場合は、 <i>interface-type</i> 引数および <i>interface-number</i> 引数を使用します。RBSCP では、インターフェイスをトンネル ソースとして指定することを推奨します。
ステップ6	<code>tunnel destination {hostname   ip-address}</code>  例： Router(config-if)# tunnel destination 172.17.2.1	トンネル宛先を設定します。  • サービス プロバイダーの IP アドレスを指定する場合は、 <i>hostname</i> 引数を使用します。  • 使用するインターフェイスを指定する場合は、 <i>ip-address</i> 引数を使用します。

	コマンドまたはアクション	目的
ステップ7	<pre>tunnel bandwidth {receive   transmit} bandwidth</pre> <p>例： Router(config-if)# tunnel bandwidth transmit 1000</p>	<p>パケットの送信に使用されるトンネル帯域幅を指定します。</p> <ul style="list-style-type: none"> <li>帯域幅を指定する場合は、<i>bandwidth</i> 引数を使用します。</li> </ul> <p>(注) <b>receive</b> は使用されなくなりました。</p>
ステップ8	<pre>tunnel mode {aurp   cayman   dvmp   eon   gre   gre multipoint   ipip [decapsulate-any]   iptalk   mpls   nos   rbscp}</pre> <p>例： Router(config-if)# tunnel mode rbscp</p>	<p>トンネルで使用されるプロトコルを指定します。</p> <ul style="list-style-type: none"> <li>RBSCP がトンネル プロトコルとして使用されるように指定する場合は、<b>rbscp</b> 引数を使用します。</li> </ul>
ステップ9	<pre>tunnel rbscp ack_split split-size</pre> <p>例： Router(config-if)# tunnel rbscp ack_split 6</p>	<p>(任意) RBSCP トンネルで分割される TCP Acknowledgement (ACK) をイネーブルにします。</p> <ul style="list-style-type: none"> <li>受信する各 ACK に送信される ACK の数を指定する場合は、<i>split-size</i> 引数を使用します。</li> <li>ACK のデフォルト数は 4 です。</li> </ul>
ステップ10	<pre>tunnel rbscp delay</pre> <p>例： Router(config-if)# tunnel rbscp delay</p>	<p>(任意) RBSCP トンネル遅延をイネーブルにします。</p> <ul style="list-style-type: none"> <li>RTT が 700 ミリ秒よりも長い場合にのみ、このコマンドを使用します。</li> </ul>
ステップ11	<pre>tunnel rbscp report</pre> <p>例： Router(config-if)# tunnel rbscp report</p>	<p>(任意) ドロップされた RBSCP パケットを SCTP にレポートします。</p> <ul style="list-style-type: none"> <li>ドロップされたパケットを SCTP にレポートすることによって、より優良な帯域幅が使用されます。これは、SCTP がエンドホストに対してドロップされたパケットを再送信するよう指示し、これによって、エンドホストでネットワークが輻輳していると思わなくなるためです。</li> </ul>
ステップ12	<pre>tunnel rbscp window_stuff step-size</pre> <p>例： Router(config-if)# tunnel rbscp window_stuff 3</p>	<p>(任意) RBSCP トンネルの TCP ウィンドウ スケールの値を増やすことによって、TCP ウィンドウ スタッフイングをイネーブルにします。</p> <ul style="list-style-type: none"> <li>ステップ増分数を指定する場合は、<i>step-size</i> 引数を使用します。</li> </ul>
ステップ13	<pre>exit</pre> <p>例： Router(config-if)# exit</p>	<p>インターフェイス コンフィギュレーションモードを終了し、グローバル コンフィギュレーションモードに戻ります。</p> <ul style="list-style-type: none"> <li>グローバル コンフィギュレーションモードを終了する場合は、この手順をもう一度繰り返します。</li> </ul>

## 次の作業

この作業は、衛星リンクのもう一方の側にあるルータ上で繰り返す必要があります。2 つ目のルータ上の IP アドレスの例、ホスト名、および他のパラメータを、適切な値に置き換えます。

## RBSCP トンネルがアクティブであるかの確認

この作業を実行して、「RBSCP トンネルの設定」の作業で設定された RBSCP トンネルがアクティブであることを確認します。

### 手順の概要

1. `enable`
2. `show rbscp [all | state | statistics] [tunnel tunnel-number]`
3. `exit`

### 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>enable</code>  例： <pre>Router&gt; enable</pre>	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	<code>show rbscp [all   state   statistics] [tunnel tunnel-number]</code>  例： <pre>Router# show rbscp state tunnel 1</pre>	トンネルの現在の状態に関する情報を表示するには、 <b>state</b> キーワードおよび <b>tunnel</b> キーワードを指定してこのコマンドを使用します。次の出力例では、トンネルがオープン状態で示されています。すべてのカウンタで、最後に <b>clear rbscp</b> コマンドを実行した以降の累積合計が表示されます。
ステップ3	<code>exit</code>  例： <pre>Router&gt;# exit</pre>	特権 EXEC コンフィギュレーション モードを終了します。

## RBSCP トラフィックの確認

トラフィックが、RBSCP トンネルを介して、また、衛星リンク全体に送信されていることを確認するには、この作業を実行します。

### 手順の概要

1. `enable`
2. `show interfaces tunnel number [accounting]`
3. `exit`



## 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>enable</code>  例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ2	<code>show interfaces tunnel number [accounting]</code>  例： Router# show interfaces tunnel 0	トラフィックが RBSCP トンネルを介して送信中であることを示すには、このコマンドを使用します。
ステップ3	<code>exit</code>  例： Router># exit	特権 EXEC コンフィギュレーション モードを終了します。

## Rate-Based Satellite Control Protocol (RBSCP) の設定例

- [「RBSCP トンネルの設定例」 \(P.9\)](#)
- [「RBSCP トンネルのルーティングの設定例」 \(P.10\)](#)

### RBSCP トンネルの設定例

次に、衛星リンク経由の RBSCP トンネルを介してトラフィックが送信されるよう、ルータ 1 およびルータ 2 を設定します。

#### ルータ 1

```
interface Tunnel 0
 ip unnumbered ethernet1
 tunnel source ethernet1
 tunnel destination 172.17.2.1
 tunnel bandwidth transmit 1000
 tunnel mode rbscp
 tunnel rbscp ack_split 6
 tunnel rbscp report
!
interface ethernet1
 description Satellite Link
 ip address 172.20.1.2 255.255.255.0
```

#### ルータ 2

```
interface Tunnel 0
 ip unnumbered ethernet1
 tunnel source ethernet1
 tunnel destination 172.20.1.2
 tunnel bandwidth transmit 1000
 tunnel mode rbscp
 tunnel rbscp ack_split 6
```

```
tunnel rbscp report
!
interface ethernet1
  description Satellite Link
  ip address 172.17.2.1 255.255.255.0
```

## RBSCP トンネルのルーティングの設定例

RBSCP トンネルを使用するトラフィックのタイプを制御するには、適切なルーティングを設定する必要があります。すべてのトラフィックをトンネルを介して送信する場合、スタティック ルートを設定できます。



(注)

ダイナミック ルーティング プロトコルが使用されている場合に、ルーティング フラップを防止するには、必ずトンネル インターフェイスをパッシブに設定してください。

次に、一部の特定のプロトコル タイプをトンネルを介して送信するために、ポリシー ベースのルーティングを使用する例を示します。この例では、拡張アクセス リストを使用して、TCP、Stream Control Transmission Protocol (SCTP)、Encapsulating Security Payload (ESP) プロトコル、および Authentication Header (AH; 認証ヘッダー) トラフィックで、トンネルを介した送信が可能です。すべての IP トラフィックは拒否されます。

### ルータ 1 (ローカル側)

```
interface Tunnell
  ip unnumbered FastEthernet1/1
  tunnel source FastEthernet1/1
  tunnel destination 10.12.0.20
  tunnel mode rbscp
  tunnel ttl 5
  tunnel bandwidth transmit 30000
  tunnel rbscp window_stuff 1
  tunnel rbscp ack_split 4
!
interface FastEthernet0/0
  ip address 10.13.0.1 255.255.255.0
  ip policy route-map rbscp-pbr
  duplex auto
  speed auto
!
interface FastEthernet1/1
  description Satellite Link
  ip address 10.12.0.1 255.255.255.0
  duplex auto
  speed auto
!
ip route 10.15.0.0 255.255.255.0 FastEthernet1/1
!
ip access-list extended rbscp-acl
  permit tcp any 10.15.0.0 0.0.0.255
  permit 132 any 10.15.0.0 0.0.0.255
  permit esp any 10.15.0.0 0.0.0.255
  permit ahp any 10.15.0.0 0.0.0.255
  deny ip any any
!
!
route-map rbscp-pbr permit 10
  match ip address rbscp-acl
  set interface Tunnell
```

**ルータ 2 (リモート側)**

```

ip dhcp pool CLIENT
  import all
  network 10.15.0.0 255.255.255.0
  default-router 10.15.0.1
  domain-name engineer.chicago.il.us
  dns-server 10.10.0.252
!
interface Tunnell
  ip unnumbered FastEthernet0/1
  tunnel source FastEthernet0/1
  tunnel destination 10.12.0.1
  tunnel mode rbscp
  tunnel ttl 5
  tunnel bandwidth transmit 30000
  tunnel rbscp window_stuff 1
  tunnel rbscp ack_split 4
!
interface FastEthernet0/0
  description Local LAN
  ip address 10.15.0.1 255.255.255.0
  ip policy route-map rbscp-pbr
  duplex auto
  speed auto
!
interface FastEthernet0/1
  description Satellite Link
  ip address 10.12.0.20 255.255.255.0
  duplex auto
  speed auto
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1
!
ip access-list extended rbscp-acl
  permit tcp any any
  permit 132 any any
  permit esp any any
  permit ahp any any
  deny ip any any
!
route-map rbscp-pbr permit 10
  match ip address rbscp-acl
  set interface Tunnell

```

## その他の参考資料

### 関連資料

関連項目	参照先
トンネル インターフェイス コマンド : コマンド構文の詳細、コマンド モード、デフォルト設定、使用に関する注意事項および例	『 <a href="#">Cisco IOS Interface and Hardware Component Command Reference</a> 』
トンネルの設定	『 <a href="#">Cisco IOS Interface and Hardware Component Configuration Guide</a> 』

## 標準

標準	タイトル
この機能によってサポートされ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
この機能によってサポートされる新しい MIB または変更された 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、およびフィチャセットの MIB の場所を検索しダウンロードするには、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 1323	『TCP Extensions for High Performance』
RFC 2018	『TCP Selective Acknowledgment Options』

## シスコのテクニカル サポート

説明	リンク
TAC のホームページには、3 万ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

# Rate Based Satellite Control Protocol の機能情報

表 1 に、この機能のリリース履歴を示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャセット、またはプラットフォームを確認できます。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 1 は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1 AToM NSF Any Transport over MPLS および AToM グレースフル リスタートに関する機能情報

機能名	リリース	機能情報
Rate-Based Satellite Control Protocol (RBSCP)	12.3(7)T	この機能が導入されました。 次のコマンドが導入または変更されました。 <b>clear rbscp、debug tunnel rbscp、show rbscp、tunnel bandwidth、tunnel mode、tunnel rbscp ack_split、tunnel rbscp delay、tunnel rbscp input_drop、tunnel rbscp long_drop、tunnel rbscp report、tunnel rbscp、window_stuff。</b>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned 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. (1110R)

このマニュアルで使用している IP アドレスは、実際のアドレス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、および図は、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 Cisco Systems, Inc.  
All rights reserved

Copyright © 2007–2012, シスコシステムズ合同会社.  
All rights reserved.

