



# Access List-Based RBSCP

---

**Last Updated: January 18, 2012**

The Access List-Based Rate-Based Satellite Control Protocol (RBSCP) feature allows you to selectively apply the TCP ACK splitting feature of RBSCP to any outgoing interface. The result is reduced effect of long latencies over a satellite link. Access List-Based RBSCP has no tunneling or queueing overhead that is associated with RBSCP tunnels. Additional benefits include more interoperability with other Cisco IOS features (such as TCP/IP header compression, DMVPN, and QoS) because the TCP and Stream Control Transmission Protocol (SCTP) packets are no longer encapsulated with an RBSCP/IP header. This feature works on process switched forwarding, fast switching, or Cisco Express Forwarding (CEF).

- [Finding Feature Information, page 1](#)
- [Prerequisites for Access List-Based RBSCP, page 1](#)
- [Restrictions for Access List-Based RBSCP, page 2](#)
- [Information About Access List-Based RBSCP, page 2](#)
- [How to Configure Access List-Based RBSCP, page 4](#)
- [Configuration Examples for Access List-Based RBSCP, page 6](#)
- [Additional References, page 8](#)
- [Feature Information for Access List-Based RBSCP, page 9](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

## Prerequisites for Access List-Based RBSCP

This document assumes that you already understand how to configure an IP access list and have one configured.



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

## Restrictions for Access List-Based RBSCP

**Caution**

Plan your network carefully so that no more than one Cisco IOS router in a given routing path has the Access List-Based RBSCP feature enabled. You do not want to recursively ACK split traffic.

- The Access List-Based RBSCP feature will process only IPv4 packets, not IPv6 packets.
- The feature will process only standalone TCP packets. Encapsulated (encrypted or tunneled) TCP packets will be left unprocessed.
- This feature is available only on non-distributed platforms.

## Information About Access List-Based RBSCP

- [Benefits of Access List-Based RBSCP, page 2](#)
- [Rate-Based Satellite Control Protocol, page 2](#)
- [TCP ACK Splitting, page 3](#)
- [Access List-Based RBSCP Functionality, page 4](#)

## Benefits of Access List-Based RBSCP

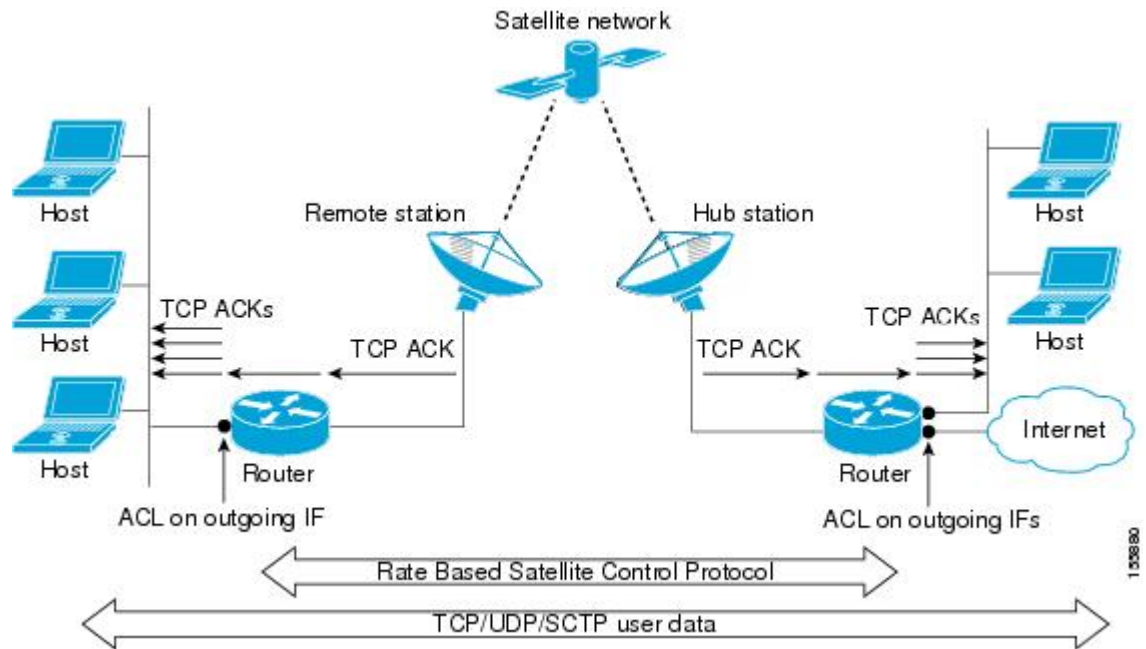
The Access List-Based Rate-Based Satellite Control Protocol (RBSCP) feature provides the following benefits:

- It allows you to selectively apply the TCP ACK splitting feature of RBSCP to any outgoing interface. TCP ACK splitting is a benefit because it reduces the effect of long latencies characteristic of satellite links. Applying this feature selectively by using an access list is a benefit because you control which packets are subject to TCP ACK splitting.
- It has no tunneling or queueing overhead that is associated with RBSCP tunnels.
- It provides more interoperability with other Cisco IOS features (such as TCP/IP header compression, DMVPN, and QoS) because the TCP and Stream Control Transmission Protocol (SCTP) packets are no longer encapsulated with an RBSCP/IP header.
- This feature works on process switched forwarding, fast switching, or CEF.
- It preserves the internet end-to-end principle.

## Rate-Based Satellite Control Protocol

Rate-Based Satellite Control Protocol (RBSCP) was designed for wireless or long-distance delay links with high error rates, such as satellite links. RBSCP can improve the performance of certain IP protocols, such as TCP and IP Security (IPsec), over satellite links without breaking the end-to-end model. For instructions on how to implement RBSCP over a tunnel, see the “Implementing Tunnels” chapter of the *Interface and Hardware Component Configuration Guide*.

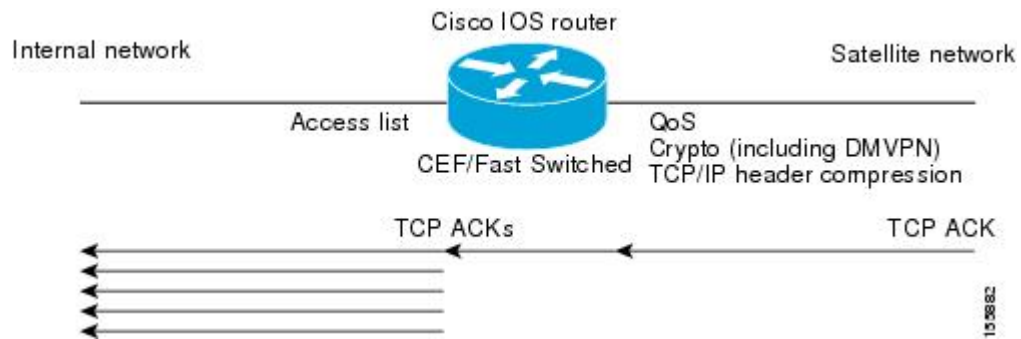
The TCP ACK splitting capability of RBSCP can be implemented without a tunnel, by using an IP access list, as shown in the figure below. The TCP ACK splitting occurs at the outgoing interface between the router and the internal network or Internet. It does not occur over the link to the satellite.



## TCP ACK Splitting

TCP ACK splitting is a software technique to improve performance for clear-text TCP traffic using acknowledgment (ACK) splitting, in which a number of additional TCP ACKs are generated for each TCP ACK received. TCP ACK splitting causes TCP to open the congestion window more quickly than usual, thus decreasing the effect of long latencies. TCP will generally open the congestion window by one maximum transmission unit (MTU) for each TCP ACK received. Opening the congestion window results in increased bandwidth becoming available. Configure this feature only when the satellite link is not using all the available bandwidth. Encrypted traffic cannot use TCP ACK splitting.

The *size* argument in the `ip rbscp ack-split` command determines how many TCP ACKs are generated from the incoming TCP ACK, as shown in the figure below.



If *n* ACKs are configured and *M* is the cumulative ACK point of the original TCP ACK, the resulting TCP ACKs exiting the router will have the following cumulative ACK points:

$M-n+1, M-n+2, M-n+3, \dots, M$

For example, if the *size* argument is set to 5, and the access list permits a TCP ACK with a cumulative ACK acknowledging bytes to 1000, then the resulting TCP ACKs exiting the router will have the following cumulative ACK points:

TCP ACK (996) (1000-5+1)

TCP ACK (997) (1000-5+2)

TCP ACK (998) (1000-5+3)

TCP ACK (999) (1000-5+4)

TCP ACK (1000) (1000-5+5)

## Access List-Based RBSCP Functionality

The Access List-Based RBSCP feature will accept a numbered or named, standard or extended IP access list. The access list controls which packets are subject to TCP ACK splitting. That is, the feature is applied to packets that a **permit** statement allows; the feature is not applied to packets that a **deny** statement filters.

An instance of this feature consists of an access list and an ACK split value. An ACK split value of 0 or 1 indicates that this feature is disabled (that is, no ACK split will be done). The ACK split value range is 0 through 32.

An interface can use only one instance of this feature at a time. Each instance of this feature can be used on multiple interfaces.

If you configure this feature but it refers to a nonexistent access list, this is interpreted as having an access list that denies all traffic from being processed by the access list-based RBSCP feature, so the feature is essentially disabled and the traffic goes through the normal switching path.

If both an RBSCP tunnel and an instance of the Access List-Based RBSCP feature are enabled along a routing or switching path, the TCP ACKs detunneled from the RBSCP tunnel will be ACK split according to the tunnel configuration and the Access List-Based RBSCP split parameters on the outgoing interface are effectively disabled.

## How to Configure Access List-Based RBSCP

- [Use RBSCP Selectively by Applying an Access List, page 4](#)

### Use RBSCP Selectively by Applying an Access List

This task illustrates how to apply the feature to an interface, and presumes that an access list is already configured. Perform this task by applying the access list on the router interface that is facing the internal network, not the satellite network.



#### Tip

---

The feature will try to process all the TCP flows as filtered by the access list. Try to make the access list applied to RBSCP as precise as possible to avoid unnecessary processing.

---

**Caution**

Plan your network carefully so that no more than one Cisco IOS router in a given routing path has this feature enabled. You do not want to recursively ACK split traffic.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip rbscp ack-split** *size* {*access-list-name* | *access-list-number*} **out**
5. Although it is not required, you should repeat this task on the router that is on the other side of the satellite, on the outgoing interface facing the network, not the satellite. Use a different access list.

**DETAILED STEPS**

Command or Action	Purpose
<b>Step 1</b> <b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b> <b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface ethernet 1	Specifies an interface. <ul style="list-style-type: none"> <li>• Specify an interface that is facing your internal network, opposite the satellite network.</li> </ul>
<b>Step 4</b> <b>ip rbscp ack-split</b> <i>size</i> { <i>access-list-name</i>   <i>access-list-number</i> } <b>out</b>  <b>Example:</b> Router(config-if)# ip rbscp ack-split 6 101 out	Configures RBSCP on the outgoing interface for packets that are permitted by the specified access list. <ul style="list-style-type: none"> <li>• The ACK split <i>size</i> determines the number of ACKs to send for every ACK received. An ACK split value of 0 or 1 indicates that this feature is disabled (that is, no ACK split will be done). The range is 0 through 32. See "TCP ACK Splitting".</li> <li>• In this example, access list 101 determines which packets are subject to TCP ACK splitting.</li> </ul>

Command or Action	Purpose
<b>Step 5</b> Although it is not required, you should repeat this task on the router that is on the other side of the satellite, on the outgoing interface facing the network, not the satellite. Use a different access list.	--

## Configuration Examples for Access List-Based RBSCP

- [Example Access List-Based RBSCP, page 6](#)

### Example Access List-Based RBSCP

In the following example, access list 101 performs TCP ACK splitting on packets going out FastEthernet interface 1/1 from a source at 1.1.1.1 to a destination at 3.3.3.1:

```

!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname IOSACL-72b
!
boot-start-marker
boot-end-marker
!
enable password lab
!
no aaa new-model
!
resource policy
!
ip cef
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
no cdp enable
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex full
speed 1000
media-type gbic
negotiation auto
no cdp enable
!
interface FastEthernet1/0
ip address 1.1.1.2 255.255.255.0
duplex half
no cdp enable
!
interface FastEthernet1/1
ip address 2.2.2.2 255.255.255.0
ip rbscp ack-split 4 101 out
duplex half
no cdp enable

```

```
!  
interface FastEthernet2/0  
  no ip address  
  shutdown  
  duplex half  
  no cdp enable  
!  
interface Serial3/0  
  no ip address  
  shutdown  
  serial restart-delay 0  
!  
interface Serial3/1  
  no ip address  
  shutdown  
  serial restart-delay 0  
  no cdp enable  
!  
interface Serial3/2  
  no ip address  
  shutdown  
  serial restart-delay 0  
  no cdp enable  
!  
interface Serial3/3  
  no ip address  
  shutdown  
  serial restart-delay 0  
  no cdp enable  
!  
interface FastEthernet4/0  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
  no cdp enable  
!  
interface FastEthernet4/1  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
  no cdp enable  
!  
router eigrp 100  
  network 1.0.0.0  
  network 2.0.0.0  
  auto-summary  
!  
no ip http server  
no ip http secure-server  
!  
logging alarm informational  
access-list 101 permit tcp host 1.1.1.1 host 3.3.3.1  
dialer-list 1 protocol ip permit  
!  
control-plane  
!  
gatekeeper  
  shutdown  
!  
!  
line con 0  
  exec-timeout 0 0  
  stopbits 1  
line aux 0  
  stopbits 1  
line vty 0 4  
  login  
!  
!  
end
```

## Additional References

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
IP access list commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Security Command Reference</i>
RBSCP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Interface and Hardware Component Command Reference</i>
Configuring Rate-Based Satellite Control Protocol (RBSCP)	“Implementing Tunnels” chapter in the <i>Cisco IOS Interface and Hardware Component Configuration Guide</i>

### Standards

Standard	Title
None	--

### MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### RFCs

RFC	Title
None	--



### Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## Feature Information for Access List-Based RBSCP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 1** Feature Information for Access List-Based RBSCP

Feature Name	Releases	Feature Information
Access List-Based RBSCP	12.4(9)T	<p>The Access List-Based Rate-Based Satellite Control Protocol feature allows you to selectively apply the TCP ACK splitting sub-feature of RBSCP to any outgoing interface. This feature has no tunneling or queueing overhead that is associated with RBSCP tunnels.</p> <p>The following commands are introduced or modified by this feature: <b>debug ip rbscp</b>, <b>debug ip rbscp ack-split</b>, <b>ip rbscp ack-split</b>.</p>

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)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2011 Cisco Systems, Inc. All rights reserved.

© 2012 Cisco Systems, Inc. All rights reserved.