Access List-Based RBSCP

First Published: June 19, 2006
Last Updated: June 19, 2006

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 compresssion, 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 in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Access List-Based RBSCP" section on page 15.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Contents

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

Prerequisites for Access List-Based RBSCP

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

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

Before you configure an access list-based RBSCP, you should understand the following concepts:

Benefits of Access List-Based RBSCP

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

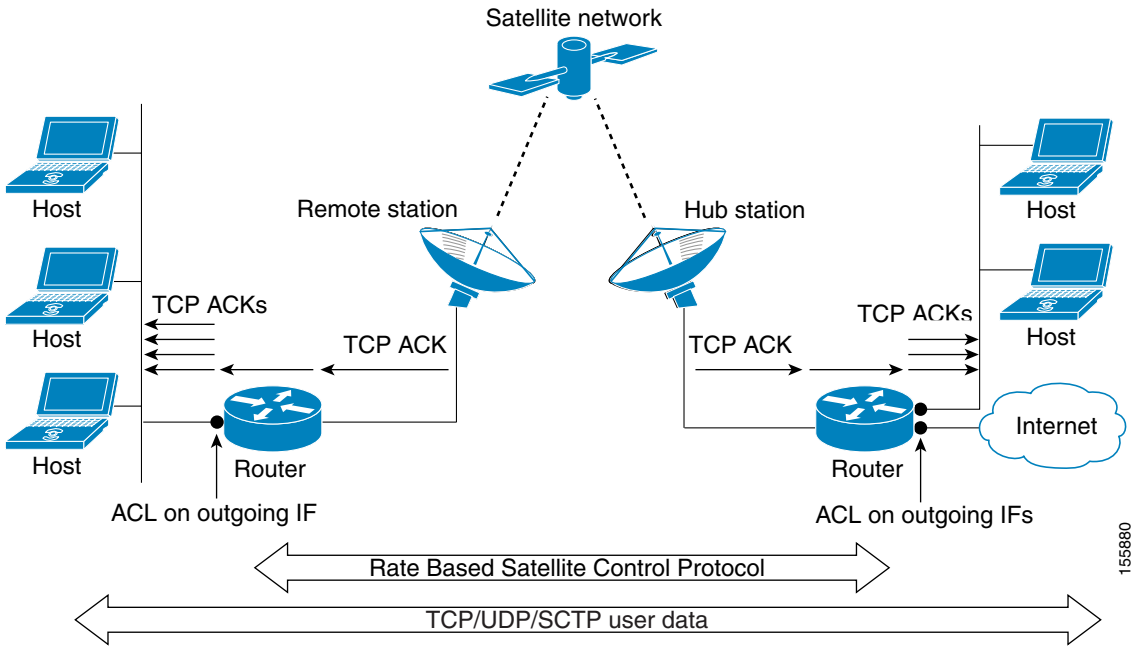
- It allows you to selectively apply the TCP ACK splitting feature of RBSCP to any outgoing interface. TCP ACK splitting is a benefit because it reduces the effect of long latencies characteristic of satellite links. Applying this feature selectively by using an access list is a benefit because you control 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 compresssion, 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 Figure 1. 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.

Figure 1 ACL-Based RBSCP on Outgoing Interfaces

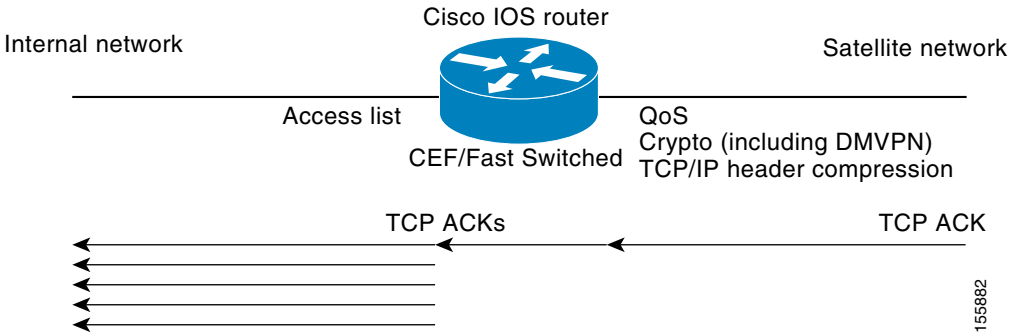


TCP ACK Splitting

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 Figure 2.

Figure 2 TCP ACK Splitting



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,...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

Perform the task in this section in order to use the TCP ACK splitting feature of RBSCP, based on an access list.

- Use RBSCP Selectively by Applying an Access List, page 5

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
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 1`	Specifies an interface. • Specify an interface that is facing your internal network, opposite the satellite network.

	Command or Action	Purpose
Step 4	**ip rbscp ack-split** *size* {*access-list-name* | *access-list-number*} **out** **Example:** `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. • The ACK split *size* 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, page 3. • In this example, access list 101 determines which packets are subject to TCP ACK splitting.
Step 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.	—

Configuration Examples for Access List-Based RBSCP

This section provides the following configuration example:

- Access List-Based RBSCP: Example, page 6

Access List-Based RBSCP: Example

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

The following sections provide references related to Access List-Based RBSCP.

Related Documents

Related Topic	Document Title
RBSCP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Interface and Hardware Component Command Reference, Release 12.4T*
IP access list commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference, Release 12.4T*
Configuring Rate-Based Satellite Control Protocol (RBSCP)	"Implementing Tunnels" chapter in the *Cisco IOS Interface and Hardware Component Configuration Guide, Release 12.4T*

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: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents the following new commands only:

- **debug ip rbscp**
- **debug ip rbscp ack-split**
- **ip rbscp ack-split**

debug ip rbscp

To display general error messages about access list-based Rate-Based Satellite Control Protocol (RBSCP), use the **debug ip rbscp** command in privileged EXEC mode. To disable debug output, use the **no** form of this command.

debug ip rbscp

no debug ip rbscp

Syntax Description

This command has no arguments or keywords.

Defaults

RBSCP debugging is disabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Caution Using this command will impact the router's forwarding performance.

Examples

The following is sample output from the **debug ip rbscp** command. The hexadecminal number is the sequence number to keep track of the flow.

```
Router# debug ip rbscp

*May 11 02:17:01.407: RBSCP process: 0x662852D0 passed access list
```

Related Commands

Command	Description
debug ip rbscp ack-split	Displays information about TCP ACK splitting done in conjunction with RBSCP.
ip rbscp ack-split	Configures the TCP ACK splitting feature of RBSCP on an outgoing interface for packets that are permitted by a specified access list.

debug ip rbscp ack-split

To display information about TCP ACK splitting done in conjunction with Rate-Based Satellite Control Protocol (RBSCP), use the **debug ip rbscp ack-split** command in privileged EXEC mode. To disable debug output, use the **no** form of this command.

debug ip rbscp ack-split

no debug ip rbscp ack-split

Syntax Description

This command has no arguments or keywords.

Defaults

RBSCP debugging for TCP ACKs is disabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Caution Using this command will impact the router's forwarding performance.

Examples

The following is sample output from the **debug ip rbscp ack-split** command when the packets match the access list applied to RBSCP. The output includes the source and destination IP addresses and port numbers, the hexadecimal sequence number, and the cumulative ACK that acknowledges bytes up to that number.

```
Router# debug ip rbscp ack-split

*May 11 02:17:01.407: RBSCP ACK split: 0x662852D0, input FastEthernet1/0 -> output
FastEthernet1/1
*May 11 02:17:01.407: RBSCP ACK split: rcvd src 1.1.1.1:38481 -> dst 3.3.3.1:21, cumack
2336109115
*May 11 02:17:01.407: RBSCP ACK split: generated 0x65FC0874 cumack 2336109112
*May 11 02:17:01.407: RBSCP ACK split: generated 0x66762A78 cumack 2336109113
*May 11 02:17:01.407: RBSCP ACK split: generated 0x6676442C cumack 2336109114
*May 11 02:17:01.407: RBSCP ACK split: releasing original ACK 2336109115
*May 11 02:17:01.415: RBSCP process: 0x662852D0 passed access list
*May 11 02:17:01.415: RBSCP ACK split: 0x662852D0, input FastEthernet1/0 -> output
FastEthernet1/1
*May 11 02:17:01.415: RBSCP ACK split: rcvd src 1.1.1.1:36022 -> dst 3.3.3.1:20240, cumack
4024420742
*May 11 02:17:01.415: RBSCP ACK split: generated 0x65FC1E7C cumack 4024420739
*May 11 02:17:01.415: RBSCP ACK split: generated 0x65FC2980 cumack 4024420740
*May 11 02:17:01.415: RBSCP ACK split: generated 0x65FC3484 cumack 4024420741
```

```
*May 11 02:17:01.415: RBSCP ACK split: releasing original ACK 4024420742
*May 11 02:17:01.419: RBSCP process: 0x662852D0 passed access list
*May 11 02:17:01.419: RBSCP ACK split: 0x662852D0, input FastEthernet1/0 -> output
FastEthernet1/1
```

Related Commands

Command	Description
debug ip rbscp	Displays general error messages about access list-based RBSCP.
ip rbscp ack-split	Configures the TCP ACK splitting feature of RBSCP on an outgoing interface for packets that are permitted by a specified access list.

ip rbscp ack-split

To configure the TCP ACK splitting feature of Rate-Based Satellite Control Protocol (RBSCP) on an outgoing interface for packets that are permitted by a specified access list, use the **ip rbscp ack-split** command in interface configuration mode. To disable the feature on the interface, use the **no** form of this command.

ip rbscp ack-split *size* {*access-list-name* | *access-list-number*} **out**

no ip rbscp ack-split

Syntax Description

size	Determines the number of TCP ACKs to send for every TCP ACK received. A *size* of 0 or 1 indicates that this feature is disabled (that is, no TCP ACK splitting will occur). The range is 0 through 32.
access-list-name | *access-list-number*	Standard or extended IP access list name or number that 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.
out	Specifies that this feature is applied to an outgoing interface.

Defaults

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command enables TCP ACK splitting for packets going out the interface that are permitted by the access list. 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.

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.

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.

Examples

In the following example, the access list performs TCP ACK splitting on packets going out Ethernet interface 0 from a source at 172.22.18.5 to a destination at 172.33.27.4:

```
ip access-list extended satellite
 permit tcp 172.22.18.5 172.33.27.4
 exit
interface ethernet 0
 ip rbscp ack-split 6 satellite out
```

Related Commands

Command	Description
debug ip rbscp	Displays general error messages about access list-based RBSCP.
debug ip rbscp ack-split	Displays information about TCP ACK splitting done in conjunction with RBSCP.

Feature Information for Access List-Based RBSCP

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Access List-Based RBSCP

Feature Name	Releases	Feature Information
Access List-Based RBSCP	12.4(9)T	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.