ACL IP Options Selective Drop

First Published: July 22, 2002
Last Updated: May 15, 2006

The ACL IP Options Selective Drop feature allows Cisco routers to filter packets containing IP options or to mitigate the effects of IP options on a router or downstream routers by dropping these packets or ignoring the processing of the IP options.

History for the ACL IP Options Selective Drop Feature

Release	Modification
12.0(22)S	This feature was introduced.
12.3(4)T	This feature was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This feature was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This feature was integrated into Cisco IOS Release 12.2(27)SBC.
12.0(32)S	Support was added for the Cisco 10720 Internet router.
12.3(19)	This feature was integrated into Cisco IOS Release 12.3(19).

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

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

Restrictions for ACL IP Options Selective Drop

- Resource Reservation Protocol (RSVP) (Multiprotocol Label Switching traffic engineering [MPLS TE]), Internet Group Management Protocol Version 2 (IGMPv2), and other protocols that use IP options packets may not function in drop or ignore modes.

- On the Cisco 10720 Internet router, the **ip option ignore** command is not supported. Only drop mode (the **ip option drop** command) is supported.

- The **ip option ignore** command (ignore mode) is supported only on the Cisco 12000 series router.

Information About ACL IP Options Selective Drop

Before you configure the ACL IP Options Selective Drop feature, you should understand the concepts in the following sections:

Using ACL IP Options Selective Drop

The ACL IP Options Selective Drop feature allows a router to filter IP options packets, thereby mitigating the effects of these packets on a router and downstream routers, and perform the following actions:

- Drop all IP options packets that it receives and prevent options from going deeper into the network.
- Ignore IP options packets destined for the router and treat them as if they had no IP options.

For many users, dropping the packets is the best solution. However, in environments in which some IP options may be legitimate, reducing the load that the packets present on the routers is sufficient. Therefore, users may prefer to skip options processing on the router and forward the packet as though it were pure IP.

Benefits of Using ACL IP Options Selective Drop

- Drop mode filters packets from the network and relieves downstream routers and hosts of the load from options packets.

- Drop mode minimizes loads to the Route Processor (RP) for options that require RP processing on distributed systems. Previously, the packets were always routed to or processed by the RP CPU. Now, the ignore and drop forms prevent the packets from impacting the RP performance.

How to Configure ACL IP Options Selective Drop

This section contains the following configuration information:

Configuring ACL IP Options Selective Drop

This section describes how to configure the ACL IP Options Selective Drop feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip options** {**drop** | **ignore**}
4. **exit**
5. **show ip traffic**

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	`ip options {drop	ignore}`  **Example:** `Router(config)# ip options drop`	Drops or ignores IP options packets that are sent to the router. **Note** On the Cisco 10720 Internet router, the **ip option ignore** command is not supported. Only drop mode (the **ip option drop** command) is supported.

Step 4	`exit`
	
	Example:
	`Router(config)# exit`
		Returns to privileged EXEC mode.

Step 5	`show ip traffic`
	
	Example:
	`Router# show ip traffic`
		(Optional) Displays statistics about IP traffic.

What to Do Next

If you are running Cisco IOS Release 12.3(4)T or a later release, you can also use the ACL Support for Filtering IP Options feature to filter packets based on whether the packet contains specific IP options. For more information, refer to *Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values*.

Configuration Example for ACL IP Options Selective Drop

This section provides the following configuration examples:

- Configuring ACL IP Options Selective Drop: Example, page 4
- Verifying ACL IP Options Selective Drop: Example, page 4

Configuring ACL IP Options Selective Drop: Example

The following example shows how to configure the router (and downstream routers) to drop all options packets that enter the network:

```
Router(config)# ip options drop

% Warning:RSVP and other protocols that use IP Options packets may not function in drop or
ignore modes.
end
```

Verifying ACL IP Options Selective Drop: Example

The following sample output is displayed after 15,000 options packets are sent using the **ip options drop** command. Note that the "forced drop" counter increases.

```
Router# show ip traffic

IP statistics:
  Rcvd:  15000 total, 0 local destination
         0 format errors, 0 checksum errors, 0 bad hop count
         0 unknown protocol, 0 not a gateway
         0 security failures, 0 bad options, 15000 with options
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 0 alert, 0 cipso
         0 other
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 couldn't fragment
  Bcast: 0 received, 0 sent
  Mcast: 0 received, 0 sent
  Sent:  0 generated, 0 forwarded
  Drop:  0 encapsulation failed, 0 unresolved, 0 no adjacency
         0 no route, 0 unicast RPF, 15000 forced drop
```

Additional References

The following sections provide references related to ACL IP Options Selective Drop.

Related Documents

Related Topic	Document Title
Configuring IP access lists	*Creating an IP Access List and Applying It to an Interface*
IP access list commands	*Cisco IOS Security Command Reference*
Using access lists for filtering IP options	*Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values*

Standards

Standards	Title
None	—

MIBs

MIBs	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

RFCs	Title
None	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features

- **ip options**

For information about these commands, see the Cisco IOS Security Command Reference at

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at

http://tools.cisco.com/Support/CLILookup or the Master Command List.