ACL Manageability

First Published: February 27, 2006
Last Updated: May 11, 2006

The ACL Manageability feature enables users to display and clear Access Control Entry (ACE) statistics per interface and per incoming or outgoing traffic direction for access control lists (ACLs).

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Restrictions for ACL Manageability

- ACL Manageability supports:
  - Only nondistributed software switched platforms.
  - Standard and extended statically configured ACLs, and Threat Mitigation Service (TMS) dynamic ACEs.

CISCO SYSTEMS

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

- ACL Manageability does not support:
  - Reflexive and user-configured dynamic ACLs and dynamic ACE blocks, such as Firewall and Authentication Proxy.
  - Virtual-template and Virtual-access interfaces.

Information About ACL Manageability

To configure the ACL Manageability feature, you should understand the following concepts:

- Benefits of ACL Manageability, page 2
- Support for Interface Level Statistics, page 2

Benefits of ACL Manageability

Previous to Cisco IOS Release 12.4(6)T, the ACL infrastructure in Cisco IOS software maintained only global statistics for each ACE in an ACL. With this method, if an ACL is applied to multiple interfaces, the maintained ACE statistics are the sum of incoming and outgoing packet matches (hits) on all the interfaces on which that ACL is applied.

However, if ACE statistics are maintained per interface and per incoming or outgoing traffic direction, users can view specific details of incoming and outgoing traffic patterns and the effectiveness of ACEs on the various interfaces of a network device. This type of information is useful for securing devices against attacks coming in on a particular interface.

Support for Interface Level Statistics

With Cisco IOS Release 12.4(6)T, the ACL infrastructure in Cisco IOS software is now extended to support the maintenance, display and clearing of ACE statistics per interface and per incoming or outgoing traffic direction for ACLs. This support is often referred to as “support for interface-level statistics.”

Note If the same access-group ACL is also used by other features, the maintained interface statistics are not updated when a packet match is detected by the other features. In this case, the sum of all the interface level statistics that are maintained for an ACL may not add up to the global statistics for that ACL.

How to Display Interface Level Statistics

This section contains the following procedures:

- Displaying Interface Level Statistics, page 3
- Display Examples for the ACL Manageability Feature, page 3

Displaying Interface Level Statistics

This section describes how to display and clear ACE statistics per interface and per incoming or outgoing traffic direction for ACLs.

SUMMARY STEPS

1. **enable**
2. **show ip access-list** [*access-list-number* | *access-list-name* | **dynamic** *access-list-name* | **interface** *interface-name* [**in** | **out**]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip access-list** [*access-list-number*	*access-list-name*	**dynamic** *access-list-name*	**interface** *interface-name* [**in**	**out**]] **Example:** `Router# show ip access-list interface FastEthernet 0/0 in`	Displays input statistics for the FastEthernet interface.

Example

The following example displays input statistics for the FastEthernet interface 0/0.

```
Router# show ip access-lists interface FastEthernet 0/0 in

Extended IP access list 150 in
   10 permit ip host 10.1.1.1 any
   30 permit ip host 10.2.2.2 any (15 matches)
```

Display Examples for the ACL Manageability Feature

This section provides the following display examples:

Displaying Input Statistics: Example

The following example displays input statistics gathered from the FastEthernet interface 0/1, associated with access list 150 (ACL number):

```
Router# show ip access-list interface FastEthernet 0/1 in

Extended IP access list 150 in
   10 permit ip host 10.1.1.1 any (3 matches)
   30 permit ip host 10.2.2.2 any (12 matches)
```

Displaying Global Statistics: Example

The following example displays global statistics for ACL 150:

```
Router# show ip access-list 150

Extended IP access list 150
   10 permit ip host 10.1.1.1 any (3 matches)
   30 permit ip host 10.2.2.2 any (27 matches)
```

Displaying Output Statistics: Example

The following example displays output statistics gathered from the FastEthernet interface 0/0:

```
Router# show ip access-list interface FastEthernet 0/0 out

Extended IP access list myacl out
    5 deny ip any 10.1.0.0 0.0.255.255
    10 permit udp any any eq snmp (6 matches)
```

Displaying Input and Output Statistics: Example

Note If no direction is specified, any input and output ACLs applied to that interface are displayed.

The following example displays input and output statistics gathered from the FastEthernet interface 0/0:

```
Router# show ip access-list interface FastEthernet 0/0

Extended IP access list 150 in
   10 permit ip host 10.1.1.1 any
   30 permit ip host 10.2.2.2 any (15 matches)
Extended IP access list myacl out
    5 deny ip any 10.1.0.0 0.0.255.255
    10 permit udp any any eq snmp (6 matches)
```

Clear Global and Interface Statistics: Example

The following example clears global and interface statistics for ACL 150:

```
Router# clear ip access-list counters 150
```

The following example clears global and interface statistics for all ACLs:

```
Router# clear ip access-list counters
```

Additional References

The following sections provide references related to the ACL Manageability feature.

Related Documents

Related Topic	Document Title
Configuring various aspects of security, including terminal access security, network access security, accounting, traffic filters, router access, and network data encryption with router authentication.	*Cisco IOS Security Configuration Guide*, Release 12.4T
Detailed information about the commands used in the configuration guide.	*Cisco IOS Security Command Reference*, Release 12.4T

Standards

Standard	Title
No new or modified standards are supported by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	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
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

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, and tools. 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 modified commands only.

- **show ip access-list**
- **debug ip access-list intstats**

show ip access-list

To display the contents of all current IP access lists, use the **show ip access-list** command in user EXEC or privileged EXEC mode.

show ip access-list [*access-list-number* | *access-list-name* | **dynamic** *access-list-name* | **interface** *interface-name* [**in** | **out**]]

Syntax Description

access-list-number	(Optional) Number of the IP access list to display.
access-list-name	(Optional) Name of the IP access list to display.
dynamic *access-list-name*	(Optional) Displays the specified dynamic IP access lists.
interface *interface-name*	(Optional) Displays the access list for the specified interface.
in	(Optional) Displays input interface statistics.
out	Optional) Displays output interface statistics.

Defaults

All standard and extended IP access lists are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.3(7)T	The **dynamic** keyword was added.
12.4(6)T	The **interface** and **in** and **out** keywords were added.

Usage Guidelines

The **show ip access-list** command provides output identical to the **show access-lists** command, except that it is IP specific and allows you to specify a particular access list.

Examples

The following is sample output from the **show ip access-list** command when all access lists are requested:

```
Router# show ip access-list

Extended IP access list 101
   deny udp any any eq ntp
   permit tcp any any
   permit udp any any eq tftp
   permit icmp any any
   permit udp any any eq domain
```

The following is sample output from the **show ip access-list** command when the name of a specific access list is requested:

```
Router# show ip access-list Internetfilter

Extended IP access list Internetfilter
   permit tcp any 10.31.0.0 0.0.255.255 eq telnet
   deny tcp any any
   deny udp any 10.31.0.0 0.0.255.255 lt 1024
   deny ip any any log
```

The following is sample output from the **show ip access-list** command, which shows input statistics from the FastEthernet interface 0/0:

```
Router# show ip access-list interface FastEthernet 0/0 in

Extended IP access list 150 in
   10 permit ip host 10.1.1.1 any
   30 permit ip host 10.2.2.2 any (15 matches)
```

debug ip access-list intstats

To display debugging information about access control lists (ACLs) interface level statistics, use the **debug ip access-list intstats** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip access-list intstats

no debug ip access-list intstats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.
12.4(6)T	This command was modified to include support for ACL interface level statistics.

Usage Guidelines

The **debug ip access-list intstats** command is useful for debugging problems associated with ACL interface level statistics. These interface level statistics are ACL statistics that are maintained per interface and per traffic direction (input/output). This means that when a packet matches an entry in an ACL, the corresponding ACL statistics are updated for the interface on which the ACL is applied and the direction (input/output) in which the ACL is applied.

Examples

The following example is sample output from the **debug ip access-list intstats** command:

```
Router# debug ip access-list intstats

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip access-group 150 in
000042: *Mar 14 11:36:04.367 UTC: IPACL-INTSTATS: ACL swsb created
000043: *Mar 14 11:36:04.367 UTC: IPACL-INTSTATS: ACL header stats structure created
000044: *Mar 14 11:36:04.367 UTC: IPACL-INTSTATS: I/P stats table created
000045: *Mar 14 11:36:04.367 UTC: IPACL-INTSTATS: Statsid bitmap created
000046: *Mar 14 11:36:04.367 UTC: IPACL-INTSTATS: Done with static ACEs

Router(config-if)# no ip access-group 150 in
000047: *Mar 14 11:36:36.575 UTC: IPACL-INTSTATS: Freeing I/P stats table
000048: *Mar 14 11:36:36.575 UTC: IPACL-INTSTATS: Succesfully removed ACL from interface
000049: *Mar 14 11:36:36.575 UTC: IPACL-INTSTATS: ACL swsb destroyed
```

Related Commands	Command	Description
	show ip access-list	Displays the contents of all current IP access lists.

Feature Information for ACL Manageability

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.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

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 ACL Manageability

Feature Name	Releases	Feature Information
ACL Manageability	12.4(6)T	The ACL Manageability feature enables users to display and clear Access Control Entry (ACE) statistics per interface and per incoming or outgoing traffic direction for access control lists (ACLs). In 12.4(6)T, this feature was introduced.