Access List Performance Improvements for Cisco 12000 Gigabit Switch Routers

Feature Overview

Access list (ACL) performance improvements are provided for two types of Cisco 12000 line cards:

- Line cards using engine 1 architecture
- Line cards using engine 2 architecture

The ACL performance improvement is implemented in a slightly different way depending on the line card type. Engine 1 line cards achieve ACL performance improvement strictly through hardware, using an improved ASIC design. Engine 2 line cards use a microcode enhancement in the packet switch ASIC (PSA) . Table 1 lists the line cards and the ACL performance improvement type.

Table 1 Line Card Engines, Line Cards, and Performance Improvement

Line Card Type	Line Cards	ACL Performance Improvement Type
Engine 1	Gigabit Ethernet 8-port Fast Ethernet	SALSA (achieved through ASIC design enhancement)
Engine 2	Enhanced OC-48 and QOC-12	PSA (achieved through ASIC microcode enhancement)

Benefits

ACL performance improvement requires separate solutions for the two line card types.

Hardware ACL Acceleration on Engine 1 Line Cards

Prior to hardware ACL acceleration, access lists were processed by the line card CPU. Access list processing occurred one entry at a time. In other words, the entire access list must be scanned one line at a time for each incoming packet. List processing performance is proportional to the number of ACL entries in the list. As access list size increases, performance degrades.

The first level of improvement was to add compiled ACL support for the line cards. Compiled ACLs rely on a compiled access list, and use lookup tables in the software to improve overall ACL processing speed. No special hardware improvements are required to support compiled ACLs. However, compiled ACLs still rely on CPU processing and can affect performance.

Implementing ACL processing in the hardware (the SALSA ASIC) increases packet switching performance. On engine 1 line cards, the line card CPU is no longer burdened with ACL processing.

ACL Performance Improvement on Engine 2 Line Cards

The situation is different for engine 2 line cards. Instead of being implemented directly in the ASIC design, engine 2 line cards rely on microcode for the PSA to achieve ACL performance improvement.

While engine 2 line cards perform very high speed forwarding by using a combination of microcode and hardware lookups, the line cards cannot apply ACLs because the line card CPU is not involved in packet forwarding path. Without the microcode enhancements in the PSA, access lists are not applied at all.

Restrictions

ACL performance improvement for engine 1 line cards is subject to the following restrictions:

- Only input ACLs are supported.
- Subinterfaces are not supported.
- If other features such as input committed access rate (CAR), output CAR, or output ACL are enabled, the performance improvement provided by the ACL hardware acceleration may be limited because these other features are checked by the linecard software.

ACL performance improvement for engine 2 line cards is subject to the following restrictions. If these limitations are not met, packets are not processed by the PSA microcode. Instead, they are processed by the line card CPU:

- There is a limit to the number of ACL entries that can be processed by the PSA microcode because of memory limitations of the table structures created in SDRAM and SRAM.
- A maximum of 16 input interfaces per line card and 128 ACL entries per interface are supported.
- A maximum of 5 output interfaces and 128 ACL entries per interface are supported.
- When you configure PSA ACL performance improvement on input and output interfaces on the same line card, the output ACL is processed by the CPU.
- Subinterfaces are not supported.
- The following ACL features are not supported in the microcode and will be passed to the line card CPU for processing:
  - Source port
  - Type of service
  - Precedence
  - Logging
  - IGMP
  - Debugging

Platforms

This feature is supported on the following Cisco 12000 series routers:

- Cisco 12016 series
- Cisco 12012 series
- Cisco 12008 series

This feature is supported on the following Cisco 12000 line cards (see Table 1):

- Line cards using engine 1 architecture
- Line cards using engine 2 architecture

Prerequisites

You must be running Cisco IOS Release 12.0(10)S or a later version of Cisco IOS Release 12.0 S.

Supported MIBs and RFCs

None.

Configuration Tasks

Perform the following tasks to configure ACL performance improvement on an interface:

- Configure ACL Performance Improvement on Engine 1-type Line Cards
- Configure ACL Performance Improvement on Engine 2-type Line Cards

Configure ACL Performance Improvement on Engine 1-type Line Cards

To configure ACL performance improvement on an engine 1 line card, perform the following task in global configuration mode:

Step	Command	Purpose
1	`Router(config)# access-list hardware salsa`	Enables ACL performance improvement on all engine 1 line cards.

Configure ACL Performance Improvement on Engine 2-type Line Cards

To configure ACL performance improvement on an engine 2 line card and enable ACL on input and output interfaces, perform the following task in global configuration mode:

Step	Command	Purpose
1	`Router(config)# access-list hardware psa`	Enables ACL performance improvement and ACL output processing on all engine 2 line cards.

Verifying ACL Performance Improvement Configuration on Engine 1 Line Cards

Use the following **execute on slot** EXEC commands to view and verify the performance improvement operations on engine 1-type line cards:

- **execute on slot** *slot* **show controller l3 | include ASIC**

  If the output shows Revision number (Rev) 4, or greater, the linecard has the Rev 4 SALSA ASIC and supports ACL performance improvement.

- **execute on slot** *slot* **show access-list hardware** *port-number*

  This command shows which fields in the TCP/IP header are used for hashing and the average number of nodes for typical types of traffic (for example, TCP, WWW, UDP).

  The displayed Rev 4 SALSA ACL hardware lookup registers include Config register, which shows whether Rev 4 SALSA ACL is enabled.

  The per packet registers show details of the ACL node visited by the last packet and the number of nodes traversed by the ACL hardware for the ACL lookup.

  The Rev 4 SALSA ACL counters display the number of packets with and without errors. These counters are cleared by the **clear access-list counters** on the linecard.

- **execute on slot** *slot* **show access-list hardware <***port-number***> detail**

  For each entry in the hash table, this shows the ACL tree of nodes. All nodes in successive match branch in the ACL tree are consecutively displayed. At the end of the match branch (STOP node), it recursively displays all the nodes in the miss branch of the starting node. It also shows the total number of ACL nodes and the current allocated nodes.

  Use this command sparingly for large ACLs (100+ lines) because of the large number of nodes displayed when used with **execute on slot** *slot-number.*

  To display a single entry in the ACL hash table—for example, by looking at a given packet and choosing bits in the TCP/IP header based on the ACL hash bits in **show access-list hardware**—use the following command:

  execute on slot *slot* **show access-list hardware** *port-number* **detail index** *index-val*

- **execute on slot** *slot* **show access-list hardware** *port-number* **error**

  This command displays the ACL hardware register, status and counters as in "**show access-list hardware** *port-number*" and also error details such as ACL node and timestamp, that will show the history/log of errors.

- **execute on slot** *slot* **show access-list psa summary**

  This command displays the ACL state and additional details for engine 2-type line cards.

Monitoring and Maintaining ACL Performance Improvements

Command	Purpose
`Router# execute on slot slot clear access-list counters`	Clears the ACL hardware counters.

Configuration Examples

This section provides the following configuration examples:

- Gigabit Ethernet Line Card (Engine 1)
- QOC-12 ATM Line Card (Engine 2)

Gigabit Ethernet Line Card (Engine 1)

The following configuration example shows how to enable ACL performance improvements on all Gigabit Ethernet line cards (engine 1) in a GSR:

```
access-list hardware salsa
```

QOC-12 ATM Line Card (Engine 2)

The following configuration example shows how to enable ACL performance improvements on all QOC-12 ATM line cards (engine 2) in a GSR:

```
access-list hardware psa
```

Note You must configure an engine 2 line card for ACL performance improvements in order to process any access lists on that line card. The ACL processing with performance improvements occurs on the input side. ACL processing on the output side is performed by the line card CPU.

Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command references.

- **access-list hardware**
- **show access-list psa summary**

access-list hardware

To configure line cards in a Cisco 12000 GSR to use access list (ACL) performance improvements, use the **access-list hardware** global configuration command. Use the no form of this command to disable ACL performance improvements

[**no**] **access-list hardware** {**salsa** | **psa** }

Syntax Description

salsa	Enables ACL performance improvements on engine 1 line cards.
psa	Enables ACL performance improvements on engine 2 line cards.

Defaults

No default behavior or values.

Command Modes

Global

Command History

Release	Modification
12.0(10)S	This command was first introduced.

Usage Guidelines

You must use this command to enable the ACL performance enhancements on the engine 1 or engine 2 line cards. Table 2 lists the line cards and the ACL performance improvement type. Using this command has no effect when non-supported line cards are installed in the GSR.

Table 2 Line Card Engines, Line Cards, and Performance Improvement

Line Card Type	Line Cards	ACL Performance Improvement Type
Engine 1	Gigabit Ethernet 8-port Fast Ethernet	SALSA (achieved through ASIC design enhancement)
Engine 2	Enhanced OC-48 and QOC-12	PSA (achieved through ASIC microcode enhancement)

Note You must configure an engine 2 line card for ACL performance improvements in order to process any access lists on that line card. The ACL processing with performance improvements occurs on the input side. ACL processing on the output side is performed by the line card CPU.

Examples

The following example enables ACL performance improvements on all Gigabit Ethernet line cards (engine 1-type) in a GSR:

```
access-list hardware salsa
```

Related Commands

None

show access-list psa summary

To display the state of the ACL and list summary information on engine 2-type line cards in a Cisco 12000 GSR, use the **show access-list psa summary** line card command.

show access-list psa summary

Syntax Description

None

Defaults

No default behavior or values.

Command Modes

Line card

Command History

Release	Modification
12.0(10)S	This command was first introduced.

Usage Guidelines

Use the **execute on** *slot* EXEC command to selet which line card will run the **show access-list psa summary** command.

Examples

The following example displays PSA ACL information for an engine 2-type line card in a GSR:

```
router# execute on 4 show access-list psa summary

PSA ACL Configured:yes, Running:yes
Access list limits:4 ingress, 5 egress (max 128 lines each)
ACL in microcode configured in input direction (Input ACL microcode loaded)

Input interface:0    1    2    3
ACL total lines:1    0    0    0
Lines on cpu:   0    0    0    0
Access List :   150  -    -    -
Run state:      mic  off  off  off

Total ACL memory allocated. PLU:5120 KBytes TLU:16 KBytes SRAM:8 KBytes
Mtrie prefixes with access lists. Src:1 Dst :2
TLU memory used for prefixes:0 Kbytes

ACL Timing Statistics
List Changes:1         Average Time taken:492.0ms
Input Interface Changes:0
Output Interface Changes:0
Times microcode loaded. ACL:1 Other:0
```

Related Commands

None

Debug Commands

This section documents new or modified **debug** commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command references.

- **debug ip access-list hardware**
- **debug ip access-list detail**
- **debug ip access-list lookup**

debug ip access-list hardware

To display debug messages for the ACL hash table and the number of nodes for each ACL line, use the **debug ip access-list hardware** privileged EXEC command. Use the **no** form of the command to disable debugging output.

[**no**] **debug ip access-list hardware**

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging for IP access hardware is not enabled.

Command History

Release	Modification
12.0(10)S	This command was first introduced.

Usage Guidelines

This command is for engine 1 line cards only.

Examples

The following example shows output when a hash table is built and you use the **debug ip access-list hardware** command.

```
example to be supplied
```

Related Commands

Command	Description
debug ip access-list detail	Displays debug messages for every node in the ACL hash table.
debug ip access-list lookup	Displays debug messages on a per packet basis.

debug ip access-list detail

To display debug messages for the every node for each ACL line in the hash table, use the **debug ip access-list detail** privileged EXEC command. Use the **no** form of the command to disable debugging output.

[**no**] **debug ip access-list detail**

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging for IP access hardware is not enabled.

Command History

Release	Modification
12.0(10)S	This command was first introduced.

Usage Guidelines

This command is for engine 1 line cards only.

Examples

The following example shows output when a hash table is built and you use the **debug ip access-list detail** command.

```
example to be supplied
```

Related Commands

Command	Description
debug ip access-list hardware	Displays debug messages for the ACL hash table.
debug ip access-list lookup	Displays debug messages on a per-packet basis

debug ip access-list lookup

To display debug messages for the every node for each ACL line in the hash table, use the **debug ip access-list lookup** privileged EXEC command. Use the **no** form of the command to disable debugging output.

[**no**] **debug ip access-list lookup**

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging for IP access hardware is not enabled.

Command History

Release	Modification
12.0(10)S	This command was first introduced.

Usage Guidelines

This command is for engine 1 line cards only.

Examples

The following example shows output when a hash table is built and you use the **debug ip access-list lookup** command.

```
example to be supplied
```

Related Commands

Command	Description
debug ip access-list hardware	Displays debug messages for the ACL hash table.
debug ip access-list detail	Displays debug messages on a per-packet basis