Turbo Access Control List Scalability Enhancements

First Published: December 5, 2006
Last Updated: December 5, 2006

The Turbo Access Control List (ACL) Scalability Enhancements feature introduced in Cisco IOS Release 12.2(31)SB2 improves overall performance on the Cisco 7304 router using a Network Services Engine (NSE) by allowing Turbo ACLs to be processed in PXF using less memory, thereby allowing more traffic traversing the Cisco 7304 router using an NSE to be PXF-accelerated. This feature also introduces user-configuration options that allow users to define the amount of memory used for Turbo ACL purposes in the Route Processor (RP) processing path.

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 Turbo ACL Scalability Enhancements on the NSEs" section on page 24.

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 Turbo Access Control List Scalability Enhancements on the NSEs

Because the portion of this feature that more expediently removes older entries works in the PXF processing path, PXF must be enabled for this particular functionality to have any benefit. PXF processing is enabled by default.

Restrictions for Turbo Access Control List Scalability Enhancements on the NSEs

This feature is not available for Cisco 7304 routers using an NPE-G100.

Information About Turbo Access Control List Scalability Enhancements on the NSEs

To benefit from the Turbo Access Control List Scalability Enhancements for the NSEs, you should understand the following concepts:

How Turbo ACL on the Cisco 7304 Router Using an NSE Works

With the exception that most Turbo ACL classification is PXF-accelerated on a Cisco 7304 router using an NSE-100 or an NSE-150, Turbo ACL classification on the Cisco 7304 router using an NSE-100 or NSE-150 is similar in behavior to Turbo ACL on other platforms. For information on Turbo ACL, see *Turbo Access Control Lists*.

For information on PXF on Cisco 7304 routers using an NSE-100 or an NSE-150, including the Turbo ACL features that are PXF-accelerated, see *PXF Information for the Cisco 7304 Router*.

How Turbo ACL Scalability Enhancements on the NSEs Improves Overall PXF Performance

The memory allocated in PXF for Turbo Access Control Lists (ACLs) on the NSE-100 especially is limited to the point where even modestly-sized ACL configurations cause a large amount of PXF memory to be used for Turbo ACL processing. As a result, a large amount of network traffic that should be processed through the PXF processing path is instead processed through the RP path.

This enhancement is part of a series of enhancements to improve Turbo ACL functionality on the Cisco 7304 router using the NSE-100. Specifically, this feature keeps the entries for PXF-based Turbo ACL classification current by more actively removing older entries. The older entries, which are no longer used for current traffic flows, still consume memory and, therefore, cause traffic that would normally be PXF-accelerated to instead be punted to the RP. This portion of the feature, which does not require user configuration, improves overall traffic flow on the Cisco 7304 router using an NSE by allowing more network traffic to be PXF-accelerated.

How Turbo ACL Scalability Enhancements on the NSEs Improves Overall Route Processing Performance

These Turbo ACL scalability enhancements also introduce an enhancement that allows users, via configuration commands, to configure the amount of memory reserved for ACL processing on the RP. The ability to configure the amount of memory reserved for ACL processing in the RP path gives users the option either to improve ACL processing performance in the RP path by reserving more memory for ACL processing, or to improve all other RP path functionality by reserving less memory for ACL processing.

In Cisco IOS releases not containing this feature, the amount of memory reserved for RP ACL handling is fixed.

Understanding Memory Limits for Turbo ACL Processes on the Route Processor

An NSE-150 has 2 GB of DRAM. NSE-100 RAM is user-configurable using an SDRAM SODIMM. While most NSE-100s have 512 MB of RAM, 256-MB and 128-MB SDRAM SODIMMs for the NSE-100 exist.

On a Cisco 7304 router using an NSE-150, the default memory limit for Turbo ACL processes (such as classification, compilation, and table storage) of Layer 3 and Layer 4 data in the RP path is always 256 MB. The default memory limit for Turbo ACL processes for Layer 2 data in the RP path for a Cisco 7304 router using an NSE-150 is always 128 MB.

On a Cisco 7304 router using an NSE-100, the default amount of memory reserved for Turbo ACL processes in the RP path is dependant upon the amount of SDRAM configured on the NSE-100. If the NSE has 512 MB of SDRAM or more, the default memory limit for Turbo ACL processes for Layer 3 and Layer 4 traffic processing is 256 MB. If the processor has less than 512 MB of SDRAM, the default memory limit for Turbo ACL processes for Layer 3 and Layer 4 traffic is 128 MB.

The default amount of memory reserved for Layer 2 Turbo ACL processes for a Cisco 7304 router using an NSE-100 is always 128 MB, regardless of the amount of memory configured on the processor.

To see the default amount of memory reserved for Layer 2 or for Layer 3 and Layer 4 Turbo ACL processing on your Cisco 7304 router, enter the **show access-list compiled** command. The “Mb default limit” output, which appears in both the “Compiled ACL statistics for IPv4” and “Compiled ACL

statistics for Data-Link" sections of the output, shows you the default memory reservations for either Layer 2 or Layer 3 and Layer 4 Turbo ACL processing. See the "Monitoring Turbo ACL Memory Usage in the Route Processing Path" section on page 5 for a more detailed explanation of this procedure.

To change the default amount of memory reserved for Layer 2 or Layer 3 and Layer 4 Turbo ACL processing on your Cisco 7304 router, enter the **access-list compiled** [**ipv4** | **data-link**] **limit memory** *number* command.

To restore the default amount of memory reserved for Layer 2 or Layer 3 and Layer 4 Turbo ACL processing on your Cisco 7304 router, enter the **default access-list compiled** [**ipv4** | **data-link**] **limit memory** command.

To learn more about the SDRAM SODIMMs that determine the amount of SDRAM available for Cisco 7304 routers using an NSE-100, see *NSE-100 Memory Information*.

Benefits

Improved Traffic Flow

This feature improves the Turbo ACL processing process in PXF by more expediently removing older entries. As a result, more Turbo ACL processing can be done in the PXF processing path, thereby allowing more router traffic to be accelerated using the PXF processing path.

Configuration of Route Processor Memory Limits for ACL Processing

This feature allows users to set the amount of memory reserved for ACL processes (such as compilation, storage, and classification) in the RP path. Users who need more memory for ACL processes now have the ability to set aside additional memory resources in the RP path for ACL processes. Users who need more more memory for other processes in the RP path now can set aside less memory for ACL processes.

How to Configure Turbo Access Control List Scalability Enhancements on the NSEs

It is important to note that the portion of this feature that more expediently removes older ACL entries for ACLs being processed in the PXF processing path occurs automatically without user configuration.

The following sections contain procedures for configuring memory reservations for Turbo ACL processing on the RP:

Monitoring Turbo ACL Memory Usage in the Route Processing Path

Before setting the actual memory limits for RP-based Turbo ACL usage, it may be helpful to gather information regarding the amount of memory being used for Turbo ACL usage.

To monitor your Turbo ACL memory usage in the RP path, you must complete the following steps.

SUMMARY STEPS

1. **enable**
2. **show access-list compiled**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show access-list compiled** **Example:** `Router# show access-list compiled`	Displays the status and condition of the Turbo ACL tables associated with each access list. When using this command to verify memory limitation settings for Turbo ACL processing, look for the following: • The output for **show access-list compiled** is separated for Layer 2 and for Layer 3 and Layer 4 data. Layer 3 and Layer 4 ACL compilation tables and information can be seen in the "Compiled ACL statistics for IPv4" section of the output, while Layer 2 ACL compilation tables and information can be seen in the "Compiled ACL statistics for Data-Link" section. • The "mem limits" output that shows the number of times a compile has occurred and the ACL has reached its configured limit. • The "Mb limit" output that shows the current memory limit setting. • The "Mb max memory" output that shows the maximum amount of memory the current ACL configuration could actually consume under maximum usage conditions. For additional information and an example, see the "Monitoring Memory Limitations for Layer 2 or Layer 3 and Layer 4 ACL Processing: Example" section on page 14.

Configuring a User-Defined Memory Limitations for Turbo ACL Processing of Layer 3 and Layer 4 Data in the Route Processing Path

To enable memory limitations for Turbo ACL processing of Layer 3 and Layer 4 data in the RP path, you must complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list compiled ipv4 limit memory** *number*

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	**access-list compiled ipv4 limit memory** *number* **Example:** `Router(config)# access-list compiled ipv4 limit memory 300`	Specifies the limit, in megabytes, reserved for Turbo ACL instance 0, which is used for processing Layer 3 and Layer 4 data.

Removing Memory Limits for Turbo ACL Processing of Layer 3 and Layer 4 Data in the Route Processing Path

Removing all memory limits for Turbo ACL processes in the Route Processor allows all route processing memory to be used for Turbo ACL processing of Layer 3 and Layer 4 data, if necessary. It is important to note that this functionality is not used to remove a previously configured limit, even though it is a **no** form of a command.

To remove all memory limits for Turbo ACL processing for Layer 3 and Layer 4 data and to allow as much memory as needed for Layer 3 and Layer 4 Turbo ACL processing in the RP path, you must complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no access-list compiled ipv4 limit memory**

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	**no access-list compiled ipv4 limit memory** **Example:** `Router(config)# no access-list compiled ipv4 limit memory`	Removes any memory limits for Layer 3 and Layer 4 Turbo ACL processing, thereby allowing all available memory to be used for Layer 3 and Layer 4 Turbo ACL processing, if necessary.

Restoring the Default Memory Limits for Turbo ACL Processing of Layer 3 and 4 Data in the Route Processing Path

The default memory limit for Turbo ACL processing of Layer 3 and Layer 4 data in the RP path is always 256 MB on the NSE-150.

On the NSE-100, the default memory limit for Turbo ACL processing of Layer 3 and Layer 4 data in the RP path is dependant on the amount of memory on your NSE-100. If you have more than 512 MB of memory configured on your processor, your default memory limit for RP-based Turbo ACL processing is 256 MB. If you have less than 512 MB of memory, your default memory limit for RP-based Turbo ACL processing is 128 MB.

To restore the default RP memory limit settings for Turbo ACL processing of Layer 3 and Layer 4 traffic, you must complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **default access-list compiled ipv4 limit memory**

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	**default access-list compiled ipv4 limit memory** **Example:** `Router(config)# default access-list compiled ipv4 limit memory`	Restores the default memory limit setting for Layer 3 and Layer 4 Turbo ACL traffic processing. The default memory limit for Turbo ACL processing of Layer 3 and Layer 4 data in the RP path is always 256 MB on the NSE-150. On the NSE-100, the default memory limit for Turbo ACL processing of Layer 3 and Layer 4 data in the RP path is dependant on the amount of memory on your NSE-100. If you have more than 512 MB of memory configured on your processor, your default memory limit for RP-based Turbo ACL processing is 256 MB. If you have less than 512 MB of memory, your default memory limit for RP-based Turbo ACL processing is 128 MB.

Configuring a User-Defined Memory Limitation for Turbo ACL Processing of Layer 2 Data in the Route Processing Path

To enable a memory limitation setting for Turbo ACL processing of Layer 2 data in the RP path, you must complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list compiled data-link limit memory** *number*

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	**access-list compiled data-link limit memory** *number* **Example:** `Router(config)# access-list compiled data-link limit memory 150`	Specifies the limit, in megabytes, reserved for Turbo ACL instance 1, which is used by the Turbo ACL algorithm to classify Layer 2 frames.

Removing Memory Limits for Turbo ACL Processing of Layer 2 Data in the Route Processing Path

Removing all memory limits for Turbo ACL processing of Layer 2 data in the Route Processor allows all route processing memory to be used for Turbo ACL processing of Layer 2 data, if necessary. It is important to note that this functionality is not used to remove a previously configured limit, even though it is a **no** form of a command.

To remove all RP-based memory limits for Turbo ACL processing for Layer 2 data and to allow as much memory as needed for Layer 2 Turbo ACL processing, you must complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no access-list compiled data-link limit memory**

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	**no access-list compiled data-link limit memory** **Example:** `Router(config)# no access-list compiled data-link limit memory`	Removes any memory limits for Layer 2 Turbo ACL processing, thereby allowing all available memory to be used for Layer 2 Turbo ACL processing, if necessary.

Restoring the Default Memory Limits for Turbo ACL Processing of Layer 2 Data in the Route Processing Path

The default memory limit for Turbo ACL processing of Layer 2 data in the RP processing path is 128 MB for the NSE-100 and NSE-150.

To restore the default RP-based memory limit setting for Turbo ACL processing of Layer 2 data, you must complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **default access-list compiled data-link limit memory**

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	**default access-list compiled data-link limit memory** **Example:** `Router(config)# default access-list compiled data-link limit memory`	Restores the default memory limit setting for Layer 2 Turbo ACL processing. The default memory limit setting for Layer 2 Turbo ACL processing is always 128 MB.

Verifying Memory Limitation Settings for Turbo ACL Processing

To verify RP-based memory limitation settings for Turbo ACL processing, you must complete the following steps.

SUMMARY STEPS

1. **enable**
2. **show access-list compiled**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show access-list compiled** **Example:** `Router# show access-list compiled`	Displays the status and condition of the Turbo ACL tables associated with each access list. When using this command to verify memory limitation settings for Turbo ACL processing, look at the "Mb limit" output for both IPv4 and Data-Link. The new MB limit setting should be listed in the "Mb limit" output for IPv4 or Data-Link, depending on which memory limit was changed. For an example of the **show access-list compiled** command with these outputs highlighted, see the "Verifying ACL Memory Limit Configurations: Example" section on page 16.

Configuration Examples for Turbo Access Control List Scalability Enhancements on the NSEs

This section provides the following configuration examples:

Monitoring Memory Limitations for Layer 2 or Layer 3 and Layer 4 ACL Processing: Example

In the following example, the **show access-list compiled** command is entered.

Note the following, which are italicized in the example output:

- The output for **show access-list compiled** is separated for Layer 2 and for Layer 3 and Layer 4 data. Layer 3 and Layer 4 ACL compilation tables and information can be seen in the "Compiled ACL statistics for IPv4" section of the output, while Layer 2 ACL compilation tables and information can be seen in the "Compiled ACL statistics for Data-Link" section.
- The "mem limits" output shows the number of times a compile has occurred and the ACL has reached its configured limit. If you have reached the configured limit numerous times, you may want to consider modifying the memory limit to allow more memory.
  In this example, ACL memory for Layer 3 and Layer 4 data has never reached its configured limit. The same is true for Layer 2 data in this example.
- The "Mb limit" output shows the current memory limit setting.
  In this example, the Layer 3 and Layer 4 memory limit was previously set to 65 MB (via the **access-list compiled ipv4 limit memory 65** command), while the Layer 2 memory limit has not been changed from its default limit of 128 MB.
- The "Mb default limit" output shows the current default memory limit setting. If the **default** form of the **access-list compiled ipv4 limit memory** command or **access-list compiled data-link limit memory** command is entered, the "Mb default limit" will become the "Mb limit."
  In this example, the default limits are 256 MB for Layer 3 and Layer 4 data and 128 MB for Layer 2 data.
- The "Mb max memory" output shows the maximum amount of memory the current ACL configuration could actually consume under maximum usage conditions. This number is helpful for configuring memory limits for ACL processing. If you want to free up RP memory, for instance, and you have a small number of ACLs with a low "max memory," you could configure a reservation of a small amount of memory for ACL processing using the **access-list compiled** [**ipv4 | data-link**] **limit memory** *number* command, thereby freeing up memory for other RP processes. Conversely, if you have a high memory limit, you may want to use the **access-list compiled** [**ipv4 | data-link**] **limit memory** *number* command to commit more memory to ACL processing, or even the **no access-list compiled** [**ipv4 | data-link**] **limit memory** command to allow as much memory as is available for ACL processing.
  In this example, the max memory for the current Layer 3 and Layer 4 Turbo ACL configuration data on the router is 1 MB, and the max memory for Layer 2 Turbo ACL configuration data is 0 Mb.

```
Router# show access-lists compiled
Compiled ACL statistics for IPv4:
ACL State      Entries Config Fragment Redundant
102 Operational    1       1      0        0
103 Operational    1       1      0        0
104 Operational    1       1      0        0
105 Operational    1       1      0        0
106 Operational    1       1      0        0
112 Operational    1       1      0        0
ws_def_acl Operational 1 1 0 0
7 ACLs, 7 active, 1 builds, 7 entries, 1408 ms last compile
1 history updates, 2000 history entries
0 mem limits, 65 Mb limit, 256 Mb default limit, 1 Mb max memory
0 compile failures, 0 priming failures
Overflows: L1 0, L2 0, L3 0
Table expands:[9]=0 [10]=0 [11]=0 [12]=0 [13]=0 [14]=0 [15]=0
L0: 1803Kb 2/3 8/9 3/4 2/3 2/3 2/3 2/3 2/3
```

```
L1: 5Kb 3/27 3/12 2/9 2/9
L2: 4Kb 3/150 2/81
L3: 7Kb 3/250
Ex: 8Kb
Tl: 1828Kb 41 equivs (18 dynamic)
Compiled ACL statistics for Data-Link:
ACL       State       Entries Config Fragment Redundant
int-l2-0  Operational    1       1      0        0
int-l2-1  Operational    2       2      0        0
int-l2-2  Operational    3       3      0        0
int-l2-3  Operational    4       4      0        0
int-l2-4  Operational    1       1      0        0
int-l2-5  Operational  199     199      0        0
int-l2-6  Operational  200     200      0        0
int-l2-8  Operational    3       3      0        0
int-l2-10 Operational    2       2      0        0
int-l2-15 Operational    1       1      0        0
int-l2-16 Operational    2       2      0        0
int-l2-17 Operational    3       3      0        0
int-l2-18 Operational    1       1      0        0
19 ACLs, 13 active, 22 builds, 422 entries, 832 ms last compile
0 history updates, 524288 history entries
0 mem limits, 128 Mb limit, 128 Mb default limit, 0 Mb max memory
0 compile failures, 0 priming failures
Overflows: L1 3
Table expands:[3]=3
L0: 593Kb 1013/1014 2/3
L1: 86Kb 1013/1518
Ex: 191Kb
Tl: 871Kb 2028 equivs (1013 dynamic)
```

Reserving a Set Amount of Memory for Layer 2 ACL Processing: Example

The following example reserves 100 MB of memory for Layer 2 ACL processing in the RP path:

```
access-list compiled data-link limit memory 100
```

Allowing All Available Memory to Be Used for Layer 2 ACL Processing: Example

The following example allows Layer 2 ACL processing to use as much memory as is needed for Layer 2 ACL processing:

```
no access-list compiled data-link limit memory
```

Restoring the Default Amount of Memory Reserved for Layer 2 ACL Processing: Example

The following example restores the default amount of memory reserved for Layer 2 ACL processing in the RP path:

```
default access-list compiled data-link limit memory
```

Reserving a Set Amount of Memory for Layer 3 and Layer 4 ACL Processing: Example

The following example reserves 100 MB of memory for Layer 3 and Layer 4 ACL processing in the RP path:

```
access-list compiled ipv4 limit memory 100
```

Allowing All Available Memory to Be Used for Layer 3 and Layer 4 ACL Processing: Example

The following example allows Layer 3 and Layer 4 ACL processing to use as much memory as is needed for Layer 3 and Layer 4 ACL data:

```
no access-list compiled ipv4 limit memory
```

Restoring the Default Amount of Memory Reserved for Layer 3 and Layer 4 ACL Processing: Example

The following example restores the default amount of memory reserved for Layer 3 and Layer 4 ACL processing in the RP path:

```
default access-list compiled ipv4 limit memory
```

Verifying ACL Memory Limit Configurations: Example

In the following example, a 65-MB limit has been configured for Layer 3 and Layer 4 ACL processing, while the Layer 2 ACL memory reservations have not been changed.

See the italicized output in the following example to view the changes:

```
Router# show access-lists compiled
Compiled ACL statistics for IPv4:
ACL State      Entries Config Fragment Redundant
102 Operational    1       1      0        0
103 Operational    1       1      0        0
104 Operational    1       1      0        0
105 Operational    1       1      0        0
106 Operational    1       1      0        0
112 Operational    1       1      0        0
ws_def_acl Operational 1 1 0 0
7 ACLs, 7 active, 1 builds, 7 entries, 1408 ms last compile
1 history updates, 2000 history entries
0 mem limits, 65 Mb limit, 256 Mb default limit, 1 Mb max memory
0 compile failures, 0 priming failures
Overflows: L1 0, L2 0, L3 0
Table expands:[9]=0 [10]=0 [11]=0 [12]=0 [13]=0 [14]=0 [15]=0
L0: 1803Kb 2/3 8/9 3/4 2/3 2/3 2/3 2/3 2/3
L1: 5Kb 3/27 3/12 2/9 2/9
L2: 4Kb 3/150 2/81
```

```
L3: 7Kb 3/250
Ex: 8Kb
Tl: 1828Kb 41 equivs (18 dynamic)
Compiled ACL statistics for Data-Link:
ACL       State       Entries Config Fragment Redundant
int-l2-0  Operational    1       1      0        0
int-l2-1  Operational    2       2      0        0
int-l2-2  Operational    3       3      0        0
int-l2-3  Operational    4       4      0        0
int-l2-4  Operational    1       1      0        0
int-l2-5  Operational  199     199      0        0
int-l2-6  Operational  200     200      0        0
int-l2-8  Operational    3       3      0        0
int-l2-10 Operational    2       2      0        0
int-l2-15 Operational    1       1      0        0
int-l2-16 Operational    2       2      0        0
int-l2-17 Operational    3       3      0        0
int-l2-18 Operational    1       1      0        0
19 ACLs, 13 active, 22 builds, 422 entries, 832 ms last compile
0 history updates, 524288 history entries
0 mem limits, 128 Mb limit, 128 Mb default limit, 0 Mb max memory
0 compile failures, 0 priming failures
Overflows: L1 3
Table expands:[3]=3
L0: 593Kb 1013/1014 2/3
L1: 86Kb 1013/1518
Ex: 191Kb
Tl: 871Kb 2028 equivs (1013 dynamic)
```

Additional References

The following sections provide references related to this feature.

Related Documents

Related Topic	Document Title
Access Lists	"IP Access Lists" section of *Cisco IOS IP Application Services Configuration Guide, Release 12.4*
Network Services Engines	*Cisco 7304 Network Services Engine Installation and Configuration Guide*
PXF	*PXF Information for the Cisco 7304 Router*
Turbo Access Control Lists	*Turbo Access Control Lists*

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 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 new commands only.

- **access-list compiled data-link limit memory**
- **access-list compiled ipv4 limit memory**

access-list compiled data-link limit memory

To change the amount of memory reserved for Turbo ACL processing for Layer 2 traffic in the Route Processor path for a Cisco 7304 router using a network services engine (NSE), use the **access-list compiled data-link limit memory** command in global configuration mode. To place no restrictions on the amount of memory reserved for Turbo ACL processing of Layer 2 traffic in the Route Processor path for a Cisco 7304 router using an NSE, use the **no** form of this command. To restore the default amount of memory reserved for Turbo ACL processing for Layer 2 traffic in the Route Processor path for a Cisco 7304 router using an NSE, use the **default** form of this command.

access-list compiled data-link limit memory *number*

no access-list compiled data-link limit memory

default access-list compiled data-link limit memory

Syntax Description

number	A number between 8 and 4095 that specifies the amount of memory, in megabytes, reserved for Turbo ACL processing of Layer 2 traffic in the Route Processor path for the Cisco 7304 router using an NSE.

Command Default

The default for *number* is 128.

Command Modes

Global configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

The **show access-list compiled** command output provides information useful in helping to consider the exact memory limit to configure. The following sections of the **show access-list compiled** output, which are found in the "Compiled ACL statistics for Data-Link" section of the output, are especially useful:

- The "mem limits" output shows the number of times a compile has occurred and the ACL has reached its configured limit.
- The "Mb limit" output shows the current memory limit setting.
- The "Mb max memory" output shows the maximum amount of memory the current ACL configuration could actually consume under maximum usage conditions.

Note that there is a direct trade-off between memory used for ACL processing in the RP path and the memory used for other RP processes. Memory reserved for ACL processing cannot be used for other RP processes, and vice versa. If you need more memory for ACL processing, you should set a higher value for *number*. If you need more memory for other RP processes, you should set a lower value for *number*.

When configuring this memory limit, also note that a certain amount of RP memory is reserved for Layer 3 and Layer 4 ACL data. The amount of memory reserved for ACL data can be viewed using the **show access-list compiled** command, and can be changed using the **access-list compiled ipv4 limit memory** command.

Note that the **no** form of this command removes all memory limits for ACL processing, thereby allowing as much memory as is needed for Layer 2 ACL processing in the RP path.

To restore a default configuration of this command, which is 128 MB, enter the **default** form of this command.

Examples

The following example reserves 100 MB of memory for Layer 2 ACL processing in the RP path:

```
access-list compiled data-link limit memory 100
```

The following example allows Layer 2 ACL processing to use as much memory as is needed for Layer 2 ACL processing:

```
no access-list compiled data-link limit memory
```

The following example restores the default amount of memory reserved for Layer 2 ACL processing in the RP path:

```
default access-list compiled data-link limit memory
```

Related Commands

Command	Description
access-list compiled ipv4 limit memory	Configures limits on the amount of memory used for Turbo ACL processing of Layer 3 and Layer 4 traffic.
show access-list compiled	Displays the status and condition of the Turbo ACL tables associated with each access list.

access-list compiled ipv4 limit memory

To change the amount of memory reserved for Turbo ACL processing for Layer 3 and Layer 4 traffic in the Route Processor path for a Cisco 7304 router using a network services engine (NSE), use the **access-list compiled ipv4 limit memory** command in global configuration mode. To place no restrictions on the amount of memory reserved for Turbo ACL processing for Layer 3 and Layer 4 traffic in the Route Processor path for a Cisco 7304 router using an NSE, use the **no** form of this command. To restore the default amount of memory reserved for Turbo ACL processing for Layer 3 and Layer 4 traffic in the Route Processor path for a Cisco 7304 router using an NSE, use the **default** form of this command.

access-list compiled ipv4 limit memory *number*

no access-list compiled ipv4 limit memory

default access-list compiled ipv4 limit memory

Syntax Description

number	A number between 8 and 4095 that specifies the memory limit in megabytes.

Command Default

On an NSE-150, the default for *number* is always 256.

On an NSE-100, the default for *number* is determined by the amount of SDRAM on the NSE-100. If the NSE-100 has 512 MB of DRAM, the default for *number* is 256. If the NSE-100 has less than 512 MB DRAM, the default for *number* is 128.

Command Modes

Global configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

The **show access-list compiled** command output provides information useful in helping to consider the exact memory limit to configure. The following sections of the **show access-list compiled** output, which are found in the "Compiled ACL statistics for IPv4:" section of the output, are especially useful:

- The "mem limits" output shows the number of times a compile has occurred and the ACL has reached its configured limit.
- The "Mb limit" output shows the current memory limit setting.
- The "Mb max memory" output shows the maximum amount of memory the current ACL configuration could actually consume under maximum usage conditions.

Note that there is a direct trade-off between memory used for ACL processing in the RP path and the memory used for other RP processes. Memory reserved for ACL processing cannot be used for other RP processes, and vice versa. If you need more memory for ACL processing, you should set a higher value for *number*. If you need more memory for other RP processes, you should set a lower value for *number*.

When configuring this memory limit, also note that a certain amount of RP memory is reserved for Layer 2 ACL data. The amount of memory reserved for ACL data can be viewed using the **show access-list compiled** command, and can be changed using the **access-list compiled data-link limit memory** command.

Note that the **no** form of this command removes all memory limits for ACL processing, thereby allowing as much memory as is needed for Layer 3 and Layer 4 ACL processing in the RP path.

To restore a default configuration of this command, enter the **default** form of this command.

Examples

The following example reserves 100 MB of memory for Layer 3 and Layer 4 ACL processing in the RP path:

```
access-list compiled ipv4 limit memory 100
```

The following example allows Layer 3 and Layer 4 ACL processing to use as much memory as is needed for Layer 3 and Layer 4 ACL processing:

```
no access-list compiled ipv4 limit memory
```

The following example restores the default amount of memory reserved for Layer 3 and Layer 4 ACL processing in the RP path:

```
default access-list compiled ipv4 limit memory
```

Related Commands

Command	Description
access-list compiled data-link limit memory	Configures memory limits on the amount of memory reserved for Turbo ACL processing of Layer 2 traffic.
show access-list compiled	Displays the status and condition of the Turbo ACL tables associated with each access list

Feature Information for Turbo ACL Scalability Enhancements on the NSEs

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 Turbo ACL Scalability Enhancements on the NSEs

Feature Name	Releases	Feature Information
Turbo ACL Scalability Enhancements on the NSEs	12.2(31)SB2	This feature was introduced.

Glossary

Access Control List—A list kept by routers to control access to or from the router for a number of services.

NSE—network services engine. The Cisco 7304 router has two types of processor, the NSE and the network processing engine (NPE). Two versions of the NSE exist, the NSE-100 and the NSE-150.

RP—Route Processor. One of two processing paths on a Cisco 7304 router using an NSE, with the Parallel eXpress Forwarding path being the other path. All traffic not supported in the PXF path on a Cisco 7304 router using an NSE is forwarded using the RP path.

Turbo Access Control Lists—A Turbo Access Control list is an access list that more expediently processes traffic by compiling the ACLs into a set of lookup tables while still maintaining the match requirements.

PXF—Parallel eXpress Forwarding. One of two processing paths on a Cisco 7304 router using an NSE, with the Route Processor (RP) path being the other path. The PXF processing path is used to accelerate the performance for certain supported features.

Note See *Internetworking Terms and Acronyms* for terms not included in this glossary.