



Turbo Access Control Lists

This feature module describes the Turbo Access Control Lists (Turbo ACL) feature. The Turbo ACL feature processes access lists more expediently, providing faster functionality for routers equipped with the feature. This feature module includes information on the benefits of the new feature, supported platforms, related documents, and so forth.

This document includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 2
- Supported Standards, MIBs, and RFCs, page 2
- Prerequisites, page 3
- Configuration Tasks, page 3
- Configuration Examples, page 5
- Configuration Examples, page 5
- Command Reference, page 6
- Glossary, page 12

Feature Overview

This feature enables Cisco 7200 and 7500 series routers, and Cisco 12000 series Gigabit Switch Routers to evaluate access control lists (ACLs) for more expedient packet classification and access checks.

Benefits

Access control lists (ACLs) are normally searched sequentially to find a matching rule, and ACLs are ordered specifically to take this factor into account. Because of the increasing needs and requirements for security filtering and packet classification, ACLs can expand to the point that searching the ACL adds a significant amount of time and memory when packets are being forwarded. Moreover, the time taken by the router to search the list is not always consistent, adding a variable latency to the packet forwarding. A high CPU load is necessary for searching an ACL with several entries.

The Turbo ACL feature compiles the ACLs into a set of lookup tables, while maintaining the first match requirements. Packet headers are used to access these tables in a small, fixed number of lookups, independently of the existing number of ACL entries. The benefits of this feature include:

- For ACLs larger than 3 entries, the CPU load required to match the packet to the pre-determined packet-matching rule is lessened. The CPU load is fixed, regardless of the size of the ACL, allowing for larger ACLs without incurring any CPU overhead penalties. The larger the ACL, the greater the benefit.
- The time taken to match the packet is fixed, so that latency of the packets are smaller (significantly in the case of large ACLs) and more importantly, consistent, allowing better network stability and more accurate transit times.

Restrictions

ACLs containing specialized processing characteristics such as evaluate and time-range entries are excluded from Turbo ACL acceleration.

Related Features and Technologies

The Turbo ACL feature improves the performance of access lists. For information on access control lists, see the *Access Control Lists: Overview and Guidelines* document on CCO.

Supported Platforms

- Cisco 7200 series routers
- Cisco 7500 series routers

Supported Standards, MIBs, and RFCs

MIBs

No new or modified MIBs are supported by this feature.

RFCs

No new or modified RFCs are supported by this feature.

Standards

No new or modified Standards for this feature.

Prerequisites

The Turbo ACL feature builds a set of lookup tables from the ACLs in the configuration; these tables increase the internal memory usage, and in the case of large and complex ACLs, tables containing 2 to 4 megabytes of memory are usually required. Routers enabled with the Turbo ACL feature should allow for this amount of memory usage. The **show access-list compiled** command displays the memory overhead of the Turbo ACL tables for each ACL.

Configuration Tasks

See the following sections for configuration tasks for the Turbo Access Control Lists feature. Each task in the list indicates if the task is optional or required.

- Configuring Turbo ACL(required)

Configuring Turbo ACL

| | Command | Purpose |
|--------|---|-----------------------------------|
| Step 1 | Router# configure terminal | Enters global configuration mode. |
| Step 2 | Router#(config) access-list compiled | Enables the Turbo ACL feature. |

Verifying Turbo ACL

Use the **show access-list compiled** command to verify that the Turbo ACL feature has been successfully configured on your router. The command output contains the following states, which are defined below:

- Operational: The access list has been compiled by Turbo ACL, and matching to this access list is performed through the Turbo ACL tables at high speed.
- Unsuitable: The access list is not suitable for compiling, perhaps because it has time-range enabled entries, evaluate references, or dynamic entries.
- Deleted: There are no entries in this access list.
- Building: The access list is in the process of being compiled. Depending on the size and complexity of the list, and the load on the router, the building process may take a few seconds.
- Out of memory: An access list cannot be compiled because the router has exhausted its memory.

Below is sample output from the **show access-lists compiled** command:

Router# **show access-lists compiled**

Compiled ACL statistics:

12 ACLs loaded, 12 compiled tables

| ACL | State | Tables | Entries | Config | Fragment | Redundant | Memory |
|-----|-------------|--------|---------|--------|----------|-----------|--------|
| 1 | Operational | 1 | 2 | 1 | 0 | 0 | 1Kb |
| 2 | Operational | 1 | 3 | 2 | 0 | 0 | 1Kb |
| 3 | Operational | 1 | 4 | 3 | 0 | 0 | 1Kb |
| 4 | Operational | 1 | 3 | 2 | 0 | 0 | 1Kb |
| 5 | Operational | 1 | 5 | 4 | 0 | 0 | 1Kb |
| 9 | Operational | 1 | 3 | 2 | 0 | 0 | 1Kb |
| 20 | Operational | 1 | 9 | 8 | 0 | 0 | 1Kb |
| 21 | Operational | 1 | 5 | 4 | 0 | 0 | 1Kb |
| 101 | Operational | 1 | 15 | 9 | 7 | 2 | 1Kb |
| 102 | Operational | 1 | 13 | 6 | 6 | 0 | 1Kb |
| 120 | Operational | 1 | 2 | 1 | 0 | 0 | 1Kb |
| 199 | Operational | 1 | 4 | 3 | 0 | 0 | 1Kb |

First level lookup tables:

| Block | Use | Rows | Columns | Memory used |
|-------|--------------------|-------|---------|-------------|
| 0 | TOS/Protocol | 6/16 | 12/16 | 66048 |
| 1 | IP Source (MS) | 10/16 | 12/16 | 66048 |
| 2 | IP Source (LS) | 27/32 | 12/16 | 132096 |
| 3 | IP Dest (MS) | 3/16 | 12/16 | 66048 |
| 4 | IP Dest (LS) | 9/16 | 12/16 | 66048 |
| 5 | TCP/UDP Src Port | 1/16 | 12/16 | 66048 |
| 6 | TCP/UDP Dest Port | 3/16 | 12/16 | 66048 |
| 7 | TCP Flags/Fragment | 3/16 | 12/16 | 66048 |

Monitoring and Maintaining Turbo ACL

| Command | Purpose |
|---|---|
| Router# show access-lists | Displays information regarding access lists, including whether the access list is compiled. |
| Router# show access-lists compiled | Displays information regarding compiled access lists, including the state of each compiled access list. |

Configuration Examples

This section provides a Turbo ACL configuration example. The **access-list compiled** command output indicates that Turbo ACL is enabled:

```
Building configuration...

Current configuration:
!
version 12.0
...
interface Ethernet2/7
 no ip address
 ip access-group 20 out
 no ip directed-broadcast
 shutdown
!
no ip classless
ip route 192.168.0.0 255.255.255.0 10.1.1.1
!
access-list compiled
access-list 1 deny any
access-list 2 deny 192.168.0.0 0.0.0.255
access-list 2 permit any
```

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 reference publications.

The Turbo ACL feature has added or modified the following commands:

- **access-list compiled**
- **show access-lists**
- **show access-list compiled**

In Cisco IOS Release 12.0(1)T or later, you can search and filter the output for **show** and **more** commands. This functionality is useful when you need to sort through large amounts of output, or if you want to exclude output that you do not need to see.

To use this functionality, enter a **show** or **more** command followed by the “pipe” character (`|`), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search or filter on:

command | {begin | include | exclude} regular-expression

Following is an example of the **show atm vc** command in which you want the command output to begin with the first line where the expression “PeakRate” appears:

show atm vc | begin PeakRate

For more information on the search and filter functionality, refer to the Cisco IOS Release 12.0(1)T feature module titled *CLI String Search*.

access-list compiled

Use the **access-list compiled** command to enable the Turbo ACL feature. To disable the Turbo ACL feature, use the **no** form of this command.

- **access-list compiled**
- **no access-list compiled**

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Configuration

| Command History | Release | Modification |
|------------------------|----------------|--|
| | 12.0(6)S | This command was introduced. |
| | 12.1(1)E | This command was introduced for Cisco 7200 series routers on Release 12.1 E. |

Usage Guidelines By default, the Turbo ACL feature is disabled. When Turbo ACL is disabled, the normal ACL processing is enabled, and no ACL acceleration occurs.

When the Turbo ACL feature is enabled using the **access-lists compiled** command, the ACLs in the configuration are scanned and, if suitable, compiled for Turbo ACL acceleration. This scanning and compilation may take a few seconds when the system is processing large and complex ACLs, or when the system is processing a configuration that contains a large number of ACLs.

Any configuration change to an ACL that is being accelerated, such as the addition of new ACL entries or the deletion of the ACL, triggers a recompilation of that ACL.

When Turbo ACL tables are being built (or rebuilt) for a particular ACL, the normal sequential ACL search is used until the new tables are ready for installation.

Examples The following example enables the Turbo ACL feature:

```
access-list compiled
```

show access-lists

To display the contents of current access lists, use the **show access-lists** privileged EXEC command.

show access-lists [*access-list-number* | *name*]

Enhancements have been made to the **show access-lists** command. The enhancement to the output of this command is that each access list displayed using this command indicates whether the access list is running as a compiled access list.

| Syntax Description | | |
|--------------------|---|--|
| access-list-number | (Optional.) Access list number to display. The range is 0 to 1199. The system displays all access lists by default. | |
| name | (Optional.) Name of the IP access list to display. | |

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|----------|---|
| | 12.0(6)S | The output was modified to identify the compiled ACLs. |
| | 12.1(1)E | The output was modified to identify the compiled ACLs for the 12.1(1)E train (on Cisco 7200 series routers only). |
| | 12.1(5)T | The command output was modified to identify compiled ACLs on Release 12.1(5)T. |

Usage Guidelines The **show access-lists** command is used to display the current ACLs operating in the router. Each access list is flagged using the Compiled indication if it is operating as an accelerated ACL.

The display also shows how many packets have been matched against each entry in the ACLs, enabling the user to monitor the particular packets that have been permitted or denied.

Examples The following is sample output of the **show access-lists** command when Turbo ACL is configured on all of the following access lists.

```
epping3#show access-lists
Standard IP access list 1 (Compiled)
  deny any
Standard IP access list 2 (Compiled)
  deny 192.168.0.0, wildcard bits 0.0.0.255
  permit any
Standard IP access list 3 (Compiled)
  deny 0.0.0.0
  deny 192.168.0.1, wildcard bits 0.0.0.255
  permit any
Standard IP access list 4 (Compiled)
  permit 0.0.0.0
  permit 192.168.0.2, wildcard bits 0.0.0.255
```

Command Types

| Command | Description |
|-----------------------------------|---|
| access-list (extended) | Provides extended access lists that allow more detailed access lists. |
| access-list (standard) | Creates a standard access list. |
| clear access-list counters | Clears the counters of an access list. |
| clear access-temp | Manually clears a temporary access list entry from a dynamic access list. |
| ip access-list | Defines an IP access list by name. |
| show ip access-list | Displays the contents of all current IP access lists. |

show access-list compiled

To display a table showing Turbo ACLs, use the **show access-list compiled** command.

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|----------|--|
| | 12.0(6)S | This command was introduced. |
| | 12.1(1)E | This command was introduced for Cisco 7200 series routers on Release 12.1 E. |
| | 12.1(5)T | This command was introduced on Cisco IOS Release 12.1(5)T. |

Usage Guidelines This command is used to display the status and condition of the Turbo ACL tables associated with each ACL. The memory usage is displayed for each table; large and complex ACLs may require significant amounts of memory. If the memory usage is greater than the memory available, the user can disable the Turbo ACL feature so that memory exhaustion does not occur, but the acceleration of the ACLs is not then enabled.

Examples The following is a partial sample output of the **show access-list compiled** command:

```
Router# show access-list compiled
Compiled ACL statistics:
12 ACLs loaded, 12 compiled tables
ACL      State      Tables  Entries  Config  Fragment  Redundant  Memory
1        Operational  1       2        1       0         0         1Kb
2        Operational  1       3        2       0         0         1Kb
3        Operational  1       4        3       0         0         1Kb
4        Operational  1       3        2       0         0         1Kb
5        Operational  1       5        4       0         0         1Kb
9        Operational  1       3        2       0         0         1Kb
20       Operational  1       9        8       0         0         1Kb
21       Operational  1       5        4       0         0         1Kb
101      Operational  1       15       9       7         2         1Kb
102      Operational  1       13       6       6         0         1Kb
120      Operational  1       2        1       0         0         1Kb
199      Operational  1       4        3       0         0         1Kb
First level lookup tables:
Block    Use              Rows      Columns  Memory used
0        TOS/Protocol     6/16     12/16   66048
1        IP Source (MS)   10/16    12/16   66048
2        IP Source (LS)   27/32    12/16   132096
3        IP Dest (MS)     3/16     12/16   66048
4        IP Dest (LS)     9/16     12/16   66048
5        TCP/UDP Src Port 1/16     12/16   66048
6        TCP/UDP Dest Port 3/16     12/16   66048
7        TCP Flags/Fragment 3/16     12/16   66048
```

| Related Commands | Command | Description |
|-------------------------|-----------------------------------|---|
| | access-list (extended) | Provides extended access lists that allow more detailed access lists. |
| | access-list (standard) | Creates a standard access list. |
| | clear access-list counters | Clears the counters of an access list. |
| | clear access-temp | Manually clears a temporary access list entry from a dynamic access list. |
| | ip access-list | Defines an IP access list by name. |
| | show ip access-list | Displays the contents of all current IP access lists. |

Glossary

ACL—Access control list. ACLs are individual filtering rules grouped together in a single list. They are generally used to provide security filtering, though they may be used to provide a generic packet classification facility.

ACE—Access control element. Each individual filtering rule that is part of an ACL is termed an ACE. A group of ACEs forms an access list.

QoS—Quality of service. Selected packet types are handled differently within the network to provide a differentiated level of reliability, cost, and so forth.

ToS—Type of service. A set of flags and values that are part of the IP packet header indicating various parameters related to handling the packet in the network.