

Security (ACL) Enhancements

The Security (ACL) enhancements features provides you the option to restrict the number of ACLs or aces or both that can be configured on a box. Restricting the number of ACLs or aces on a box enables you to prevent depletion or over usage of tcam space which can adversely affect the performance of a box.

- Restrictions , on page 1
- Configuring Security (ACL) Enhancements, on page 2
- Feature Information for IPv6 ACL Extensions for Hop by Hop Filtering, on page 2

Restrictions

- The acl-ace-limit set is per ACL and is applicable to all the ACLs on the box.
- The acl-limit and acl-ace-limit are mutually exclusive to global-ace-limit. You cannot configure global-ace-limit when acl-limit and acl-ace-limt are configured and vice-versa.

  The limit that will be set cannot be less than the existing number of ACLs/aces in the box.
- The ACL-limit or acl-ace-limit or global-ace-limit set will be applicable to the ACLs/aces created internally while device booting up.
- The ACL with object group ace (ogace) expansion is not supported in this release, based on the customer requirements this can be investigated further. Each ogace is counted as one ace.
- The ACL-limit or acl-ace-limit or global-ace-limit set is applicable to all static and dynamically created ACLs except for template ACLs.
- The configurable ACL-limit or acl-ace-limit or global-ace-limit doesn't guarantee that the tcam space will never be overused or depleted. You must know the exact limit configurable that can be supported on the box from prior testing in the lab.
- The assumption is that all the ACLs configured on the box will be applied to the interface, which affects the tcam space.
- When the box reaches max ACL-limit or acl-ace-limit or global-ace-limit configurable, and if any client tries to create a dynamic ACL/aces then the request is rejected with the syslog error message. It is up to you to handle the failure accordingly.

Configuring Security (ACL) Enhancements

To configure ACL and ACE limits for V4 and V6:

```
enable
configure terminal
 access-list acl-limit 10
 access-list acl-ace-limit 12
 access-list global-ace-limit 14
 end
```

Note The acl-limit and acl-ace-limit are mutually exclusive to global-ace-limit.

Important Notes

- The max ACL limit range configurable is 1 to 2^{16}.
- The max ace limit range per ACL configurable is 1 to 2^{32}.
- The max global ace limit range configurable is 1 to 2^{32}.
- The acl-ace-limit set is applicable to all the ACLs that are already configured and will be configured.

Verifying Security (ACL) Enhancements Configuration

You can use the **show access-list acl-limit** command to display the number of ACLs and ACEs that are configured.

```
Device# show access-list acl-limit
Max ACLs configurable:       50
Number of ACLs configured:   10

Max aces/ACL configurable:   10

Max aces configurable:       100
Number of aces configured:   67
```

Feature Information for IPv6 ACL Extensions for Hop by Hop Filtering

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for IPv6 ACL Extensions for Hop by Hop Filtering

Feature Name	Releases	Feature Information
IPv6 ACL Extensions for Hop by Hop Filtering	Cisco IOS Release XE 3.4S Cisco IOS Release XE 3.5S Cisco IOS Release XE 3.6S Cisco IOS Release XE 3.3SG	Allows you to control IPv6 traffic that might contain hop-by-hop extension headers. The following commands were introduced or modified: **deny** (IPv6), **permit** (IPv6).