Configuring ACL Logging

This chapter contains the following sections:

Information About ACL Logging

The ACL logging feature allows you to monitor ACL flows and to log dropped packets on an interface.

IPv6 ACL Logging Overview

When the ACL logging feature is configured, the system monitors ACL flows and logs dropped packets and statistics for each flow that matches the deny conditions of the ACL entry.

Statistics and dropped-packet logs are generated for each flow. A flow is defined by the source interface, protocol, source IP address, source port, destination IP address, and destination port values. The statistics maintained for a matching flow is the number of denies of the flow by the ACL entry during the specified time interval.

When a new flow is denied (that is a flow that is not already active in the system), the system generates an initial Syslog message with a hit count value of 1. Then each time the flow is denied, the system creates a flow entry and increments the hit count value.

When an existing flow is denied, the system generates a Syslog message at the end of each interval to report the hit count value for the flow in the current interval. After the Syslog message is generated, the hit count value for the flow is reset to zero for the next interval. If no hit is recorded during the interval, the flow is deleted and no Syslog message is generated.

Guidelines and Limitations for ACL Logging

ACL Logging has the following configuration guidelines and limitations:

- The system logs packets that match deny ACE conditions only. Logging for permit ACE conditions is not supported.
- The logging option may be applied to any ACL deny entry. To apply the logging option to implicitly denied traffic, you must configure the logging option for a specific deny-all ACL entry.
- ACL logging applies to port ACLs (PACL) configured by the **ipv6 port traffic-filter** command and to routed ACLs (RACL) configured by the **ipv6 traffic-filter** commands only.
- The total number of flows and deny-flows are limited to a user-defined maximum value to prevent DOS attacks. If this limit is reached, no new logs are created until an existing flow finishes.
- The system uses a hash table to locate a flow so that a large number of flows can be supported without impacting CPU utilization. The system uses a timer queue to efficiently manage the aging of large number of flows.
- The number of Syslog entries generated by the ACL logging process is limited by the configured logging level of the ACL logging process. If the amount of Syslog entries exceed this limit, the logging facility may drop some logging messages. Therefore, ACL logging should not be used as a billing tool or as an accurate source of the number of matches to an access list.
- The hardware rate-limiter rate-limits traffic on a packet basis, but control plane policing (COPP) rate-limits traffic on a byte basis. If the packet size and the hardware rate-limiter both have high values, the COPP default value can be exceeded and the system drops the packet. To overcome this limitation you must increase the default CIR value (64000 bytes) to a higher value such as 2560000 bytes. When the default CIR is increased packet logging happens normally.
- IPv6 logging is not supported on management or VTY (Terminal) ports
- IPv6 logging is not supported on egress RACLs (due to ASIC limitations).
- IPv6 logging is not supported on egress VACLs (due to ASIC limitations).

Configuring ACL Logging

To configure the ACL logging process, you first create the access list, then enable filtering of IPv6 traffic on an interface using the specified ACL, and finally configure the ACL logging process parameters.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	**ipv6 access-list** *name* **Example:** `switch(config)# ipv6 access-list logging-test`	Defines an IPv6 access list and enters IPv6 access list configuration mode.
Step 3	**deny ipv6 any** *destination-address* **log** **Example:** `switch(config-ipv6-acl)# deny ipv6 any 2001:DB8:1::1/64 log`	Sets deny conditions for an IPv6 access list. To enable the system to log matches against this entry, you must use the **log** keyword when configuring the deny conditions.

	Command or Action	Purpose
Step 4	**exit** **Example:** `switch(config-ipv6-acl)# exit`	Updates the configuration and exits IPv6 access list configuration mode.
Step 5	**interface ethernet** *slot/port* **Example:** `switch(config)# interface ethernet 1/1`	Enters interface configuration mode.
Step 6	**ipv6 traffic-filter logging-test** {**in** | **out**} **Example:** `switch(config-if)# ipv6 traffic-filter logging-test in`	Enables the filtering of IPv6 traffic on an interface using the specified ACL. You can apply an ACL to outbound or inbound traffic.
Step 7	**exit** **Example:** `switch(config-if)# exit`	Updates the configuration and exits interface configuration mode.
Step 8	**logging ip access-list cache interval** *interval* **Example:** `switch(config)# logging ip access-list cache interval 5`	Configures the log-update interval (in seconds) for the ACL logging process. The default value is 300 seconds. The range is from 5 to 86400 seconds.
Step 9	**logging ip access-list cache entries** *number-of-flows* **Example:** `switch(config)# logging ip access-list cache entries 1000`	Specifies the maximum number of flows to be monitored by the ACL logging process. The default value is 8000. The range of values supported is from 0 to 1048576.
Step 10	**logging ip access-list cache threshold** *threshold* **Example:** `switch(config)# logging ip access-list cache threshold 1`	If the specified number of packets are logged before before the expiry of the alert interval the system generates a Syslog message.
Step 11	**hardware rate-limiter access-list-log** *packets* **Example:** `switch(config)# hardware rate-limiter access-list-log 200`	Configures rate limits in packets per second for packets copied to the supervisor module for access list logging. The range is from 0 to 30000.
Step 12	**acllog match-log-level** *severity-level* **Example:** `switch(config)# acllog match-log-level 3`	Specifies the minimum severity level to log ACL matches. The default is 6 (informational). The range is from 0 (emergency) to 7 (debugging). **Note** Acllogs can only support logging levels of 3 or later.

Verifying ACL Logging Configuration

To display ACL logging configuration information, perform one of the following tasks:

Command	Purpose
show logging ip access-list status	Displays the deny maximum flow count, the current effective log interval and the current effective threshold value.
show logging ip access-list cache	Displays information on the active logged flows, such as source IP and destination IP addresses, S-Port and D-Port information and so on.

Configuration Examples for ACL Logging

This example shows how to configure the ACL logging process.

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ipv6 access-list logging-test
switch(config-ipv6-acl)# deny ipv6 any 2001:DB8:1::1/64 log
switch(config-ipv6-acl)# exit
switch(config)# interface ethernet 1/1
switch(config-if)# ipv6 traffic-filter logging-test in
switch(config-if)# exit
switch(config)# logging ip access-list cache entries 1000
switch(config)# logging ip access-list cache interval 5
switch(config)# logging ip access-list cache threshold 1
switch(config)# hardware rate-limiter access-list-log 200
switch(config)# acllog match-log-level 3
switch(config)# exit
switch#
```

This example shows a typical PACL logging configuration.

```
switch(config)# interface ethernet 8/11
switch(config-if)# ipv6 port traffic-filter v6log-pacl in
switch(config-if)# switchport access vlan 4064
switch(config-if)# speed 1000

switch(config)# interface Vlan 4064
switch(config-if)# no shutdown
switch(config-if)# no ip redirects
switch(config-if)# ipv6 address 4064::1/64


Switch# show vlan filter
vlan map v6-vaclmap:
Configured on VLANs: 4064

Switch# show vlan access-map v6-vaclmap
Vlan access-map v6-vaclmap
match ipv6: v6-vacl
```

```
action: drop
statistics per-entry
```