Configuring Security Access Control Lists

This chapter describes how to configure security access control lists (ACLs) on your Cisco ME 1200 NID. ACLs provide basic security for your network by filtering traffic and controlling network connections.

Creating Access Control Entry

SUMMARY STEPS

1. **SECURITYACL**
2. **setACLGlobalConfig ace-global-config { ace-id | ace-enable {enable | disable} | action { deny | Permit | filter{ any | intf-range} } | dot1q-tag { any | tagged | untagged} | evc-policer { disable | policer-id} | frame-type { any | arp { arp-req-rep { any | reply | request} | arp-sender-mac-match { any | value} | arp-type {any | arp | other | rarp} | ethernet { any | value} | ip { any | value } ip-length { any | value } rarp-target-mac-match { any | value } sip-filter { any | ip-subnet } tip-filter { any | ip-subnet} | ethernet-type { dmac-filter { any | dmac-type | specific} | ethertype-filter { any | specific} | smac-filter { any | specific } | ipv4 { dip-filter { any | ipv4-subnet} | dmac-filter { dmac-type} | ip-protocol-filter { icmp { code-filter { any | code-value} |ip-fragment { value | any} | ip-option { value | any } | ip-ttl { value | any} type-filter { any | type-value } | other { any | ip-protocol-value} | tcp { dest-port-filter { any | port-number | range} | ip-fragment { value | any} | ip-option { value | any} | ip-ttl { value | any} | src-port-filter { any | port-number | range } | tcp-ack { value | any} | tcp-fin { value | any} | tcp-psh { value | any} | tcp-rst { value | any} | tcp-rst { value | any} | tcp-syn { value | any} | tcp-urg { value | any} }| udp { dest-port-filter { any | port-number | range} | ip-fragment { value | any} | ip-option { value | any} | ip-ttl { value | any} | src-port-filter { any | port-number | range } | sip-filter { ipv4-subnet | any}| ipv6 { dmac-filter { dmac-type}| hop-limit { any | value} | ip-protocol-filter { icmp { code-filter | type-filter} | other { next-header-value} | tcp { dest-port-filter { any | port-number | range} | ip-ttl { value | any} | src-port-filter { any | port-number | range } | tcp-ack { value | any} | tcp-fin { value | any} | tcp-psh { value | any} | tcp-rst { value | any} | tcp-rst { value | any} | tcp-syn { value | any} | tcp-urg { value | any} | udp { dest-port-filter { any | port-number | range} | src-port-filter { any | port-number | range} } | sip-filter { any | specific}} | ingress-port { any | intf-range} | logging { enable | disable } mirror { enable | disable } next { disable | last | next-ace-id} policy-filter { any | policy-value} | rate-limiter { disable| value} | shutdown { enable | disable } | tag-priority { any | value } vid { any | vlan-type} }**
3. **setaclglobalconfig review**
4. **setaclglobalconfig commit**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**SECURITYACL** **Example:** `Switch# SECURITYACL`	Enters the SecurityACL mode.
Step 2	**setACLGlobalConfig ace-global-config { ace-id	ace-enable {enable	disable}	action { deny	Permit	filter{ any	intf-range} }	dot1q-tag { any	tagged	untagged}	evc-policer { disable	policer-id}	frame-type { any	arp { arp-req-rep { any	reply	request} |**	Applies the ACL global configuration. • **ace-enable—**Specifies the port number. ◦**—**port number. The range is from 1 to 6.

	Command or Action	Purpose
	arp-sender-mac-match { **any** | **value**} | **arp-type** {**any** | **arp** | **other** | **rarp**} | **ethernet** { **any** | **value**} | **ip** { **any** | **value** } **ip-length** { **any** | **value** } **rarp-target-mac-match** { **any** | **value** } **sip-filter** { **any** | **ip-subnet** } **tip-filter** { **any** | **ip-subnet**} | **ethernet-type** { **dmac-filter** { **any** | **dmac-type** | **specific**} | **ethertype-filter** { **any** | **specific**} | **smac-filter** { **any** | **specific** } | **ipv4** { **dip-filter** { **any** | **ipv4-subnet**} | **dmac-filter** { **dmac-type**} | **ip-protocol-filter** { **icmp** { **code-filter** { **any** | **code-value**} |**ip-fragment** { **value** | **any**} | **ip-option** { **value** | **any** } | **ip-ttl** { **value** | **any**} **type-filter** { **any** | **type-value** } | **other** { **any** | **ip-protocol-value**} | **tcp** { **dest-port-filter** { **any** | **port-number** | **range**} | **ip-fragment** { **value** | **any**} | **ip-option** { **value** | **any**} | **ip-ttl** { **value** | **any**} | **src-port-filter** { **any** | **port-number** | **range** } | **tcp-ack** { **value** | **any**} | **tcp-fin** { **value** | **any**} | **tcp-psh** { **value** | **any**} | **tcp-rst** { **value** | **any**} | **tcp-rst** { **value** | **any**} | **tcp-syn** { **value** | **any**} | **tcp-urg** { **value** | **any**} }| **udp** { **dest-port-filter** { **any** | **port-number** | **range**} | **ip-fragment** { **value** | **any**} | **ip-option** { **value** | **any**} | **ip-ttl** { **value** | **any**} | **src-port-filter** { **any** | **port-number** | **range** } | **sip-filter** { **ipv4-subnet** | **any**}| **ipv6** { **dmac-filter** { **dmac-type**}| **hop-limit** { **any** | **value**} | **ip-protocol-filter** { **icmp** { **code-filter** | **type-filter**} | **other** { **next-header-value**} | **tcp** { **dest-port-filter** { **any** | **port-number** | **range**} | **ip-ttl** { **value** | **any**} | **src-port-filter** { **any** | **port-number** | **range** } | **tcp-ack** { **value** | **any**} | **tcp-fin** { **value** | **any**} | **tcp-psh** { **value** | **any**} | **tcp-rst** { **value** | **any**} | **tcp-rst** { **value** | **any**} | **tcp-syn** { **value** | **any**} | **tcp-urg** { **value** | **any**} | **udp** { **dest-port-filter** { **any** | **port-number** | **range**} | **src-port-filter** { **any** | **port-number** | **range**} } | **sip-filter** { **any** | **specific**}} | **ingress-port** { **any** | **intf-range**} | **logging** { **enable** | **disable** } **mirror** { **enable** | **disable** } **next** { **disable** | **last** | **next-ace-id**} **policy-filter** { **any** | **policy-value**} | **rate-limiter** { **disable**| **value**} | **shutdown** { **enable** | **disable** } | **tag-priority** { **any** | **value** } **vid** { **any** | **vlan-type**} }	• **ace-id —**Specify a valid ACE ID. The available options are from 1-512. • **action —**Specify the action to take with a frame that hits this ACE. ◦ **permit —**The frame that hits this ACE is granted permission for the ACE operation. ◦ **deny —**The frame that hits this ACE is dropped. ◦ **filter —**Frames matching the ACE are filtered . • **dot1q-tag —**Specifies tagging. • **evc-policer —**Select whether EVC policer is enabled or disabled. The default value is "Disabled". Note that the ACL rate limiter and EVC policer can not both be enabled. If enabled, specify the EVC policer ID. You can specify EVC policer Id from 1-1022 • **frame-type—** Select the frame type for this ACE. These frame types are mutually exclusive. ◦ **any —**Any frame can match this ACE. ◦ **ethernet-type —**Only Ethernet Type frames can match this ACE. The available options are : ◦ **dmac-filter—**Specifies destination MAC address field. Available values are any, dmac-type and specific. ◦ **ethertype-filter—**Specifies Etype value. Available values are any and specific. ◦ **smac-filter—**Specifies source MAC address field. ◦ **arp —**Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type. ◦ **arp-req-rep—**Specifies request or reply. Available options are any, request or reply. ◦ **arp-sender-mac-match—**Specifies arp sender MAC match. Available options are any or value 0-1. ◦ **arp-type—**Specifies ARP parameters. Available options are any, arp, other, and rarp. ◦ **ethernet—**Specifies Ethernet value. Available options are any or value 0-1. ◦ **ip—**Specifies IP value. Available options are any or value 0-1.

Command or Action	Purpose

Example:
`Switch(SecurityACL)# setaclglobalconfig ace-global-config ?`
`  ace-enable  Enable or disable ACE`
`  ace-id  ACE ID`
`  action  Access list action`
`  dot1q-tag  Tag`
`  evc-policer  EVC policer`
`  frame-type  Frame Type`
`  ingress-port  Ingress port`
`  logging  Logging frame information`
`  lookup  Second lookup`
`  mirror  Mirror frame to destination mirror port`
`  next  insert the current ACE before the next ACE ID`
`  policy-filter  Policy`
`  rate-limiter  Rate Limiter`
`  shutdown  Shutdown incoming port`
`  tag-priority  Tag priority`
`  vid  VID field`
	◦ **ip-length—**Specifies IP or Ethernet length value. Available options are any or value 0-1.
	◦ **rarp-target-mac-match—**Specifies rarp target mismatch. Available options are any or value 0-1.
	◦ **sip-filter—**Specifies source IP address field. Available options are any or **ip-subnet**. IP Subnet specify the host IP address and mask.
	◦ **tip-filter—**Specifies target IP address field. Available options are any or **ip-subnet**. IP Subnet specify the host IP address and mask.
	◦ **ipv4 —**Only ipv4 frames can match this ACE. Notice the ipv4 frames won't match the ACE with ethernet type.
	◦ **dip-filter—**Specifies destination IP address field. Available options are any or **ipv4-subnet**. IP Subnet specify the host IP address and mask.
	◦ **dmac-filter—**Specifies destination MAC address field. DMAC type includes, any/unicast/multicast/broadcast.
	◦ **ip-protocol-filter—**Specifies IP protocol filter.
	◦ **icmp—**Specifies frame type of IPv6 ICMP. You can configure code-filter, IP-fragment field, IP option field, IP TTL field and ICMP type field.
	◦ **other—**Specifies protocol value. Allowed range is 0,2-5,7-16,18-255 .
	◦ **tcp—**Specifies frame type of IPv6 TCP. You can configure following parameters :
	◦ dest-port-filter — TCP destination port field
	◦ ip-fragment — IP fragment field
	◦ ip-option — IP option fiield
	◦ ip-ttl —IP TTL field
	◦ src-port-filter —TCP source port field
	◦ tcp-ack —TCP ack field
	◦ tcp-fin —TCP fin field
	◦ tcp-psh —TCP psh field
	◦ tcp-rst— TCP rst field
	◦ tcp-syn— TCP syn field
	◦ tcp-urg —TCP urg field

	Command or Action	Purpose
		◦ **udp—**Specifies frame type of IPv6 UDP. You can configure code-filter and type-filter field. ◦ **sip-filter—**Specifies source IP address field. Available options are any or **ipv4-subnet**. IP Subnet specify the host IP address and mask. ◦ **ipv6 —**Only ipv6 frames can match this ACE. Notice the ipv6 frames won't match the ACE with ethernet type. ◦ **dmac-filter—**Specifies destination MAC address field. Available values are any/unicast/multicast/broadcast. ◦ **hop-limit—**Specifies hop limit value. Available values are any and value ranges from 0-1. ◦ **ip-protocol--ilter—**Specifies IP protocol filter. ◦ **icmp—**Specifies frame type of IPv6 ICMP. You can configure code-filter and type-filter field. ◦ **other—**Specifiesnext-header-value value. Allowed range is 0-65535 . ◦ **tcp—**Specifies frame type of IPv6 TCP. You can configure following parameters : ◦ dest-port-filter — TCP destination port field ◦ src-port-filter —TCP source port field ◦ tcp-ack —TCP ack field ◦ tcp-fin —TCP fin field ◦ tcp-psh —TCP psh field ◦ tcp-rst— TCP rst field ◦ tcp-syn— TCP syn field ◦ tcp-urg —TCP urg field ◦ **udp—**Specifies frame type of IPv6 UDP. You can configure dest-port-filter and src-port-filter. • **ingress-port—**Select the ingress port for which this ACE applies. ◦ **any —**No policy filter is specified. (policy filter status is "don't-care".) ◦ **intf-range —**If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value

Command or Action	Purpose
	and bitmask appears. Select an Interface Number/Range [1-6]/1,2,3,4,5,6 • **logging—**Specify the logging operation of the ACE. Notice that the logging message doesn't include the 4 bytes CRC information. ◦ **enable —**Frames matching the ACE are stored in the System Log. ◦ **disable —**Frames matching the ACE are not logged. **Note** The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited. • **lookup—**Specify to enable or disable the second lookup operation of the ACE. • **mirror—**Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port. ◦ **enable —**Frames received on the port are mirrored. ◦ **disable —**Frames received on the port are not mirrored. The default value is "Disabled". • **next—**Specify the current ACE before the next ACE ID • **policy-filter—**Specify the policy number filter for this ACE. ◦ **any —**No policy filter is specified. (policy filter status is "don't-care".) ◦ **specific —**If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears. • **rate-limiter—**Specify the rate limiter in number of base units. The allowed range is 1 to 16. Disabled indicates that the rate limiter operation is disabled. • **shutdown—**Specify the port shut down operation of the ACE. ◦ **enable —**If a frame matches the ACE, the ingress port will be disabled. ◦ **disable —**Port shut down is disabled for the ACE. **Note** The shutdown feature only works when the packet length is less than 1518(without VLAN tags). • **tag-priority—**Specifies tag priority.

	Command or Action	Purpose
		• **vid—**Specifies vid. **Note** EVC policer and rate limiter can not be configured at the same time .
Step 3	**setaclglobalconfig review** **Example:** `Switch(SecurityACL)# setaclglobalconfig review`	Displays the configuration.
Step 4	**setaclglobalconfig commit** **Example:** `Switch(SecurityACL)# setaclglobalconfig commit`	Sends the configuration to the controller.
Step 5	**exit** **Example:** `Switch(SecurityACL)# exit`	Exits the ProvisionACL mode.

Configuration Example

```
Switch(SecurityACL)# configure terminal
Switch(setACLGlobalConfig)# ace-global-config ace-id 30
setACLGlobalConfig ace-global-config ace-enable enable
setACLGlobalConfig ace-global-config lookup enable
setACLGlobalConfig ace-global-config lookup enable
setACLGlobalConfig ace-global-config ingress-port intf-range 3-4
setACLGlobalConfig ace-global-config policy-filter policy-value 4
setACLGlobalConfig ace-global-config frame-type ethernet-type dmac-filter specific
00-00-00-00-10-01
setACLGlobalConfig ace-global-config frame-type ethernet-type smac-filter specific
00-00-00-00-20-02
setACLGlobalConfig ace-global-config action permit


setACLGlobalConfig ace-global-config ace-id 30
setACLGlobalConfig ace-global-config ace-enable enable
setACLGlobalConfig ace-global-config lookup enable
setACLGlobalConfig ace-global-config lookup enable
setACLGlobalConfig ace-global-config ingress-port intf-range 3-4
setACLGlobalConfig ace-global-config policy-filter policy-value 4
setACLGlobalConfig ace-global-config frame-type ethernet-type dmac-filter specific
00-00-00-00-10-01
setACLGlobalConfig ace-global-config frame-type ethernet-type smac-filter specific
00-00-00-00-20-02
setACLGlobalConfig ace-global-config action permit
setACLGlobalConfig ace-global-config evc-policer policer-id 10
setACLGlobalConfig ace-global-config mirror disable
setACLGlobalConfig ace-global-config shutdown disable
setACLGlobalConfig ace-global-config logging disable
whales1(config-controller-SecurityACL)#setaclglobalConfig commit
 SetACLGlobalConfig Commit Success!!!

Mac acl rule :

setACLGlobalConfig ace-global-config ace-enable enable
setACLGlobalConfig ace-global-config ace-id 2
```

```
setACLGlobalConfig ace-global-config lookup enable
setACLGlobalConfig ace-global-config ingress-port intf-range 2-5
setACLGlobalConfig ace-global-config policy-filter policy-value 63
setACLGlobalConfig ace-global-config frame-type ethernet-type smac-filter specific
00-00-00-00-00-01
setACLGlobalConfig ace-global-config frame-type ethernet-type dmac-filter any
setACLGlobalConfig ace-global-config frame-type ethernet-type ethertype-filter specific
0xffff
setACLGlobalConfig ace-global-config dot1q-tag tagged
setACLGlobalConfig ace-global-config vid vlan-value 80
setACLGlobalConfig ace-global-config tag-priority value 6-7
setACLGlobalConfig ace-global-config action deny redirect intf-range 6
setACLGlobalConfig ace-global-config evc-policer policer-id 2
setACLGlobalConfig ace-global-config logging enable
setACLGlobalConfig ace-global-config shutdown enable
setACLGlobalConfig ace-global-config mirror enable
setACLGlobalConfig review
setACLGlobalConfig commit


IP acl rule :


setACLGlobalConfig ace-global-config lookup enable
setACLGlobalConfig ace-global-config ace-enable enable
setACLGlobalConfig ace-global-config ace-id 3
setACLGlobalConfig ace-global-config policy-filter policy-value 62
setACLGlobalConfig ace-global-config frame-type ipv4 dip-filter any
setACLGlobalConfig ace-global-config frame-type ipv4 sip-filter ipv4-subnet 10.20.10.2/16
setACLGlobalConfig ace-global-config shutdown enable
setACLGlobalConfig ace-global-config mirror enable
setACLGlobalConfig ace-global-config frame-type ipv4 dmac-filter dmac-type broadcast
setACLGlobalConfig ace-global-config frame-type ipv4 ip-protocol-filter icmp code-filter
code-value 1
setACLGlobalConfig ace-global-config frame-type ipv4 ip-protocol-filter icmp type-filter
type-value 1
setACLGlobalConfig ace-global-config dot1q-tag tagged
setACLGlobalConfig ace-global-config vid vlan-value 100
setACLGlobalConfig ace-global-config tag-priority value 5
setACLGlobalConfig ace-global-config action deny redirect intf-range 5
setACLGlobalConfig ace-global-config evc-policer policer-id 5
setACLGlobalConfig review
setACLGlobalConfig commit

ipv6 :

setACLGlobalConfig ace-global-config ace-enable enable
setACLGlobalConfig ace-global-config ace-id 55
setACLGlobalConfig ace-global-config policy-filter policy-value 63
setACLGlobalConfig ace-global-config ingress-port intf-range 2-3
setACLGlobalConfig ace-global-config frame-type ipv6 sip-filter specific ipv6-address
0:0:0:0:0:0:0:5
setACLGlobalConfig ace-global-config frame-type ipv6 dmac-filter dmac-type unicast
setACLGlobalConfig ace-global-config frame-type ipv6 hop-limit value 1
setACLGlobalConfig ace-global-config frame-type ipv6 ip-protocol-filter icmp code-filter
code-value 1
setACLGlobalConfig ace-global-config frame-type ipv6 ip-protocol-filter icmp type-filter
type-value 1
setACLGlobalConfig ace-global-config action deny redirect intf-range 4
setACLGlobalConfig ace-global-config mirror enable
setACLGlobalConfig ace-global-config rate-limiter value 10
setACLGlobalConfig review
setACLGlobalConfig commit
```

Configuring Rate Limiter

SUMMARY STEPS

1. **setaclrateLimiter**
2. **setaclrateLimiter acl-rate-limiter id | unit| { rate-in-kbps | rate-in-pps}**
3. **setaclrateLimiter review**
4. **setaclrateLimiter commit**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**setaclrateLimiter** **Example:** `Switch# setaclrateLimiter`	Enters the applyACLtoport mode.

Step 2	**setaclrateLimiter acl-rate-limiter id	unit| { rate-in-kbps	rate-in-pps}**
			
			Example:
			`Switch(SecurityACL)#setaclrateLimiter acl-rate-limiter ?`
			`  id    Rate limiter ID`
			`  unit  Specify Unit and rate value`
				Configure the rate limiter for the of the switch. .
				• **id—**The rate limiter ID for the settings contained in the same row and its range is 1 to 16.
				• **unit —**Specify the rate unit. The allowed values are: pps: packets per second. kbps: Kbits per second.

Step 3	**setaclrateLimiter review** **Example:** `Switch(SecurityACL)# setaclrateLimiter review`	Displays the configuration.
Step 4	**setaclrateLimiter commit** **Example:** `Switch(SecurityACL)# setaclrateLimiter commit`	Sends the configuration to the controller.
Step 5	**exit** **Example:** `Switch(SecurityACL)# exit`	Exits the ProvisionACL mode.

Configuration Example

```
Switch# ProvisionACL
Switch(ProvisionACL)# SetACLRateLimiter acl-rate-limiter id 2
Switch(ProvisionACL)# setACLRateLimiter acl-rate-limiter unit rate-in-kbps 10000
```

```
Switch(ProvisionACL)# exit
```

Applying ACL to Ports

SUMMARY STEPS

1. **applyACLtoPort**
2. **applyACLtoPort acl-port-config** { **action-deny** { **enable**| **disable**} | **evc-policy** { **enable** | **evc-policer-id**} | **logging** { **enable**| **disable**} | **mirror** { **enable**| **disable**} | **policy** { **enable**| **policer-id**} | **port-number** | **rate-limiter** { **disable** | **rate-limiter-id**} | **redirect** { **disable**| **intf-range**} | **shutdown** { **enable**| **disable**} }
3. **applyACLtoPort review**
4. **applyACLtoPort commit**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**applyACLtoPort** **Example:** `Switch# applyACLtoPort`	Enters the applyACLtoport mode.
Step 2	**applyACLtoPort acl-port-config** { **action-deny** { **enable**| **disable**}	**evc-policy** { **enable**	**evc-policer-id**}	**logging** { **enable**| **disable**}	**mirror** { **enable**| **disable**}	**policy** { **enable**| **policer-id**}	**port-number**	**rate-limiter** { **disable**	**rate-limiter-id**}	**redirect** { **disable**| **intf-range**}	**shutdown** { **enable**| **disable**} } **Example:** `Switch(SecurityACL)#applyACLtoPort acl-port-config ?` `  action-deny  Access list action deny if enabled to true, else permit` `  evc-policy  EVC policer` `  logging  Logging frame information.` `  mirror  Mirror frame to destination mirror port` `  policy  Policy` `  port-number  Port Number` `  rate-limiter  Rate Limiter` `  redirect  Redirect frame to specific port` `  shutdown  Shutdown incoming port`	Configure the ACL parameters of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE. • **action-deny—**Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit". ◦ **enable —**Access list action deny if enabled to true, denies forwarding. ◦ **disable —**Access list action deny if disabled, permits forwarding. • **evc-policy —**Select which EVC policer ID to apply on this port. ◦ **enable —**Enabling evc-policy disable policer . ◦ **evc-policer-id —**Enter an EVC Policy ID. The The allowed values are Disabled or the values 1 through 1022. . • **logging —**Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC. ◦ **enable —**Frames received on the port are stored in the System Log.

	Command or Action	Purpose
		◦ **disable —**Frames received on the port are not logged. **Note** The default value is "Disabled". The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited. • **mirror —**Specify the mirror operation of this port. ◦ **enable —**Frames received on the port are mirrored. ◦ **disable —**Frames received on the port are not mirrored. **Note** The default value is "Disabled". • **policy—**Select which EVC policer ID to apply on this port. ◦ **enable —**Enabling evc-policy disable policy.. ◦ **policy-id —**Enter an EVC Policy ID. The The allowed values are Disabled or the values 0 through 63. • **port-number—**The logical port for the settings contained in the same row. . • **rate-limiter—**Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled". • **redirect—**Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled". ◦ **disable —**Disable direct. ◦ **intf-range —**Interface number ranges from 1-6. • **shutdown—**Specify the port shut down operation of this port. ◦ **enable —**To reopen ports by changing the volatile port configuration of the ACL user module. ◦ **disable —**To close ports by changing the volatile port configuration of the ACL user module. The default value is "Enabled".
Step 3	**applyACLtoPort review** **Example:** `Switch(SecurityACL)# applyACLtoPort review`	Displays the configuration.

	Command or Action	Purpose
Step 4	**applyACLtoPort commit** **Example:** `Switch(SecurityACL)# applyAclToPort commit`	Sends the configuration to the controller.
Step 5	**exit** **Example:** `Switch(SecurityACL)# exit`	Exits the ProvisionACL mode.

Configuration Example

```
Switch# ProvisionACL
Switch(ProvisionACL)# applyACLtoPort acl-port-config port-number 3
applyACLtoPort acl-port-config evc-policy enable enable
applyACLtoPort acl-port-config evc-policy enable enable
applyACLtoPort acl-port-config evc-policy evc-policer-id 55
applyACLtoPort acl-port-config policy enable enable
applyACLtoPort acl-port-config policy policy-id 33


Switch(ProvisionACL)# applyAclToPort commit

    ApplyAclToPort  Commit Success!!!

Switch(ProvisionACL)# exit
```

Viewing Access Control Entry

SUMMARY STEPS

1. **SECURITYACL**
2. **getACLGlobalConfig get-acl-global-config ace-id**
3. **getaclglobalconfig review**
4. **setaclglobalconfig commit**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**SECURITYACL** **Example:** `Switch# SECURITYACL`	Enters the SecurityACL mode.

	Command or Action	Purpose

Step 2	**getACLGlobalConfig get-acl-global-config ace-id**
	
	Example:
	`Switch(SecurityACL)#setaclglobalconfig ace-global-config ?`
	
	`ace-enable Enable or disable ACE`
	`ace-id ACE ID`
	`action Access list action`
	`dot1q-tag Tag`
	`evc-policer EVC policer`
	`frame-type Frame Type`
	`ingress-port Ingress port`
	`logging Logging frame information`
	`lookup Second lookup`
	`mirror Mirror frame to destination mirror port`
	`next insert the current ACE before the next ACE ID`
	
	`policy-filter Policy`
	`rate-limiter Rate Limiter`
	`shutdown Shutdown incoming port`
	`tag-priority Tag priority`
	`vid VID field`
		Retrives the ACL global configuration.
		
		• **ace-id —**Specify a valid ACE ID. The available options are from 1-512.

Step 3	**getaclglobalconfig review** **Example:** `Switch(SecurityACL)# getaclglobalconfig review`	Displays the configuration.
Step 4	**setaclglobalconfig commit** **Example:** `Switch(SecurityACL)# getaclglobalconfig commit`	Sends the configuration to the controller.
Step 5	**exit** **Example:** `Switch(SecurityACL)# exit`	Exits to the SecurityACL mode.

Configuration Example

```
Switch(SecurityACL)# GetACLGlobalConfig-Output.ace-global-config.ace-id = 30
GetACLGlobalConfig-Output.ace-global-config.ace-enable = true
GetACLGlobalConfig-Output.ace-global-config.lookup = true
GetACLGlobalConfig-Output.ace-global-config.ingress-port.t = 2
GetACLGlobalConfig-Output.ace-global-config.ingress-port.u.intf-range = '2-3'
GetACLGlobalConfig-Output.ace-global-config.policy-filter.t = 2
GetACLGlobalConfig-Output.ace-global-config.policy-filter.u.policy-value = 4
GetACLGlobalConfig-Output.ace-global-config.dot1q-tag.t = 1
GetACLGlobalConfig-Output.ace-global-config.dot1q-tag.u.any = 'any'
GetACLGlobalConfig-Output.ace-global-config.tag-priority.t = 1
GetACLGlobalConfig-Output.ace-global-config.tag-priority.u.any = 'any'
GetACLGlobalConfig-Output.ace-global-config.vid.t = 1
GetACLGlobalConfig-Output.ace-global-config.vid.u.any = 'any'
GetACLGlobalConfig-Output.ace-global-config.rate-limiter.t = 1
GetACLGlobalConfig-Output.ace-global-config.rate-limiter.u.disable = 'disable'
GetACLGlobalConfig-Output.ace-global-config.mirror = false
GetACLGlobalConfig-Output.ace-global-config.logging = false
GetACLGlobalConfig-Output.ace-global-config.shutdown = false
GetACLGlobalConfig-Output.ace-global-config.evc-policer.t = 1
GetACLGlobalConfig-Output.ace-global-config.evc-policer.u.disable = 'disable'
```

```
GetACLGlobalConfig-Output.ace-global-config.action.t = 2
GetACLGlobalConfig-Output.ace-global-config.action.u.deny.redirect.t = 1
GetACLGlobalConfig-Output.ace-global-config.action.u.deny.redirect.u.disable = '0'
GetACLGlobalConfig-Output.ace-global-config.frame-type.t = 2
GetACLGlobalConfig-Output.ace-global-config.frame-type.u.ethernet-type.smac-filter.t = 2
GetACLGlobalConfig-Output.ace-global-config.frame-type.u.ethernet-type.smac-filter.u.specific
 = '00-00-00-00-20-02'
GetACLGlobalConfig-Output.ace-global-config.frame-type.u.ethernet-type.dmac-filter.t = 1
GetACLGlobalConfig-Output.ace-global-config.frame-type.u.ethernet-type.dmac-filter.u.specific
 = '00-00-00-00-10-01'
GetACLGlobalConfig-Output.ace-global-config.frame-type.u.ethernet-type.ethertype-filter.t
= 1
GetACLGlobalConfig-Output.ace-global-config.frame-type.u.ethernet-type.ethertype-filter.u.any
 = 'default'
GetACLGlobalConfig-Output.ace-global-config.next.t = 3
GetACLGlobalConfig-Output.ace-global-config.next.u.disable = 'disable'
```

Viewing ACL Rate Limiter

SUMMARY STEPS

1. **getaclrateLimiter**
2. **getaclrateLimiter get-acl-rate-limiter id | unit| { rate-in-kbps | rate-in-pps}**
3. **getaclrateLimiter review**
4. **getaclrateLimiter commit**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**getaclrateLimiter** **Example:** `Switch# getaclrateLimiter`	Enters the applyACLtoport mode.

Step 2	**getaclrateLimiter get-acl-rate-limiter id | unit| { rate-in-kbps | rate-in-pps}**
	
	Example:
	`Switch(config-controller-SecurityACL)#getaclrateLimiter get-acl-rate-limiter ?`
	`rate-id  Rate limiter ID`
		Configure the rate limiter for the of the switch. .
		• **id—**The rate limiter ID for the settings contained in the same row and its range is 1 to 16.
		• **unit —**Specify the rate unit. The allowed values are: pps: packets per second. kbps: Kbits per second.

Step 3	**getaclrateLimiter review** **Example:** `Switch(SecurityACL)# getaclrateLimiter review`	Displays the configuration.

	Command or Action	Purpose
Step 4	**getaclrateLimiter commit** **Example:** `Switch(SecurityACL)# getaclrateLimiter commit`	Sends the configuration to the controller.
Step 5	**exit** **Example:** `Switch(SecurityACL)# exit`	Exits the ProvisionACL mode.

Configuration Example

```
Switch# ProvisionACL
Switch(ProvisionACL)# getACLrateLimiter commit
GetACLRateLimiter-Output.acl-rate-limiter.id = 2
GetACLRateLimiter-Output.acl-rate-limiter.unit.t = 2
GetACLRateLimiter-Output.acl-rate-limiter.unit.u.rate-in-kbps = 10000

GetACLRateLimiter Commit Success!!!


Switch(ProvisionACL)# exit
```

Viewing ACL Ports

SUMMARY STEPS

1. **getaclportConfig**
2. **getaclportConfig get-acl-port-config port port-number**
3. **ggetaclportConfig review**
4. **getaclportConfig commit**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**getaclportConfig** **Example:** `Switch# getaclportConfig`	Enters the applyACLtoport mode.

	Command or Action	Purpose

Step 2	**getaclportConfig get-acl-port-config port port-number**
	
	Example:
	`Switch(SecurityACL)#getaclportConfig get-acl-port-config port?`
	`port-number Port Number`
		Configure the ACL parameters of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.
		• **port-number—**The logical port for the settings contained in the same row. .

Step 3	**ggetaclportConfig review** **Example:** `Switch(SecurityACL)# getaclportConfig review`	Displays the configuration.
Step 4	**getaclportConfig commit** **Example:** `Switch(SecurityACL)# getaclportConfig commit`	Sends the configuration to the controller.
Step 5	**exit** **Example:** `Switch(SecurityACL)# exit`	Exits the ProvisionACL mode.

Configuration Example

```
Switch# ProvisionACL
Switch(ProvisionACL)# GetACLPortConfig-Output.acl-port-config.port-number = 3
GetACLPortConfig-Output.acl-port-config.action-deny = false
GetACLPortConfig-Output.acl-port-config.policy.enable = true
GetACLPortConfig-Output.acl-port-config.policy.policy-id = 33
GetACLPortConfig-Output.acl-port-config.rate-limiter.t = 2
GetACLPortConfig-Output.acl-port-config.rate-limiter.u.rate-limiter-id = 18
GetACLPortConfig-Output.acl-port-config.evc-policy.enable = true
GetACLPortConfig-Output.acl-port-config.evc-policy.evc-policer-id = 55
GetACLPortConfig-Output.acl-port-config.mirror = false
GetACLPortConfig-Output.acl-port-config.logging = false
GetACLPortConfig-Output.acl-port-config.shutdown = false
GetACLPortConfig-Output.acl-port-config.redirect.t = 1
GetACLPortConfig-Output.acl-port-config.redirect.u.disable = true

GetACLPortConfig Commit Success!!!


Switch(ProvisionACL)# exit
```