



Error Messages for Security and QoS Configurations

This appendix describes the error messages for configuring network security with ACLs and configuring QoS. In [Table A-1](#), Access Control Parameters (ACPs) are referred to as masks. For more information on ACPs, see the “[Understanding Access Control Parameters](#)” section on page 12-4.

These error messages are applicable only if you have installed the enhanced software image on your switch.

Table A-1 Common ACL Error Messages

Error Message	Explanation and Suggested Solution
%Error:Class-map has a different mask than the Policymap	The policy map has a different mask than the class map. Use the same mask in both the class map and the policy map.
%Error:Class-maps have a mix of System Defined and User Defined masks within the Policymap	In a policy map, the class maps can have ACLs that use either a system-defined mask or a user-defined mask. A combination of system-defined and user-defined masks cannot be used in the multiple class maps that are a part of a policy map. A policy map can contain multiple class maps that all use the same user-defined mask or the same system-defined mask.
%Error:System Defined ACEs of tcp and ip can not exist together in a policy-map	A combination of Layer 3 system-defined ACEs and Layer 4 system-defined ACEs is not supported in a policy map. You cannot have masks such as permit tcp/udp any any and permit ip any any within the same policy map. A policy map must have either Layer 4 system-defined ACEs or Layer 3 system-defined ACEs.
%Error:Service-Policy is not supported on VLAN interface	A policy map cannot be attached to a VLAN interface. A policy map can be attached only to physical interfaces.
%Error:Invalid policy_map	The policy map is invalid due to multiple reasons. Normally, this error message is preceded by a more explicit error message that gives details about the reasons for the invalidity of the policy map.
%Error:Match Numbered Attach Filter :ONLY one ACL allowed in a class-map	Only one ACL can be allowed in a class map. This error means that there was an attempt to add another numbered ACL in the class map.

Table A-1 Common ACL Error Messages (continued)

Error Message	Explanation and Suggested Solution
<code>%Error:Deny ACE not supported in access-group within a class-map</code>	A deny ACE is not supported in an access group within a class map.
<code>%Error:System Defined and User Defined ACEs can not exist together in access-group within a class-map</code>	In a class map, the access group can have ACLs that have either system-defined masks or user-defined masks. A combination of system-defined and user-defined masks cannot be used in an access group within a class map.
<code>%Error:System Defined ACEs of tcp and ip can not exist together in access-group within a class-map</code>	In a class map, the access group cannot have system-defined ACEs of both the Layer 4 and Layer 3. The access group can have either Layer 4 system-defined ACEs or Layer 3 system-defined ACEs.
<code>%Error:Match Attach Filter :ONLY one ACL allowed in a class-map</code>	In a class map, only one ACL is allowed. This error message means that an attempt was made to add another ACL in the class map.
<code>%Error:the ACL has a different mask than the Policy-map</code>	In a policy map, all ACLs within the same class maps must have the same mask. This error message means that an attempt was made to create an ACL with a different mask within a policy map.
<code>%Error:Service policy can not be configured</code>	The Catalyst 2950 switches support the policy-map global configuration command with certain restrictions. This error message means that the policy map cannot be configured due to certain reasons. The exact cause is provided in separate error messages that precede this error message.
<code>%Error:Service policy can not be supported - Policers required exceed Maximum Allowed on this interface</code>	A maximum of six policers are supported on a Fast Ethernet port and 60 policers on Gigabit Ethernet port. This policy map cannot be supported because the number of policers required on this interface are more than permitted.
<code>%Error:Service policy can not be supported - Rules required exceed available resources in ASIC.</code>	The policy map cannot be supported because the number of resources required to support this policy map are not available in the hardware. In order to support this policy map, you need to reduce the number of resources on this policy map.
<code>%Error:Removing service-policy <i>policy-map name</i> from interface <i>interface_number</i></code>	A policy map is removed from an interface if it is found to be invalid. There are multiple reasons for a policy map to become invalid (incorrect number of policers, ACLs in a class map cannot be supported, and so on). If there is a policy map attached to an interface and you modify the policy map so that it becomes invalid, the system removes the policy map from the interface.
<code>%Error:ASIC memory read write issues</code>	The error message means that the switch hardware is having problems.
<code>%Error:ASIC Resources unavailable</code>	This error message means that the hardware does not have sufficient resources to support the user policies.
<code>%Error:Invalid mask</code>	This error message means that the user-defined mask is not entered correctly in the hardware. Remove the mask, and re-enter it.

Table A-1 Common ACL Error Messages (continued)

Error Message	Explanation and Suggested Solution
%Error:Invalid rule	This error message means that the hardware had a problem programming the resource. Re-enter the command to program the hardware.
%Error:Invalid ingress port	This error message means that an invalid ingress port was detected by the hardware. Re-enter the command for the interface.
%Error:Another security mask on this interface	This error message means that there is another security mask present on the interface. On any interface, only one security mask is allowed. Remove all the security access groups on this interface, and attach the security access group that is required.
%Error:Another qos mask on this interface	This error message means that more than one QoS mask on the interface. On any interface, only one QoS mask is allowed. Remove all the QoS policy maps on this interface, and attach the policy map that is required.
%Error:No sec mask on this interface	This error message means that no security mask has been applied on this interface. Therefore, there is no security access group running on this interface.
%Error:No qos mask on this interface	This error message means that there is no QoS mask has been applied on this interface. Therefore, no QoS policy map is applied on the interface.
%Error:No sec rules on this interface	This error message means that there are no security resources on this interface.
%Error:No qos rules on this interface	This error message means that there are no QoS resources on this interface.
%Error:No free masks available	This error message means that there are no free masks available for the user. You have to use one of the user-defined masks that is already configured. As an alternative, you can free up one of the masks by removing all the policies that use that mask.
%Error:Invalid ace	The ACE entered is invalid. This is an error message that is preceded by a more explicit error message that gives the reasons for the ACE being invalid.
%Error:Invalid sequence - IP protocol ACE not allowed after TCP/UDP protocol ACE	In an ACL, a Layer 4 (TCP/UDP) ACE cannot precede a Layer 3 (IP protocol) ACE.

Table A-1 Common ACL Error Messages (continued)

Error Message	Explanation and Suggested Solution
%Error:Access Group is not supported on EtherChannel interface	This error message means that an access group is applied on an EtherChannel interface. Access groups can be applied only to Layer 2 physical interfaces or management VLANs.
%Error:A MAC Access Group exists on this interface	This error means that a MAC access group was previously configured on this interface. Delete the MAC access group by using the no mac access-group interface configuration command, and re-enter the ip access-group interface configuration command.
%Error:An IP Access Group exists on this interface	This error means that an IP access group was previously configured on this interface. Delete the IP access group by using the no ip access-group interface configuration command, and re-enter the mac access-group interface configuration command.
%Error:Out of Rule Resources	This error means that the hardware has run of resources. Re-enter the command with fewer ACEs.
%Error:No free rules on this interface	This error means that the hardware has run out of resources. Re-enter the command with fewer ACEs.
%Error:ASIC error	This error means that the hardware has returned an error and that the command cannot be completed.
%Error:ASIC out of resources	This error message means that the hardware does not have sufficient resources to support the user policies.
%Error:Mask/rule entry failure, errcode=XX	This error means that the hardware displays an unknown error with the specified error code.
%Error:FAILURE to reinsert old ACL	This error means a hardware failure. Delete the access group, and re-enter the command.
%Error:Max limit reached for number of ACEs in ACL :<acl_name>	The maximum limit for the number of ACEs in an ACL is reached. The ACE can not be added to the ACL.
%Error:access-list too large to support on this interface	The access list can not be applied on this interface because the interface does not have sufficient resources to meet the requirement of this access list. Re-enter the command with fewer ACEs.
%Error:FAILURE to reinsert old ACL, errcode=XX	This error means a hardware failure. Delete the access group, and re-enter the command.
%Error:Egress port invalid	This error message means that an invalid egress port was detected by the hardware. Re-enter the command for the interface.
%Error:The field sets of all the ACEs in an ACL should match	All the ACEs in an ACL must have the same mask. Change the ACE to have the same mask as the other ACEs in the ACL.