

VLAN Access List Configuration



Table of Contents

Chapter 1 Configuring VLAN Access List.....	1
---	---

Chapter 1 Configuring VLAN Access List

S2226 and all layer-3 switches support the VLAN-based access control function. The function can help users to filter unnecessary message in VLAN. In this way, high security is provided.

Each VLAN ACM consists of several access control lists (VLAN ACL) with different priorities. Each access control list comprises a match item and an action item. The match item can be an IP access control list or a MAC list. That the access list is not configured in the match item means that all flows are matched. That a null IP/MAC access control list is configured in the match item means that no flows can be matched. If an inexistent IP/MAC access control list is configured in the match item, items of VLAN ACL do not function. Only one IP/MAC access control list can be configured. If multiple IP/MAC access control lists are configured, only the last one is effective. Only one **permit** match item is in the IP/MAC access control list. If not, problem will occur if VLAN ACM is applied to a VLAN. Multiple permit match items can be created by configuring VLAN ACL for multiple times. The action item is **forward** or **drop**. The action item is **forward** by default. VLAN ACL performs the operation defined in the action item on flows that match the IP/MAC access control list. VLAN ACM uses each VLAN ACL according to its serial number in VLAN ACM and drops flows that cannot match any VLAN ACL. In this way, the access control is achieved. If you want to forbid the designated flow, configure a VLAN ACL that can forward all flows. In this way, flows that are not forbidden can be forwarded.

Run the following commands to configure VLAN access control list:

Run...	To...
vlan access-map <i>name seq</i>	Create a VLAN-based access control list. All configurations with the same parameter name belong to the same VLAN ACM. The parameter seq means the priority of VLAN ACL in VLAN ACM. The default value is the highest priority of VLAN ACM plus 5.
match <ip-acl mac-acl> <i>name</i>	Configure ip acl or mac acl of the VLAN acl whose match item's name is name .
action <drop forward>	Configure the action item of VLAN acl to drop or forward . The default value of the action item is forward .
vlan filter <i>name vlan</i>	Apply VLAN ACM whose name is name to VLAN. The parameter VLAN means the VLAN where the acm is applied to.