

配置VLAN访问列表

目 录

第 1 章	配置VLAN访问列表.....	1
1.1	配置基于VLAN的访问控制模型	1
1.2	配置示例.....	1

第1章 配置VLAN访问列表

1.1 配置基于VLAN的访问控制模型

通过使用该功能，可以将用户不希望收到的报文在 Vlan 上过滤掉。这样可以提供更好的安全性能。

每个 VLAN ACM 由若干条不同优先级的访问控制列表（VLAN ACL）组成，每个访问控制列表只允许匹配(match)一个匹配项，以及一种 action（forward or drop）。匹配项可以是一个 ip 访问控制列表或一个 mac 访问控制列表，匹配项中不配置访问列表表示匹配所有的流，如果配置了一个空的 IP/MAC 访问控制列表则匹配不到任何流，配置一个不存在的 ip/mac 访问控制列表则该 VLAN ACL 条目不起作用；通常在 ACM 的尾部配置一个这样的 ACL，作为默认规则，以允许或禁止转发所有前面未被匹配的报文。

动作分为转发和丢弃两种，默认为转发。

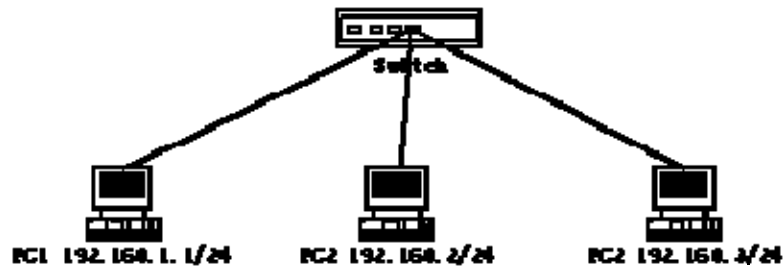
VLAN ACL 将能够匹配到该 ip 或 mac 访问控制列表的流执行动作中定义的操作，VLAN ACM 将按照序列号依次使用该 VLAN ACM 中每个 VLAN ACL，对于不能匹配到任何一个 VLAN ACL 的流不做任何操作，从而达到访问控制的目的。

使用下面的命令可以配置 VLAN 访问控制列表：

命令	说明
vlan access-map name seq	建立一个基于VLAN的访问控制列表。 所有name参数相同的配置被认为属于同一个VLAN ACM。 seq参数，表示该VLAN ACL在该VLAN ACM中的优先级，如果最大序列号与次大序列号之前的差值小于5，则在最大序列号的基础上加上5；否则在次大序列号的基础上加上5。
match <ip-acl mac-acl> name	配置该VLAN acl的匹配项为名字为name的ip acl或mac acl。
action <drop forward>	配置该VLAN acl的动作为转发或丢弃，默认为转发。
vlan filter name vlan vlan-list	将名字为name的VLAN ACM应用到VLAN上，VLAN参数表示需要应用该acm的VLAN列表。

1.2 配置示例

有如下网络环境：



三台 PC 机分别连接在交换机的 1、2、3 端口,同属于 VLAN 1, 要求这三台机器可以相互通过网络邻居访问, 这三台 PC 机都可以使用 IP 地址 192.168.1.10/24 telnet 到交换机上对其进行管理。由于交换机 VLAN 1 是默认的 VLAN, 端口的 pvid 也默认为 1, 因此只需要在 VLAN 1 接口下进行如下的配置

```
ip address 192.168.1.10 255.255.255.0
```

此外, 用户还希望三台 PC 机相互不能 ping 通, 这需要使用基于 VLAN 的访问控制模型来实现:

```
ip access-list extend ping
permit icmp any any
!
vlan access-map ping 5
action drop
match ip-acl ping
!
vlan access-map ping 10
action forward
!
vlan filter ping vlan 1
```