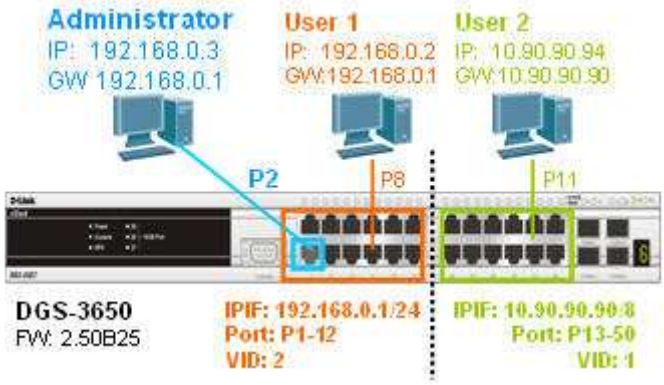
We try to use cpu acl for reduce traffic direct forward switch's cpu, and our demand acl policy was: Reserve one port which administrator user can access switch via web,telnet,ping...etc, but block **all traffic** which destination address is switch's CPU ip.

Example:
Assume that there are 2 ipif within DGS-3600, and only Administrator (port 2) can access to each ipif, the other ports do not allow to access it.

[Topology]



[Configuration]

```
reset config
create vlan v2 tag 2
config vlan v2 add untagged 1-12
config vlan default delete 1-12
create ipif i2 192.168.0.1/24 v2
create cpu access_profile profile_id 1 ip destination_ip_mask 255.255.255.255
config cpu access_profile profile_id 1 add access_id 1 ip destination_ip 10.90.90.90  port 1,3-50 deny
config cpu access_profile profile_id 1 add access_id 2 ip destination_ip 192.168.0.1  port 1,3-50 deny
enable cpu_interface_filtering
```

[Procedure]

0) set the topology, configuration into switch. Then connect each PCs onto DGS-3650.

1) Only "Administrator" on port 2 can access to both 10.90.90.90 and 192.168.0.1, with all the traffic handled by CPU (ex: snmp, icmp, telnet, web...etc).

2) Both "User 1" and "User 2" cannot access to CPU IP, but they can ping to each other successfully (192.168.0.2 can ping to 10.90.90.94, and vice versa). So it means switch will not drop user's traffic to internet, only deny the traffic onto CPU IP.