Access Control List

(Classifier & Policy Rule)

Ethernet Switch

Support Notes

Version 3.70

April 2006

ZyXEL

Unleash Networking Power

Setting up Classifier & Policy rule to perform Access Control on your Switch

Introduction to ACL

ACL (Access Control List) is the name of a combination of Classifier and Policy Rule. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow. A policy rule ensures that a traffic flow gets the requested treatment in the network. Please be advised, that you must first configure a classifier in the Classifier screen before you configure a policy rule.

The relative weight of parameters in ACL

In the classifier, there are a lot of parameters that we can set. Each parameter has a relative weight. This relative weight is meaningless unless there is a multiple match (or conflict) of the rules.

Here is the order of weight from lowest to the highest:

1. [Source-port]
2. [Destination-port]
3. [Packet-format]
4. [Destination-mac]
5. [Source – mac]
6. [Priority]
7. [VLAN ID]
8. [Ethernet-type]
9. [DSCP]
10. [IP-Protocol]
11. [Source-IP]
12. [Destination-IP]
13. [Source – Socket]
14. [Destination – Socket]
15. [Establish Only]

If you choose a combination of parameters as your rules, the rule with a

higher weight of parameter gets the highest weight. For example, you have defined the first classifier to have “Source Port” plus “Source Socket” as your rule parameters; and your second classifier has only “Destination Socket” as your rule parameter; at this time, since “Destination Socket” has a relatively higher weight compared to “Source Port” or “Source Socket”, the second classifier will have a higher weight.

The higher the weight a classifier has, the higher the priority its related policy rule will have. A higher priority policy rule can always overrun a lower priority policy rule.

ACCESS CONTROL ACL Flow Example

In general, access control is done by assigning a policy for traffic at-large and a specific policy for a subset. An example is if the network administrator wants to deny all IP traffic originated from the subnet 192.168.3.xx, except from the ICMP traffic. The ICMP traffic is a subset of generic IP traffic. To implement this policy, the ACL conflict resolution logic is required to handle this multiple matching scenario.

In this scenario, all IP traffic originating from the 192.168.3.xx subnet is discarded. This is implemented by the **first rule**, which includes the following:

• Layer 3 protocol type = IP

• IP source address = 192.168.3.0/24

Any packet matching is discarded as specified in ACTION—but if there is ICMP traffic originated from the 192.168.3.xx subnet, it should be forwarded. This is supported by the **second rule**, with the following:

• Layer 3 protocol type = IP

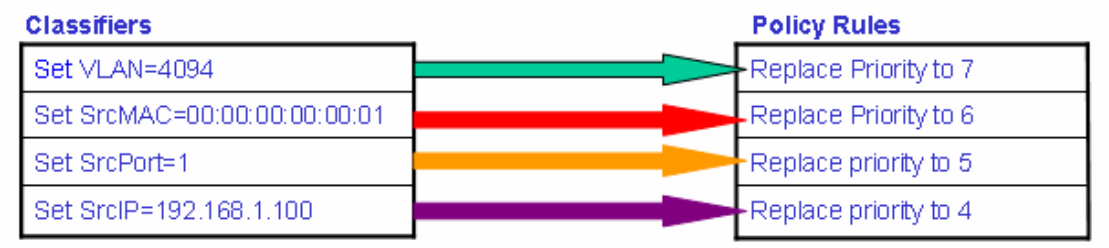
• Layer 4 protocol type = ICMP

• IP source address = 192.168.3.0/24

The action of the second rule is not to discard the packet (Do not drop the matching frame previously marked for dropping).

When two rules match a packet and the resulting actions are conflicting (discard versus not-discard), a higher layer rule has priority over lower layer rule. In this case, the action of the second rule (Layer 4) is carried out because the first rule is only Layer 3 and lower.

QoS ACL Flow Example



Here is another scenario to help you understanding the flow of ACL. There are totally 4 rules.

First rule contains the following:

• When there is traffic from Layer 2 VLAN ID = 4094

Any matching packet will be set the Priority to 7

Second rule contains the following:

•When there is traffic from Layer 2 Source MAC address = 00:00:00:00:00:01

Any matching packet will be set the Priority to 6

Third rule contains the following:

•When there is traffic from Layer 2 Source Port = 1

Any matching packet will be set the Priority to 5

Fourth rule contains the following:

•When there is traffic from IP source address = 192.168.1.100/32

Any matching packet will be set the Priority to 4

The above four rules are conflicting with each other since you can have traffic coming from port 1 and also come with a source IP address of 192.168.1.100.

When two or more rules match a packet and the resulting actions are conflicting (Set to different priority value), a higher layer rule has priority over lower layer rule. In this case, the action of the fourth rule (Layer 3) is carried out because the other rules are only Layer 2 and lower. Although VLAN, MAC, Port are all belonging to Layer two, their carrying out priority would be VLAN>MAC>Port.

In conclusion, every parameter (or rule) in the packet header has a weight. The deeper the parameter in the packet header, the higher the weight is.

Furthermore, the parameter deeper in the packet header has much higher weight than shallower parameters.

ACL Scenario

How should I configure if I only allow certain IP address on a certain port to forward its traffic but deny all others?

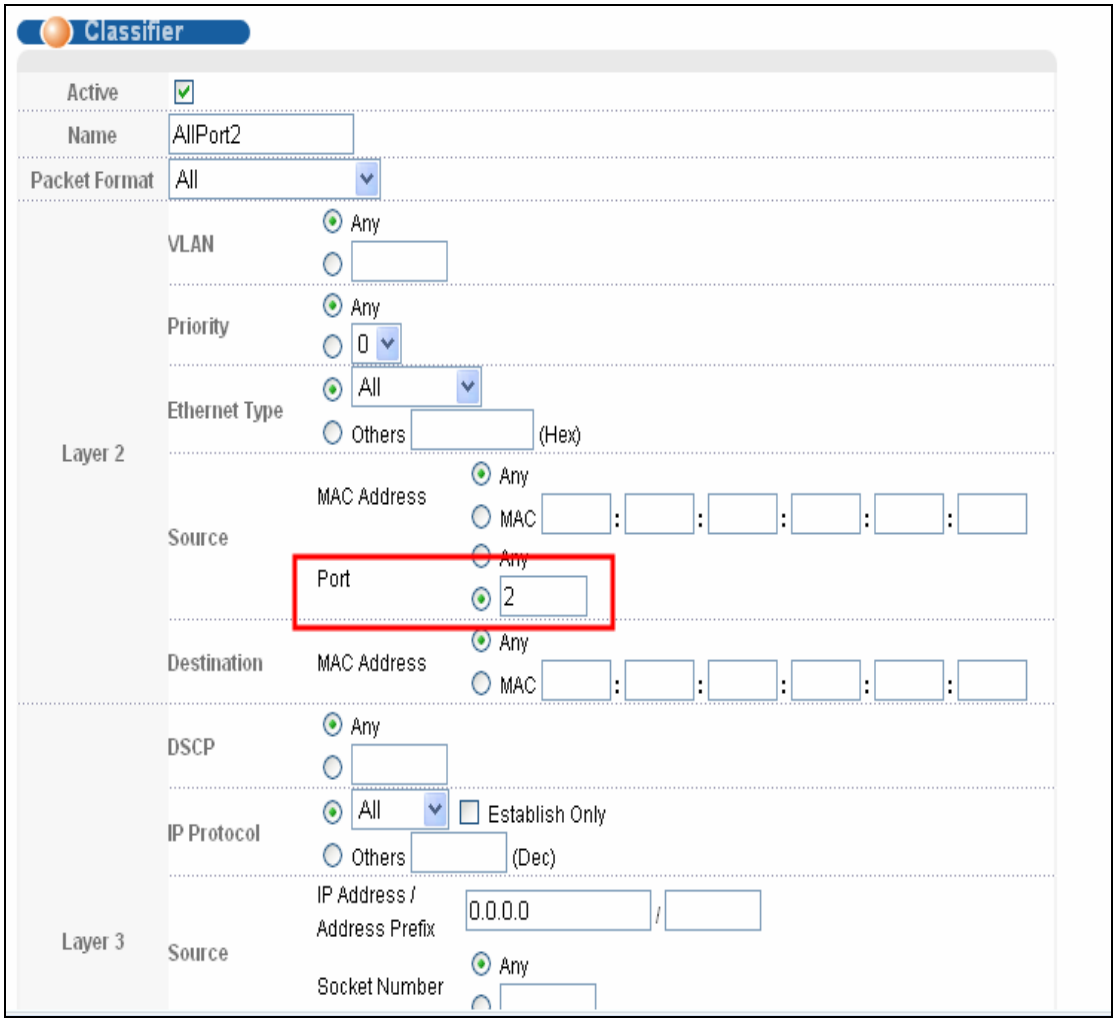
In the beginning, we need to set up the classifier to group traffic into data flows based on some criteria such as source address, destination address, port number and packet format. In this example, we specify which format of the packet the Switch will apply its policy rules to. We define three rules. First, we define a classifier for the traffic that is coming from port 2 and its source address 172.23.3.120; second, we specify a classifier for the traffic from port 2. Finally we specify a classifier for ARP.

After the classification, we need to define the policy rule to ensure that the traffic gets the deserved treatment in the network. Here, we also define three policy rules. The first policy rule is to forward (do not drop the matching frame previously marked for dropping) only the traffic from port 2 and with the ip address of 172.23.3.120. The second policy rule is to discard all the traffic from port 2 on first classifier; and we apply the second policy rule on second classifier. Moreover, do not forget to apply a policy rule (do not drop the matching frame previously marked for dropping) for our last classifier.

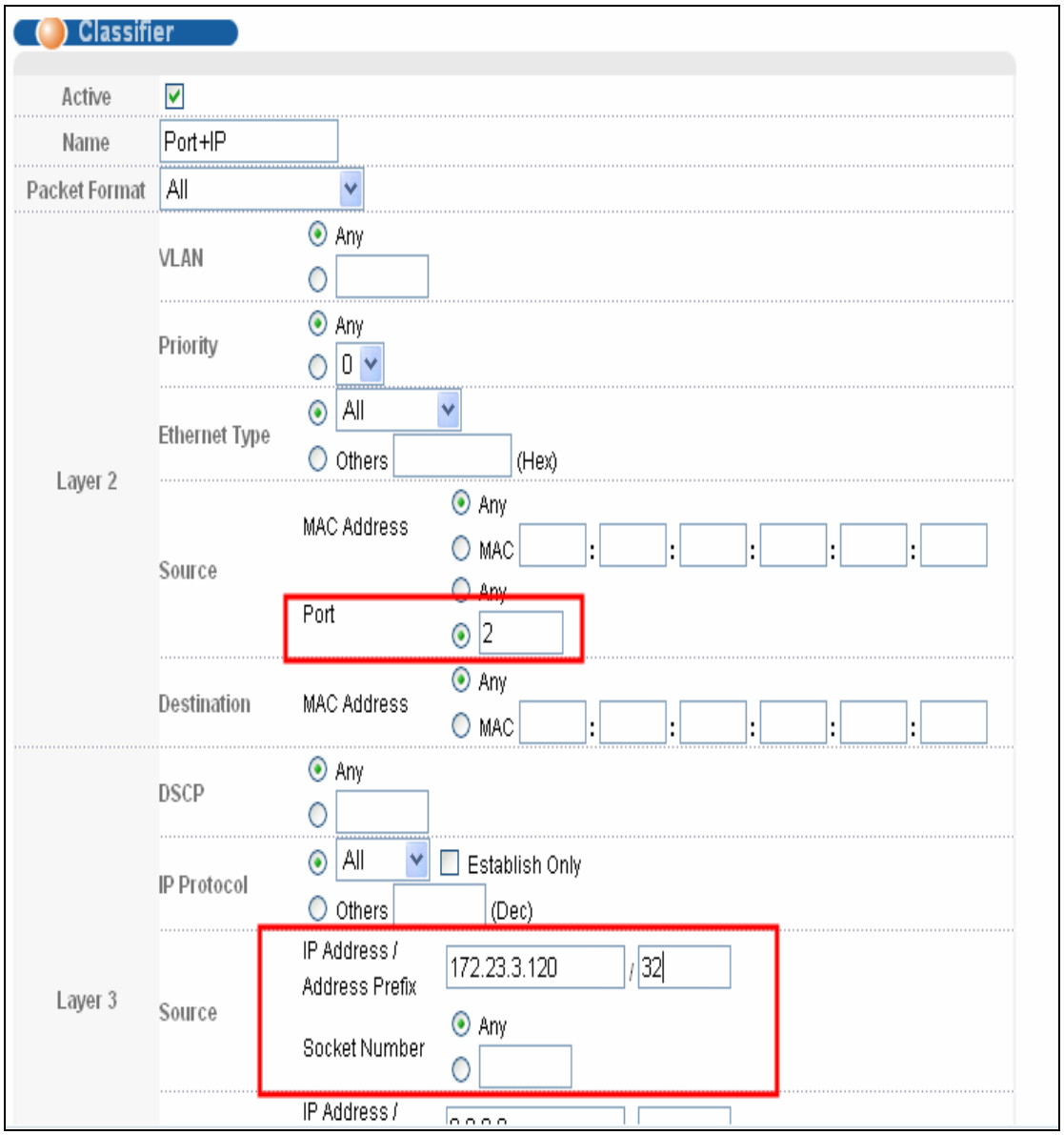
The logic is like this. Since the first rule has a higher weight (layer 3 V.S. layer2) then the second rule and third rule, although the second rule says “drop all from port 2”, the first rule will overwrite the action of all other rules since rule one has the higher weight. Therefore, all other traffic from port 2 will be dropped, but traffic coming from port 2 with 172.23.3.120 will be forwarded.

GUI configuration of classifier and policy rule.

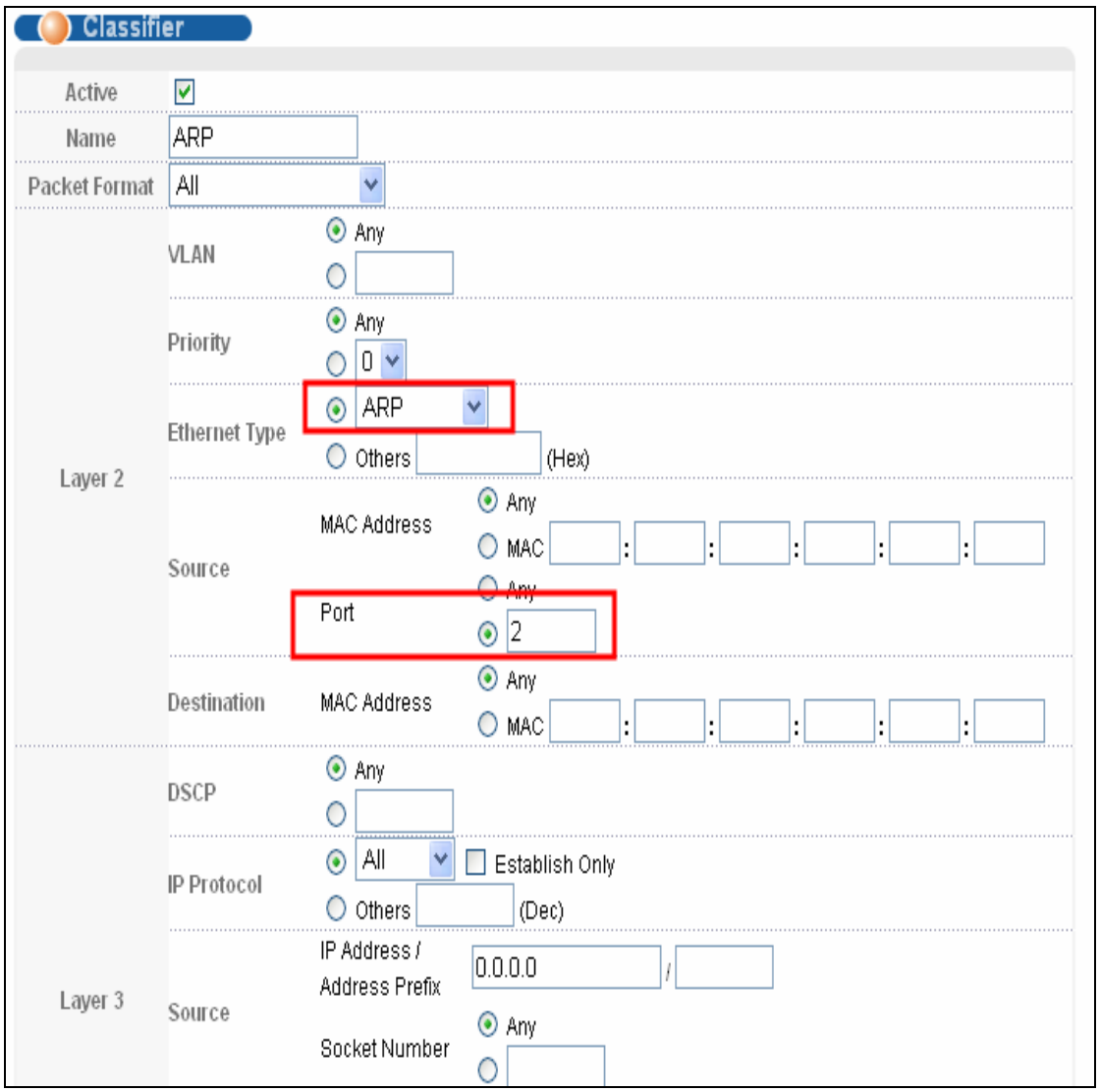
Classifier 1



Classifier 2

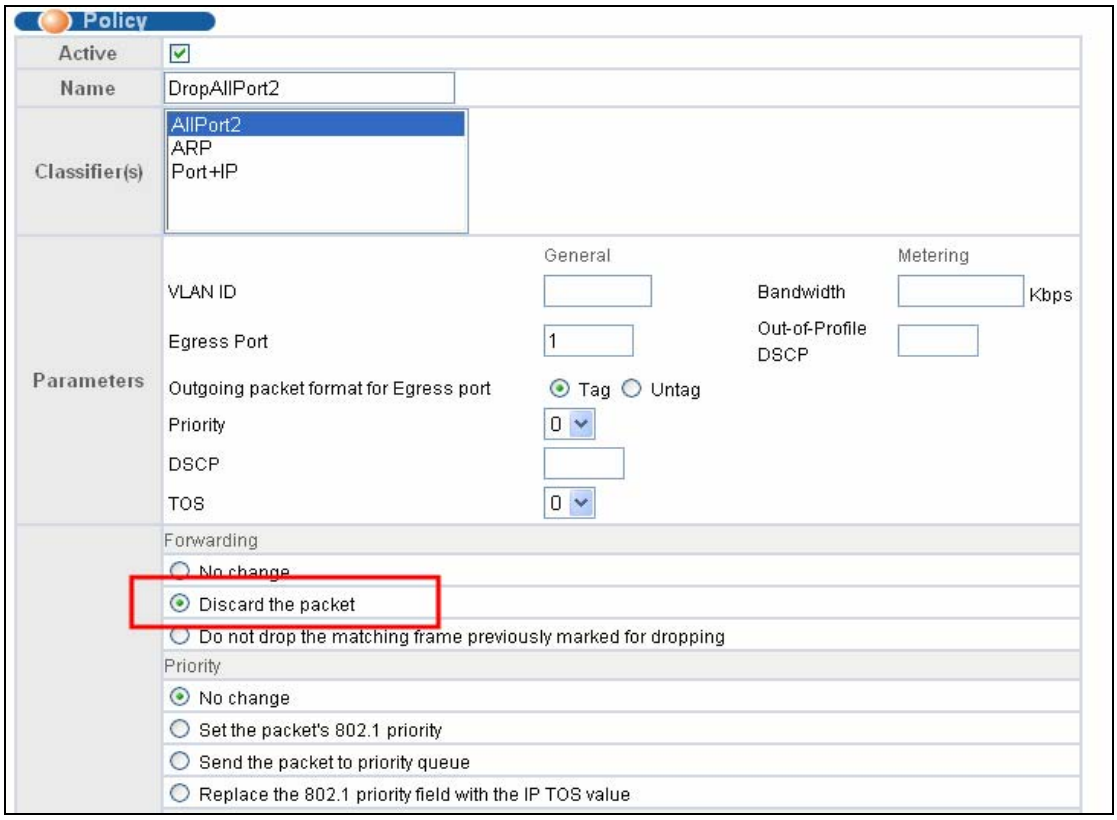


Classifier 3

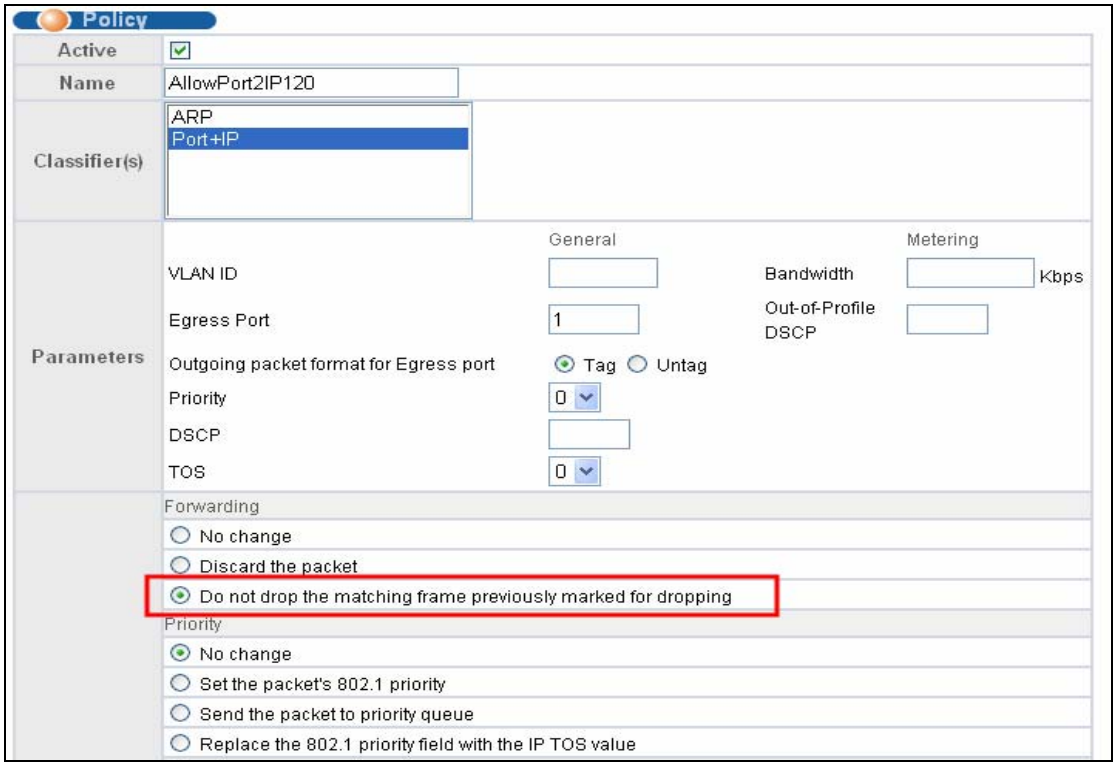


Policy Rule Configuration

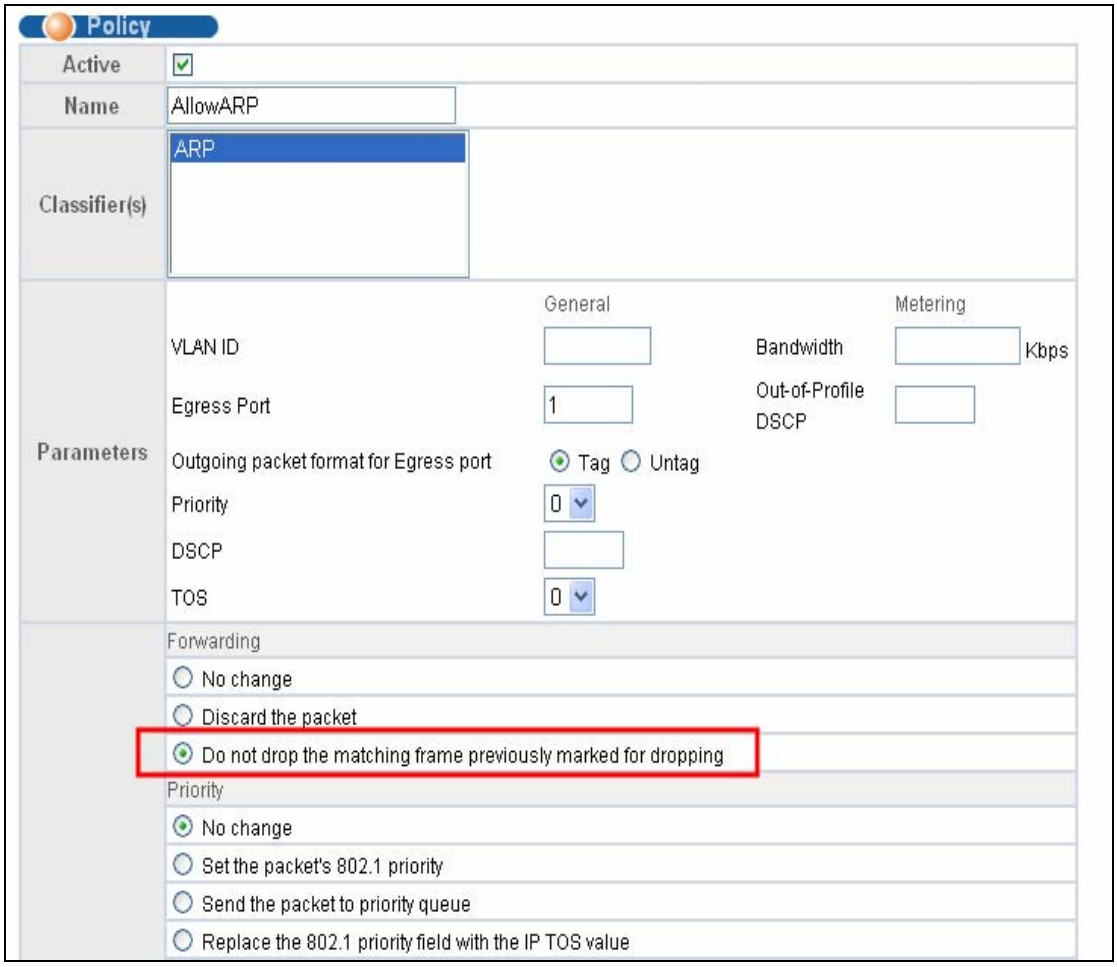
Policy rule on Classifier 1



Policy rule on classifier 2



Policy rule on classifier 3



CLI configuration of classifier and policy rule.

Please logon to the Switch by either telnet, SSH or Console.
Switch into the configuration mode and issue the following commands:

Classifier 1
Switch(config)#classifier AllPort2 source-port 2

Classifier 2
Switch(config)#classifier ARP ethernet-type arp source-port 2

Classifier 3
Switch(config)#classifier Port+IP ethernet-type ip source-port 2 source-ip 172.23.3.120 mask-bits 32

Policy rule on classifier 1
Switch(config)#policy AllowARP classifier ARP vlan 1 egress-port 1 priority 0 dscp 0 tos 0 bandwidth 0 outgoing-packet-format tagged out-of-profile-dscp 0 forward-action forward

Policy rule on classifier 2
Switch(config)#policy AllowPort2IP120 classifier Port+IP vlan 1 egress-port 1 priority 0 dscp 0 tos 0 bandwidth 0 outgoing-packet-format tagged out-of-profile-dscp 0 forward-action forward

Policy rule on classifier 3
Switch(config)#policy DropAllPort2 classifier AllPort2 vlan 1 egress-port 1 priority 0 dscp 0 tos 0 bandwidth 0 outgoing-packet-format tagged out-of-profile-dscp 0 forward-action drop

Verifying your result

Connect a PC “A” to the Switch on port2. Connect another PC “B” to the Switch on port10 with IP 172.23.3.191. First set the IP of PC “A” to 172.23.3.120. At this time, PC “A” can ping PC “B”. However, if you set the IP of PC “A” to another IP besides 172.23.3.120, it can no longer ping PC “B”.