Allied Telesis

How To | Configure Filtering Actions On QoS Flow Groups And Traffic Classes

Introduction

Just as you can configure dedicated hardware filters, it is also possible to achieve filtering activity as part of the QoS process.

This is carried out by using the **action** parameter that is available on QoS flow groups and traffic classes:

```
set qos flowgroup=<id-list>
   action={none|forward|forward,sendmirror|discard|
   discard,sendmirror|sendmirror|sendmirror,sendvlanport|
   sendvlanport}
   [vlan=<vlan-id>] [port=<port>] [<other-options>]

set qos trafficclass=<id-list>
   action={forward|forward,sendmirror|discard|discard,sendmirror|
   sendmirror|sendmirror,sendvlanport|sendvlanport}
   [vlan=<vlan-id>] [port=<port>] [<other-options>]
```

What information will you find in this document?

This Note provides information to allow you to understand in detail how filtering actions can be used in conjunction with QoS. We will:

- look at the operation of each of the values of the **action** parameter.
- examine the difference between configuring actions on a flow group and configuring actions on a traffic class.
- see how this ability to configure actions within QoS policies effectively gives you the ability to create filters on a per-ingress-port basis.

Which products does it apply to?

This Note applies to the following Allied Telesis routers and managed layer 3 switches:

- AT-8948 switches
- AT-9900 series switches
- AT-9900s series switches
- x900 series switches

It requires AlliedWare software version 2.7.3 or later, or 3.1.1 or later.

Related How To Notes

You may also find the following How To Notes useful:

- *Overview of Quality Of Service (QoS) Features On AT-8948, AT-9900, AT-9900s, And x900 Series Switches*
- *How To Configure QoS On AT-8948, AT-9900, AT-9900s, And x900 Series Switches*
- *How To Use Hardware Filters On AT-8948, AT-9900, AT-9900s, And x900 Series Switches*

How To Notes are available from www.alliedtelesis.com/resources/literature/howto.aspx.

How different actions operate

action = discard

What it does

If you specify an action of discard, the traffic will be dropped.

When to use it

This action is used when one aspect of the QoS policy is a decision to simply disallow certain traffic flows.

How to configure it

Consider a situation where multiple clients are attached to the switch, each client being attached to a different port. Each client is offered a specific service, which includes a particular QoS profile, and a set of allowed traffic types.

Suppose that the client on port 1 is using a service that does not allow any multicast packets to be sent. The QoS policy for this client could be configured as shown in the following configuration.

1. Create a classifier to match all multicast packets

```
create classifier=1 ipdaddress=224.0.0.0/3
```

2. Create a flow group which uses the classifier

```
create qos flowgroup=1
add qos flowgroupow=1 classifier=1
set qos flowgroup=1 action=discard
```

3. Create a traffic class and add the flow to the traffic class

```
create qos trafficclass=1  <other-options>
add qos trafficclass=1 flowgroup=1
```

4. Create a policy and add the traffic class to the policy

```
create qos policy=1
add qos policy=1 trafficclass=1
```

5. Apply the policy to port 1

```
set qos port=1 policy=1
```

action = forward

What it does

If you specify an action of forward, the traffic will be forwarded normally.

When to use it

The packets matched to the classifiers of the flow group will be forwarded normally. The circumstance where you need to explicitly forward some particular traffic flow would be in a case where you want to discard a wide range of traffic, but still want to forward some small subset of traffic within that range. For example, if you wish to prevent the forwarding of multicast traffic in general, but wish to support an application that needs to sends packets to one particular multicast address.

How to configure it

1. Create the classifiers

Create one classifier to match all multicast packets, and one classifier to match packets to the particular multicast address 236.5.8.213

```
create classifier=1 ipdaddress=236.5.8.213/32
create classifier=2 ipdaddress=224.0.0.0/4
```

2. Create two flow groups, one for each classifier

```
create qos flowgroup=1
add qos flowgroup=1 classifier=1
set qos flowgroup=1 action=forward
create qos flowgroup=2
add qos flowgroup=2 classifier=2
set qos flowgroup=2 action=discard
```

3. Create a traffic class and add the flows to the traffic class

```
create qos trafficclass=1  <other parameters …>
add qos trafficclass=1 flowgroup=1,2
```

4. Create a policy and add the traffic class to the policy

```
create qos policy=1
add qos policy=1 trafficclass=1
```

5. Apply the policy to port 1

```
set qos port=1 policy=1
```

Now when a packet is received on port 1, it will be matched against the flow groups in order. And when there is a match, the packet will be associated with the first flow group whose classifier it matches, and the packet will not be matched against the rest of the classifiers. Then the action configured on that flow group will be applied.

action = sendvlanport

What it does

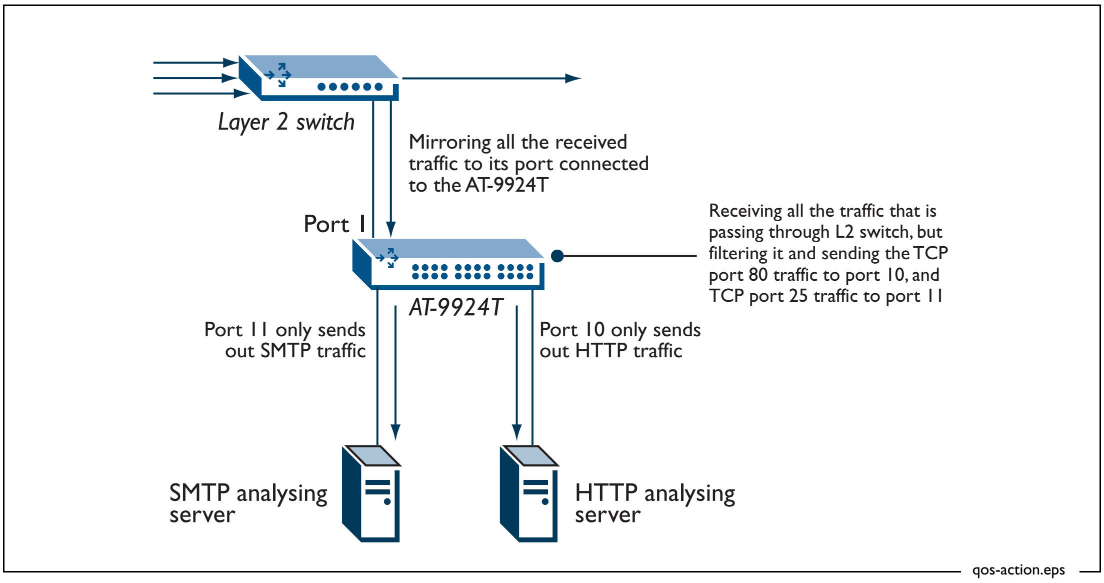
If you specify an action of sendvlanport, both VLAN and port must also be specified. Traffic will be sent to the VLAN specified by the VLAN parameter and the port specified by the port parameter. The VLAN must exist and the specified port must be a member of that VLAN. The switch determines whether the port is tagged or untagged for that VLAN, and sends the traffic with the correct tag if the port is tagged. If the port is untagged for the specified VLAN the frame is sent untagged.

When to use it

You need to configure this action whenever you want to force the flow to leave from a specific port of the switch.

How to configure it

Let's suppose you are receiving mirrored traffic from a Layer 2 switch, and want to analyse the HTTP and SMTP packets that we receive by using some special application servers, as shown in the illustration below.


Layer 2 switch
Mirroring all the received traffic to its port connected to the AT-9924T
Port 1
Receiving all the traffic that is passing through L2 switch, but filtering it and sending the TCP port 80 traffic to port 10, and TCP port 25 traffic to port 11
AT-9924T
Port 11 only sends out SMTP traffic
Port 10 only sends out HTTP traffic
SMTP analysing server
HTTP analysing server
qos-action.eps

1. Create the classifiers

Create classifiers for the packets you want a match for.

```
create classifier=1 tcpdport=80
create classifier=2 tcpdport=25
```

2. Create two flow groups

Creating two flow groups will put the two classifiers into different groups. After assigning them to different flows, you can set the destination switch port for these flows.

```
create qos flowgroup=1
add qos flowgroup=1 class=1
set qos flowgroup=1 action=sendvlanport vlan=1 port=10
create qos flowgroup=2
add qos flowgroup=2 classifier=2
set qos flowgroup=2 action=sendvlanport vlan=1 port=11
```

3. Create a traffic class and add the flows to the traffic class

```
create qos trafficclass=1
add qos trafficclass=1 flowgroup=1,2
```

4. Create a policy and add the traffic class to the policy

```
create qos policy=1
add qos policy=1 trafficclass=1
```

5. Set the policy

Set the policy you created to port 1 where you are receiving the mirrored traffic.

```
set qos port=1 policy=1
```

action = sendmirror

What it does

If you specify an action of sendmirror, a copy of the traffic will be sent to the preconfigured mirror port.

When to use it

If you want to mirror the specific kind of traffic(s) from specific port(s), you will need to use this action. The standard port mirroring process sends ALL the traffic from the mirrored port to the mirror port, but the act of configuring the sendmirror action on a flowgroup makes it possible to send just certain traffic to the mirror port.

How to configure it

Suppose that we want to capture the HTTP (80) and SMTP (25) traffic coming to users who are connected to ports 1 and 2.

1. Set a mirror port and enable switch mirroring

```
set switch mirror=10
enable switch mirror
```

2. Create classifiers

Create classifiers for the packets you want a match for.

```
create classifier=1 tcpdport=80
create classifier=2 tcpdport=25
```

3. Create a flow group

Create a flow group which puts these two classifiers together.

```
create qos flowgroup=1
add qos flowgroup=1 classifier=1,2
set qos flowgroup=1 action=sendmirror
```

4. Create a traffic class and add the flow to the traffic class

```
create qos trafficclass=1
add qos trafficclass=1 flowgroup=1
```

5. Create a policy and add the traffic class to the policy

```
create qos poliicy=1
add qos policy=1 trafficclass=1
```

6. Set the policy

Set the policy you created to ports 1 and 2 to mirror the HTTP and SMTP traffic.

```
set qos port=1,2 policy=1
```

action = none (default action)

What it does

If you specify an action of **none** for a flow group, the action will be overridden with the setting of the flow group's traffic class. This action is the default action.

When to use it

You use this action when you want to set an action for the flow group in a traffic class at a traffic class level.

How to configure it

The example given below is an alternative way to configure a policy to discard a wide range of traffic, but allow through a small subset of that range.

To fully understand how this example configuration works, look at the discussion on the relative precedence of actions configured on a flow group and actions configured on a traffic class section on page 11.

1. Create classifiers

Create one classifier to match all multicast packets, and one classifier to match packets to the particular multicast address 236.5.8.213.

```
create classifier=1 ipdaddress=236.5.8.213/24
create classifier=2 ipdaddress=224.0.0.0/3
```

2. Create flow groups

Create two flow groups - one for each classifier.

```
create qos flowgroup=1
add qos flowgroup=1 classifier=1
set qos flowgroup=1 action=forward
create qos flowgroup=2
add qos flowgroup=2 classifier=2
set qos flowgroup=2 action=none
```

3. Create a traffic class and add the flows to the traffic class

Create a traffic class and add these flows to the traffic class

```
create qos trafficclass=1 action=discard
add qos trafficclass=1 flowgroup=1,2
```

4. Create a policy and add the traffic class to the policy

```
create qos policy=1
add qos policy=1 trafficclass=1
```

5. Apply the policy to port 1

```
set qos port=1 policy=1
```

action = *x*, sendmirror

Where *x* can be either **forward** or **discard** as discussed above.

What it does

This action does the same thing as discussed earlier with the action *x*, and also sends a copy of the packets matching that action to the mirror port.

When to use it

You use this action when you want to do action *x*, and also capture the packet to which action *x* is applied.

How to configure it

Suppose that the users in port 1 and 2 are banned from using HTTP (80) and HTTPS (443) traffic, but allowed to use other applications. You want to capture (mirror) the packets that you are blocking, and keep a track of which users are trying to use banned applications.

All other users on the switch are allowed to use all applications.

1. Set a mirror port on the switch and enable mirroring

```
set switch mirror=10
enable switch mirror
```

2. Create classifiers for the packets you want a match for

```
create classifier=1 tcpdport=80
create classifier=2 tcpdport=443
```

3. Create a flow group

Create a flow group which puts the two classifiers together.

```
create qos flowgroup=1
add qos flowgroup=1 classifier=1,2
set qos flowgroup=1 action=discard,sendmirror
```

4. Create a traffic class and add the flow to the traffic class

```
create qos trafficclass=1
add qos trafficclass=1 flowgroup=1
```

5. Create a policy and add the traffic class to the policy

```
create qos policy=1
add qos policy=1 trafficclass=1
```

6. Set the policy

Set the policy that you created to ports 1 and 2 to discard the HTTP and HTTPS traffic.

```
Set qos port=1,2 policy=1
```

An example configuration with a combination of actions

Suppose that our network has the following rules:

1. Users are connected to ports 1 to 15. The switch mirror port is 21, and there is a virus-checking server on port 20.
2. Users are allowed to surf the Internet (HTTP and HTTPS only).
3. 10.1.1.99 has right to use telnet, but this request will be logged.
4. Any other telnet request is discarded and logged.

All other applications will not be allowed. Any packet that does not comply with the defined rules will be sent to the virus-checking server for further examination.

1. Set a mirror port on the switch and enable mirroring

```
set switch mirror=21
enable switch mirror
```

2. Create classifiers

Create classifiers for the packets you want to match. Classifier 3 is for DNS, and classifier 6 is for the ARP protocol.

```
create classifier=1 tcpdp=80
create classifier=2 tcpdp=443
create classifier=3 udpdp=53
create classifier=4 ipsaddr=10.1.1.99 tcpdp=23
create classifier=5 tcpdp=23
create classifier=6 protocol=0806 ethformat=ethii-untag
```

3. Create flow groups

Create a flow group which puts these classifiers into groups according to the actions we wanted to set.

Also, create a flow group for the allowed HTTP and HTTPS traffic. Note that the DNS port and ARP protocol are also allowed for name resolution.

```
create qos flowgroup=1
add qos flowgroup=1 classifier=1,2,3,6
```

4. Create a flow group for allowed telnet requests

Create flow group for the allowed telnet requests from 10.1.1.99, and send a copy of them to the mirror port so the server can log them.

```
create qos flowgroup=2
add qos flowgroup=2 classifier=4
set qos flowgroup=2 action=forward,sendmirror
```

5. Create a flow group for banned telnet requests

Create a flow group for the banned telnet requests, and send a copy of them to the mirror port so the server can log them.

```
create qos flowgroup=3
add qos flowgroup=3 classifier=5
set qos flowgroup=3 action=discard,sendmirror
```

6. Create a traffic class and add the flows to the traffic class

```
create qos trafficclass=1
add qos trafficclass=1 flowgroup=1,2,3
```

7. Create a policy and add the traffic class to the policy

Do not forget that the default action is forward, so you do not need to change it.

```
create qos policy=1
add qos policy=1 trafficclass=1
```

8. Set the action for traffic that doesn't match any of the classifiers

Set the action for the traffic which did not match to any of the classifiers (default traffic class) for this policy. You are going to send all the unmatched traffic to your anti-virus checking server for further examination.

```
set qos policy=1 dtcaction=sendvlanport vlan=1 port=20
```

9. Set the policy to the needed customer ports

```
set qos port=1-15 policy=1
```

A discussion on the relative precedence between actions configured on flow groups and those configured on traffic classes

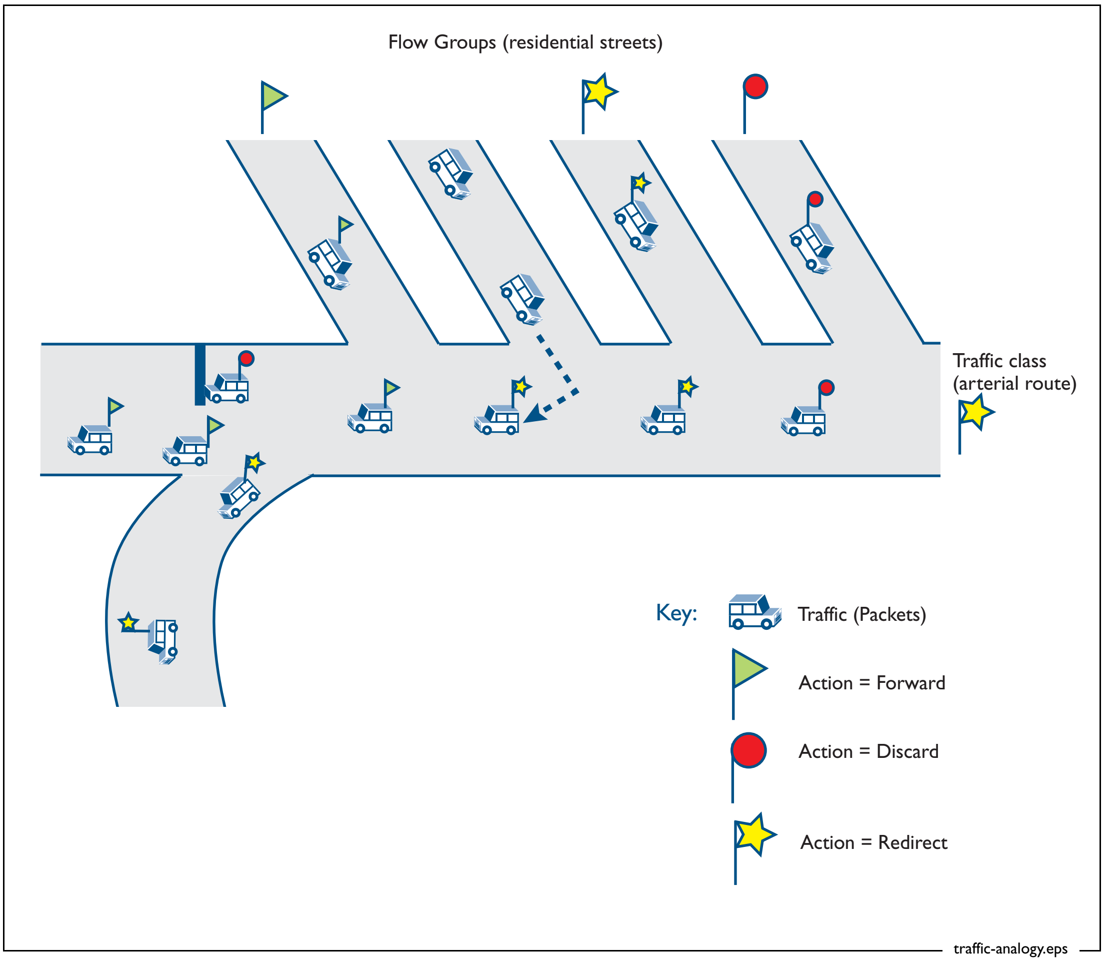
A flow group can have an action defined on it, and then the flow group is added to a traffic class, and the traffic class can also have an action defined on it. In this situation, if the action defined on the flow group is different to that defined on the traffic class, what happens? What action is actually applied to the packets that match this flow group?

The answer is that the action on a flow group takes precedence. For example, if you mark a packet **forward** in a flow group, it will be forwarded even if its traffic class's action is set to **discard**. If you mark the packet **discard** at flow group level, it will be discarded even if its traffic class's action is set to **forward**.

The logic behind flow group and traffic class relationship

What is the reasoning behind this choice to make the traffic class take precedence over the flow group?

To explain the best way to think about this, we will introduce a road-traffic analogy, as shown in the following figure. The analogy is discussed on the next page.



Think of the flow group as being a residential street, and the traffic class as an arterial route that the residential streets connect to.

All the cars that come down the residential streets must then proceed onto the arterial route.

Imagine that as cars enter the residential streets they are adorned with a flag that indicates the 'action' allocated to their street. A green flag represents 'forward', a red flag represents 'discard', a yellow flag represents 'redirect', etc. On those streets to which no action is allocated, the cars do not receive a flag.

As the cars turn out of the residential streets and enter the arterial routes, those cars that do not currently have a flag are adorned with the flag that represents the action allocated to the arterial route (traffic class). Those cars that already have a flag do not receive a new flag.

The arterial routes lead into motorways (policies).

As the cars try to enter the motorway, their flags are examined, and appropriate actions are taken: cars with red flags are blocked from going any further, cars with green flags are waved on through, cars with yellow flags are directed into a special lane, etc.

Effective filtering per ingress port

You can also discard packets by creating a hardware filter, so what is the main difference?

When you create a hardware filter, it is applied to the all ports of the switch. Remember that you can apply the QoS policy to one or more specific ports of the switch. By creating a QoS flow group with a discard action, and assigning it to a traffic class, and a QoS policy, and assigning that QoS policy to specific port(s), you are able to discard the specified flow **only on the applied ports**.

For example, suppose that the users on ports 1 and 2 are banned from using HTTP (80) and HTTPS (443) traffic, but allowed to use other applications. All other users on the switch are allowed to use all applications.

Assume our example has are more than 50 PCs connected to each port, so writing a hardware filter with all IP addresses as source addresses would take a long time.

To use QoS actions to discard the IP traffic received from switch ports 1 and 2 with destination address set to **any**, with protocol TCP, port 80 and 443, do the following steps.

1. Create classifiers

Create classifiers for the packets you want a match for.

```
create classifier=1 tcpdport=80
create classifier=2 tcpdport=443
```

2. Create a flow group which puts the two classifiers together

```
create qos flowgroup=1
add qos flowgroup=1 classifier=1,2
set qos flowgroup=1 action=discard
```

3. Create a traffic class and add the flow to the traffic class

```
create qos trafficclass=1
add qos trafficclass=1 flowgroup=1
```

4. Create a policy and add the traffic class to the policy

```
create qos policy=1
add qos policy=1 trafficclass=1
```

5. Set the policy

Set the policy that you created to ports 1 and 2 to discard the HTTP and HTTPS traffic.

```
set qos port=1,2 policy=1
```

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

Connecting The IP World

Allied Telesis