Hewlett Packard Enterprise

HPE aruba networking

AOS-CX 10.13 Update: QoS Policing – Exceed action of Remark

Corey Dow

November 14, 2023

Agenda

1	Overview
2	Use Cases
3	Details
4	Configuration
5	Best Practices
6	Troubleshooting
7	Demo

Overview

Overview

- Why is it important to customers?
  - QoS traffic policing is widely used in policing traffic entering ISP networks
  - Traffic policies act based on match criteria with different traffic classes that can achieve the following results:
    - Forward the packet if the result is “conforming”
    - Drop the packet if the result is “exceed”, i.e., non-conforming bandwidth
    - **Remark the packet**, i.e., downgrade the service, if the result is exceed **(New with 10.13)**
      - For example, on a downstream switch, traffic marked with Expedited Forwarding (EF) DSCP values set may be remarked to CS5 as it leaves towards an upstream switch
      - An upstream switch could then, upon receipt, forward the exceed traffic into a lower priority queue to allow only the highest priority traffic to be serviced 1st, i.e., VoIP traffic in most cases where there is competing EF traffic less critical than voice
  - Traffic policing policies may be applied either in the inbound (ingress) direction or outbound (egress) direction

Policing Acronyms – RFC 2697

CIR – Committed Information Rate
Threshold defines the average bandwidth limit (kbps on AOS-CX) guaranteed for traffic that conforms to the configured traffic policy

CBS – Committed Burst Size
A “Byte” token bucket value that defines the number of bytes in the token bucket that is allowed to exceed the CIR; **MUST NOT be ZERO**

EBS – Excess Burst Size (Unused on AOS-CX)
Used by some vendors with tri-color policing policies, i.e., red, yellow, or green that “color” the packet based on what is available in each of the token buckets, and allows different remarks based on the color

QoS Policing Exceed Action of Remark DSCP Overview

Platform Support

Ingress Only

Ingress Only

Feature	4100i	6000	6100	6200	6300	6400	8100	8320	8325	8360	8400	9300	10000	OVA
Policing Exceed Action of Remark DSCP **(New to 10.13.0001)**	No	No	No	No	**Yes**	**Yes**	**Yes**	No	**Yes**	**Yes**	No	No	**Yes**	No

- Note: 8325 and 10K platforms do not support applying traffic policies in the egress direction
- Links to existing QoS Documentation

https://www.arubanetworks.com/techdocs/AOS-CX/10.12/PDF/qos_6200-6300-6400.pdf
https://www.arubanetworks.com/techdocs/AOS-CX/10.12/PDF/qos_8100-8360.pdf
https://www.arubanetworks.com/techdocs/AOS-CX/10.10/PDF/qos_832x-10000.pdf

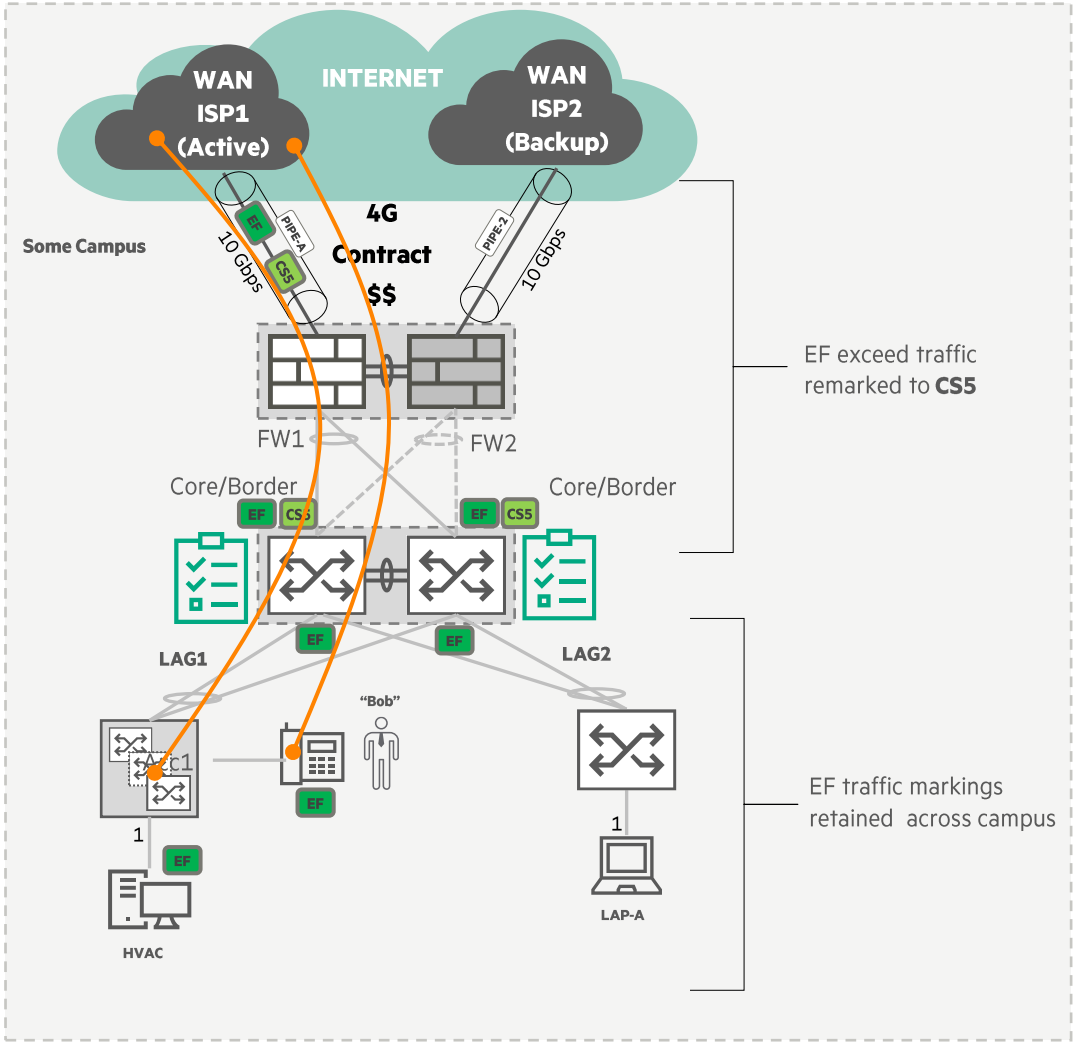
Use Cases

Use Cases – Single or Dual ISP with Bandwidth Allocation Contracts

Outbound (Egress) Policy Applied at Campus Core – Primary Use Case

- Large school district that pays a service for a **minimum bandwidth of 4Gbps** but will be charged for traffic that exceeds that bandwidth up to the 10Gbps physical connection to the two ISPs
  - A bit rate contract is negotiated with the Service Provider
- Priority for Voice is always given highest priority and is marked with **DSCP 46** for Expedited Forwarding (EF)
- HVAC monitoring is also considered high priority and is marked with **DSCP 46**, however, the traffic needs to be marked down if it exceeds specified rates to not violate the service provider contract
- Prior to 10.13 the only option for traffic policing was to **drop the traffic if it exceeds CIR/CBS thresholds**
- Now, with 10.13, a policy may be applied to **remark the HVAC monitoring traffic** to ensure QoS is maintained for voice quality

- The remark policy is **configured on the Campus Core**, in the outbound (egress) direction, so that HVAC monitoring traffic is capped at 50Mbps for EF traffic while exceed traffic above 50Mbps **is remarked with CS5**
- The ISPs Next Hop can decide what to do with the lower priority HVAC traffic marked with CS5
  - Drop or recolor the packets with lower precedence
- ISP2 may also have a different QoS policy depending upon how much the customer pays for the afforded bandwidth which may need to be considered in policy creation



Details

Details

- IPv4 and IPv6 supported traffic classes and policies
- A policy may be applied to physical interfaces: Link Aggregation Groups (LAGs), VLANs, sub-interfaces, or global
- Inbound (ingress) or Outbound (Egress) directions
- Policies may be configured through either CLI or REST
- Multiple actions are not permitted when the exceed remark action is used in a policy, e.g., **exceed dscp CS1 action mirror 1** as mirror 1 is a secondary option
- VXLAN or non-VXLAN connected ports
- The meters in traffic policing policies are shared across all interfaces assigned to the policy unless the **per-interface argument** is used when applying the policy
  - If you apply a CIR/CBS based policy to all 48 ports in the switch, for example, with a 5 Mbps CIR, that 5 Mbps is aggregated across all ports. The **per-interface** option addresses this issue (released in 10.08)
- CBS internally is set to 1500 Bytes if set to 0 in the policy
  - CBS determines how fast the token bucket fills. If the value is too small the bucket runs out of tokens and the rate limit cannot be reached.
    - Must not be set to zero or the rate limit will not be achieved
- Port Based policies have higher precedence over policies applied to the VLAN

Configuration

Configuration

- Configure **qos trust dscp** ; default is not to trust DSCP markings
- Configure the desired traffic to remark in classes
- Specify the CIR and CBS values in a remark policy that matches on specific classes
- Apply the policy to an interface in either the ingress direction with keyword 'in' or egress direction with keyword 'out' to activate the policy on the port
- Common DSCP code points used by our customers are shown below:

<0-63> A valid DSCP codepoint
AF11 DSCP 10 (Assured Forwarding class 1, low drop probability)
AF12 DSCP 12 (Assured Forwarding class 1, medium drop probability)
AF13 DSCP 14 (Assured Forwarding class 1, high drop probability)
AF21 DSCP 18 (Assured Forwarding class 2, low drop probability)
AF22 DSCP 20 (Assured Forwarding class 2, medium drop probability)
AF23 DSCP 22 (Assured Forwarding class 2, high drop probability)
AF31 DSCP 26 (Assured Forwarding class 3, low drop probability)
AF32 DSCP 28 (Assured Forwarding class 3, medium drop probability)
AF33 DSCP 30 (Assured Forwarding class 3, high drop probability)
AF41 DSCP 34 (Assured Forwarding class 4, low drop probability)
AF42 DSCP 36 (Assured Forwarding class 4, medium drop probability)
AF43 DSCP 38 (Assured Forwarding class 4, high drop probability)
CS0 DSCP 0 (Class Selector 0: Default)
CS1 DSCP 8 (Class Selector 1: Scavenger)
CS2 DSCP 16 (Class Selector 2: OAM)
CS3 DSCP 24 (Class Selector 3: Signaling)
CS4 DSCP 32 (Class Selector 4: Realtime)
CS5 DSCP 40 (Class Selector 5: Broadcast video)
CS6 DSCP 48 (Class Selector 6: Network control)
CS7 DSCP 56 (Class Selector 7)
EF DSCP 46 (Expedited Forwarding)

Policer Min and Max :
CIR : 22 to 720,000,000 Kbps
CBS : 1 to 4,161,500 Bytes

Bit rate in kbps

Burst size in Bytes

Remark Name/code

Ingress Example

```
class ip any-traffic
    10 match any any any count
policy Remark_on_Exceed
    10 class ip any-traffic action cir kbps 1000 cbs 15625 exceed dscp CS5

interface 1/1/1
    apply policy Remark_on_Exceed in
    ! apply policy Remark_on_Exceed in per-interface ! unique policy not shared
```

DSCP Class Matches

Egress Example

```
class ip any-traffic
    10 match any any any dscp CS0 count
    20 match any any any dscp CS1 count
    30 match any any any dscp EF count
    40 match any any any dscp AF21 count

policy Remark_on_Exceed
    10 class ip any-traffic action cir kbps 1000 cbs 15625 exceed dscp CS5

interface 1/1/2
    apply policy Remark_on_Exceed out
    ! apply policy Remark_on_Exceeed out per-interface ! unique policy not shared
```

Equivalent Configurations

AOS-CX configuration comparisons

AOS-CX

Ingress Example

```
class ip any-traffic
    10 match any any any count
policy Remark_on_Exceed
    10 class ip any-traffic action cir kbps 1000 cbs 15625 exceed dscp CS5

interface 1/1/1
    apply policy Remark_on_Exceed in
```

Egress Example

```
class ip any-traffic
    10 match any any any dscp CS0 count
    20 match any any any dscp CS1 count
    30 match any any any dscp EF count
    40 match any any any dscp AF21 count
policy Remark_on_Exceed
    10 class ip any-traffic action cir kbps 1000 cbs 15625 exceed dscp CS5

interface 1/1/2
    apply policy Remark_on_Exceed out
```

H3C/HPE Comware

Ingress Example

```
acl basic 2001
rule permit source any any

traffic classifer any-traffic
if-match acl 2001

traffic behavior Remark_on_Exceed
car cir 1024 cbs 15625 ebs 0 green remark-dscp-pass CS0 red remark-dscp-pass CS5

qos policy car
classifer any-traffic behavior Remark_on_Exceed

interface gi1/0/1
qos apply policy car inbound
```

Egress Example

```
acl basic 2001
rule permit source any any

traffic classifer any-traffic
if-match acl 2001

traffic behavior Remark_on_Exceed
car cir 1024 cbs 15625 ebs 0 green remark-dscp-pass CS0 red remark-dscp-pass CS5

qos policy car
classifer any-traffic behavior Remark_on_Exceed

interface gi1/0/1
qos apply policy car outbound
```

Equivalent Configurations

AOS-CX configuration comparisons

AOS-CX

Ingress Example

```
class ip any-traffic
    10 match any any any count

policy Remark_on_Exceed
    10 class ip any-traffic action cir kbps 1000 cbs 15625 exceed dscp CS5

interface 1/1/1
    apply policy Remark_on_Exceed in
```

Egress Example

```
class ip any-traffic
    10 match any any any dscp CS0 count
    20 match any any any dscp CS1 count
    30 match any any any dscp EF count
    40 match any any any dscp AF21 count

policy Remark_on_Exceed
    10 class ip any-traffic action cir kbps 1000 cbs 15625 exceed dscp CS5

interface 1/1/2
    apply policy Remark_on_Exceed out
```

Cisco-IOS

Ingress Example

```
policy-map INGRESS_QOS
 class ANY
  police cir 1000 bc 15625
   conform-action transmit
   exceed-action set-dscp-transmit dscp table MARKDOWN

interface gi0/1
   service policy input INGRESS_QOS
```

Egress Example

```
ip access-list extended ANY
 permit any any any dscp cs0
 permit any any any dscp cs1
 permit any any any dscp ef
 permit any any any dscp af21

class-map match-all ANY
 match access-group name ANY

policy-map EGRESS_QOS
 class ANY
  priority level 1
  police rate percent 10
   conform-action transmit
   exceed-action set-dscp-transmit dscp table MARKDOWN

interface gi0/2
   service policy output EGRESS_QOS
```

Equivalent Configurations

AOS-CX configuration comparisons

AOS-CX

Ingress Example

```
class ip any-traffic
    10 match any any any count
policy Remark_on_Exceed
    10 class ip any-traffic action cir kbps 1000 cbs 15625 exceed dscp CS5

interface 1/1/1
    apply policy Remark_on_Exceed in
```

Egress Example

```
class ip any-traffic
    10 match any any any dscp CS0 count
    20 match any any any dscp CS1 count
    30 match any any any dscp EF count
    40 match any any any dscp AF21 count
policy Remark_on_Exceed
    10 class ip any-traffic action cir kbps 1000 cbs 15625 exceed dscp CS5

interface 1/1/2
    apply policy Remark_on_Exceed out
```

AOS-S

No CIR/CBS

Ingress Example

```
class ipv4 "any-traffic"
     10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.25
   exit
policy qos "qos-policy"
     10 class ipv4 "any-traffic" action rate-limit kbps 1000 action dscp
default
   exit

switch(eth-1)# service-policy qos-policy in
 in                    Apply the policy to inbound packets on the port.
 out                   Apply the policy to outbound packets on the port.
```

Egress Example

```
class ipv4 "any-traffic"
     10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
   exit
policy qos "qos-policy"
     10 class ipv4 "any-traffic" action rate-limit kbps 1000 action dscp
default
   exit

switch(eth-1)# service-policy qos-policy out
 in                    Apply the policy to inbound packets on the port.
 out                   Apply the policy to outbound packets on the port.

Cannot apply qos policy with action to remark 802.1p priority or ip-precedence
 or DSCP to port or vlan in the outbound direction.
```

REST – class creation

```
#!/bin/bash

curl --noproxy 127.0.0.1 -k -X POST \
-c /tmp/cookie \
-H 'Content-Type: multipart/form-data' \
"https://127.0.0.1/rest/v10.13/login" -F 'username=admin' -
F 'password=somepass'
```

Retrieve cookie to begin session

```
#!/bin/bash

curl -k --noproxy 127.0.0.1 -X POST -b /tmp/cookie \
"https://127.0.0.1/rest/v10.13/system/classes" -H "accept:
*/*" \
-H "Content-Type: application/json" -d '{
"cfg_version":0,
"name":"iperf3-traffic",
"type":"ipv4"
}'
```

Create IPv4 class iperf3-traffic

```
#!/bin/bash

curl -k --noproxy 127.0.0.1 -X POST -b /tmp/cookie \
"https://127.0.0.1/rest/v10.13/system/classes/iperf3-
traffic,ipv4/cfg_entries" -H "accept: */*" \
-H "Content-Type: application/json" -d '{
"count": true,
"dscp": 46,
"dst_ip": "192.168.0.56/255.255.255.255",
"protocol": 6,
"sequence_number": 10,
"src_ip": "192.168.0.1/255.255.255.255",
"src_l4_port_max": 5001,
"src_l4_port_min": 5001,
"type": "match"
}'
```

Create class entry with sequence 10

```
#!/bin/bash

curl -k --noproxy 127.0.0.1 -X PUT -b /tmp/cookie \
--url "https://127.0.0.1/rest/v10.13/system/classes/iperf3-traffic,ipv4" -d \
'{"cfg_version":1}'
```

Update the config version to apply the change to hardware

```
6300# show class commands
class ip iperf3-traffic
    10 match tcp 192.168.0.1 eq 5001 192.168.0.56 dscp EF
count
```

REST – Policy Creation

```
#!/bin/bash

curl --noproxy 127.0.0.1 -k -X POST \
-c /tmp/cookie \
-H 'Content-Type: multipart/form-data' \
"https://127.0.0.1/rest/v10.13/login" -F 'username=admin'
-F 'password=somepass'
```

Retrieve cookie to begin session

```
#!/bin/bash

curl -k --noproxy 127.0.0.1 -X POST -b /tmp/cookie \
"https://127.0.0.1/rest/v10.13/system/policies" -H "accept:
*/*" \
-H "Content-Type: application/json" -d '{
"cfg_version":0,
"name":"Remark_on_Exceed"
}'
```

Create Policy Remark_on_Exceed

```
#!/bin/bash

curl -k --noproxy 127.0.0.1 -X POST -b /tmp/cookie \
"https://127.0.0.1/rest/v10.13/system/policies/Remark_on_Ex
ceed/cfg_entries" -H "accept: */*" \
-H "Content-Type: application/json" -d '{
"class": "/rest/v10.13/system/classes/iperf3-traffic,ipv4",
"policy_action_set": null,
"sequence_number": 10
}'
```

Create Policy sequence 10 with empty action set

```
#!/bin/bash

curl -k --noproxy 127.0.0.1 -X POST -b /tmp/cookie \
"https://127.0.0.1/rest/v10.13/system/policies/Remark_on_Ex
ceed/cfg_entries/10/policy_action_set" -H "accept: */*" \
-H "Content-Type: application/json" -d '{
"cbs": 15625,
"cir": 1000,
"exceed_dscp": 40
}'
```

Apply the Policy Action Set

```
#!/bin/bash

curl -k --noproxy 127.0.0.1 -X PUT -b /tmp/cookie \
--url "https://127.0.0.1/rest/v10.13/system/policies/Remark_on_Exceed" -d \
'{"cfg_version":1}'
```

Update the config version to apply the change to hardware

```
6300# show policy commands
policy Remark_on_Exceed
    10 class ip iperf3-traffic action cir kbps 1000 cbs 15625
exceed dscp CS5
```

REST with Swagger UI

Example retrieving the policies configured on the system

Curl

```
curl -X GET "https://10.6.8.6/rest/v10.13/system/policies?depth=3" -H  "accept: application/json" -H  "x-csrf-token: ILFoPG4_Kw4K7fvJJdeG4w=="
```

Request URL

https://10.6.8.6/rest/v10.13/system/policies?depth=3

Server response

Code	Details
200	Response body


```
{
  "Remark_on_Exceed": {
    "cfg_entries": {
      "20": "/rest/v10.13/system/policies/Remark_on_Exceed/cfg_entries/20"
    },
```


Example retrieving a policy entry action set : CIR = 1000, CBS = 15625

Curl

```
curl -X GET "https://10.6.8.6/rest/v10.13/system/policies/Remark_on_Exceed/cfg_entries/20/policy_action_set" -H  "accept: application/json" -H  "x-csrf-token: ILFoPG4_Kw4K7fvJJdeG4w=="
```

Request URL

https://10.6.8.6/rest/v10.13/system/policies/Remark_on_Exceed/cfg_entries/20/policy_action_set

Server response

Code	Details
200	Response body


```
{
  "acl_drop": false,
  "cbs": 15625,
  "cir": 1000,
  "dscp": null,
  "ecn": null,
  "exceed_drop": false,
  "exceed_dscp": 20,
  "ip_precedence": null,
  "local_priority": null,
  "mirror": [],
  "origin": "static",
  "pbr_action_list": null,
  "pcp": null
}
```


Download

Best Practices

Best Practices

- Need to consider using the **per-interface** argument to the policy so that the CIR bandwidth isn't shared among policy port members
- When taking packet captures, add the DSCP field as a column so that it is easy to compare and count both conforming and non-conforming packets
- Configure QoS even if there are no oversubscription ratios or congestion
  - Micro-bursting can still cause congestion and TX queue drops
- Determine which direction you want to apply the policy
  - Inbound (Ingress)
    - When you want rate limits applied as close as possible to the source of the traffic
  - Outbound (Egress)
    - When you only want to rate limit traffic leaving the aggregation switches
    - When you only want to rate limit traffic leaving the core routers to the ISP **(main use case)**
- To maintain quality of service
  - Make sure the marked down non-conforming packets egress the same output queue as the conforming packets but with a new remark
  - For example, **EF and CS5 both use queue 5** so remark exceed traffic as CS5 **to prevent out of order packet delivery**
- Specify the correct burst rate when apply CIR / CBS values
  - CBS should be 1/8 the CIR which means the token bucket will be reset every 1/8 sec
  - CBS (Bytes) = CIR (kbps) * 15.625 (Bytes per kbit)
  - (15,625 Bytes * 8 bits per byte / 0.125 seconds) / 1000 bits per kilobit = 1000 kbps
  - CBS determines how fast the token bucket fills. If the value is too small the bucket runs out of tokens and the rate limit cannot be reached

1Mbps CIR or 1000 kbps
1000000 / 8
125000 Bytes
125000 * .125 (1/8 sec)
15625.000 Bytes per 1/8 sec token = **CBS**

5Mbps CIR
5000000 / 8
625000 Bytes
625000 * .125 (1/8 sec)
78125.000 Bytes per 1/8 sec token = **CBS**

1Gbps CIR
1000000000 / 8
125000000 Bytes
125000000 * .125 (1/8 sec)
15625000.000 Bytes per 1/8 sec token = **CBS**

```
class ip any-traffic
    10 match any any any count
policy Remark_on_Exceed
    10 class ip any-traffic action cir kbps 1000 cbs 15625 exceed dscp CS5
```

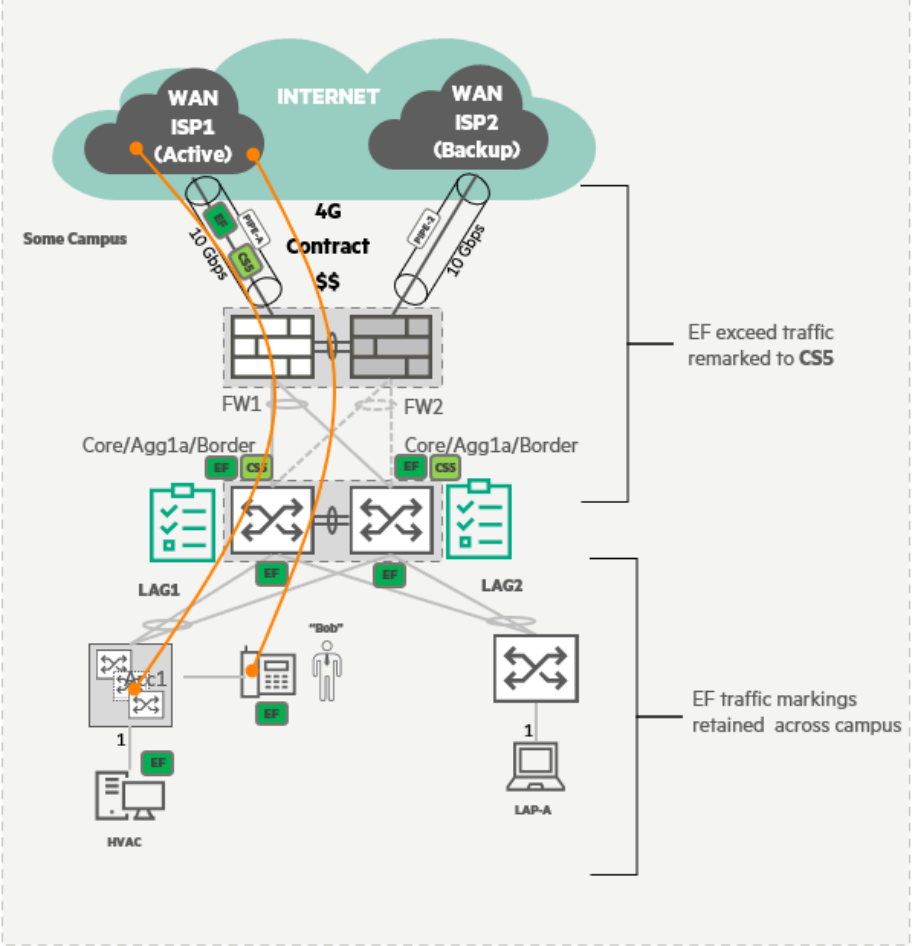
Troubleshooting

QoS Policing Exceed Action of Remark

Troubleshooting

- Have a topology diagram ready showing where the packets are getting remarked and the forwarding path
- Recommended troubleshooting flow:

1. Check that the sending switch is remarking the non-conforming packets
2. Check that the receiving switch is queuing the traffic into the configured queues
3. Check that the destination is receiving the non-conforming packets with correct DSCP values
4. Verify that the diagnostic data is showing the correct details for validation of the feature
5. Verify using tools that the desired CIR and CBS values meters the conforming packets correctly
6. Check show resources and event logs



Troubleshooting

1. Check that the sending switch is remarking the non-conforming packets

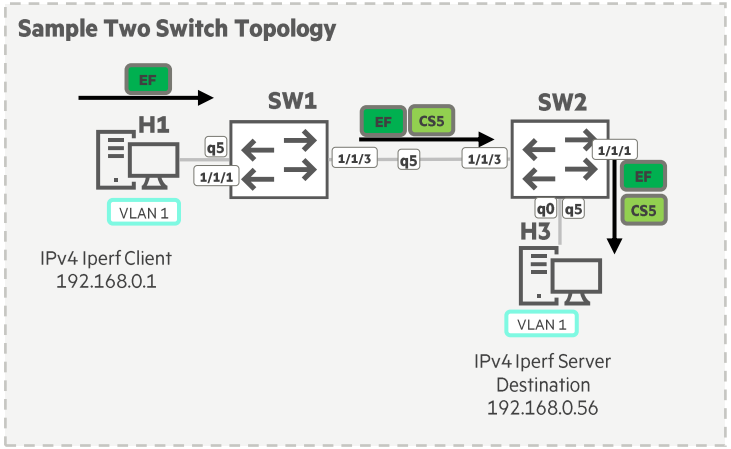
- Apply a counter policy to the egress interface of SW1 to verify the packets are getting remarked, i.e., port 1/1/3 in this example

SW1

```
class ip iperf3-traffic
    10 match any any any dscp EF
    20 match any any any dscp CS1
    30 match any any any dscp AF21
    40 match any any any dscp CS5

policy Count_Packets
    10 class ip iperf3-traffic

interface 1/1/3
    apply policy Count_Packets out
```

SW1

```
6300-1# show policy hitcounts Count_Packets
Statistics for Policy Count_Packets:

Interface 1/1/3 (out):
     Matched Packets  Configuration
10 class ip iperf3-traffic
                1045  10 match any any any dscp EF count
                   0  20 match any any any dscp CS1 count
                   0  30 match any any any dscp AF21 count
                8169  40 match any any any dscp CS5 count
```

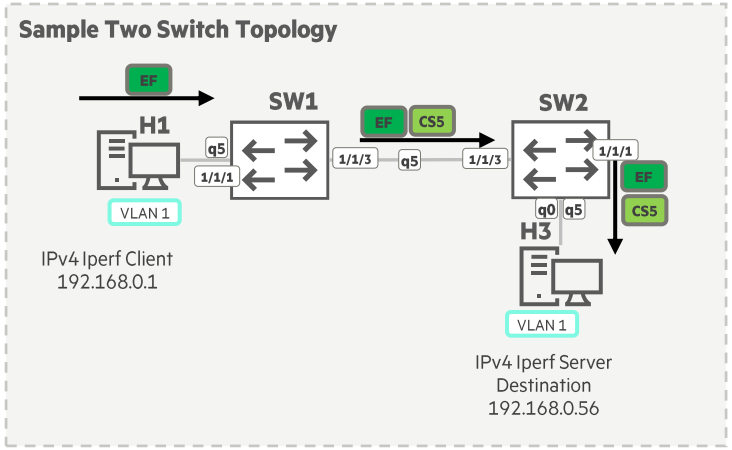


Troubleshooting

2. Check that the receiving switch is queuing the traffic into the configured queues

- In this screen shot, we can see that EF and CS5 traffic is correctly egressing Q5
  - Default queue profiles configured on the switch

```
6300-2# show interface 1/1/1 queues
Interface 1/1/1 is up
 Admin state is up
                Tx Bytes          Tx Packets          Tx Drops
 Q0                    0                   0                 0
 Q1                    0                   0                 0
 Q2                    0                   0                 0
 Q3                    0                   0                 0
 Q4                    0                   0                 0
 Q5             13733686                9557                 0
 Q6                    0                   0                 0
 Q7                    0                   0                 0
```

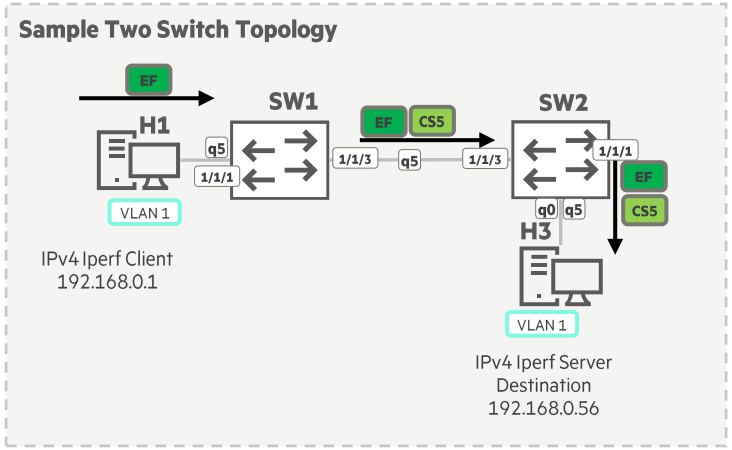


Troubleshooting

3. Check the destination is receiving non-conforming packets with DSCP modified

- Hitcounts with class matches for DSCP values for counting purposes
- In this screen shot, we can see that CS5, and EF counters populated for the matching traffic

```
6300-2(config)# show class commands
class ip iperf3-traffic
    10 match any any any dscp EF count
    20 match any any any dscp CS0 count
    30 match any any any dscp CS1 count
    40 match any any any dscp CS5 count

6300-2(config)# show policy commands
policy Count_Packets
    10 class ip iperf3-traffic
interface 1/1/1
    apply policy Count_Packets out

6300-2(config)# show policy hitcounts Count_Packets
Statistics for Policy Count_Packets:

Interface 1/1/1 (out):
     Matched Packets  Configuration
10 class ip iperf3-traffic
                 873  10 match any any any dscp EF count
                  18  20 match any any any dscp CS0 count
                   0  30 match any any any dscp CS1 count
                 951  40 match any any any dscp CS5 count
```



Troubleshooting

- Packet captures
  - Look that the DSCP field is correctly tagged for the remarked frames

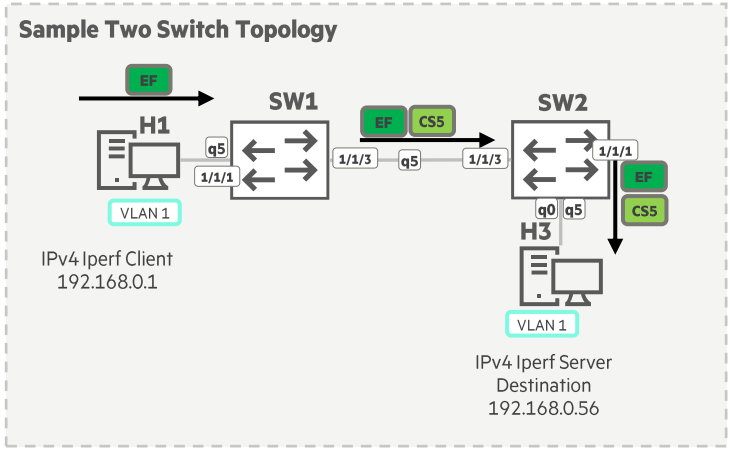
```
Internet Protocol Version 4, Src: 192.168.0.10, Dst: 192.168.0.56
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 ⌄ Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
      1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
```

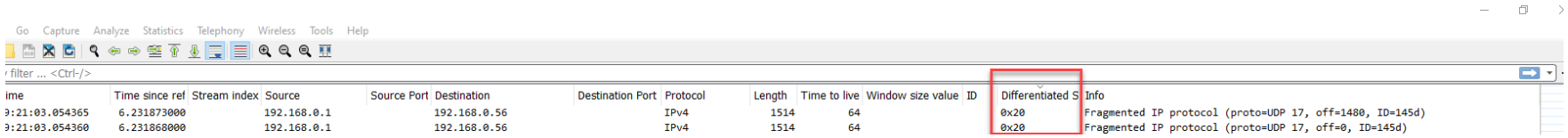
```
Internet Protocol Version 4, Src: 192.168.0.10, Dst: 192.168.0.56
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 ⌄ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
```

```
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.56
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 ⌄ Differentiated Services Field: 0x48 (DSCP: AF21, ECN: Not-ECT)
      0100 10.. = Differentiated Services Codepoint: Assured Forwarding 21 (18)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
```

```
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.56
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 ⌄ Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
      0010 00.. = Differentiated Services Codepoint: Class Selector 1 (8)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
```

```
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.56
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 ⌄ Differentiated Services Field: 0xa0 (DSCP: CS5, ECN: Not-ECT)
      1010 00.. = Differentiated Services Codepoint: Class Selector 5 (40)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
```





ime	Time since ref	Stream index	Source	Source Port	Destination	Destination Port	Protocol	Length	Time to live	Window size value	ID	Differentiated S	Info
9:21:03.054365	6.231873000		192.168.0.1		192.168.0.56		IPv4	1514	64			0x20	Fragmented IP protocol (proto=UDP 17, off=1480, ID=145d)
9:21:03.054360	6.231868000		192.168.0.1		192.168.0.56		IPv4	1514	64			0x20	Fragmented IP protocol (proto=UDP 17, off=0, ID=145d)

Troubleshooting - Software

4. Verify the diagnostic data is showing the correct details for validation of the feature

- Ovs-appctl commands

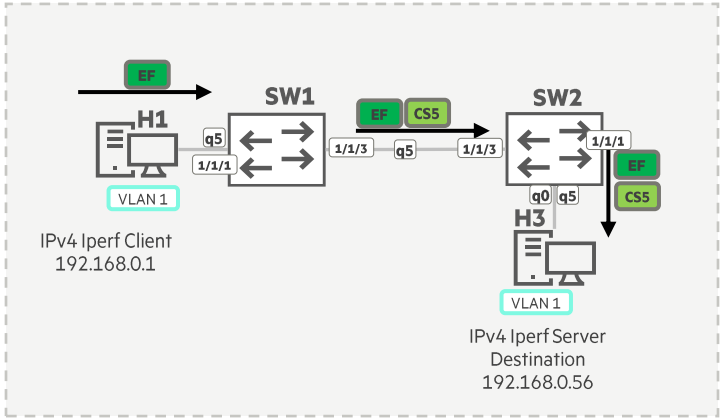
```
Bldg1-Acc-6300-VSF:/home/admin# ovs-appctl policer/read-entry -a
Reading all entries
Policer ID = 0xffff8d453730
   SDK Handle      = 2
   Reference count = 2
   Agent           = 0
   TCAM Table ID   = 8
   HA key name = Remark_on_Exceed-policy-in-port-0-0-0-(null)-cir=1000-cbs=15625-ebs=0-
exceed_remark_ip_dscp=20
   HA key size = 95
   Committed information rate (cir) = 1000 kbps
   Committed burst size (cbs)       = 15625 bytes
   Exceed remark ip dscp = 20
Policer ID = 0xffff8d4537a0
   SDK Handle      = 2
   Reference count = 2
   Agent           = 1
   TCAM Table ID   = 14
   HA key name = Remark_on_Exceed-policy-out-port-0-0-1-(null)-cir=1000-cbs=15625-ebs=0-
exceed_remark_ip_dscp=20
   HA key size = 96
   Committed information rate (cir) = 1000 kbps
   Committed burst size (cbs)       = 15625 bytes
   Exceed remark ip dscp = 20
```

```
6300-1:/home/admin# ovsdb-client dump Policy -flist
Policy table

_uuid               : 4699f64a-2e01-409e-ba8f-19fae3c52d61
cfg_entries         : {30=23545d75-6754-45e3-aaf7-812e1dec7a06}
cfg_version         : -6667536666265929
cur_entries         : {30=23545d75-6754-45e3-aaf7-812e1dec7a06}
external_ids        : {}
global_conform_rate : {}
global_in_conform_rates: {}
global_in_statistics: {}
global_statistics   : {}
in_progress_entries : {30=23545d75-6754-45e3-aaf7-812e1dec7a06}
in_progress_version : -6667536666265929
interfaces_in_conform_rates: {1=994}
interfaces_in_statistics: {{1={packets=10}}, {2={packets=0}}, {3={packets=1452}}}
interfaces_out_conform_rates: {}
interfaces_out_statistics: {}
interfaces_routed_in_conform_rates: {}
interfaces_routed_in_statistics: {}
l3vnis_routed_in_conform_rates: {}
l3vnis_routed_in_statistics: {}
name                : Remark_on_Exceed
origin              : []
other_config        : {}
parent_policy       : []
routed_in_statistics_clear_performed: {}
routed_in_statistics_clear_requested: {}
statistics_clear_performed: {all="1"}
statistics_clear_requested: {all="1"}
statistics_requested_vrf: []
status              : {code="0", message="", state=applied, version="-6667536666265929"}
subinterfaces_in_conform_rates: {}
subinterfaces_in_statistics: {}
subinterfaces_out_conform_rates: {}
subinterfaces_out_statistics: {}
subinterfaces_routed_in_conform_rates: {}
subinterfaces_routed_in_statistics: {}
vlans_in_conform_rates: {}
vlans_in_statistics : {}
vlans_out_conform_rates: {}
vlans_out_statistics: {}
vlans_routed_in_conform_rates: {}
vlans_routed_in_statistics: {}
vsx_sync            : []
```

Troubleshooting

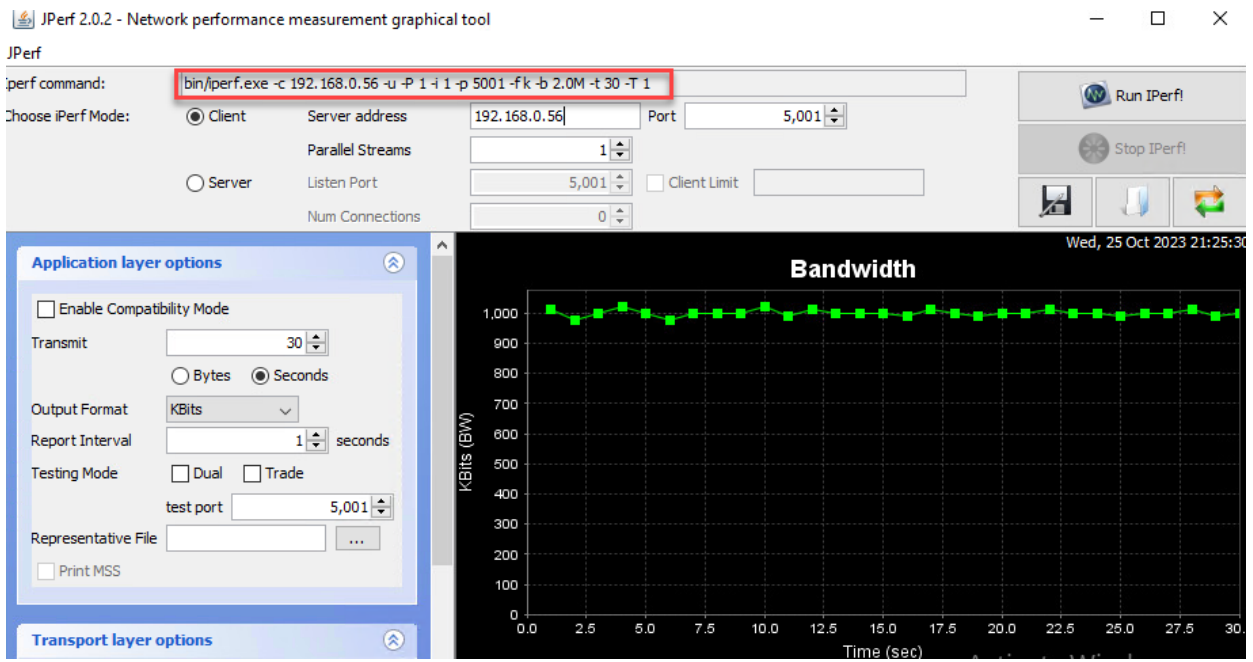
5. Verify using tools the desired CIR and CBS values meter the conforming packets correctly

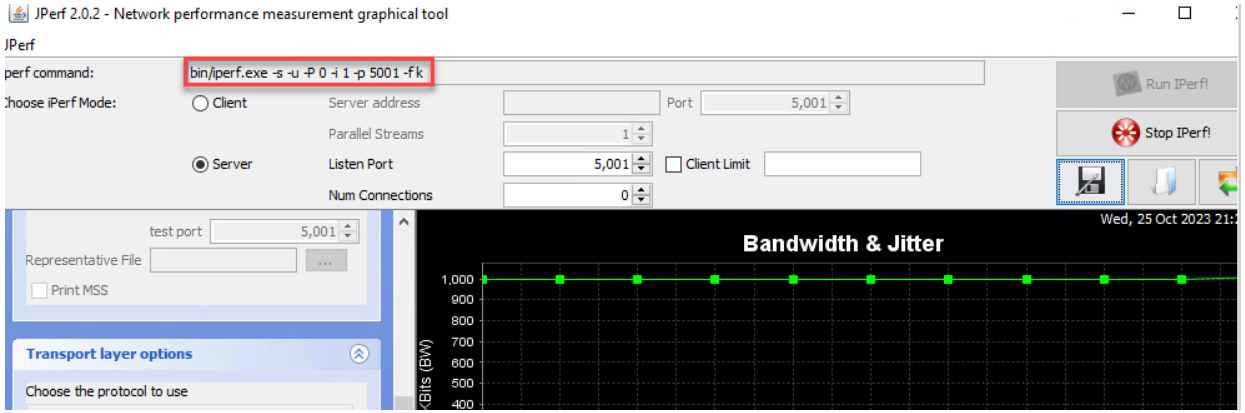
- Iperf3 on *NIX platforms
  - Can set any DSCP values like shown below if you send in the correct ToS value in Hex
- Jperf on Windows Platforms
  - Note: Jperf is unable to set DSCP values for the operating system but is useful in sending at different rates




```
client# iperf3 -c 192.168.0.56 -i -t 10 -u -b 2000k -S 0xB8 (EF)
client# iperf3 -c 192.168.0.56 -i -t 10 -u -b 2000k -S 0x48 (AF21)
client# iperf3 -c 192.168.0.56 -i -t 10 -u -b 2000k -S 0x20 (CS1)
client# iperf3 -c 192.168.0.56 -i -t 10 -u -b 2000k (CS0)
client# iperf3 -c 192.168.0.56 -i -t 10 -u -b 2000k -S 0xA0 (CS5)
```

```
server# iperf3 -s
bash-5.0# iperf3 -s
-----------------------------------
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
-----------------------------------
```



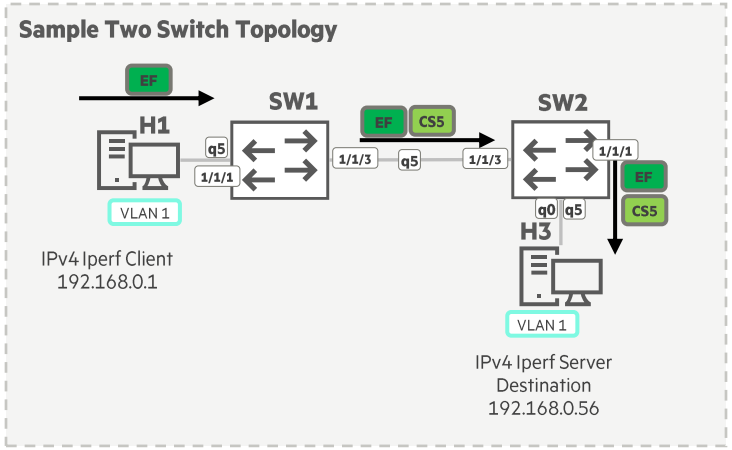


Troubleshooting

6. Check resources for TCAM usage

- Show resources

```
6300# sh res

Resource Usage:

Mod  Description
        Resource                                  Used Reserved    Free
-------------------------------------------------------------------------
1/1  Ingress Port Policy Lookup
        Ingress TCAM Entries                     20007    20480
        Ingress Policers                          1000
     Total
        Ingress TCAM Entries                     20007    20480       0
        Egress TCAM Entries                          0        0    8192
        Ingress Lookups                              1                8
        Ingress Flex Lookups                         0                1
        Egress Lookups                               0                4
        Ingress Policers                          1000             1047
        Egress Policers                              0             2047
2/1  Ingress Port Policy Lookup
        Ingress TCAM Entries                      9607    10240
        Ingress Policers                           480
     Total
        Ingress TCAM Entries                      9607    10240   10240
        Egress TCAM Entries                          0        0    8192
        Ingress Lookups                              1                8
        Ingress Flex Lookups                         0                1
        Egress Lookups                               0                4
        Ingress Policers                           480             1567
        Egress Policers                              0             2047
```



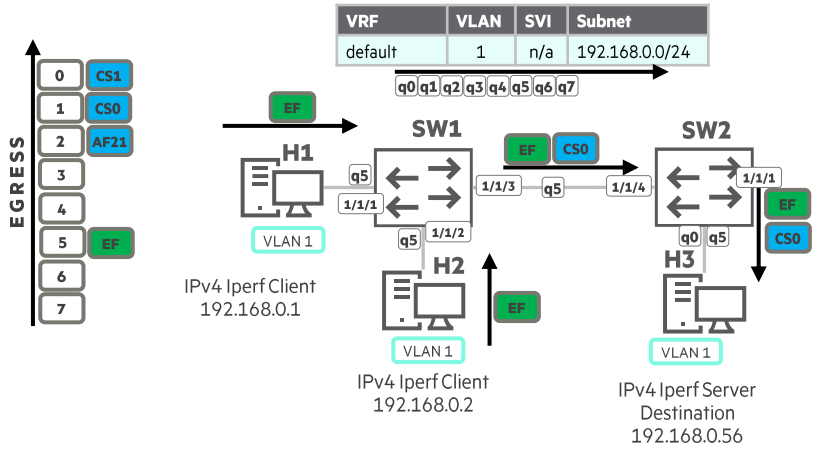
- Event Logs / Debug Messages
  - show events –s err –c tcam
  - show events –s err –c policy
  - show debug buffer module tcam
  - show debug buffer module classifier
  - show debug buffer module policy

```
6300# show debug buffer module tcam
-----------------------------------------------------------------------------------------------------------------------------------
show debug buffer
-----------------------------------------------------------------------------------------------------------------------------------
2023-10-27:00:06:03.457508|switchd_agent|LOG_ERR|CDTR|1|TCAM|TCAM|[tcam_agent_bank_grow_table] No available banks to expand the Table ID 8
2023-10-27:00:06:03.461181|ops-switchd|LOG_ERR|CDTR|1|TCAM|TCAM|[tcam_hw_entry_installed_callback:2123] failed
6300#
6300#
6300# show debug buffer module classifier
-----------------------------------------------------------------------------------------------------------------------------------
show debug buffer
-----------------------------------------------------------------------------------------------------------------------------------
2023-10-27:00:06:03.463316|ops-switchd|LOG_ERR|CDTR|1|CLASSIFIER|CLASSIFIER|Not able to install pd_cls_list_instance error code = 1
2023-10-27:00:06:03.536550|ops-switchd|LOG_ERR|CDTR|1|CLASSIFIER|CLASSIFIER|[pd_cls_list_apply_ports] pd_cls_list_agents_apply() failed
2023-10-27:00:06:03.539010|ops-switchd|LOG_ERR|CDTR|1|CLASSIFIER|CLASSIFIER|[pd_cls_apply] failed
6300#
6300# show debug buffer module policy
-----------------------------------------------------------------------------------------------------------------------------------
show debug buffer
-----------------------------------------------------------------------------------------------------------------------------------
2023-10-27:00:06:03.539083|ops-switchd|LOG_ERR|CDTR|1|POLICY|POLICY|POLICY_PORT_MAP 1/1/6:IN -- PD apply failed
```

Demo

Feature Demo #1 - IPerf

- Show H1 Iperf to H3
  - Conform and non-conforming traffic via hitcounts display
- Unique policies per-interface to show the CIR/CBS policies can be used; released in 10.08 but we didn't have content explaining the functionality
  - Show H1 and H2 Iperf to H3 with shared policy
  - Show H1 and H2 Iperf to H3 with per-interface policy applied




```
H1/H2# iperf3 -c 192.168.0.56 -i -t 10 -u -b 2000k -S 0xB8 (EF)
H1/H2# iperf3 -c 192.168.0.56 -i -t 10 -u -b 2000k -S 0x48 (AF21)
H1/H2# iperf3 -c 192.168.0.56 -i -t 10 -u -b 2000k -S 0x08 (CS1)
H1/H2# iperf3 -c 192.168.0.56 -i -t 10 -u -b 2000k (CS0)
```

```
H3# iperf3 -s
bash-5.0# iperf3 -s
-----------------------------------
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
-----------------------------------
```

SW1

```
class ip iperf3-traffic
    10 match any any any dscp CS0
    20 match any any any dscp CS1
    30 match any any any dscp EF
    40 match any any any dscp AF21

class ip any-traffic
    10 match any any any

policy Remark_on_Exceed
    10 class ip any-traffic
    20 class ip any-traffic action cir kbps 1000 cbs 15625 exceed drop
    30 class ip any-traffic action cir kbps 1000 cbs 15625 exceed dscp CS0

interface 1/1/1
    apply policy Remark_on_Exceed in
interface 1/1/2
    apply policy Remark_on_Exceed in
```

SW2

```
class ip iperf3-traffic
    10 match any any any dscp CS0 count
    20 match any any any dscp CS1 count
    30 match any any any dscp EF count
    40 match any any any dscp AF21 count

policy Count_Packets
    10 class ip iperf3-traffic

interface 1/1/1
    apply policy Count_Packets out
```

Thank you

aruba_switching_tme@hpe.com

© 2023 Hewlett Packard Enterprise Development LP