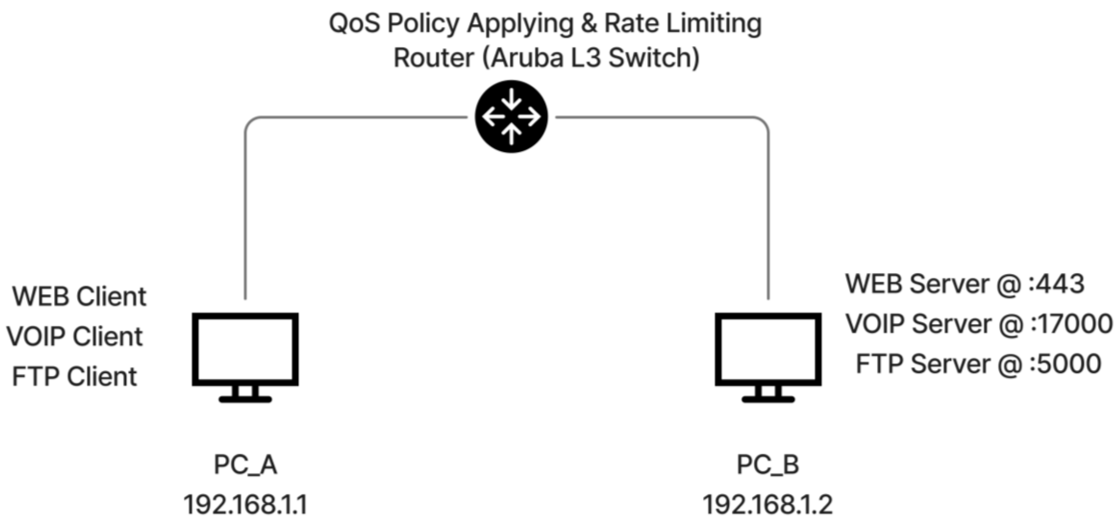
CO513: Advanced Computer Communication Networks - Lab 04

E/19/309, E/19/349, E/19/372, E/19/409,
E/19/413, E/19/426, E/19/ 432, E/19/443,
E/19/446, E/19/452, E/19/455

19/05/2025

Network Configuration and Setup Summary



Equipment used:

- Routing: Aruba HP 2920 Layer 3 Switch
  Firmware Version: 15 (https://www.hpe.com/psnow/doc/c04111401?ver=15)
- Switching: Cisco Layer 2 Switch

Although the initial lab instructions recommended using a Layer 2 switch between the router and the PC clients, we opted to exclude it from our topology. This decision was made to avoid the unnecessary complications we encountered in the previous lab, particularly with configuration issues and compatibility challenges. By simplifying the setup, we were able to focus more effectively on the core objective of the lab, implementing and testing QoS policies without compromising the validity of the classification and rate limiting processes conducted on the router.

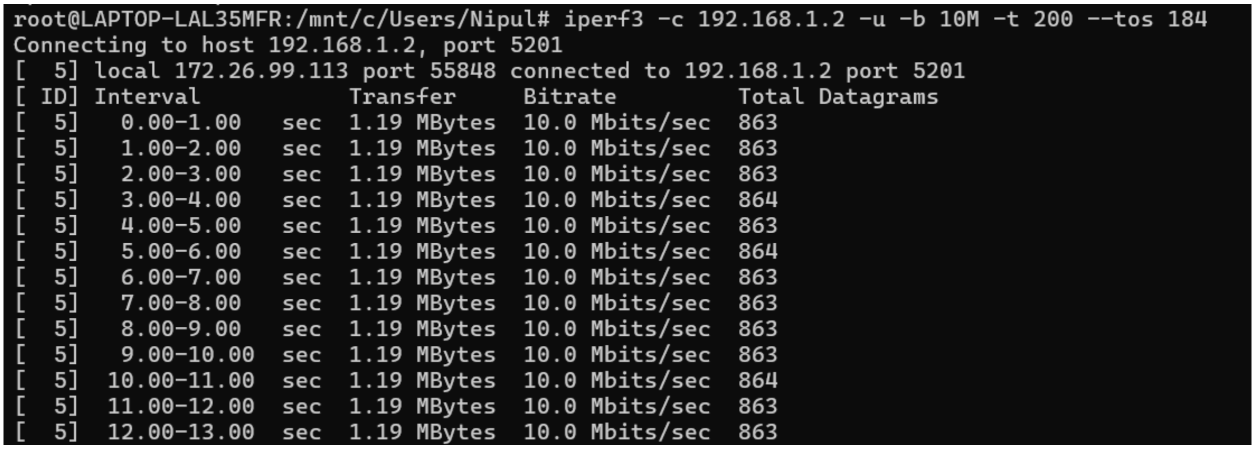
Lab Tasks:

1. Generate Traffic

For traffic generation, we used iPerf3 to simulate all three FTP (for Bulk Data), VoIP (for Voice Data) and HTTP (for Web) traffic. The corresponding iPerf3 servers were also configured on PC-B to receive the traffic by executing the command “iperf3 -s”.

The following are the traffic generation snapshots (iperf3 clients)

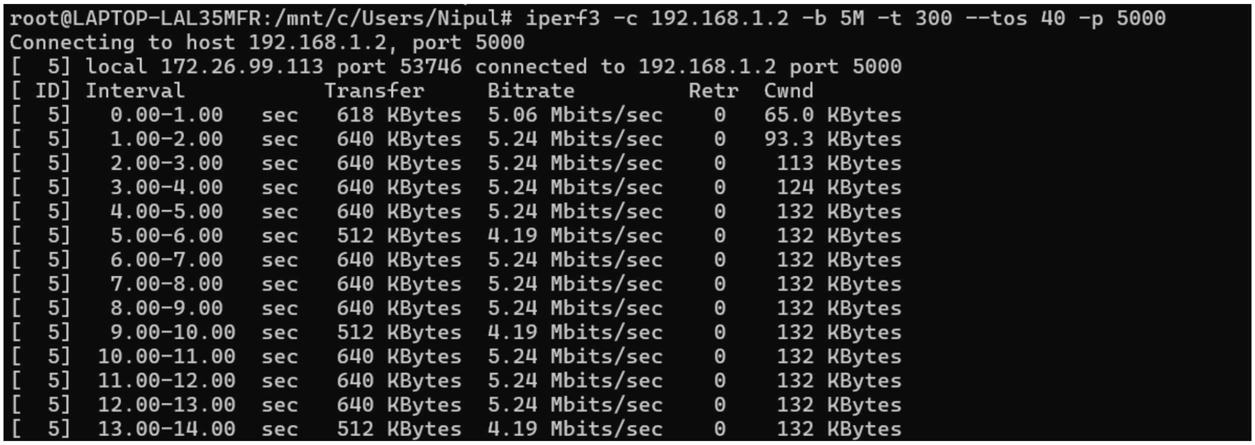
a. VOIP Traffic



```
root@LAPTOP-LAL35MFR:/mnt/c/Users/Nipul# iperf3 -c 192.168.1.2 -u -b 10M -t 200 --tos 184
Connecting to host 192.168.1.2, port 5201
[  5] local 172.26.99.113 port 55848 connected to 192.168.1.2 port 5201
[ ID] Interval           Transfer     Bitrate         Total Datagrams
[  5]   0.00-1.00   sec  1.19 MBytes  10.0 Mbits/sec  863
[  5]   1.00-2.00   sec  1.19 MBytes  10.0 Mbits/sec  863
[  5]   2.00-3.00   sec  1.19 MBytes  10.0 Mbits/sec  863
[  5]   3.00-4.00   sec  1.19 MBytes  10.0 Mbits/sec  864
[  5]   4.00-5.00   sec  1.19 MBytes  10.0 Mbits/sec  863
[  5]   5.00-6.00   sec  1.19 MBytes  10.0 Mbits/sec  864
[  5]   6.00-7.00   sec  1.19 MBytes  10.0 Mbits/sec  863
[  5]   7.00-8.00   sec  1.19 MBytes  10.0 Mbits/sec  863
[  5]   8.00-9.00   sec  1.19 MBytes  10.0 Mbits/sec  863
[  5]   9.00-10.00  sec  1.19 MBytes  10.0 Mbits/sec  863
[  5]  10.00-11.00  sec  1.19 MBytes  10.0 Mbits/sec  864
[  5]  11.00-12.00  sec  1.19 MBytes  10.0 Mbits/sec  863
[  5]  12.00-13.00  sec  1.19 MBytes  10.0 Mbits/sec  863
```

This command sends UDP traffic at 10 Mbps for 200 seconds from the client to 192.168.1.2 using iperf3, with a Type of Service (ToS) value of 184 (which corresponds to DSCP value af11) to test QoS policies.

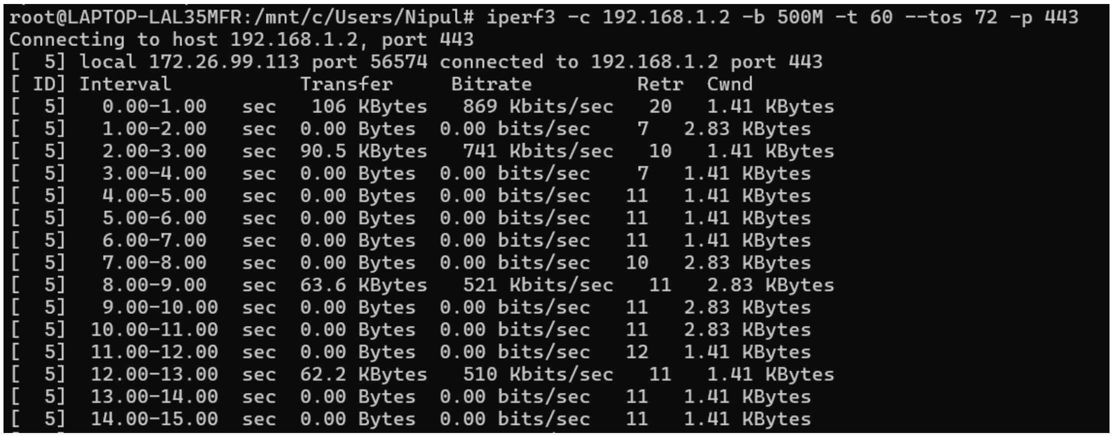
b. Bulk Data Traffic



```
root@LAPTOP-LAL35MFR:/mnt/c/Users/Nipul# iperf3 -c 192.168.1.2 -b 5M -t 300 --tos 40 -p 5000
Connecting to host 192.168.1.2, port 5000
[  5] local 172.26.99.113 port 53746 connected to 192.168.1.2 port 5000
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec   618 KBytes  5.06 Mbits/sec    0   65.0 KBytes
[  5]   1.00-2.00   sec   640 KBytes  5.24 Mbits/sec    0   93.3 KBytes
[  5]   2.00-3.00   sec   640 KBytes  5.24 Mbits/sec    0    113 KBytes
[  5]   3.00-4.00   sec   640 KBytes  5.24 Mbits/sec    0    124 KBytes
[  5]   4.00-5.00   sec   640 KBytes  5.24 Mbits/sec    0    132 KBytes
[  5]   5.00-6.00   sec   512 KBytes  4.19 Mbits/sec    0    132 KBytes
[  5]   6.00-7.00   sec   640 KBytes  5.24 Mbits/sec    0    132 KBytes
[  5]   7.00-8.00   sec   640 KBytes  5.24 Mbits/sec    0    132 KBytes
[  5]   8.00-9.00   sec   640 KBytes  5.24 Mbits/sec    0    132 KBytes
[  5]   9.00-10.00  sec   512 KBytes  4.19 Mbits/sec    0    132 KBytes
[  5]  10.00-11.00  sec   640 KBytes  5.24 Mbits/sec    0    132 KBytes
[  5]  11.00-12.00  sec   640 KBytes  5.24 Mbits/sec    0    132 KBytes
[  5]  12.00-13.00  sec   640 KBytes  5.24 Mbits/sec    0    132 KBytes
[  5]  13.00-14.00  sec   512 KBytes  4.19 Mbits/sec    0    132 KBytes
```

The command starts a 300-second TCP transmission from PC-A to the iPerf3 server at 192.168.1.2, sending data at 5 Mbps using port 5000. The ToS value is set to 40, corresponding to DSCP af11, typically used for bulk data traffic like FTP.

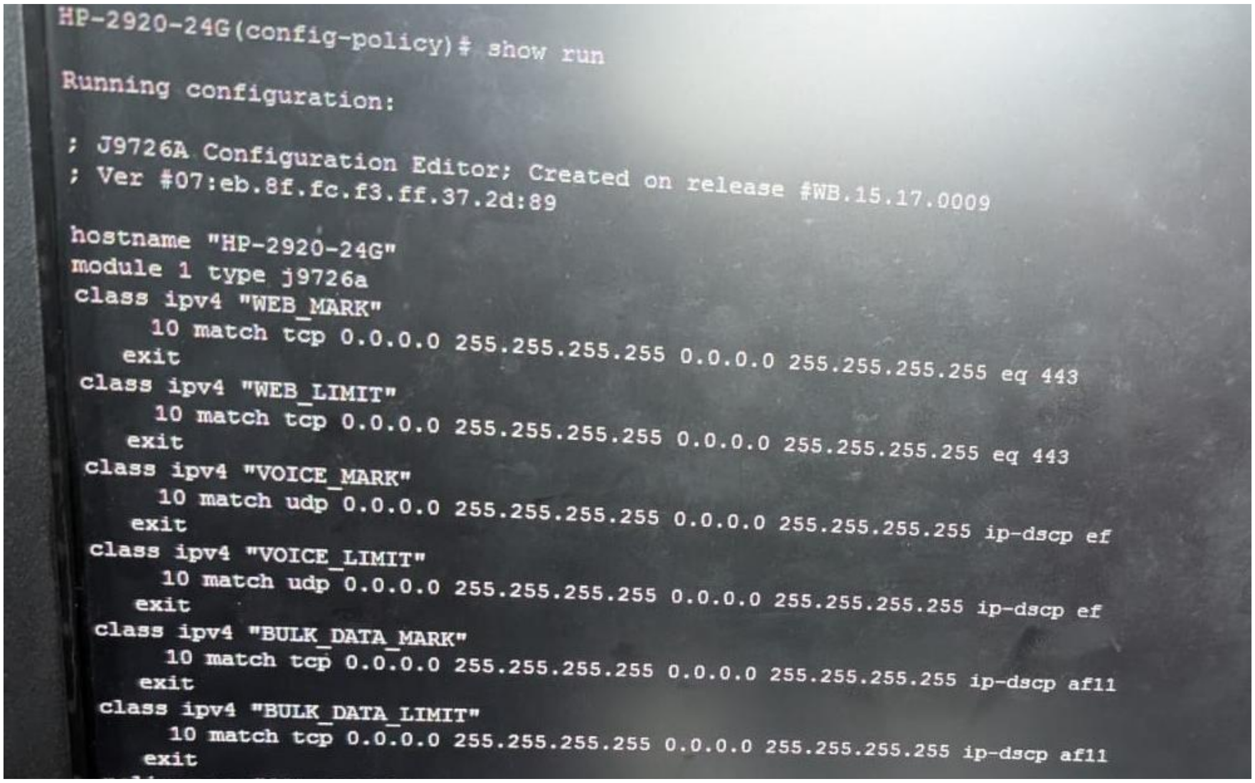
c. Web Traffic



```
root@LAPTOP-LAL35MFR:/mnt/c/Users/Nipul# iperf3 -c 192.168.1.2 -b 500M -t 60 --tos 72 -p 443
Connecting to host 192.168.1.2, port 443
[  5] local 172.26.99.113 port 56574 connected to 192.168.1.2 port 443
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec   106 KBytes   869 Kbits/sec   20   1.41 KBytes
[  5]   1.00-2.00   sec  0.00 Bytes  0.00 bits/sec    7   2.83 KBytes
[  5]   2.00-3.00   sec  90.5 KBytes   741 Kbits/sec   10   1.41 KBytes
[  5]   3.00-4.00   sec  0.00 Bytes  0.00 bits/sec    7   1.41 KBytes
[  5]   4.00-5.00   sec  0.00 Bytes  0.00 bits/sec   11   1.41 KBytes
[  5]   5.00-6.00   sec  0.00 Bytes  0.00 bits/sec   11   1.41 KBytes
[  5]   6.00-7.00   sec  0.00 Bytes  0.00 bits/sec   11   1.41 KBytes
[  5]   7.00-8.00   sec  0.00 Bytes  0.00 bits/sec   10   2.83 KBytes
[  5]   8.00-9.00   sec  63.6 KBytes   521 Kbits/sec   11   2.83 KBytes
[  5]   9.00-10.00  sec  0.00 Bytes  0.00 bits/sec   11   2.83 KBytes
[  5]  10.00-11.00  sec  0.00 Bytes  0.00 bits/sec   11   2.83 KBytes
[  5]  11.00-12.00  sec  0.00 Bytes  0.00 bits/sec   12   1.41 KBytes
[  5]  12.00-13.00  sec  62.2 KBytes   510 Kbits/sec   11   1.41 KBytes
[  5]  13.00-14.00  sec  0.00 Bytes  0.00 bits/sec   11   1.41 KBytes
[  5]  14.00-15.00  sec  0.00 Bytes  0.00 bits/sec   11   1.41 KBytes
```

This command sends TCP traffic at 500 Mbps for 60 seconds to 192.168.1.2 on port 443 using a ToS value of 72(corresponds to DCSP value of af21), simulating high-bandwidth http traffic for QoS testing.

2. Configure Traffic Classification (Router)



```
HP-2920-24G(config-policy)# show run

Running configuration:

; J9726A Configuration Editor; Created on release #WB.15.17.0009
; Ver #07:eb.8f.fc.f3.ff.37.2d:89

hostname "HP-2920-24G"
module 1 type j9726a
class ipv4 "WEB_MARK"
     10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 443
   exit
class ipv4 "WEB_LIMIT"
     10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 443
   exit
class ipv4 "VOICE_MARK"
     10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 ip-dscp ef
   exit
class ipv4 "VOICE_LIMIT"
     10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 ip-dscp ef
   exit
class ipv4 "BULK_DATA_MARK"
     10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 ip-dscp af11
   exit
class ipv4 "BULK_DATA_LIMIT"
     10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 ip-dscp af11
   exit
```

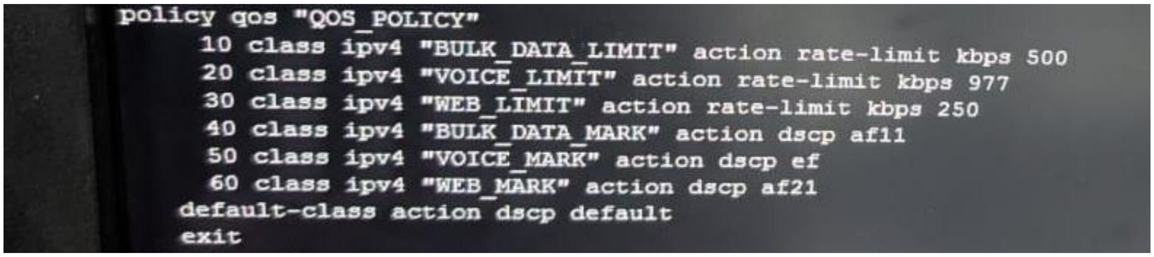
For traffic classification, we used Method A: Protocol-based Class Maps, and created six IPv4 classes on the router. We created two classes to per each WEB, VOIP, FTP so that we can use one dedicated to marking and the other to rate limiting when applying QoS policies.

1. “WEB_MARK” and “WEB_LIMIT” to match all TCP traffic through port 80 or 443 and marked with AF21 (used for HTTP traffic traffic)
2. "VOICE_MARK" and “VOICE_LIMIT " to match all UDP traffic marked with DSCP EF (used for VoIP),
3. "BULK DATA_MARK" and "BULK DATA_LIMIT" to match all TCP traffic marked with DSCP AF11 (used for FTP and similar bulk data transfers)

Each class uses a wildcard mask of any-any to match all source and destination IP addresses.

3. Create a Policy Map with Rate Limiting

To create the QoS policy, we defined a policy map named "QOS_POLICY" that binds the previously defined traffic classes to specific actions of marking and rate limiting.



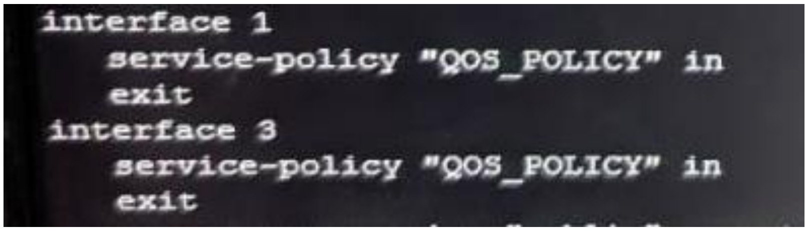
```
policy qos "QOS_POLICY"
     10 class ipv4 "BULK_DATA_LIMIT" action rate-limit kbps 500
     20 class ipv4 "VOICE_LIMIT" action rate-limit kbps 977
     30 class ipv4 "WEB_LIMIT" action rate-limit kbps 250
     40 class ipv4 "BULK_DATA_MARK" action dscp af11
     50 class ipv4 "VOICE_MARK" action dscp ef
     60 class ipv4 "WEB_MARK" action dscp af21
    default-class action dscp default
    exit
```

The above configuration

1. Limits bandwidth for bulk data, voice, and web traffic.
   The lab sheet originally provided Cisco commands specifying rate limits in bits per second (bps):
   - VOICE: 1,000,000 bps
   - BULK DATA: 512,000 bps
   - WEB: 256,000 bps

   Since the Aruba switch QoS configuration requires bandwidth limits in kilobits per second (kbps), we converted these values by dividing each by 1024, resulting in:
   - VOICE: approximately 977 kbps
   - BULK DATA: approximately 500 kbps
   - WEB: approximately 250 kbps
2. Marks packets for QoS treatment by upstream devices.
3. Ensures unclassified traffic receives standard best-effort handling

4. Apply the Policy to an Interface

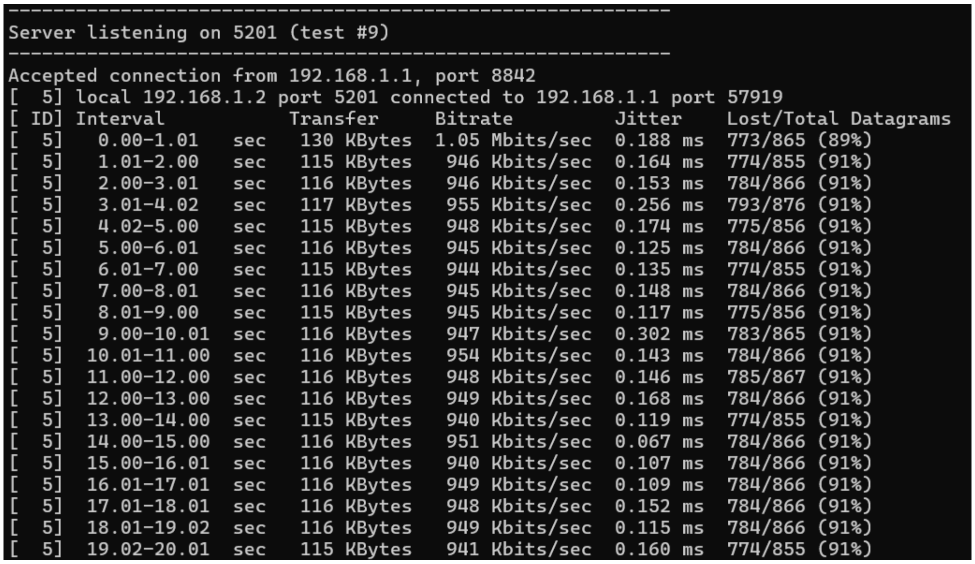


```
 interface 1
    service-policy "QOS_POLICY" in
    exit
 interface 3
    service-policy "QOS_POLICY" in
    exit
```

We applied the "QOS_POLICY" in the inbound direction on both interface 1 and interface 3 because the Aruba Layer 3 switch (version 15) we used only supports applying QoS policies in the inbound direction, unlike Cisco devices which typically support both inbound and outbound directions for service policies.

5. Verification and Testing

a. Verification of the VOIP traffic received from the server side



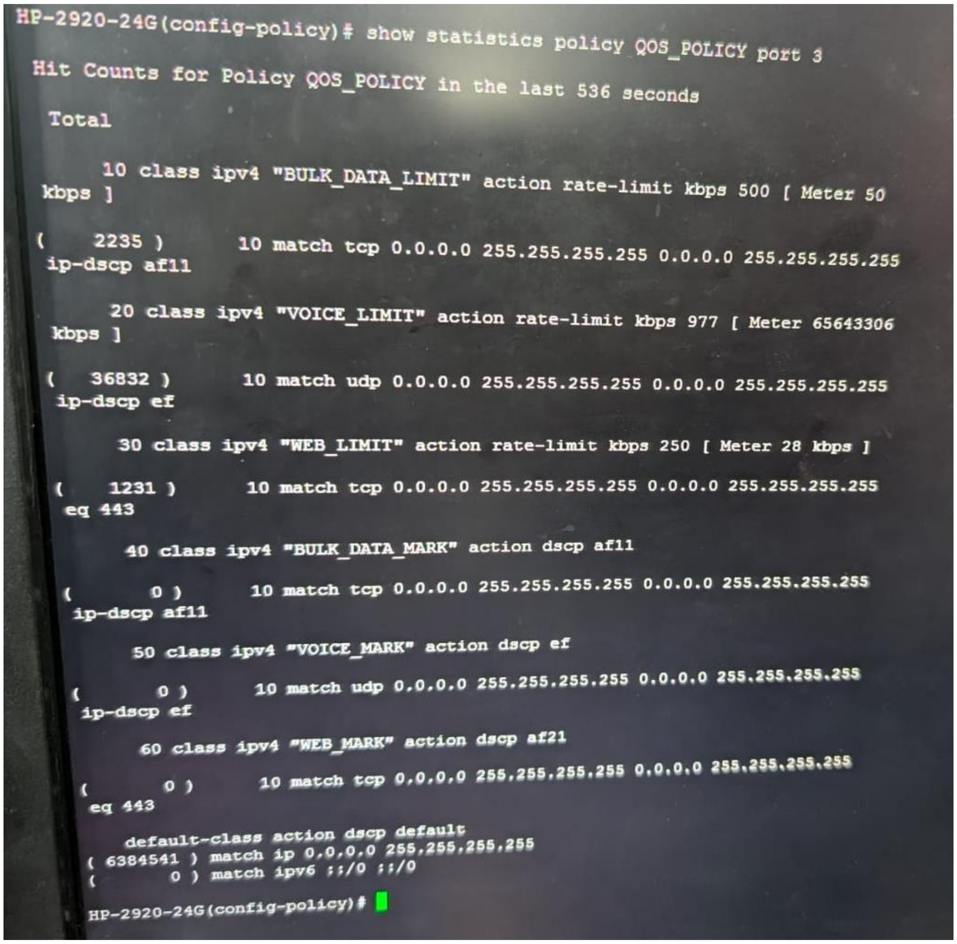
```
-----------------------------------------------------------
Server listening on 5201 (test #9)
-----------------------------------------------------------
Accepted connection from 192.168.1.1, port 8842
[  5] local 192.168.1.2 port 5201 connected to 192.168.1.1 port 57919
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  5]   0.00-1.01   sec   130 KBytes  1.05 Mbits/sec  0.188 ms  773/865 (89%)
[  5]   1.01-2.00   sec   115 KBytes   946 Kbits/sec  0.164 ms  774/855 (91%)
[  5]   2.00-3.01   sec   116 KBytes   946 Kbits/sec  0.153 ms  784/866 (91%)
[  5]   3.01-4.02   sec   117 KBytes   955 Kbits/sec  0.256 ms  793/876 (91%)
[  5]   4.02-5.00   sec   115 KBytes   948 Kbits/sec  0.174 ms  775/856 (91%)
[  5]   5.00-6.01   sec   116 KBytes   945 Kbits/sec  0.125 ms  784/866 (91%)
[  5]   6.01-7.00   sec   115 KBytes   944 Kbits/sec  0.135 ms  774/855 (91%)
[  5]   7.00-8.01   sec   116 KBytes   945 Kbits/sec  0.148 ms  784/866 (91%)
[  5]   8.01-9.00   sec   115 KBytes   945 Kbits/sec  0.117 ms  775/856 (91%)
[  5]   9.00-10.01  sec   116 KBytes   947 Kbits/sec  0.302 ms  783/865 (91%)
[  5]  10.01-11.00  sec   116 KBytes   954 Kbits/sec  0.143 ms  784/866 (91%)
[  5]  11.00-12.00  sec   116 KBytes   948 Kbits/sec  0.146 ms  785/867 (91%)
[  5]  12.00-13.00  sec   116 KBytes   949 Kbits/sec  0.168 ms  784/866 (91%)
[  5]  13.00-14.00  sec   115 KBytes   940 Kbits/sec  0.119 ms  774/855 (91%)
[  5]  14.00-15.00  sec   116 KBytes   951 Kbits/sec  0.067 ms  784/866 (91%)
[  5]  15.00-16.01  sec   116 KBytes   940 Kbits/sec  0.107 ms  784/866 (91%)
[  5]  16.01-17.01  sec   116 KBytes   949 Kbits/sec  0.109 ms  784/866 (91%)
[  5]  17.01-18.01  sec   116 KBytes   948 Kbits/sec  0.152 ms  784/866 (91%)
[  5]  18.01-19.02  sec   116 KBytes   949 Kbits/sec  0.115 ms  784/866 (91%)
[  5]  19.02-20.01  sec   115 KBytes   941 Kbits/sec  0.160 ms  774/855 (91%)
```

It can be observed that even though the client sends at a rate of 10Mbps the client server receives approximately at 977 kbps which is the rate limit set by the Router's QoS policy.

Hence, we can conclude that VOICE traffic has been successfully rate limited by the "VOICE_LIMIT" class along with the policy applied to that class.

Since VoIP (UDP) lacks built-in congestion control and retransmission, its sending rate remains steady even when rate-limited. In contrast to this the next results of TCP traffic (FTP,HTTP) rates will show falling far below the rate limit margin due to TCP's congestion control and retransmission mechanisms.

b. Overall Verification through the Router using live statistics: At interface 3 (connected to client)



```
HP-2920-24G(config-policy)# show statistics policy QOS_POLICY port 3

 Hit Counts for Policy QOS_POLICY in the last 536 seconds

  Total

      10 class ipv4 "BULK_DATA_LIMIT" action rate-limit kbps 500 [ Meter 50
 kbps ]

 (    2235 )      10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
  ip-dscp af11

      20 class ipv4 "VOICE_LIMIT" action rate-limit kbps 977 [ Meter 65643306
 kbps ]

 (   36832 )      10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
  ip-dscp ef

      30 class ipv4 "WEB_LIMIT" action rate-limit kbps 250 [ Meter 28 kbps ]

 (    1231 )      10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
  eq 443

      40 class ipv4 "BULK_DATA_MARK" action dscp af11

 (       0 )      10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
  ip-dscp af11

      50 class ipv4 "VOICE_MARK" action dscp ef

 (       0 )      10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
  ip-dscp ef

      60 class ipv4 "WEB_MARK" action dscp af21

 (       0 )      10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
  eq 443

      default-class action dscp default
 ( 6384541 ) match ip 0.0.0.0 255.255.255.255
 (       0 ) match ipv6 ::/0 ::/0

 HP-2920-24G(config-policy)#
```

According to these live statistics output we can observe that:
Bulk Data Traffic (BULK_DATA_LIMIT):

- Configured Rate: 500 kbps
- Observed Meter Rate: 50 kbps
- Matched Packets: 2,235

Conclusion: Traffic is correctly matched based on DSCP AF11 and is being effectively rate limited. The observed rate is well below the configured limit, indicating that the policy is working as expected.

Also from the above live statistics we can observe that:
Web Traffic (WEB_LIMIT):

- Configured Rate: 250 kbps
- Observed Meter Rate: 28 kbps
- Matched Packets: 1,231

Conclusion: Web traffic (TCP port 443) is being correctly classified and limited. The metered rate is significantly below the 250 kbps cap, confirming that the rate limiting is functioning properly.

Therefore, considering outputs observed at a and b, we can conclude that all three traffic types VOICE, BULK_DATA, WEB have been successfully rate limited by the router.

Reflection Questions:

1. **What is the purpose of rate limiting in QoS?**

Rate limiting controls the maximum bandwidth allocated to specific traffic classes by enforcing a fixed bandwidth caps on specific traffic classes, ensuring fair usage and preventing lower-priority traffic from overwhelming the network.

2. **How does policing affect different traffic classes in your setup?**

In this setup, policing enforces strict bandwidth limits per class (e.g., 500 kbps for bulk data, 250 kbps for web, and 977 kbps for VoIP), dropping excess packets once the limit is exceeded. This ensures that high-priority services like VoIP are protected with more generous bandwidth allocation, while lower-priority traffic is more aggressively constrained.

3. **What happens to packets that exceed the configured rate?**

Packets exceeding the configured rate were dropped, leading to lower throughput and packet loss. UDP traffic (e.g., VoIP) maintained rates near the limit since it sends continuously without adjusting for loss, while TCP traffic (e.g., FTP, HTTPS) fell well below the limit due to its built-in congestion control and retransmission behavior.

4. **Compare the behavior of rate-limited FTP vs. VoIP traffic.**

Rate-limited FTP (TCP) traffic experienced noticeably lower throughput because TCP is sensitive to packet loss. When packets are dropped due to rate limiting, TCP's congestion control mechanisms reduce the sending rate and attempt to recover through retransmissions, which further slows down the flow. In contrast, VoIP (UDP) traffic maintained throughput close to the configured rate limit, as UDP does not respond to packet loss as there are no retransmissions or congestion control, so it continues sending at a steady rate regardless of network conditions. This difference makes TCP traffic more reactive and adaptive but less efficient under strict rate limits, while UDP remains consistent but risks higher loss.

5. When should you prefer shaping over policing, and why?

Rate limiting (policing) strictly enforces a bandwidth cap by dropping packets that exceed the limit, which can cause packet loss. In contrast, shaping buffers excess packets and sends them later to smooth traffic bursts, avoiding packet loss but adding some delay. Shaping is generally preferred for delay-sensitive or TCP traffic because it maintains a smoother flow and reduces the impact of retransmissions and congestion control triggered by dropped packets.