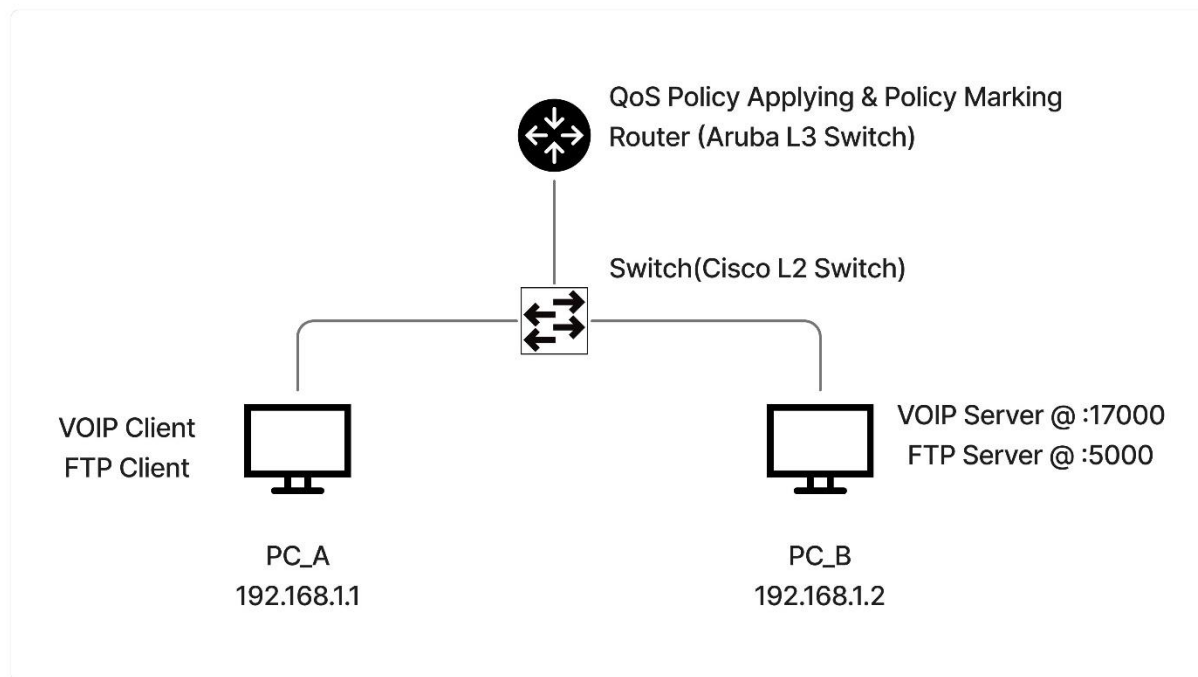


CO513: Advanced Computer Communication Networks - Lab 03

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

16/05/2025

Network Configuration and Setup Summary



We initially began the lab with the recommended network topology consisting of two PCs (Client A and Client B), one router, and one switch. However, we faced ongoing challenges in finding the correct Aruba version and its commands for the router, which was also running an older version of the firmware. These issues complicated the configuration process and diverted focus from the main objective of the lab. As a result, we were instructed to remove the switch from the topology in order to simplify the setup. This adjustment did not impact the core QoS policy implementation or testing, as the switch was not essential for the classification and marking processes carried out on the router.

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

Lab Tasks:

1. Generate Traffic

For traffic generation, we used iPerf3 to simulate both FTP (for Bulk Data) and VoIP (for Voice Data) 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 512k -t 300 --tos 184 -p 17000
Connecting to host 192.168.1.2, port 17000
[ 5] local 172.26.99.113 port 58233 connected to 192.168.1.2 port 17000
ID] Interval      Transfer      Bitrate      Total Datagrams
[ 5] 0.00-1.00    sec  63.6 KBytes  521 Kbits/sec  45
[ 5] 1.00-2.00    sec  62.2 KBytes  510 Kbits/sec  44
[ 5] 2.00-3.00    sec  62.2 KBytes  510 Kbits/sec  44
[ 5] 3.00-4.00    sec  62.2 KBytes  510 Kbits/sec  44
[ 5] 4.00-5.00    sec  62.2 KBytes  510 Kbits/sec  44
[ 5] 5.00-6.00    sec  63.6 KBytes  521 Kbits/sec  45
[ 5] 6.00-7.00    sec  62.2 KBytes  510 Kbits/sec  44
[ 5] 7.00-8.00    sec  62.2 KBytes  510 Kbits/sec  44
[ 5] 8.00-9.00    sec  62.2 KBytes  510 Kbits/sec  44
[ 5] 9.00-10.00   sec  62.2 KBytes  510 Kbits/sec  44
[ 5] 10.00-11.00  sec  63.6 KBytes  521 Kbits/sec  45
[ 5] 11.00-12.00  sec  62.2 KBytes  510 Kbits/sec  44
```

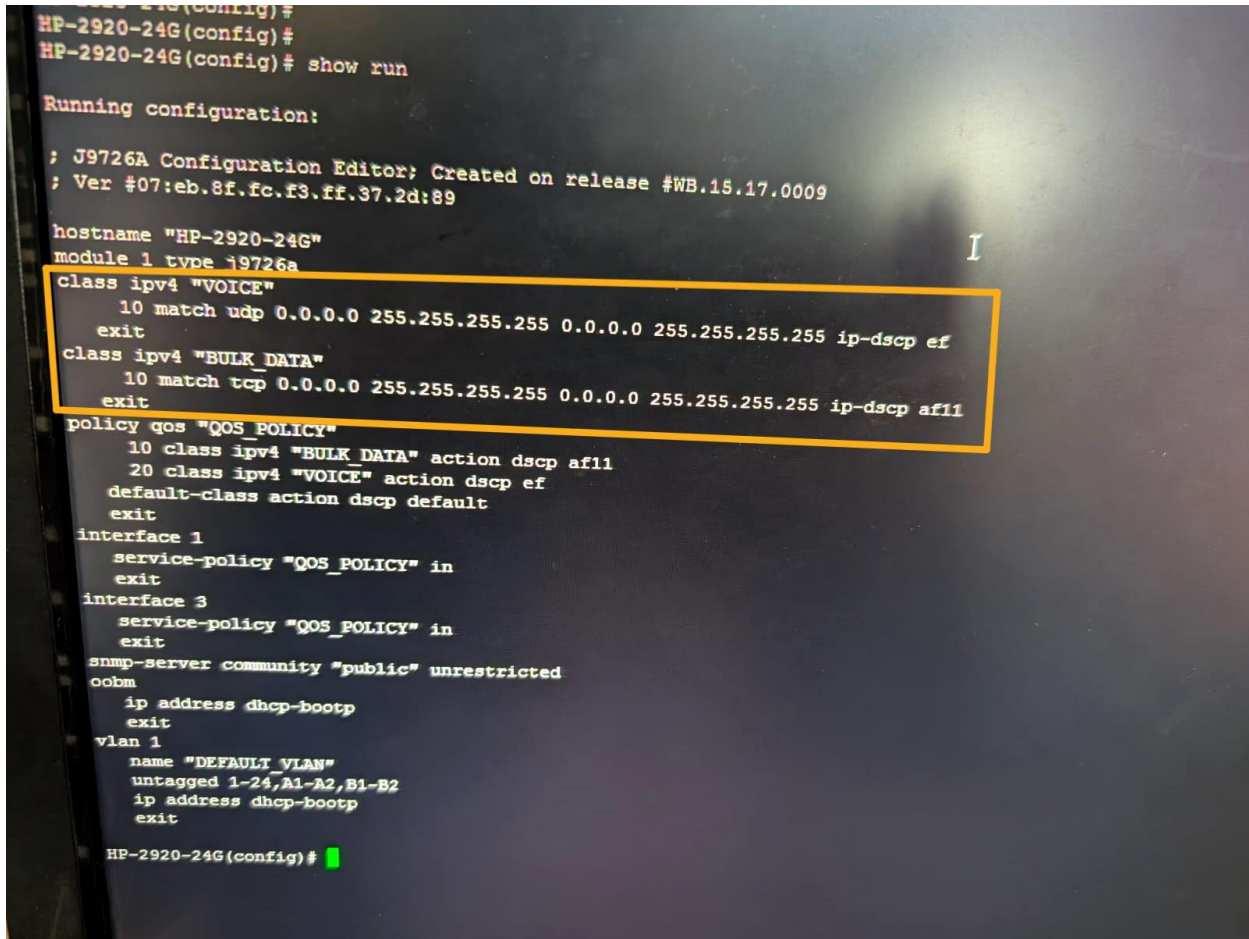
This command sends UDP traffic from PC-A to PC-B at a rate of 512 Kbps for 300 seconds, representing a typical VoIP stream. The --tos 184 option sets the ToS byte to 184, which maps to DSCP EF (Expedited Forwarding)—a class used for latency-sensitive traffic such as VoIP. Port 17000 was chosen as it falls within the standard RTP range which is commonly used for VOIP.

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 above command initiates a TCP connection from PC-A to the iPerf3 server on PC-B at IP address 192.168.1.2, sending data at a rate of 5 Mbps for 300 seconds. The --tos 40 option sets the Type of Service (ToS) byte to 40, which corresponds to DSCP AF11 (Assured Forwarding class 1), commonly used for bulk data transfers like FTP. The traffic is directed through port 5000.

2. Configure Traffic Classification (Router)



```
HP-2920-24G(config)#
HP-2920-24G(config)#
HP-2920-24G(config)# 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 "VOICE"
  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"
  10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 ip-dscp af11
  exit
policy qos "QOS_POLICY"
  10 class ipv4 "BULK_DATA" action dscp af11
  20 class ipv4 "VOICE" action dscp ef
  default-class action dscp default
  exit
interface 1
  service-policy "QOS_POLICY" in
  exit
interface 3
  service-policy "QOS_POLICY" in
  exit
snmp-server community "public" unrestricted
oobm
  ip address dhcp-bootp
  exit
vlan 1
  name "DEFAULT_VLAN"
  untagged 1-24,A1-A2,B1-B2
  ip address dhcp-bootp
  exit
HP-2920-24G(config)#
```

For traffic classification, we used Method A: Protocol-based Class Maps, and created two IPv4 classes on the router: "VOICE" to match all UDP traffic marked with DSCP EF (used for VoIP), and "BULK DATA" 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

To create the QoS policy, we defined a policy map named "QOS_POLICY" that binds the previously defined traffic classes to specific actions: "BULK_DATA" traffic is marked with DSCP AF11, "VOICE" traffic with DSCP EF, and all other unmatched traffic is assigned the default DSCP value.

The highlighted part of the following snapshot is our Policy Map configuration.

```

class ipv4 "BULK_DATA"
  10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 ip-dscp ef
  exit
policy qos "QOS_POLICY"
  10 class ipv4 "BULK_DATA" action dscp af11
  20 class ipv4 "VOICE" action dscp ef
  default-class action dscp default
  exit
interface 1
  service-policy "QOS_POLICY" in
  exit
interface 3
  service-policy "QOS_POLICY" in
  exit

```

4. Apply the Policy to an Interface

```

class ipv4 "BULK_DATA" action dscp af11
20 class ipv4 "VOICE" action dscp ef
default-class action dscp default
exit
interface 1
  service-policy "QOS_POLICY" in
  exit
interface 3
  service-policy "QOS_POLICY" in
  exit
snmp-server community "public" unrestricted
coba
ip address dhcp-bootp
exit
vlan 1
  name "DEFAULT_VLAN"
  untagged 1-24,A1-A2,B1-B2
  ip address dhcp-bootp
  exit
HP-2920-24G(config)#

```

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

```
C:\Windows\System32\cmd.e X + v - □ X

[ 5] 279.01-280.00 sec 62.2 KBytes 517 Kbits/sec 0.291 ms 0/44 (0%)
[ 5] 280.00-281.00 sec 62.2 KBytes 508 Kbits/sec 0.441 ms 0/44 (0%)
[ 5] 281.00-282.00 sec 62.2 KBytes 510 Kbits/sec 0.332 ms 0/44 (0%)
[ 5] 282.00-283.00 sec 63.6 KBytes 521 Kbits/sec 0.582 ms 0/45 (0%)
[ 5] 283.00-284.00 sec 62.2 KBytes 510 Kbits/sec 0.618 ms 0/44 (0%)
[ 5] 284.00-285.01 sec 62.2 KBytes 509 Kbits/sec 0.486 ms 0/44 (0%)
[ 5] 285.01-286.01 sec 62.2 KBytes 509 Kbits/sec 0.982 ms 0/44 (0%)
[ 5] 286.01-287.01 sec 63.6 KBytes 521 Kbits/sec 0.749 ms 0/45 (0%)
[ 5] 287.01-288.01 sec 62.2 KBytes 509 Kbits/sec 0.650 ms 0/44 (0%)
[ 5] 288.01-289.01 sec 62.2 KBytes 509 Kbits/sec 0.448 ms 0/44 (0%)
[ 5] 289.01-290.01 sec 62.2 KBytes 510 Kbits/sec 0.787 ms 0/44 (0%)
[ 5] 290.01-291.01 sec 63.6 KBytes 520 Kbits/sec 0.469 ms 0/45 (0%)
[ 5] 291.01-292.01 sec 62.2 KBytes 509 Kbits/sec 0.578 ms 0/44 (0%)
[ 5] 292.01-293.01 sec 62.2 KBytes 510 Kbits/sec 0.748 ms 0/44 (0%)
[ 5] 293.01-294.01 sec 62.2 KBytes 509 Kbits/sec 0.589 ms 0/44 (0%)
[ 5] 294.01-295.01 sec 62.2 KBytes 509 Kbits/sec 0.453 ms 0/44 (0%)
[ 5] 295.01-296.01 sec 63.6 KBytes 520 Kbits/sec 0.897 ms 0/45 (0%)
[ 5] 296.01-297.01 sec 62.2 KBytes 509 Kbits/sec 0.587 ms 0/44 (0%)
[ 5] 297.01-298.02 sec 62.2 KBytes 509 Kbits/sec 0.642 ms 0/44 (0%)
[ 5] 298.02-299.00 sec 62.2 KBytes 517 Kbits/sec 0.314 ms 0/44 (0%)
[ 5] 299.00-300.00 sec 62.2 KBytes 509 Kbits/sec 1.114 ms 0/44 (0%)

-----
[ ID] Interval      Transfer      Bitrate      Jitter      Lost/Total Da
tagrams
[ 5] 0.00-300.01 sec 18.3 MBytes  512 Kbits/sec 1.114 ms    0/13260 (0%)
receiver
-----
Server listening on 17000 (test #2)
-----
```

```

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ipdst == 192.168.1.2

No. Time Source Destination Protocol Length Info
25108 623.499665 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25109 623.522846 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25110 623.544871 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25111 623.568677 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25112 623.590774 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25115 623.612733 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25116 623.636368 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25117 623.658606 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25118 623.680707 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25119 623.704149 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25120 623.725925 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25121 623.748906 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25122 623.772335 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25123 623.794557 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25124 623.816796 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25125 623.839682 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25126 623.861690 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25127 623.884974 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25128 623.907495 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448
25129 623.929829 192.168.1.1 192.168.1.2 UDP 1490 EF 65036 → 17000 Len=1448

> Frame 25123: 1490 bytes on wire (11920 bits), 1490 bytes captured (11920 bits) on interface \DeviceN
> Ethernet II, Src: ASUSTekCOMPU_88:99:d7 (24:4b:fe:88:99:d7), Dst: CompalInform_e3:7e:b3 (08:97:98:e3:
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0xb8 (DSCP: EF, ECN: Not-ECT)
Total Length: 1476
Identification: 0x1145 (4421)
010. .... = Flags: 0x2, Don't Fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 63
Protocol: UDP (17)
Header Checksum: 0xa0d8 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.1
0000 08 97 98 e3 7e b3 24 4b fe 88 99 d7 08 00 45 b8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0010 05 c4 11 45 40 00 3f 11 a0 d8 c0 a8 01 01 c0 a8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0020 01 02 fe bc 42 68 05 b0 5d d2 00 00 0e de 00 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0030 a5 c9 00 00 1a bc 54 70 cc cd cb 4c a9 d0 b4 69 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 0c bf 9f 16 48 73 ef b3 6f ed 26 b6 17 0b b1 f2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 3f 2a bc 0d 8f 32 45 62 5d e3 f1 80 48 8a 6a 5b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 f2 8c a6 a1 6b de 22 06 6d f2 b8 b2 f8 20 2f 82 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 f5 3d 0e 7e 90 77 39 f4 1c 50 b5 0f 50 b6 b8 3d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 b0 ff 49 bc 8e 36 34 d3 25 6c 2d 01 e5 04 c1 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 c7 a5 8b 9b 60 1b e4 04 8f a9 0b 5f ea 8c de d9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00a0 9f 51 39 5a 2a 23 2c 98 99 85 bc d9 a7 0b 99 49 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0 34 a3 25 71 33 33 dc 49 08 42 ec bd b9 76 1d c7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0 aa e6 eb 26 69 dc c2 88 ba 82 79 43 28 bd ee ce 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00d0 f4 db c5 54 d5 a8 3a 01 3b 1d 5a f4 53 48 ae e9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00e0 cd 1a 1b c5 11 60 57 6f 3d fa 88 40 1d bd c8 ad 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00f0 5e 24 11 66 cf e8 b9 0b da b7 84 6f bc 05 f8 3d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0100 ce a1 9d 26 9f 87 09 d1 45 6f 47 00 ff 41 0d dd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110 a1 3f 4e 37 56 9e 9e 1f a1 b8 49 f5 a2 5e 68 c5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0120 88 30 8e 91 a7 cd 64 2f 8a 93 30 da 5c f2 6c a4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

It can be observed from the above wireshark output, that the traffic marked as EF (VOIP) was successfully received by the server.

b. Verification of the BULK DATA traffic received from the server side

```
C:\Windows\System32\cmd.e x + v - □ x

[ 5] 186.01-187.01 sec 512 KBytes 4.19 Mb/s/sec
[ 5] 187.01-188.00 sec 640 KBytes 5.32 Mb/s/sec
[ 5] 188.00-189.00 sec 640 KBytes 5.24 Mb/s/sec
[ 5] 189.00-190.00 sec 640 KBytes 5.24 Mb/s/sec
[ 5] 190.00-191.00 sec 512 KBytes 4.19 Mb/s/sec
[ 5] 191.00-192.00 sec 640 KBytes 5.24 Mb/s/sec
[ 5] 192.00-193.00 sec 640 KBytes 5.24 Mb/s/sec
[ 5] 193.00-194.00 sec 640 KBytes 5.24 Mb/s/sec
[ 5] 194.00-195.00 sec 512 KBytes 4.19 Mb/s/sec

[ 5] 195.00-196.00 sec 640 KBytes 5.24 Mb/s/sec
[ 5] 196.00-197.00 sec 640 KBytes 5.24 Mb/s/sec
[ 5] 197.00-198.01 sec 640 KBytes 5.23 Mb/s/sec
[ 5] 198.01-199.00 sec 640 KBytes 5.25 Mb/s/sec
[ 5] 198.01-199.00 sec 640 KBytes 5.25 Mb/s/sec

-----
[ ID] Interval          Transfer    Bitrate
[ 5]  0.00-199.00 sec  119 MBytes 5.01 Mb/s/sec
receiver
iperf3: the client has terminated
-----
Server listening on 5000 (test #3)
-----
```

Capturing from Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 192.168.1.2

No.	Time	Source	Destination	Protocol	Length	Difference	Info
1210921	4341.279531	192.168.1.1	192.168.1.2	TCP	1514		AF11 4290 → 5000 [PSH, ACK] Seq=124635726 Ack=1 Win=64256 Len=1448 TSval=277765825 TSecr=265734024
1210923	4341.279953	192.168.1.1	192.168.1.2	TCP	1514		AF11 4290 → 5000 [ACK] Seq=124637174 Ack=1 Win=64256 Len=1448 TSval=277765825 TSecr=265734024
1210924	4341.279953	192.168.1.1	192.168.1.2	RSL	1514		AF11 DELETE INDICATION (CCH) (LS)
1210925	4341.279953	192.168.1.1	192.168.1.2	TCP	1514		AF11 4290 → 5000 [ACK] Seq=124640070 Ack=1 Win=64256 Len=1448 TSval=277765825 TSecr=265734024
1210927	4341.280157	192.168.1.1	192.168.1.2	TCP	1514		AF11 4290 → 5000 [ACK] Seq=124641518 Ack=1 Win=64256 Len=1448 TSval=277765825 TSecr=265734024
1210928	4341.280157	192.168.1.1	192.168.1.2	RSL	1514		AF11 MEASUREMENT RESULT
1210930	4341.280485	192.168.1.1	192.168.1.2	TCP	1514		AF11 4290 → 5000 [ACK] Seq=124644414 Ack=1 Win=64256 Len=1448 TSval=277765825 TSecr=265734024
1210931	4341.280485	192.168.1.1	192.168.1.2	TCP	1514		AF11 4290 → 5000 [PSH, ACK] Seq=124645862 Ack=1 Win=64256 Len=1448 TSval=277765825 TSecr=265734024
1210932	4341.280485	192.168.1.1	192.168.1.2	TCP	1514		AF11 4290 → 5000 [ACK] Seq=124647310 Ack=1 Win=64256 Len=1448 TSval=277765826 TSecr=265734024
1210934	4341.280791	192.168.1.1	192.168.1.2	TCP	1514		AF11 4290 → 5000 [ACK] Seq=124648758 Ack=1 Win=64256 Len=1448 TSval=277765826 TSecr=265734024
1210935	4341.280791	192.168.1.1	192.168.1.2	TCP	1514		AF11 4290 → 5000 [ACK] Seq=124650206 Ack=1 Win=64256 Len=1448 TSval=277765826 TSecr=265734024
1210937	4341.281075	192.168.1.1	192.168.1.2	TCP	1514		AF11 4290 → 5000 [ACK] Seq=124651654 Ack=1 Win=64256 Len=1448 TSval=277765826 TSecr=265734024
1210938	4341.281075	192.168.1.1	192.168.1.2	TCP	1514		AF11 4290 → 5000 [ACK] Seq=124653102 Ack=1 Win=64256 Len=1448 TSval=277765826 TSecr=265734024
1210940	4341.281191	192.168.1.1	192.168.1.2	TCP	1514		AF11 4290 → 5000 [ACK] Seq=124654550 Ack=1 Win=64256 Len=1448 TSval=277765826 TSecr=265734024
1210942	4341.281239	192.168.1.1	192.168.1.2	TCP	1514		AF11 4290 → 5000 [PSH, ACK] Seq=124655998 Ack=1 Win=64256 Len=1448 TSval=277765826 TSecr=265734024
1210943	4341.281516	192.168.1.1	192.168.1.2	TCP	1514		AF11 4290 → 5000 [ACK] Seq=124657446 Ack=1 Win=64256 Len=1448 TSval=277765826 TSecr=265734024
1210944	4341.281516	192.168.1.1	192.168.1.2	TCP	1514		AF11 4290 → 5000 [ACK] Seq=124658894 Ack=1 Win=64256 Len=1448 TSval=277765826 TSecr=265734024
1210946	4341.281801	192.168.1.1	192.168.1.2	TCP	1514		AF11 4290 → 5000 [ACK] Seq=124660342 Ack=1 Win=64256 Len=1448 TSval=277765826 TSecr=265734024
1210947	4341.281801	192.168.1.1	192.168.1.2	TCP	1514		AF11 4290 → 5000 [ACK] Seq=124661790 Ack=1 Win=64256 Len=1448 TSval=277765826 TSecr=265734024
1210949	4341.281921	192.168.1.1	192.168.1.2	TCP	1514		AF11 4290 → 5000 [ACK] Seq=124663238 Ack=1 Win=64256 Len=1448 TSval=277765826 TSecr=265734024

> Frame 1210932: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device NPF{...}

> Ethernet II, Src: ASUSTekCOMP...88:99:d7 (24:4b:fe:88:99:d7), Dst: CompallInform_e3:7e:b3 (08:97:98:e3:7e:b3)

> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2

> 0100 = Version: 4

> 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x28 (DSCP: AF11, ECN: Not-ECT)

> Total Length: 1500

> Identification: 0x23e2 (9186)

> 010. = Flags: 0x2, Don't fragment

> 000000000000 = Fragment Offset: 0

> Time to Live: 63

> Protocol: TCP (6)

> Header Checksum: 0x8ebe [validation disabled]

> [Header checksum status: Unverified]

> Source Address: 192.168.1.1

> 0000 08 97 98 e3 7e b3 24 4b fe 88 99 d7 00 00 45 28\$K.....E

> 0010 05 dc 23 e2 40 00 3f 06 8e be c0 a8 01 01 c0 a8@?.....

> 0020 01 02 10 c2 13 88 b2 be 2f 01 f9 01 cd df 80 10/.....

> 0030 01 f6 cd 65 00 00 01 01 08 0a 10 8e 5e c2 0f d6:.....

> 0040 c7 88 5b fa 61 27 a2 ad f6 30 a8 f3 93 8c ed e5[a].....

> 0050 b0 68 01 ff 4a af 42 a0 ef f1 ea 6b d8 58 90 5ahJ BkXZ

> 0060 43 69 2d e0 68 d3 5a d8 3e 2c f4 7c a3 ac ec 9eCI-hZ: >.....

> 0070 9e 16 3c 78 c0 63 da 61 c5 2d 37 4b d9 92 7c ba<x c a -7K-|

> 0080 92 2d 85 56 ce f0 8a f6 e3 4c ed c7 83 52 52 5fV.....RR

> 0090 28 44 66 f3 2f f3 7b 51 b8 a5 5b 19 c8 78 51 2c(Df-/Q-[-xQ,

> 00a0 65 3a 35 9e 76 5b ba 0d 3b cf a2 e8 7e 3a 2f 53eISv[-j...:/5

> 00b0 97 f2 c7 69 d4 3b 6b b6 53 d7 d8 aa 11 4c 7d 34:i:f: S.....J4

> 00c0 0c e0 bd 88 d9 5a 89 1d 49 47 bc f9 ff 77 b0 e7-Z: IG.....

> 00d0 2f c4 1d 56 ed 17 21 2d 65 80 c5 87 5e 61 1b 1a/V-l- e...A...

> 00e0 fc ec 18 33 61 bd e9 44 dc bb fb 9c 6d d5 80 073a: Dm

> 00f0 a3 56 ee fc f7 f5 ce 5c bd 9d 8d cd 7a 7d db f6V:~\.....2

> 0100 d9 b9 f0 71 bc 3f e0 a4 c7 78 ac 11 ad b1 fb df-q-?.....x.....

> 0110 ef 2b 63 48 18 83 9c b6 1d 55 1e ac 98 da d0 88<H.....U.....

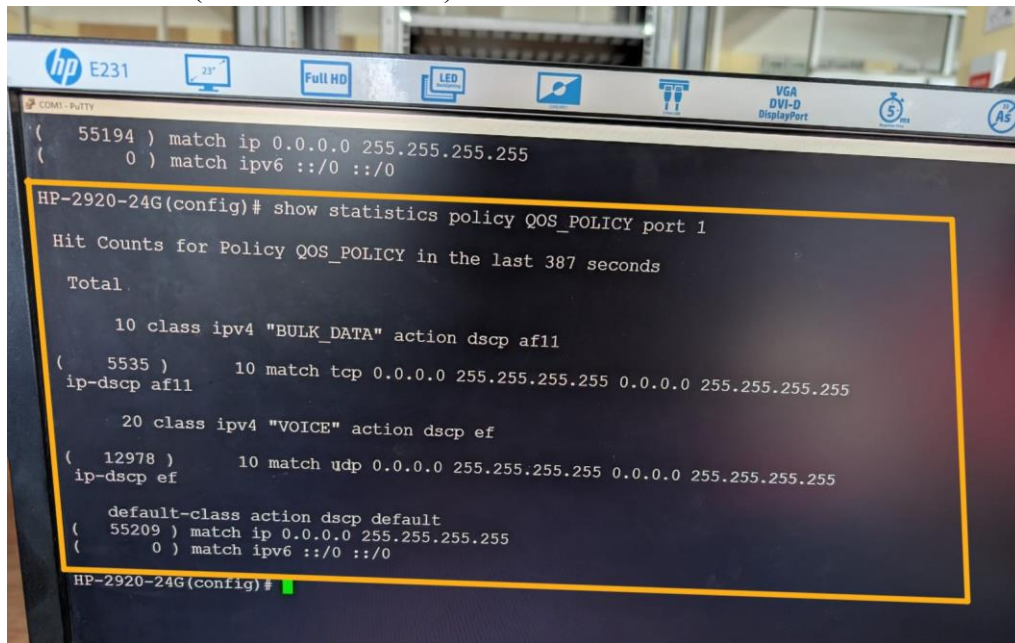
> 0120 43 75 f4 a9 ec f4 1a d7 b5 d4 2f 28 15 db be e7CuO.....-/(.....

Packets: 1211866 - Displayed: 1110617 (91.6%) Profile: Default

It can be observed from the above wireshark output, that the traffic marked as AF11 (BULK_DATA) was successfully received by the server.

c. Overall Verification through the Router using live statistics

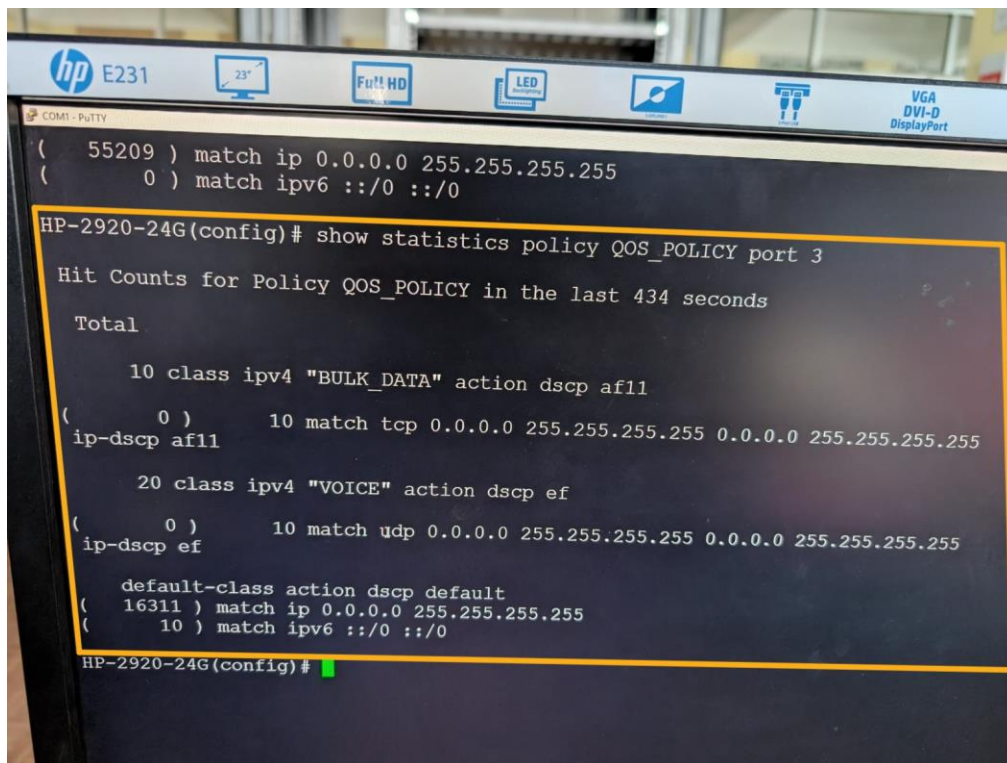
At interface 1 (connected to client)



The screenshot shows a terminal window with a dark background and white text. The terminal title bar at the top reads "COM1 - PuTTY". The main content shows the configuration of a QoS policy named "QOS_POLICY" on interface 1. The policy has two classes: "BULK_DATA" and "VOICE". The "BULK_DATA" class has a match for TCP traffic from 0.0.0.0/255.255.255.255 to 0.0.0.0/255.255.255.255 with an action of dscp af11. The "VOICE" class has a match for UDP traffic from 0.0.0.0/255.255.255.255 to 0.0.0.0/255.255.255.255 with an action of dscp ef. The default class action is dscp default. The statistics show that the "BULK_DATA" class has 55194 hits and the "VOICE" class has 12978 hits. The terminal text is as follows:

```
( 55194 ) match ip 0.0.0.0 255.255.255.255
( 0 ) match ipv6 ::/0 ::/0
HP-2920-24G(config)# show statistics policy QOS_POLICY port 1
Hit Counts for Policy QOS_POLICY in the last 387 seconds
Total
    10 class ipv4 "BULK_DATA" action dscp af11
( 5535 )      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" action dscp ef
( 12978 )     10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
ip-dscp ef
    default-class action dscp default
( 55209 ) match ip 0.0.0.0 255.255.255.255
( 0 ) match ipv6 ::/0 ::/0
HP-2920-24G(config)#
```

At interface 3 (connected to the server)



The screenshot shows a terminal window with a dark background and white text. The terminal title bar at the top reads "COM1 - PuTTY". The main content shows the configuration of a QoS policy named "QOS_POLICY" on interface 3. The policy has two classes: "BULK_DATA" and "VOICE". The "BULK_DATA" class has a match for TCP traffic from 0.0.0.0/255.255.255.255 to 0.0.0.0/255.255.255.255 with an action of dscp af11. The "VOICE" class has a match for UDP traffic from 0.0.0.0/255.255.255.255 to 0.0.0.0/255.255.255.255 with an action of dscp ef. The default class action is dscp default. The statistics show that the "BULK_DATA" class has 55209 hits and the "VOICE" class has 16311 hits. The terminal text is as follows:

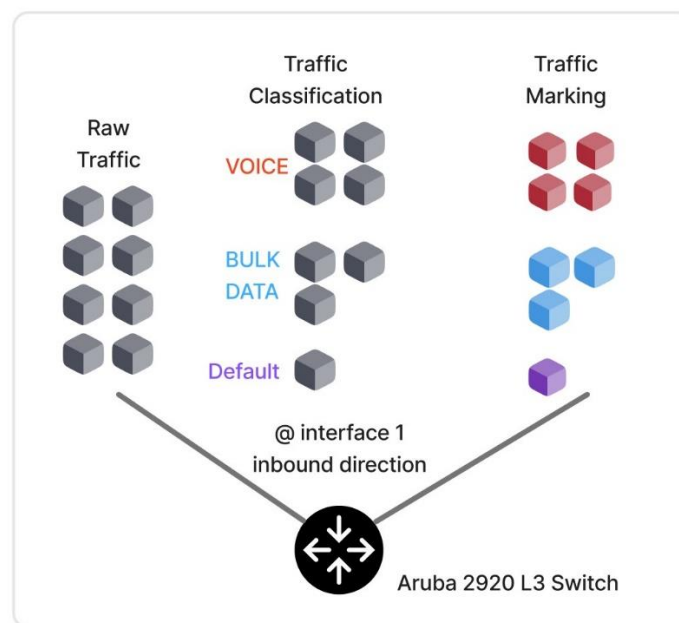
```
( 55209 ) match ip 0.0.0.0 255.255.255.255
( 0 ) match ipv6 ::/0 ::/0
HP-2920-24G(config)# show statistics policy QOS_POLICY port 3
Hit Counts for Policy QOS_POLICY in the last 434 seconds
Total
    10 class ipv4 "BULK_DATA" action dscp af11
( 0 )      10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
ip-dscp af11
    20 class ipv4 "VOICE" 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
    default-class action dscp default
( 16311 ) match ip 0.0.0.0 255.255.255.255
( 10 ) match ipv6 ::/0 ::/0
HP-2920-24G(config)#
```

The above output confirms that QoS classification and marking occurred successfully on the client-facing interface (Interface 1). However, no matching was observed on the server-facing interface (Interface 3), because QoS policies were applied in the inbound direction only, as Aruba HP switches do not support applying QoS on outbound interfaces.

Reflection Questions:

1. How does traffic classification differ from traffic marking?

Traffic classification is the process of identifying and categorizing packets based on attributes like protocol, port, IP or DSCP value. In contrast to that traffic marking is assigning specific QoS values (like DSCP) to those classified packets. The following figure depicts the high level behavior of the QoS classification and marking that was observed in this lab experiment.



2. Why is classification a prerequisite before applying other QoS mechanisms like queuing or policing?

Classification is essential because it tells the router how to identify different types of traffic. Without first identifying the traffic, applying mechanisms like queuing, policing, or prioritization would not make sense and would be meaningless. Even if these mechanisms were somehow applied blindly to individual packets without classification, it would lead to inefficient resource usage and inconsistent treatment of traffic, ultimately defeating the purpose of QoS.

3. How are RTP or VoIP packets identified in a live network?

The Aruba L3 switch used in this lab had the capability to identify RTP or VoIP packets using two main methods: by matching UDP port ranges (specifically the range 16384–32767, commonly used by RTP for VoIP traffic) and by inspecting the DSCP value, such as EF (Expedited Forwarding), which is typically used to mark real-time voice traffic. However, in our configuration, we used DSCP-based matching to classify the traffic, relying on previously marked packets to apply QoS policies.

4. What challenges arise when classifying traffic that is encrypted (e.g., HTTPS or VPN)? How might network devices handle such cases?

In the context of encrypted traffic such as HTTPS or VPN, matching using DSCP values is often not possible because encryption may hide or strip QoS markings, or intermediate devices may overwrite them. As a result, network devices cannot rely solely on DSCP for classification and must instead use alternative methods like matching based on port numbers, or employ deep packet inspection (DPI) if available.