Lab 3: Traffic Classification in Quality of Service (QoS) Networks

Objective:

To understand and implement traffic classification and marking in a **QoS-enabled** network by simulating various types of traffic and applying Cisco IOS configurations to classify and manage the traffic effectively.

Problem Statement:

In modern networks, various applications (like video calls, file transfers, and web browsing) compete for bandwidth. **Quality of Service (QoS)** ensures that time-sensitive data like VoIP is prioritized over less critical traffic like FTP downloads. This lab explores how routers classify different types of traffic and apply specific QoS policies.

Network Topology:

- 2 PCs (Client A and Client B)
- 1 Router
- 1 Switch

Configure basic IP addressing and routing to ensure end-to-end connectivity between the PCs through the router.

Lab Tasks:

1. Generate Traffic

Simulate the following traffic from PC-A to PC-B:

- **ICMP:** Use ping for network testing
- **HTTP/HTTPS:** Browse websites using the browser simulation.
- **FTP:** Transfer a file using the FTP client/server.
- **VoIP/UDP:** Use simulated VoIP or UDP streaming tools to create real-time traffic.

2. Configure Traffic Classification (Router)

Method A: Using Protocol-based Class Maps (if supported)

```
class-map match-any VOICE
 match protocol rtp
```

Method B: Using Access Control Lists (ACLs)

```
access-list 101 permit udp any any range 16384 32767   ! RTP for VoIP
access-list 102 permit tcp any any eq ftp              ! FTP traffic

class-map match-any VOICE
 match access-group 101

class-map match-any BULK_DATA
 match access-group 102
```

3. Create a Policy Map

Bind the traffic classes to QoS policies and assign DSCP values:

```
policy-map QOS_POLICY
 class VOICE
  set dscp ef
 class BULK_DATA
  set dscp af11
 class class-default
  set dscp default
```

4. Apply the Policy to an Interface

Choose the appropriate interface (e.g. LAN side or WAN exit interface)

```
interface FastEthernet0/0
 service-policy output QOS_POLICY
```

5. Verification and Testing

- Use `show policy-map interface` to confirm traffic classification.
- Use Wireshark on a PC to capture packets and inspect DSCP markings.
- Perform the traffic tests again:
  - Ping
  - Web browsing
  - FTP transfer
  - VoIP call
- Observe and note how traffic is matched and marked.

Reflection Questions:

1. How does traffic classification differ from traffic marking?
2. Why is classification a prerequisite before applying other QoS mechanisms like queuing or policing?
3. How are RTP or VoIP packets identified in a live network?
4. What challenges arise when classifying traffic that is encrypted (e.g., HTTPS or VPN)? How might network devices handle such cases?

Submission Format:

All observations, screenshots and answers to the questions to be submitted as a PDF named `E19XXX_Lab03.pdf`, where `<XXX>` is your e no.