Lab 4: Applying Rate Limiting to Different Traffic Classes

Objective:

To understand and implement traffic rate limiting (policing and shaping) on different types of network traffic using class-based traffic policies in a QoS-enabled Cisco network.

Problem Statement:

Modern networks carry a mix of traffic types from real-time VoIP calls to large file transfers, each with different sensitivity to delay and packet loss. Without Quality of Service (QoS), critical traffic can suffer due to congestion caused by lower-priority or high-bandwidth applications. In this lab, you are tasked with configuring a QoS-enabled router to enforce **bandwidth constraints** on different traffic classes (VoIP, FTP, Web), using **rate-limiting mechanisms** like **policing** and **shaping**. You will classify traffic, mark it with appropriate DSCP values, apply rate limits, and verify that packets are prioritized and dropped according to defined policies. Your challenge is to ensure that **real-time traffic remains protected**, while **bulk and web traffic are rate-limited** in a way that avoids congestion and promotes fair resource usage.

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

class-map match-any WEB
 match protocol http
 match protocol https
```

3. Create Policy Map with Rate Limiting

Apply **policing** to each traffic class using `police` commands:

```
policy-map RATE_LIMIT_POLICY
 class VOICE
  set dscp ef
  police 1000000 8000 conform-action transmit exceed-action drop

 class BULK_DATA
  set dscp af11
  police 512000 8000 conform-action transmit exceed-action drop

 class WEB
  set dscp af21
  police 256000 4000 conform-action transmit exceed-action drop

 class class-default
  set dscp default
```

4. Apply the Policy to an Interface

Apply policy **on ingress** (from PC-A) or **egress** (to PC-B):

```
interface FastEthernet0/0
 service-policy input RATE_LIMIT_POLICY
```

Or for output:

```
interface FastEthernet0/1
 service-policy output RATE_LIMIT_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, and analyze packet loss and traffic rate differences between FTP, HTTP, and VoIP.
- Perform the traffic tests again:
    - Ping
    - Web browsing
    - FTP transfer
    - VoIP call
- Observe and note the traffic rate differences between the classes.

Reflection Questions:

1. What is the purpose of rate limiting in QoS?
2. How does policing affect different traffic classes in your setup?
3. What happens to packets that exceed the configured rate?
4. Compare the behavior of rate-limited FTP vs. VoIP traffic.
5. When should you prefer shaping over policing, and why?

Submission Format:

All observations, screenshots and answers to the questions to be submitted as a PDF named `E19XXX_Lab04.pdf`, where `<XXX>` is your e no.