# **47. QoS (Quality of Service) - Part 2**

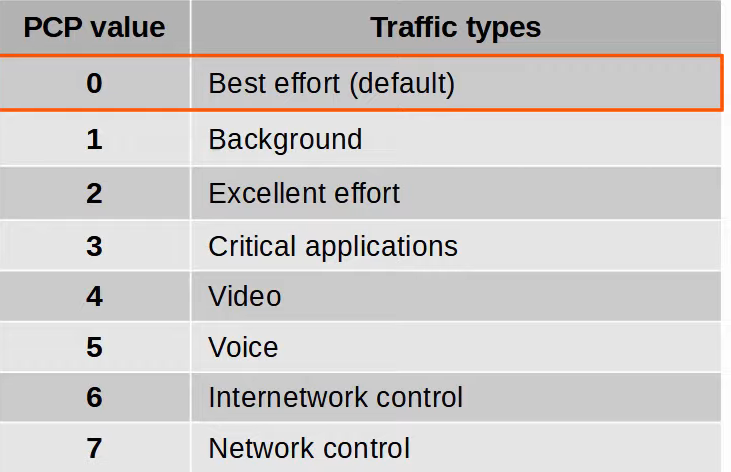
## **Classification / Marking**

* The purpose of QoS is to give certain types of **network traffic** priority over others during congestion.
* **Classification** organizes network **traffic (packets)** into **traffic classes (categories)**.
* **Classification** is fundamental to QoS:
  + To give **priority** to certain types of traffic, you must **identify** which types of traffic deserve priority.
* There are **many methods** of classifying traffic:
  + **ACL (Access Control List):** Traffic permitted by the ACL will receive specific treatment; other traffic will not.
  + **NBAR (Network-Based Application Recognition):** Performs **deep packet inspection (DPI)**, looking beyond **Layer 3 & Layer 4** up to **Layer 7** to identify specific types of traffic.
  + **Layer 2 & Layer 3 Headers:** Specific fields in headers are used for traffic classification.
* **Key Fields for Classification:**
  + **PCP (Priority Code Point) Field** in the **802.1Q tag (Ethernet header)** can be used to identify high/low priority traffic.
    - **Only applicable when a dot1q tag is present!**
  + **DSCP (Differentiated Services Code Point) Field** in the **IP header** can also be used to classify traffic.

## **PCP / CoS (Class of Service)**

* **PCP** is also known as **Class of Service (CoS)**.
* Defined by **IEEE 802.1p**.
* **Uses 3 bits = 8 possible values (2³ = 8).**

### **PCP Values:**



* **PCP Value 0 (Best Effort Delivery):**
  + No guarantee of delivery or QoS standard adherence.
  + Regular traffic (not high priority).
* **PCP Values 3 & 5:**
  + **IP Phones** mark **call signaling traffic** as **PCP 3**.
  + **Voice traffic** is marked as **PCP 5**.
* **PCP is found in the dot1q header, so it is only used over:**
  + **Trunk Links**
  + **Access Links with a Voice VLAN**

## **IP ToS Byte**

* The **Type of Service (ToS) Byte** in the IP header contains 6 bits for **DSCP** and 2 bits for **ECN (Explicit Congestion Notification).**

### **IP Precedence (Old System)**

* Similar to **PCP:**
  + **6 & 7** reserved for **network control traffic** (e.g., **OSPF messages between routers**).
  + **5 = Voice**
  + **4 = Video**
  + **3 = Voice signaling**
  + **0 = Best Effort**
* **Limitations:**
  + Only **6 usable values**, which may not be enough for some networks.

## **DSCP (Current System)**

* **RFC 2474 (1998)** defines **DSCP**, with later RFCs elaborating on its use.
* **Advantages of DSCP over IPP:**
  + More flexible **traffic classification**.
  + **Standardized** QoS markings across ISPs and enterprises.

### **Standard DSCP Markings:**

* **Default Forwarding (DF):** Best Effort Traffic (**DSCP 0**)
* **Expedited Forwarding (EF):** Low loss, latency, jitter traffic (e.g., **Voice**, **DSCP 46**)
* **Assured Forwarding (AF):** 12 standard values
* **Class Selector (CS):** 8 standard values for backward compatibility with **IP Precedence**

## **Assured Forwarding (AF)**

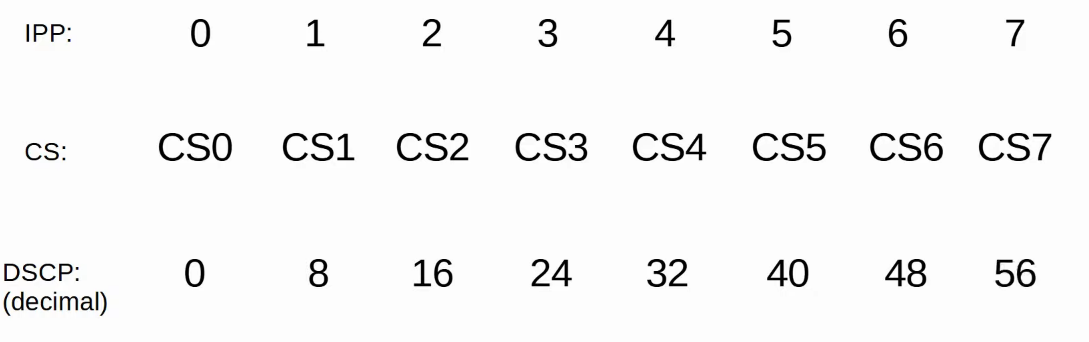
* Defines **4 traffic classes**, each with **3 drop precedence levels**.
  + **Higher drop precedence = Higher chance of being dropped during congestion.**

****

* **Examples:**
  + **AF41:** Highest priority, lowest drop
  + **AF13:** Lowest priority, highest drop

## **Class Selector (CS)**

* Defines **8 DSCP values** for **backward compatibility** with IP Precedence.
* The **3 additional DSCP bits** are set to **0**, and the original IP Precedence bits remain unchanged.



## **RFC 4954 (Standardization of QoS Markings)**

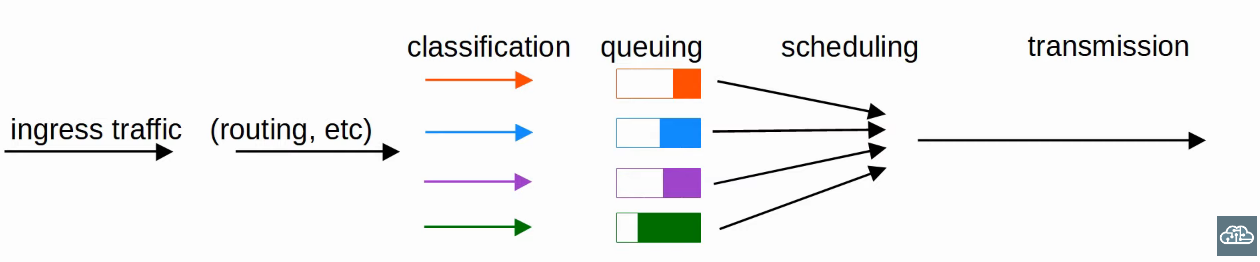
* Developed with **Cisco** to standardize QoS values.
* Key recommendations:
  + **Voice Traffic:** EF
  + **Interactive Video:** AF4x
  + **Streaming Video:** AF3x
  + **High-Priority Data:** AF2x
  + **Best Effort Traffic:** DF

## **Trust Boundaries**

* **Defines where network devices trust or modify QoS markings.**
* **Trusted markings:** Passed without modification.
* **Untrusted markings:** Changed according to policy.
* **Recommended practice:** Move the trust boundary to **IP Phones** using switch port configurations.
* **Example:**
  + **PC traffic with high priority marking is modified to prevent misuse.**

## **Queuing & Congestion Management**

* **When traffic enters a network device faster than it can be forwarded, packets wait in queues.**
* **Full queues lead to packet drops (Tail Drop).**
* **RED (Random Early Detection) & WRED (Weighted RED) mitigate tail drop.**

****

### **Queue Scheduling:**

* **Multiple queues** improve QoS.
* **Scheduling determines which queue’s traffic is forwarded next.**
* **Prioritization:** Some queues get higher priority.

### **Weighted Round-Robin (WRR) Scheduling:**

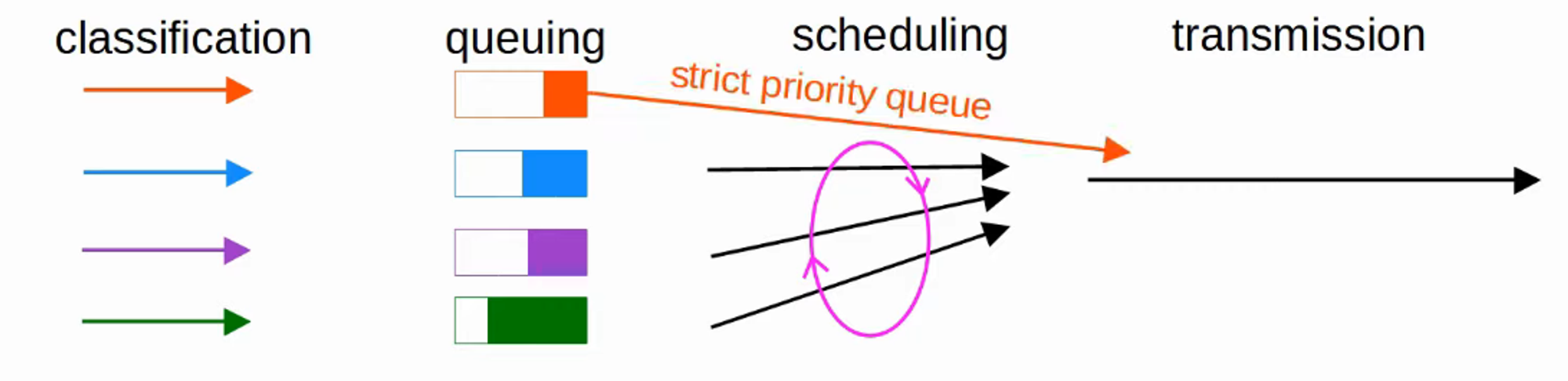
* **Round-Robin:** Packets are taken from queues in order.
* **Weighted:** High-priority queues get more bandwidth.

### **CBWFQ (Class-Based Weighted Fair Queuing):**

* **Popular scheduling method.**
* Uses **WRR scheduler** while guaranteeing each queue a specific bandwidth percentage during congestion.

## **LLQ (Low Latency Queuing)**

* Designates **one or more queues** as **strict priority queues**.
* If there is **traffic** in the queue, the **scheduler will always** take the next packet from that queue **until it is empty**.
* **Very effective** for reducing **delay and jitter** in **voice/video traffic**.
* **Downside:**
  + **Other queues may be starved** if there is always traffic in the **strict priority queue**.
  + **Policing** can control the **amount of traffic** allowed in the **strict priority queue** so it **doesn't consume all the link’s bandwidth**.



## **Traffic Shaping & Policing**

Both **traffic shaping** and **policing** are used to **control the rate of traffic**.

### **Traffic Shaping**

* **Buffers traffic** in a queue if the **traffic rate** exceeds the **configured rate**.

### **Traffic Policing**

* **Drops traffic** if the **traffic rate** exceeds the **configured rate**.
* **Alternative to dropping:**
  + Can **re-mark traffic** instead of dropping it.
  + Allows **burst traffic** over the configured rate for a **short period**.
  + Useful for **data applications**, which typically send data in **bursts** rather than a constant stream.
  + The **amount of burst traffic allowed** is configurable.

### **Classification in Both Cases**

* **Different rates** can be applied to **different types of traffic**.

### **Why Limit Traffic Rates?**

* To **prevent congestion** and **ensure fair bandwidth distribution**.

