Quality of Service

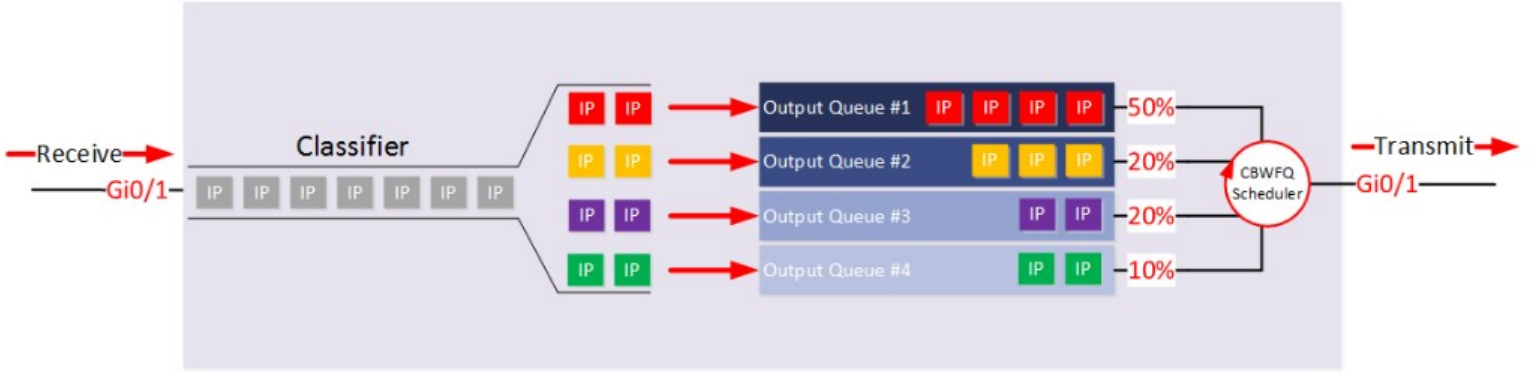
Class 3
QoS Mechanisms
(Continued)

Announcements

- Schedule changes
  - 14/02 at 14h00 —> 15/02 at 08h00
  - 05/03 at 10h15 —> 20/03 at 08h00
- Issues with Moodle

Recall from last class...

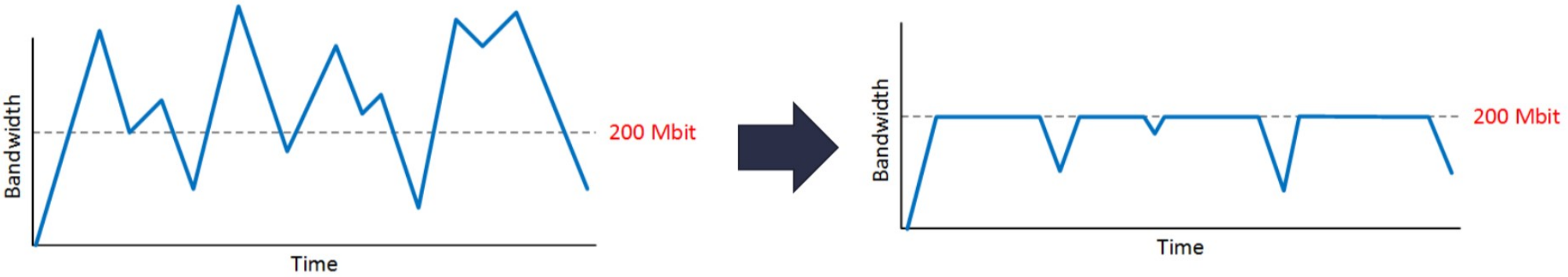
- Classification – Marking - Queuing



What does it mean “percentage of capacity”?

Recall from last class...

- Policing

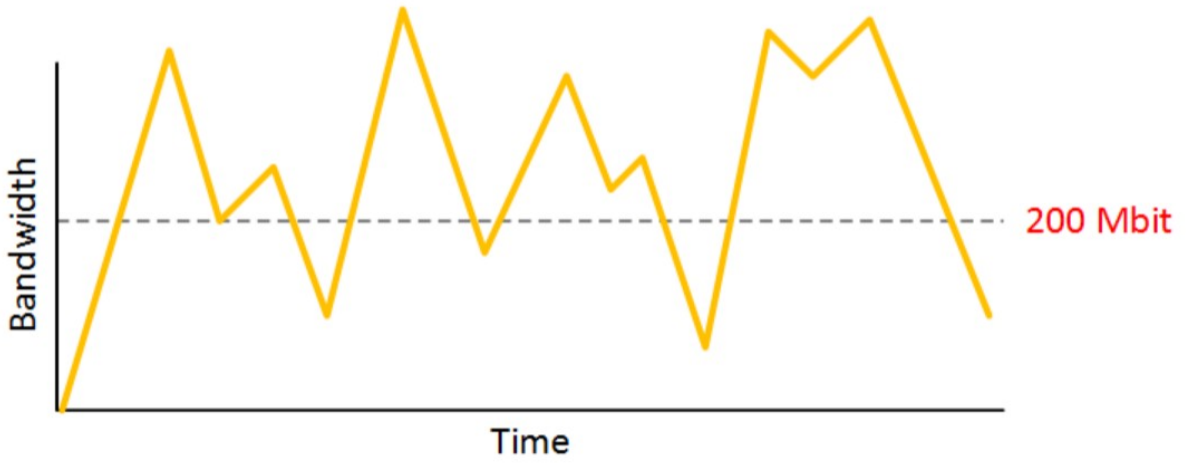


How traffic is limited in practice?

Shaping

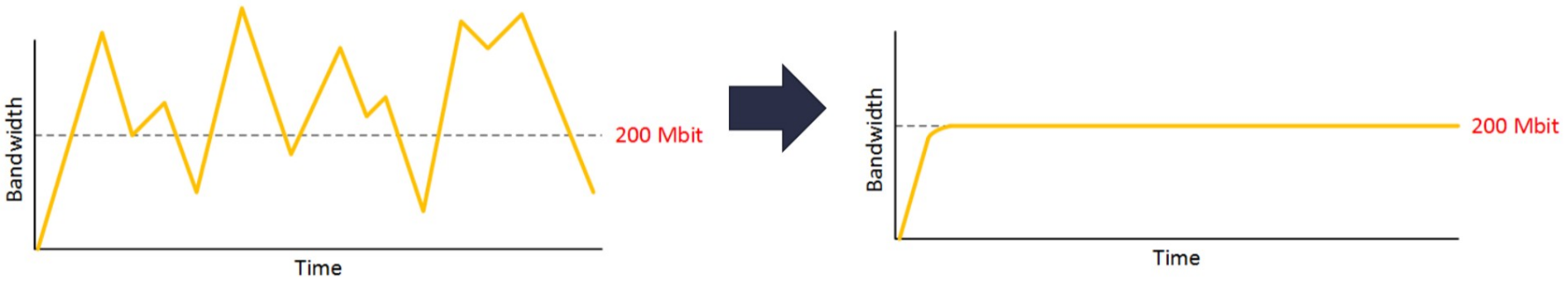
Shaping

- In practice, traffic arrives in bursts and can be severely affected bu policing drops causing unstable or worse average throughput than agreed.



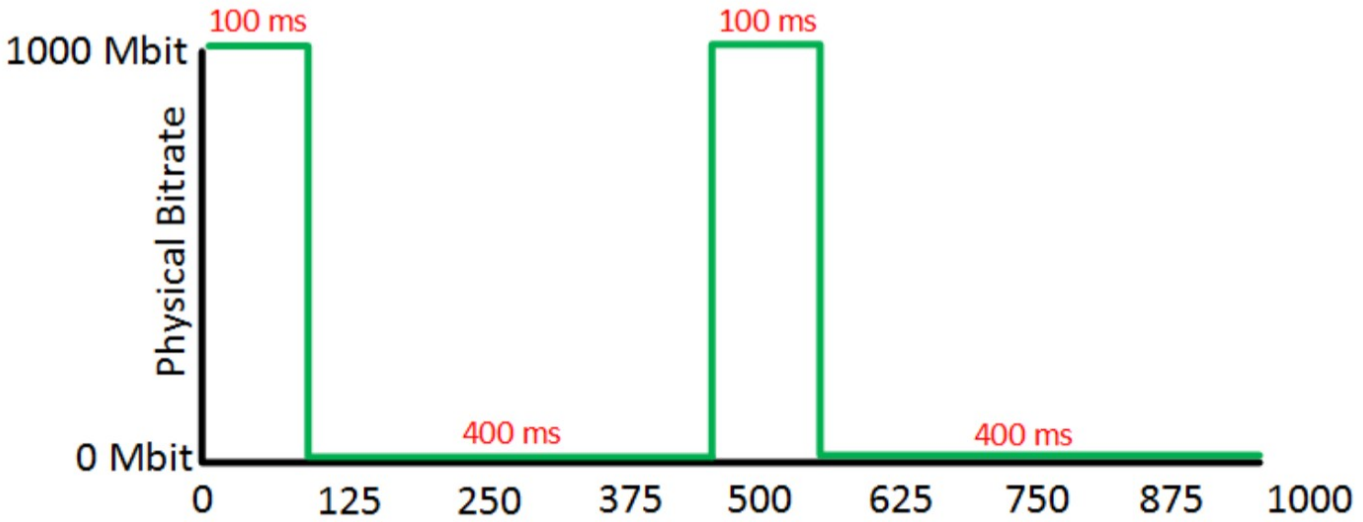
Shaping

- Definition: Shaping is a QoS mechanism used to limit throughput of a given traffic flow by delaying packets.



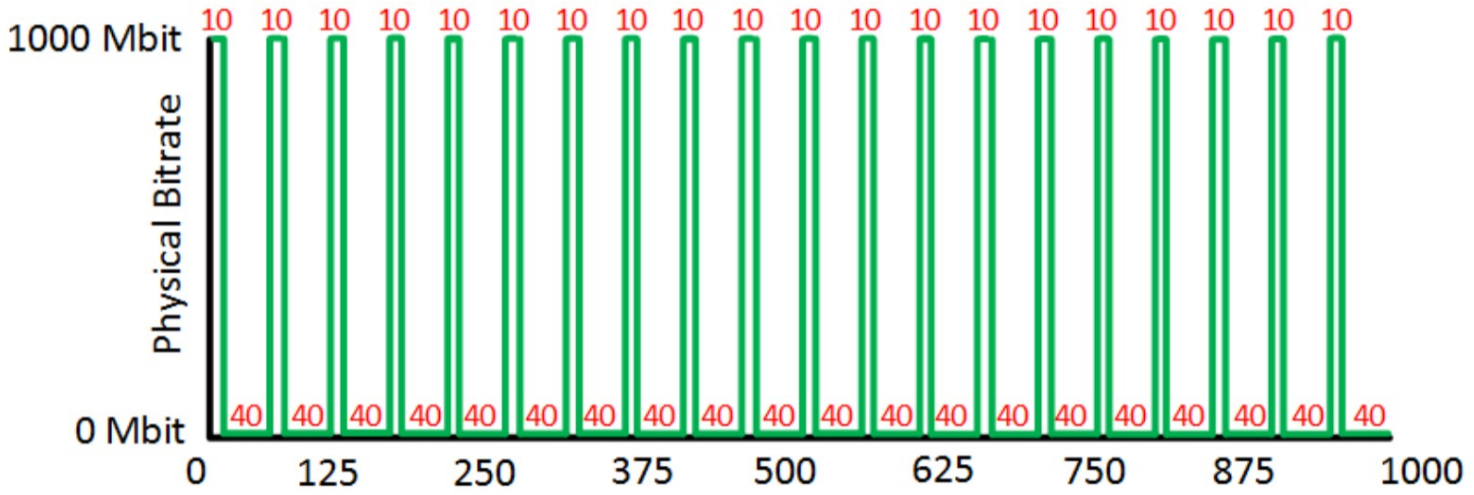
Shaping

- Example: Link capacity is 1Gbps, how to limit throughput to 200Mbps



Shaping

- If jitter-sensitive applications are considered, e.g., VoIP (admitted jitter of 150ms), how can we guarantee its normal operation?

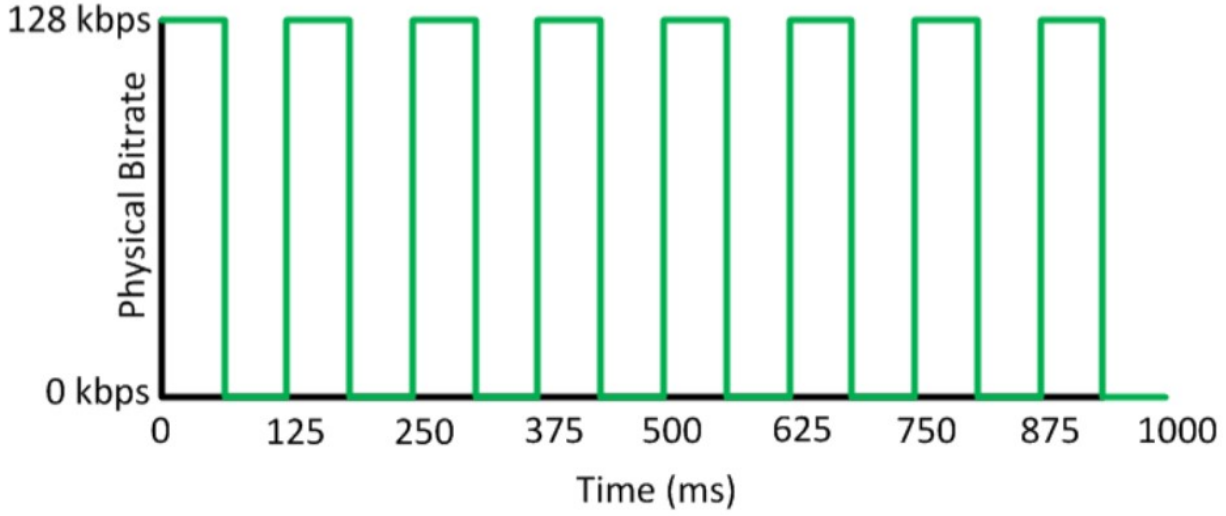


Token Bucket

- Split into (I) Transmission (Tx) phase and (ii) Wait (W) phase
- Time Interval (Tc): period consisting of one Tx phase and one W phase.
  - In CISCO routers, the default value is Tc=125ms
- Committed Burst (Bc): amount of bits to be transmitted in a Tc to guarantee the CRI
  - Bc = CRI x Tc

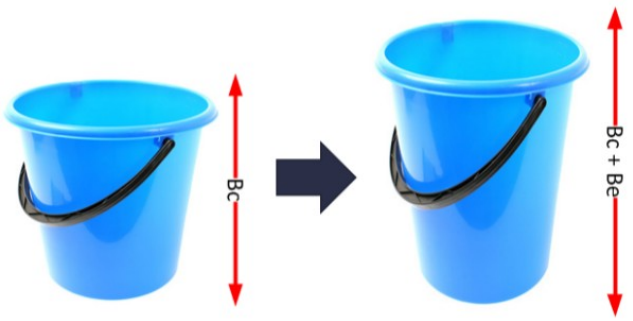
Shaping - Example

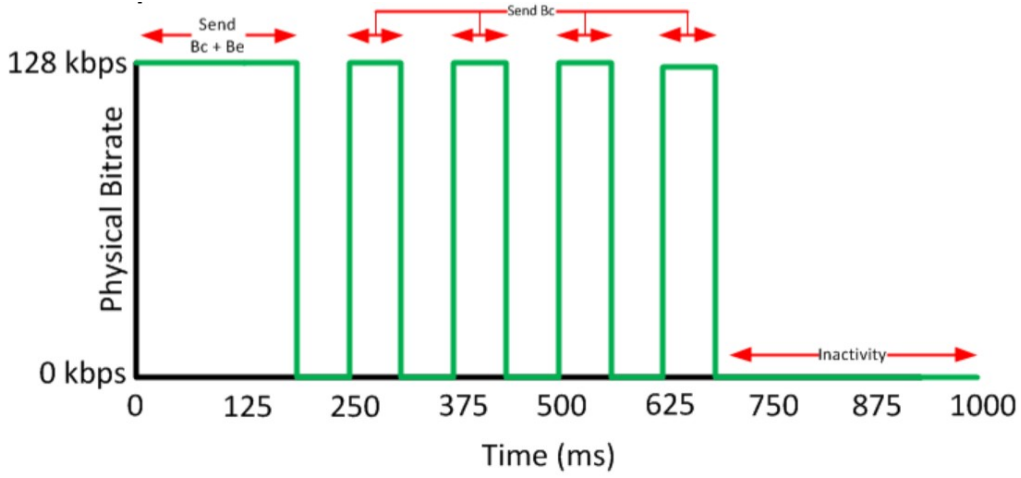
- If we want to ensure CIR=32kbps in a 128-kbps link for a traffic flow, how long should be the packets wait time in a single Tc?



Shaping – Traffic Bursts

- Traffic often arrives in bursts, i.e., non-uniform arrival over time.
- Problems:
  - In inactive periods, it wastes a Tc
  - In busy periods, it accumulate packets

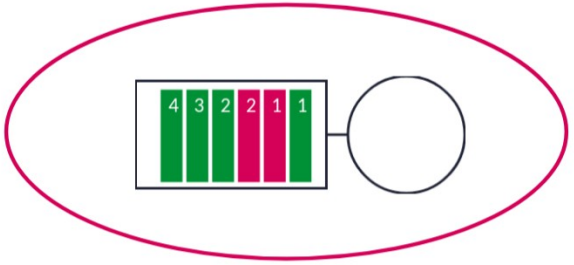


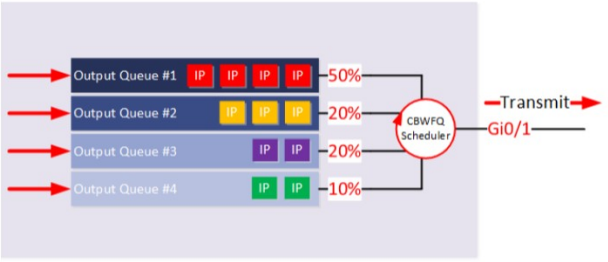


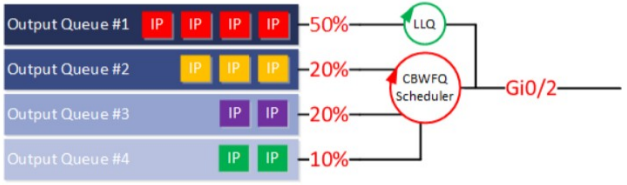
Congestion Management

Output Queues

- We have seen that Classification and Marking relay on different types of queuing systems. A few examples:

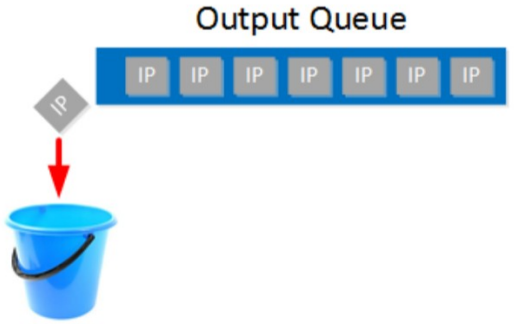






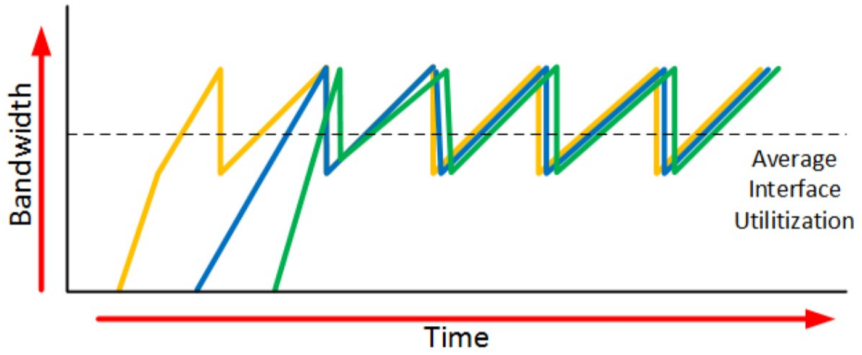
Congested Queues

- Definition: Tail Drop is the simples queue management mechanism where packets are servced on a FIFO-basis and, once buffer is full, reject incoming packets.
- Tail Drop is a remedial measure and is used for Best-Effor traffic.
- We will discuss a few preventive measures to avoid congestion.



Tail Drop: TCP Global Synchronization

- When multiple flows traverse a tail-drop router, they tend to reach congestion at the same time. Then, all flows simultaneously get dropped packets and their TCP reduce their rates. They go slow start all together, which makes congestion happen again. The cycle goes on...
- The class of QoS mechanisms designed to handle TCP-GS and avoid other congestion-related issues is called Active Queue Management (AQM)

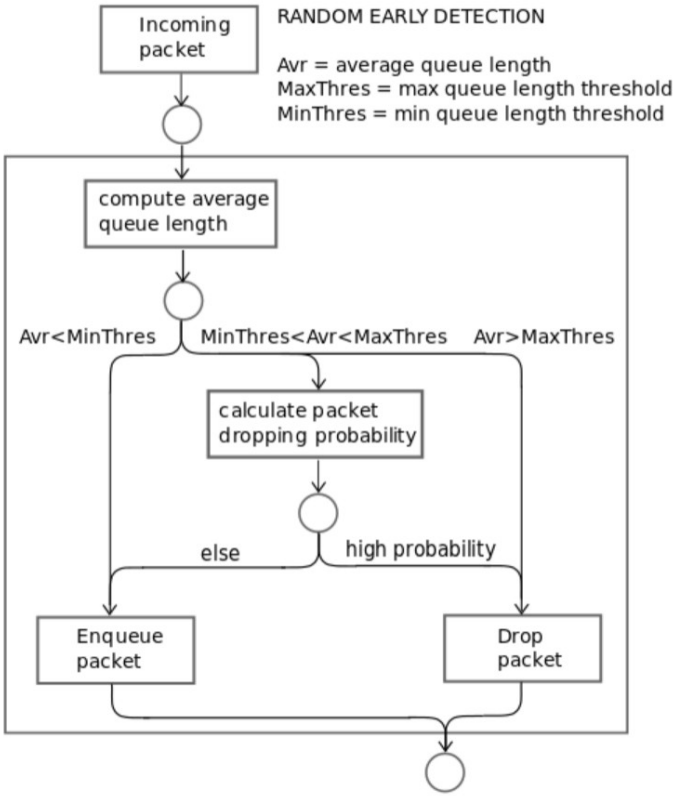


Random Early Detection (RED)

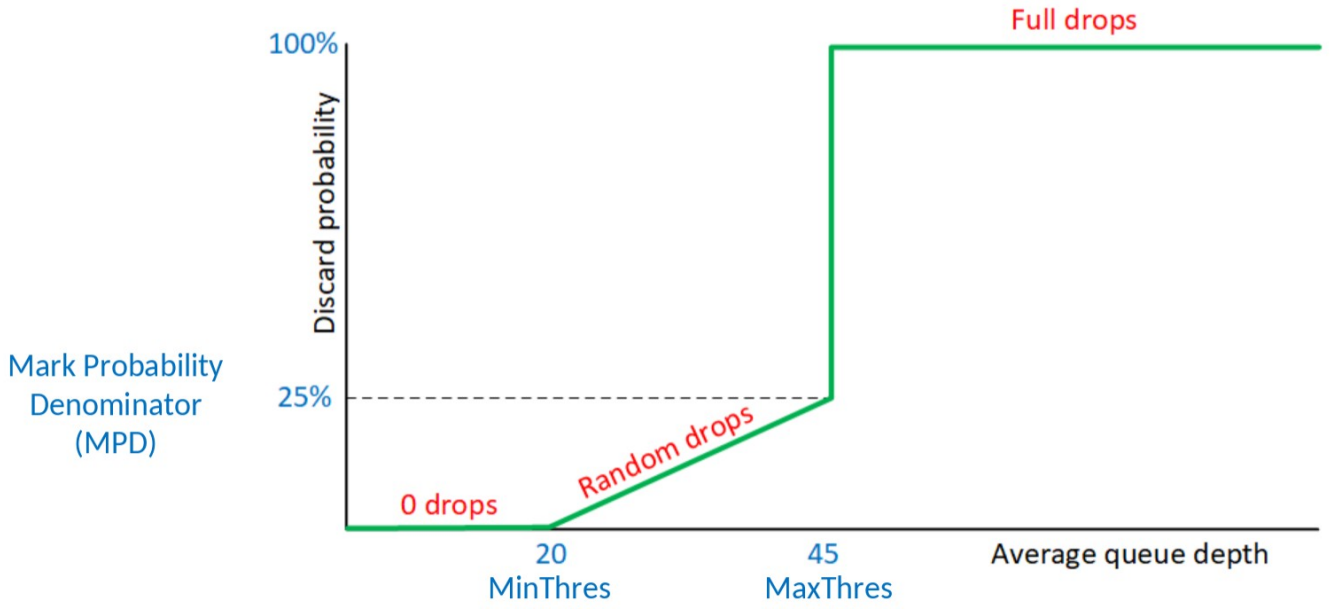
- Definition: Random Early Detection (RED) is a QoS mechanism for congestion avoidance that drops packets depending on the average queue size.

- Average queue size:

$$avg = o * (1 - 2^{-n}) + c * (2^{-n})$$



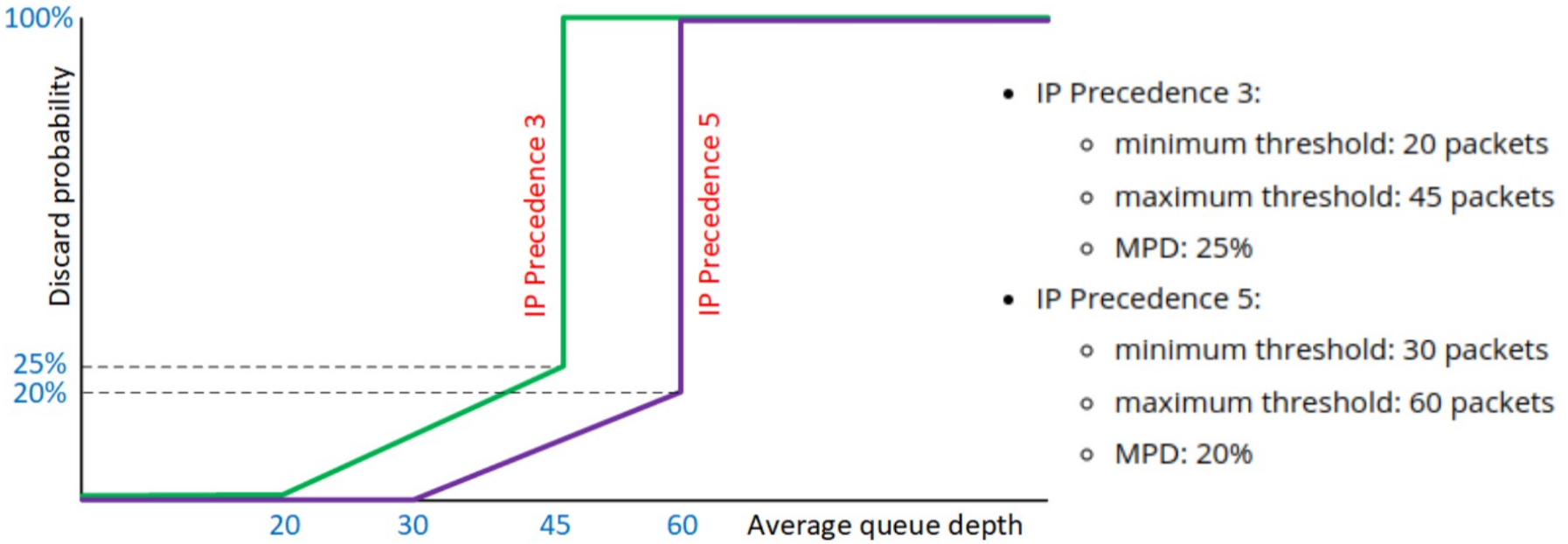
Random Early Detection (RED)



Why do we drop packets at an arbitrary threshold and how is it better than Tail Drop?

Weighted Random Early Detection (WRED)

- Definition: Weighted Random Early Detection (WRED) is an extension of RED where different classes of traffic have different thresholds.



Weighted Random Early Detection (WRED)

Average queue depth	Action	WRED action name
average queue depth < minimum threshold	No packets are dropped.	No drop
average queue depth > minimum threshold AND average queue depth < maximum threshold	Percentage of packets is dropped. This percentage increases to a maximum (MPD) until we reach the maximum threshold.	Random drop
Average queue depth > maximum threshold	All packets are dropped. This is the same as tail drop.	Full drop

Weighted Random Early Detection (WRED)

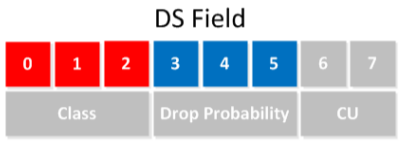
- For higher granularity, WRED is usually deployed with DSCP
- Recall that DCSP has “classes” and “drop probabilities (dp)”:

Drop	Class 1	Class 2	Class 3	Class 4
Low	AF11	AF21	AF31	AF41
Medium	AF12	AF22	AF32	AF42
High	AF13	AF23	AF33	AF43

- Every class-dp will have its own queue

Explicit Congestion Notification (ECN)

- RFC 3168
- Definition: Explicit Congestion Notification (ECN) is a QoS mechanism used to notify congestion to traffic endpoints (TCP agents).
  - If packets go through congested routers (called congestion points), then they are marked with congestion information
  - ECN uses the two least significant bits of DiffServ field for marking:



Bits	Congestion Status	Abbreviation
00	Non ECN-Capable Transport	Non-ECT
01	ECN Capable Transport	ECT(1)
10	ECN Capable Transport	ECT(0)
11	Congestion Encountered	CE

Explicit Congestion Notification (ECN)