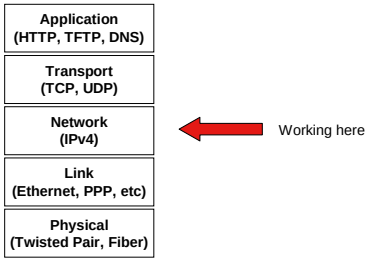
COMP312-09A Communications and Systems Software

Lecture 14 – IPv4 Quality of Service

Overview



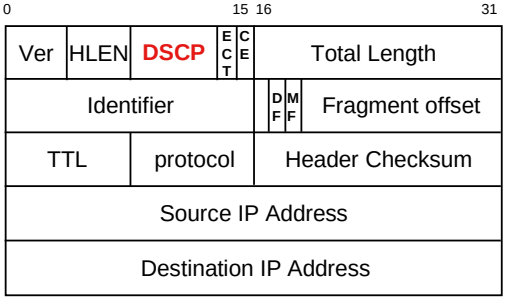
Overview

- The Internet is a best-effort network.
  - What we're talking about today occurs inside a single network
- Why Quality of Service
- Policing vs. shaping, effect on voice, video, games.
- DSCP
- Call Admission and Control (CAC)

Why QoS?

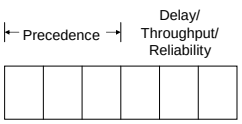
- Some applications require better than best-effort service
  - Bandwidth requirements
  - Delay requirements
  - Jitter requirements
  - Reordering requirements
- Ability to offer premium services
  - make more money

IPv4 Header



DSCP: DiffServ Code Point.
Was once known as Type of Service (TOS)

Type of Service



- 111: Network Control
- 110: Internetwork Control
- 101: CRITIC/ECP
- 100: Flash Override
- 011: Flash
- 010: Immediate
- 001: Priority
- 000: Routine

US DoD
Automatic Voice Network
(autovon)

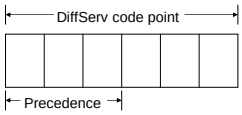
TOS Byte

- The use of the TOS byte was never formalised
- Therefore not possible to offer service guarantees across the Internet

IntServ vs. DiffServ

- IntServ: Integrated services
  - Flow-based mechanism
  - Fine-grained
  - Does not scale well as it requires significant flow state to be kept by routers in the network
- DiffServ: Differentiated services
  - Class-based mechanism, packet marked with class
  - Course-grained
  - Scales well, requires compatible classes to be defined and deployed
  - Has scope inside a single network. Networks owned and operated by two separate entities will need to come to some (legal) understanding about what DiffServ means.

DiffServ Code Point (DSCP)



- Backwards compatible with TOS precedence bits
- Use DSCP to map to a Per-hop Behaviour to enforce.

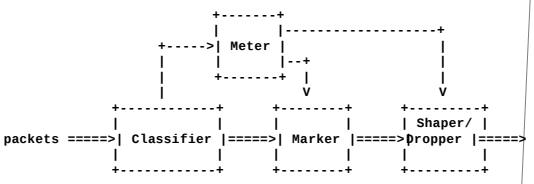
DSCP Per-Hop Behaviours

- Best-Effort: 000000
- Expedited Forwarding: 101110
- Assured Forwarding:
  - Class 1
    - AF11 (low drop): 001010
    - AF12 (med drop): 001100
    - AF13 (high drop): 001110
  - Class 2
    - AF21 (low drop): 010010
    - AF22 (med drop): 010100
    - AF23 (high drop): 010110
  - Class 3, 4.

DSCP and QoS

- Given we have DSCP, need to define methods to give packets priority

Packet Classifier / Conditioner



Logical View of a Packet Classifier and Traffic Conditioner

Source: RFC 2475

Definitions

- Classification: identify traffic by attributes and assign it a traffic class
  - Source, Destination IP addresses
    - Prioritise traffic by the parties involved
  - Protocol Type
    - Prioritise traffic by IP protocol type (TCP, ICMP, UDP, …)
  - Port numbers
    - Prioritise traffic by the applications apparently involved
  - Incoming interface
    - Prioritise traffic based on the physical interface it arrives on
  - Deep packet inspection
    - Look inside the data packets to determine actual application and prioritise that way

Definitions

- Marking: process of marking classified traffic
  - Signals priority to downstream switches and routers
  - In this case, we would mark IP DSCP field
  - Other protocols (Ethernet, MPLS, ATM, …) provide similar ways to mark traffic
  - We'll look at these in the coming lectures

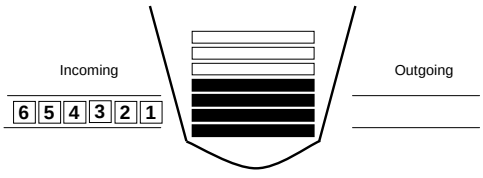
Policing vs. Shaping

- Policing
  - Enforce compliant traffic profile by dropping some packets
  - Dropper
- Shaping
  - Enforce compliant traffic profile by delaying some packets
  - Shaper

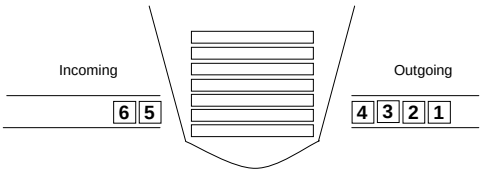
Rate-limiting

- Implemented using a token bucket algorithm
  - A token is a credit
  - When a packet is transmitted, the number of credits is reduced
  - Rate-limit is achieved by specifying the rate at which tokens are replenished
  - Allows a burst of packets through, depending on how many tokens the bucket has at arrival time

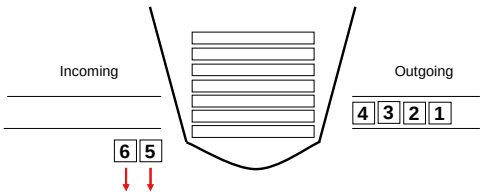
Token Bucket



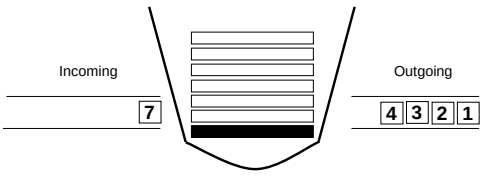
Token Bucket



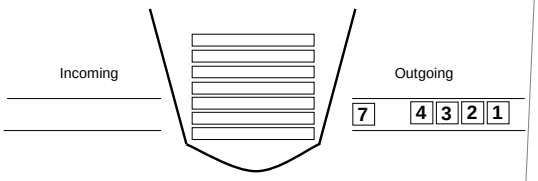
Token Bucket



Token Bucket



Token Bucket



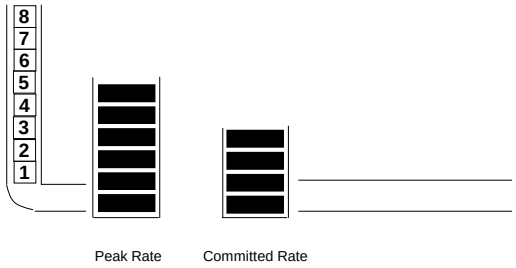
Token bucket

- Implemented as a simple counter
- Counter increments at a specified rate
  - Up to a maximum value
  - Rate could be defined in packets, or it could be defined in bytes
- Counter is decreased with each packet sent
- When counter reaches zero, packets arriving are not transmitted immediately
  - Could be discarded

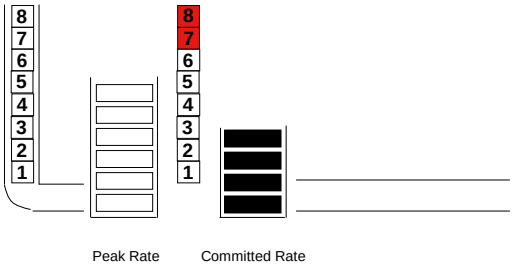
Dual Token Bucket Rate Limiter

- Used to implement bursty links
  - First bucket: peak rate
  - Second bucket: committed rate
- First bucket is bigger than second bucket
  - When it over-flows, packet is coloured red
  - Excess packets arriving at second bucket are coloured yellow
  - Otherwise, packet is coloured green
- Green packets will be forwarded, red discarded, yellow will be forwarded in best-effort fashion

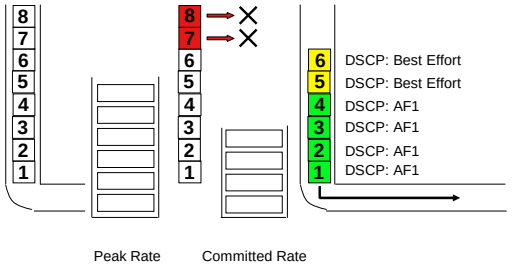
Dual Token Bucket Rate Limiter



Dual Token Bucket Rate Limiter



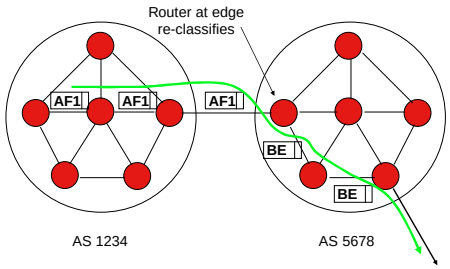
Dual Token Bucket Rate Limiter



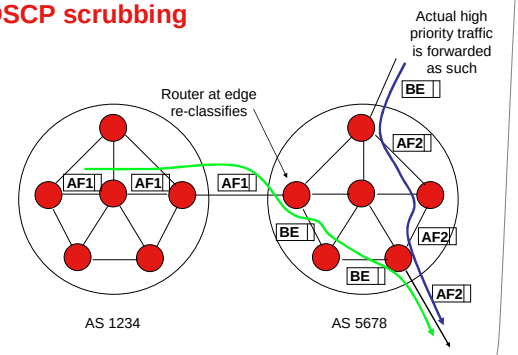
Impact on engineering

- Green defines the minimum throughput that should be reserved for a single entity
  - Yellow defines the rate at which it might 'burst' to.
- Network must be provisioned so that if all entities want to send their committed amount, they will be forwarded.
- Routers at the edge of a network should scrub the DSCP bits on arriving packets and re-classify them
  - Don't want a customer to mark all their packets as high priority and forward them as such unless they are paying money for it.

DSCP scrubbing



DSCP scrubbing



Call Admission and Control (CAC)

- It is possible even with QoS that a network might not be able to support a specified service, e.g.
  - Another voice call
  - Streaming video
- Have network
  - Signal if call may enter
  - Police other traffic so call can be supported

Further reading

- Quality of service useful for some types of traffic priority
- Implemented by classifying packets, and then recording that classification as a number in the header of the packet
  - Downstream devices forward packet based on that marking, so only one device has to make classification decision.
- Further reading: Pages 397 to 415