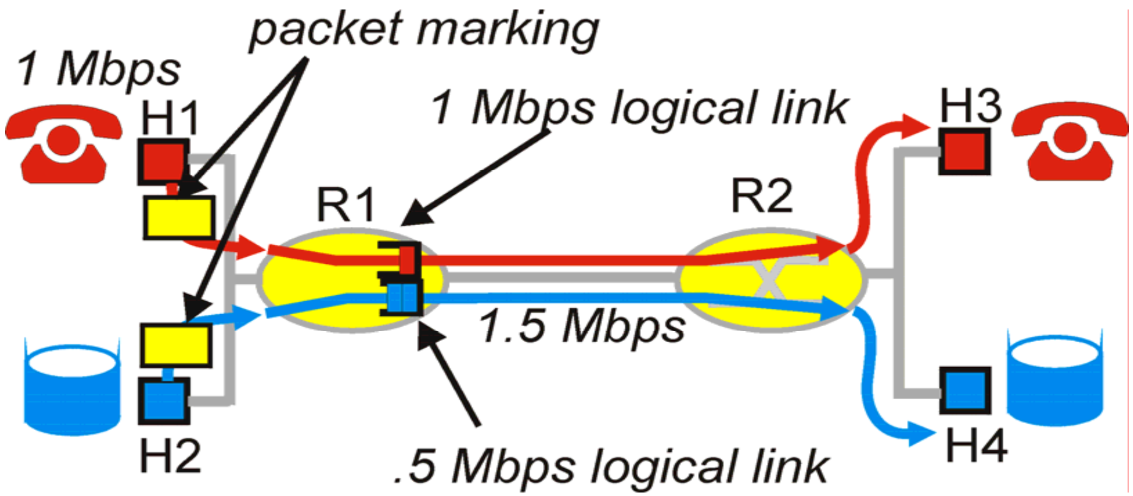
IPv6 (IP version 6) Essentials
Ch6 Aux: QoS

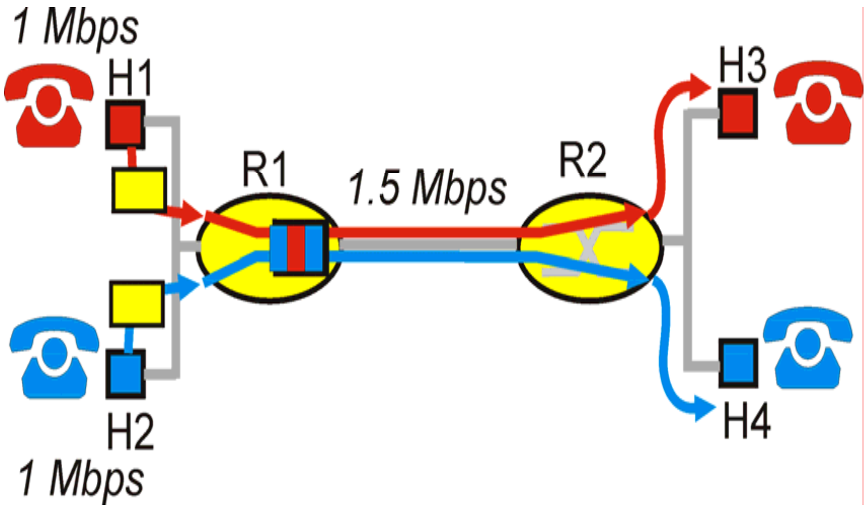
Louis Chuang
Fu Jen Catholic University
EE ENCL

Outline

- Scheduling and Policing Mechanisms.
  - Scheduling Mechanism.
  - Policing: the Leaky Bucket.
- Integrated Services.
  - Guaranteed Quality of Service (QoS).
  - Controlled-load Network Service.
- RSVP.
- Differentiated Services.
  - Traffic Classification and Conditioning.
  - Per-hop Behaviors.

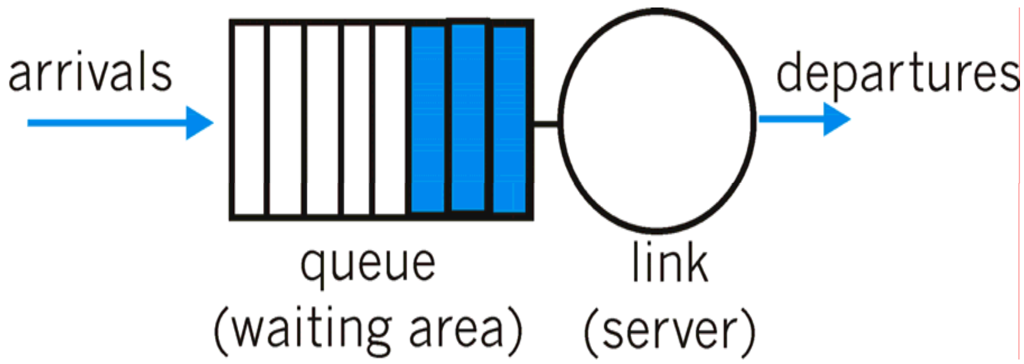
Scheduling and Policing Mechanisms (1)





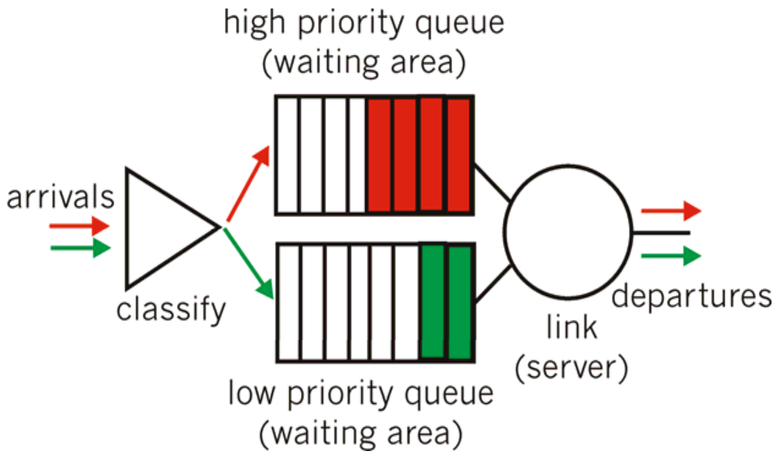
Scheduling and Policing Mechanisms (2)

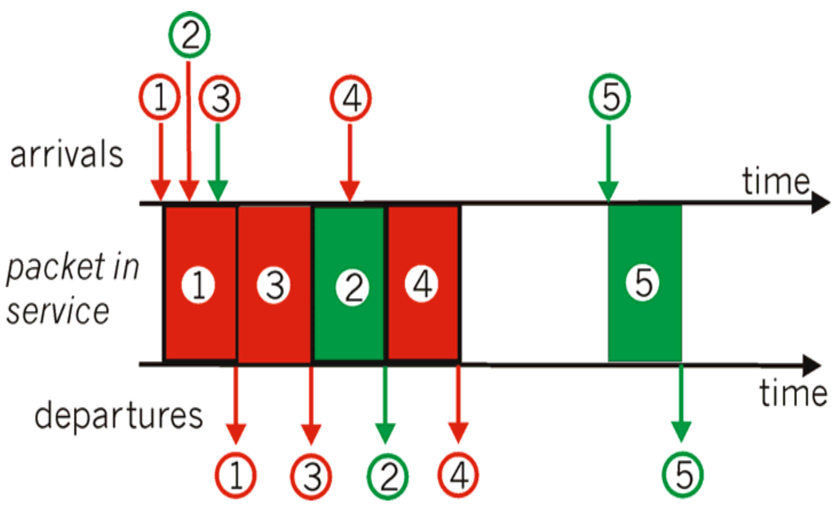
- Scheduling mechanisms: choose next packet to send on link
- FIFO (first in first out) scheduling: send in order of arrival to queue
  - Real world example?
    - For getting on a bus, or buying something, etc..
  - Discard policy: if packet arrives to full queue: who to discard?
    - Tail drop: drop arriving packet.
    - Priority: drop/remove on priority basis.
    - Random: drop/remove randomly.



Scheduling and Policing Mechanisms (3)

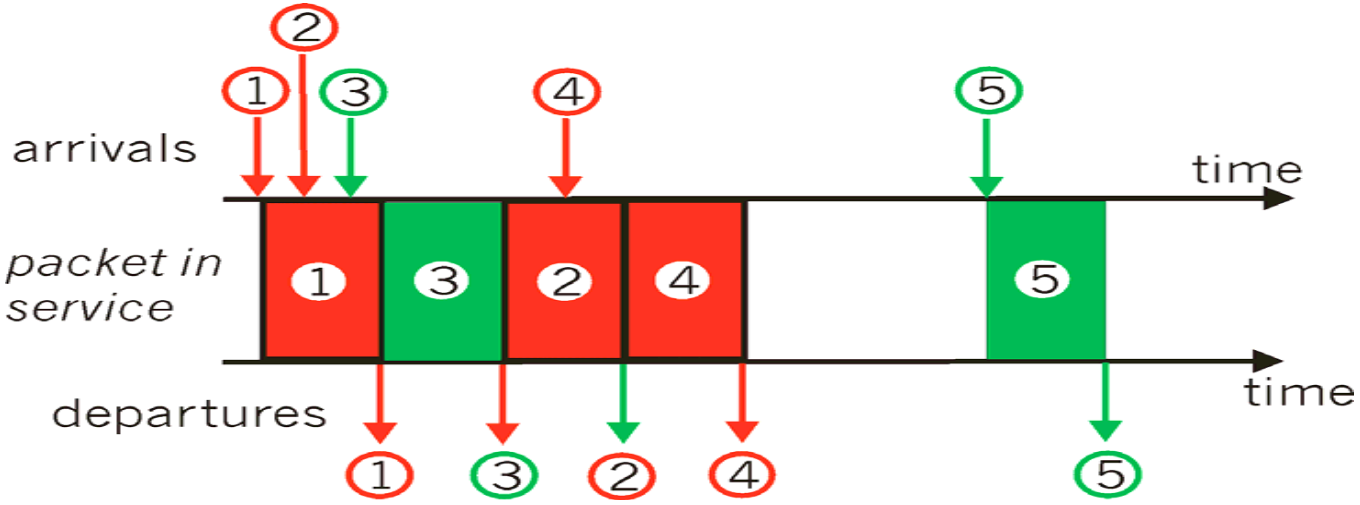
- Priority scheduling: transmit highest priority queued packet.
  - Having several priorities queue in output port.
    - Multiple classes, with different priorities.
      - To classify different classes may depend on marking (TOS in IPv4 header) or other header info, e.g. IP source/dest, port numbers, and other rules.
      - Using non-preemptive priority queuing discipline.
      - Real world example?





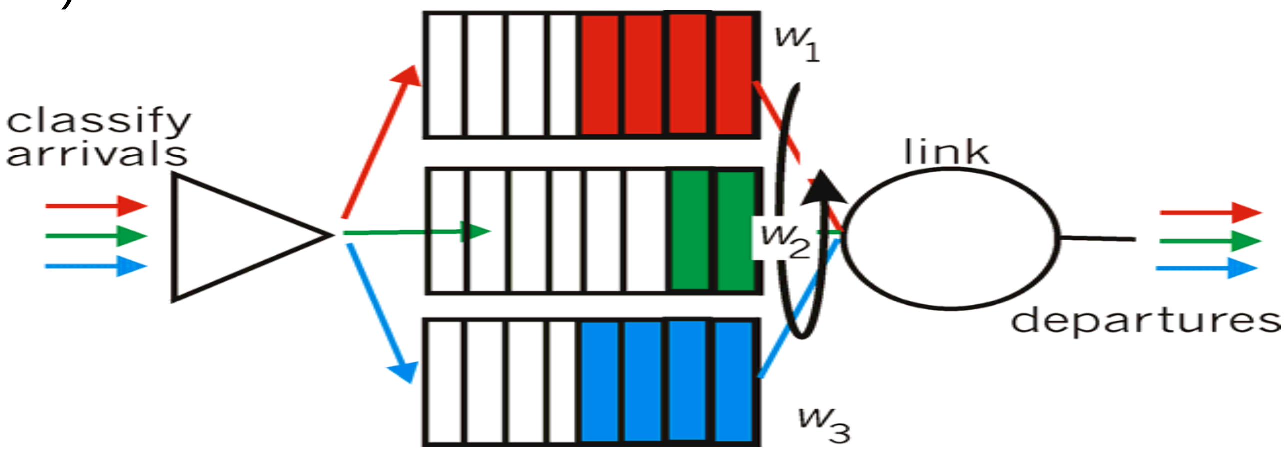
Scheduling and Policing Mechanisms (4)

- Round robin scheduling:
  - To classify multiple classes/queues like the priority scheduling.
  - Using work-conserving around robin discipline.
  - Cyclically scan class queues, serving one from each class (if available)
  - real world example?



Scheduling and Policing Mechanisms (5)

- Weighted fair queuing (WFQ):
  - To classify multiple classes/queues like the round robin scheduling.
    - Serving Class1 → Class2 → Class3 → …… (repeat).
  - Also using work-conserving around robin discipline.
  - Each class gets weighted amount of service in each cycle: $r_i = \left(w_i \Big/ \sum_j w_j \right) \times R$
  - Real-world example?
  - WFQ plays important role in QoS scheduling (e.g., Cisco QoS router).

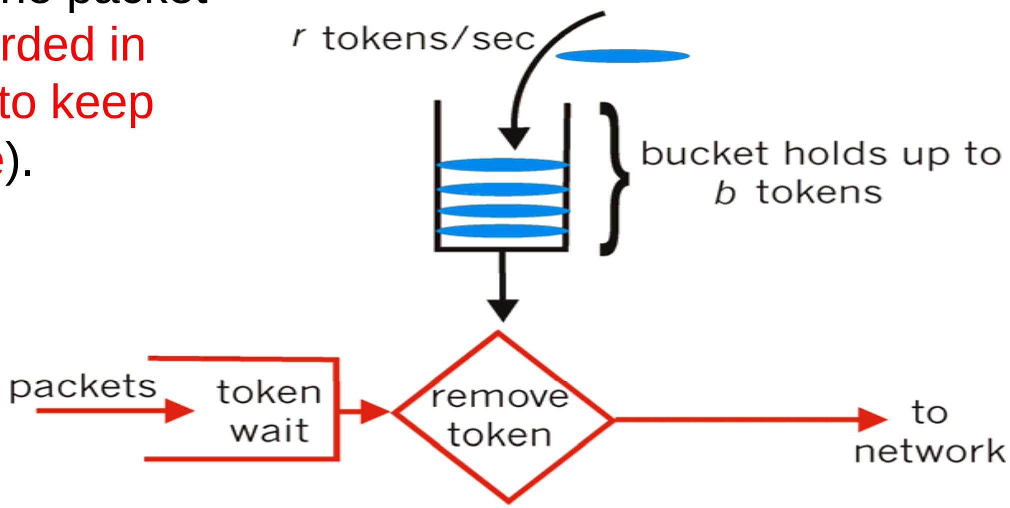


Scheduling and Policing Mechanisms (6)

- Policing mechanism:
  - Goal: limit traffic, entering network, to not exceed declared parameters.
- Three common-used criteria for policy:
  - (Long term) Average rate: how many packets can be sent per unit time (in the long run).
    - A crucial question: what is the length of time interval.
      - Although 100 packets per sec & 6000 packets per min have same average.
      - But the limit of 100 packets per sec is more!
  - (Short term) Peak rate:
    - Ex) the average rate is 6000 packets per min, but the peak rate is 1500 packets per second.
  - (Very short term) Burst size: the max. number of packets sent consecutively (with no intervening idle).

Scheduling and Policing Mechanisms (7)

- Token Bucket: limit the input to specified Burst Size and Average Rate.
- The capacity of a bucket is *b* tokens.
- Token generation rate: *r* token/sec unless bucket is full.
- How to use the leaky bucket policy:
  - Before sending a packet into the network, it first gets a token from the bucket.
  - If the bucket is empty, the packet should be kept or discarded in the queue (it is usually to keep the packet in the queue).

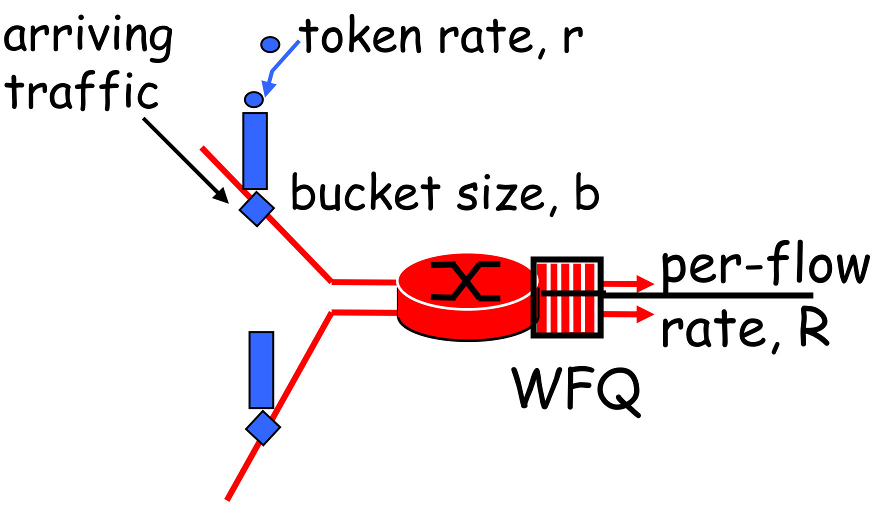


Scheduling and Policing Mechanisms (8)

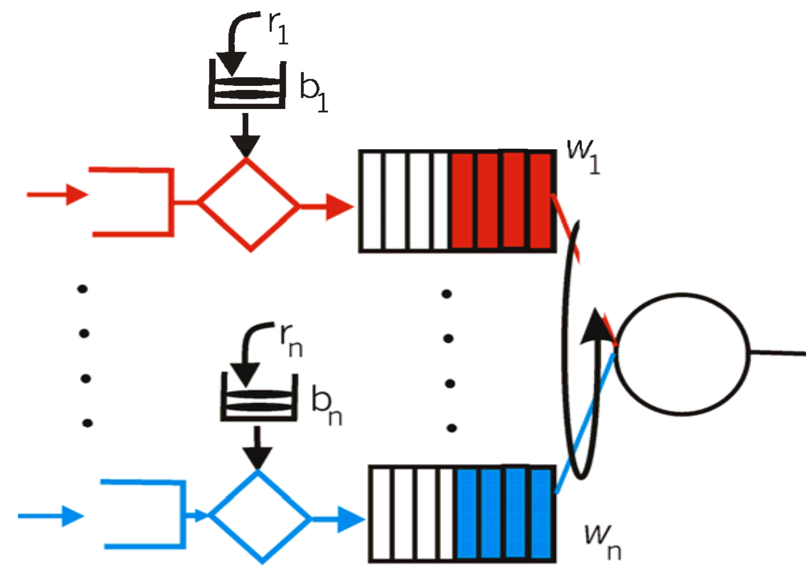
- How does the policy work for traffic control:
  - A bucket has at most *b* token → the burst size is controlled to *b* packets.
  - The token generation rate is *r* per second.
    - Hence, the average rate over a interval length *t* is: less than or equal to ($r\, t + b$) packets.
  - To cooperate several leaky buckets to control the totally max. traffic rate.

Scheduling and Policing Mechanisms (9)

- Leaky bucket + WFQ provide guaranteed upper bound on delay (max. delay) in a queue (i.e., QoS guarantee) .
  - Ex) The output of a router can forward *n* input streams (connections).
    - WFQ: for stream *i*, it can guarantee the data rate: $r_i = \left(w_i \Big/ \sum_j w_j \right) \times R$
      - *R* is the totally available data rate (packets/second).



$$D_{max} = b/R$$



Scheduling and Policing Mechanisms (10)

- What is the max delay of a packet in a WFQ to wait for service.
  - Based on the leaky bucket.
  - For stream 1: its bucket is initially full (*b* tokens).
    - Arriving *b* packets, then they all enter the (WFQ) queue.
    - The service rate (data rate) is: $r_i = \left(w_i \Big/ \sum_j w_j \right) \times R$
    - The max. delay (d_{max}) is the last packet:

$$d_{\max} = \frac{b_1}{\left(w_i \Big/ \sum_j w_j \right) \times R}$$

    - Little's Law: queue length = queuing delay x service rate.

Outline

- Scheduling and Policing Mechanisms.
  - Scheduling Mechanism.
  - Policing: the Leaky Bucket.
- Integrated Services.
  - Guaranteed Quality of Service (QoS).
  - Controlled-load Network Service.
- RSVP.
- Differentiated Services.
  - Traffic Classification and Conditioning.
  - Per-hop Behaviors.

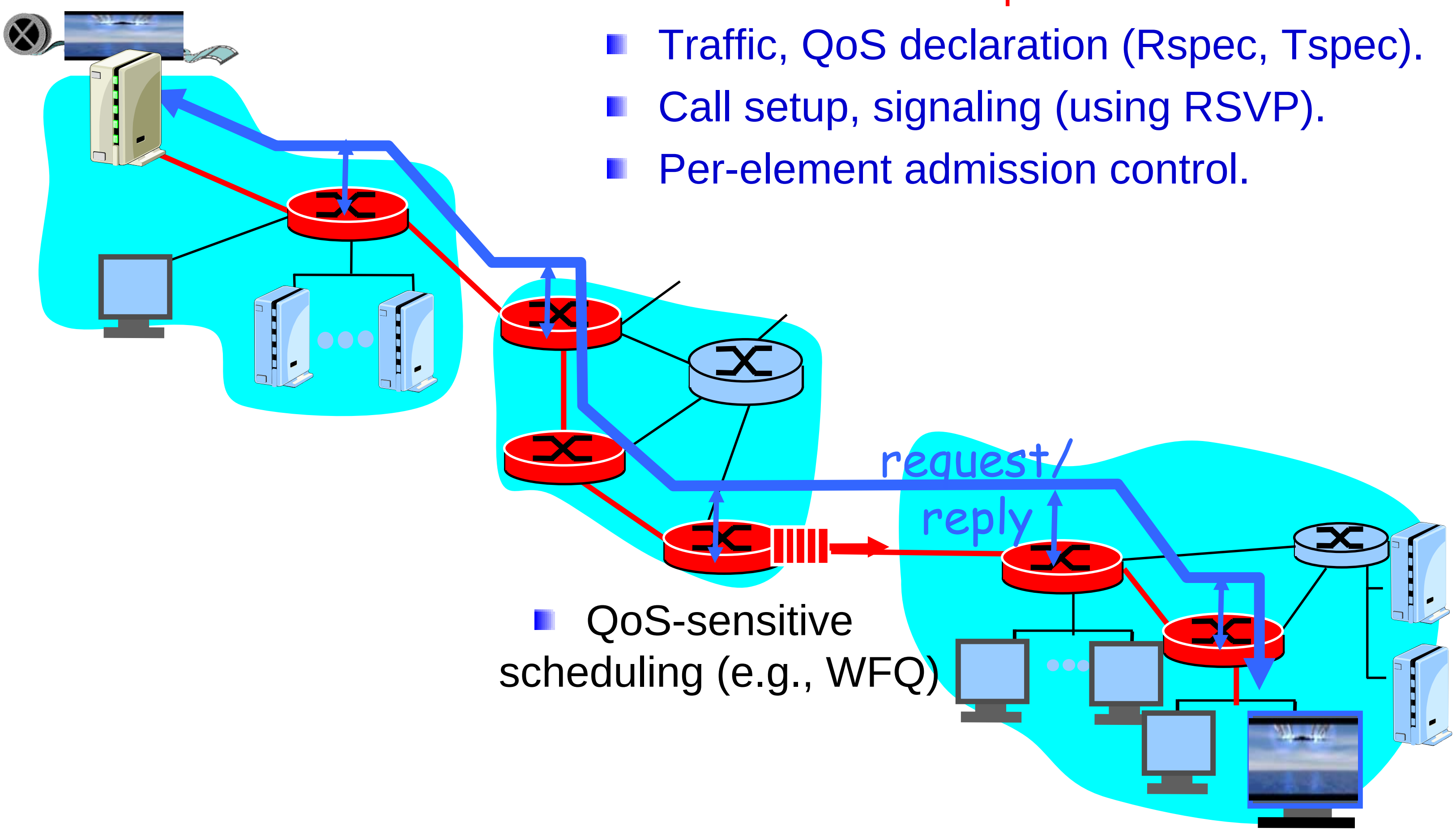
Integrated Services (1)

- Integrated services (Intserv) was developed by IETF to provide QoS in Internet.
- The architecture is to provide QoS guarantee in IP networks for individual application sessions.
- It has 2 mainly features:
  - Resource reservation: router has to know how many resources have been allocated.
    - Routers maintain state info (a la VC) of allocated resources.
  - Call setup: to admit / deny the new call setup requests.
    - Depending on its remaining resources.

Question: can newly arriving flow be admitted with performance guarantees while not violated QoS guarantees made to already admitted flows?

Integrated Services (2)

- Resource reservation procedures:
  - Traffic, QoS declaration (Rspec, Tspec).
  - Call setup, signaling (using RSVP).
  - Per-element admission control.



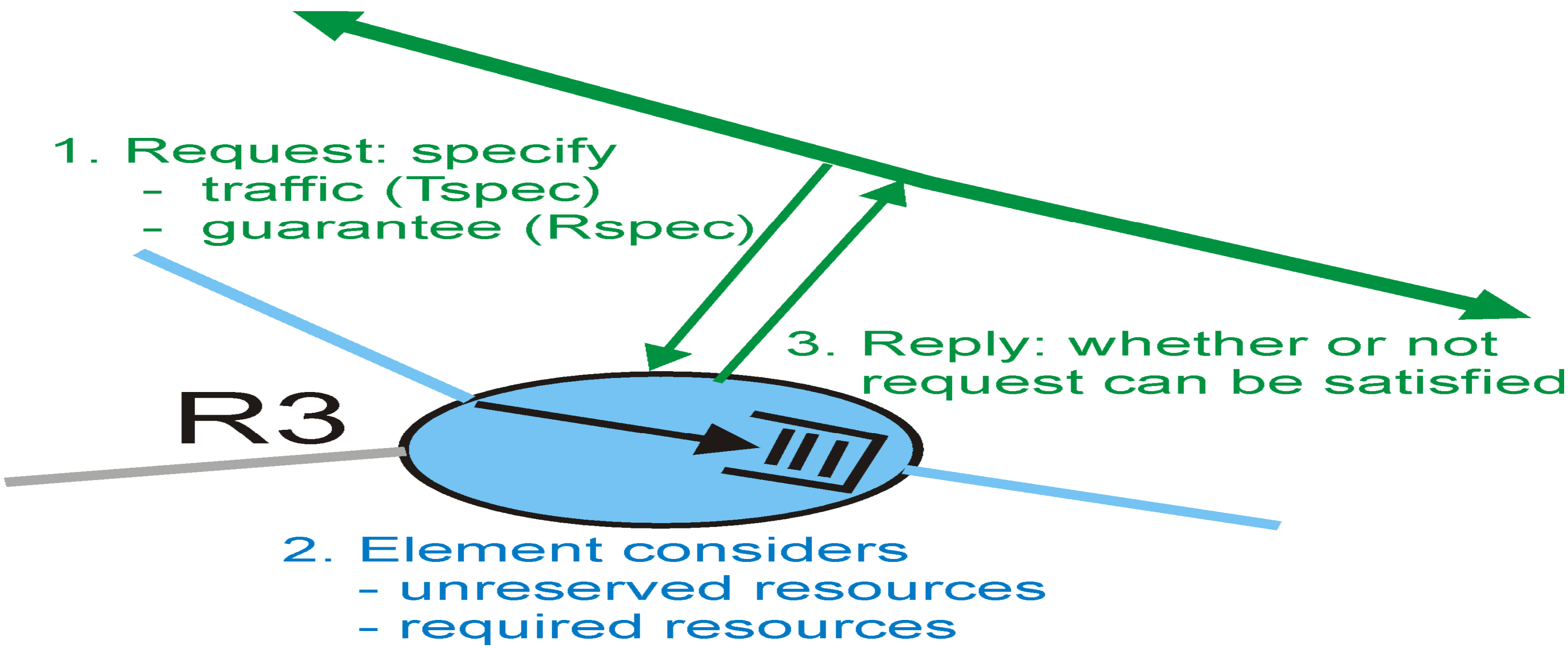
- QoS-sensitive scheduling (e.g., WFQ)

Integrated Services (3)

- In call admission, arriving session must:
  - Declare its QoS requirement.
    - R-spec: defines the QoS being requested (R is reservation, RFC 2210).
  - Declare its traffic characteristics, which will send into network.
    - T-spec: defines traffic characteristics (T is traffic, RFC 2215).
  - Establish connection signaling (RFC 2210).
    - Sending R-spec & T-spec to routers (where reservation is required).
    - Using RSVP.
  - Per-element call admission.
    - As router receives the session request, it judges to accept / reject based on the R-spec & T-spec.

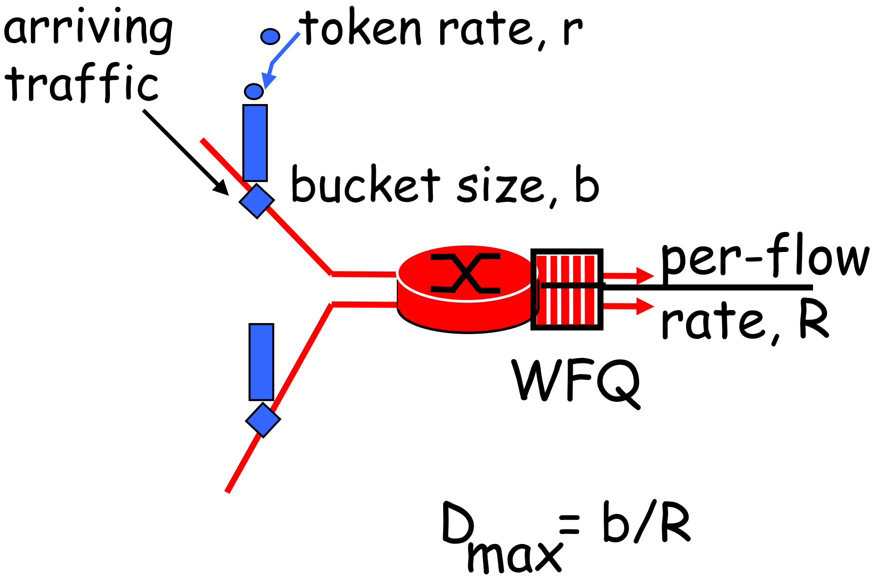
Integrated Services (4)

- Per-element call admission.



Integrated Services (5)

- Two service models for Intserv QoS:
- Guaranteed service (RFC 2212):
  - Clearly limits the queuing delay in a router.
  - A source: leaky bucket policy with parameters (*r*, *b*).
    - For a session, the arrival rate is *r*, & the service rate is *R*.
    - During a time interval *t*, the traffic bound is (*rt* + *b*).
    - If *r* < *R*, the queuing delay is bounded in (*b*/*R*).
- Simple (mathematically provable) bound on delay [Parekh 1992, Cruz 1988]



Integrated Services (6)

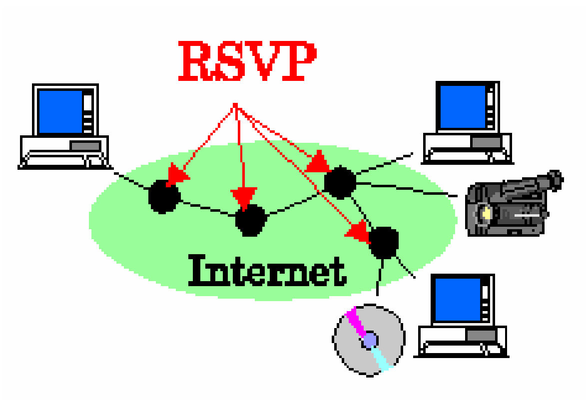
- Controlled-load network service (RFC 2211):
  - To control traffic load.
  - For today's multimedia applications, they work well during network traffic is low.
    - When the network traffic becomes heavily, the application traffic loads are controlled (but still keep above its low bound).

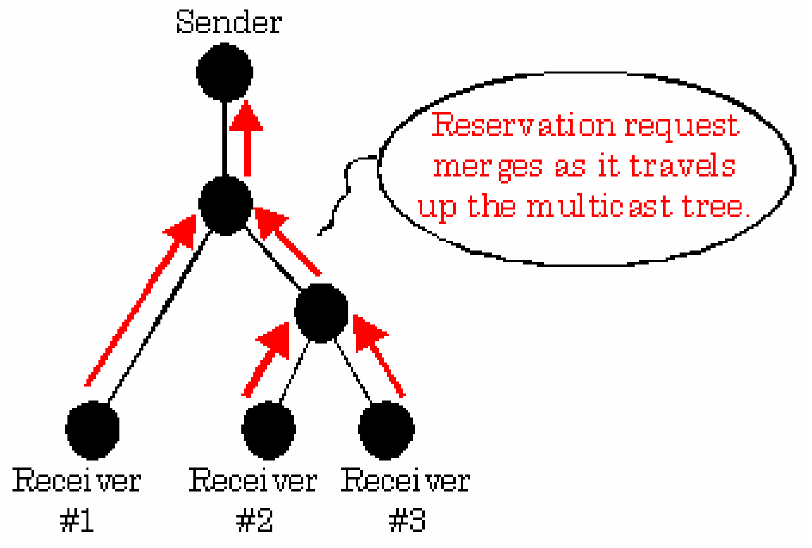
Outline

- Scheduling and Policing Mechanisms.
  - Scheduling Mechanism.
  - Policing: the Leaky Bucket.
- Integrated Services.
  - Guaranteed Quality of Service (QoS).
  - Controlled-load Network Service.
- RSVP.
- Differentiated Services.
  - Traffic Classification and Conditioning.
  - Per-hop Behaviors.

RSVP (1)

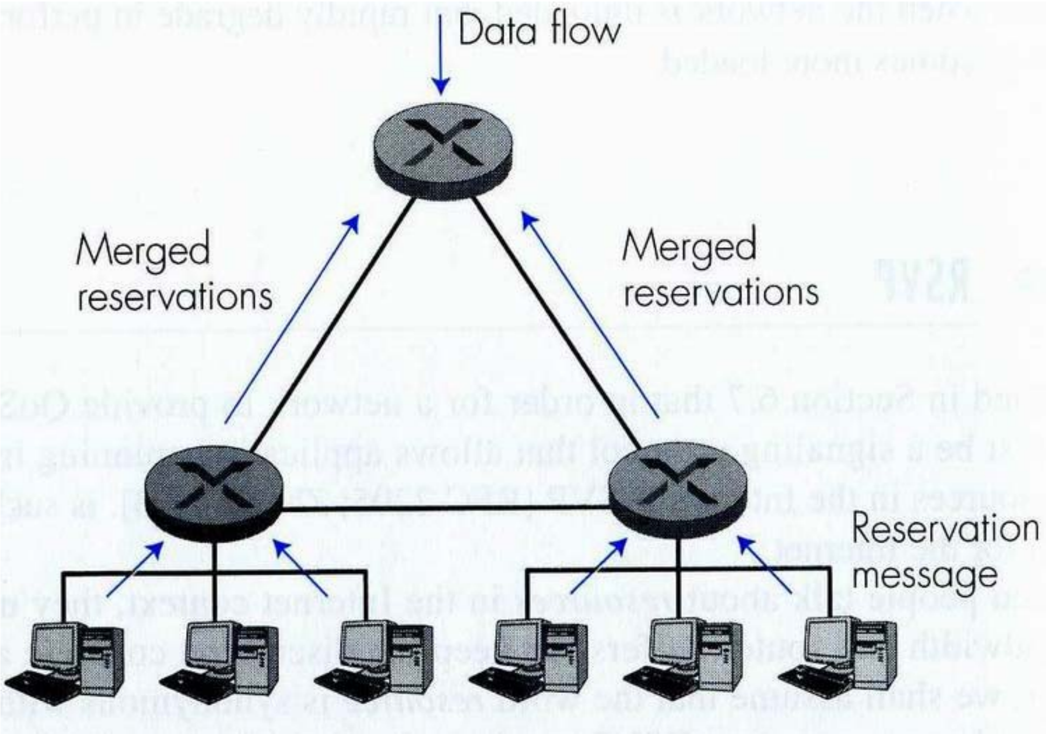
- RSVP (Resource ReSerVation Protocol) in RFC 2205.
- To provide QoS, it must have a signaling protocol to reserve resource in routers → RSVP.
- Resource reservation means to reserve link bandwidth (data rate, throughput, buffers) → call admission, to reserve resource.
- The essence of RSVP:
  - Router will forward RSVP request to another router.





RSVP (2)

- RSVP: multicast & receiver-oriented.



RSVP (3)

  - To implement RSVP: RSVP software must work at sender, routers, and receivers.
- Two RSVP features:
  - Reservations for bandwidth in multicast tree.
    - Unicast is a case of multicast.
  - Received-oriented.
    - Although data is sent from sender to receiver.
    - Resource request starts from the receiver back to the sender.
    - Router will combine the resource requests from different destinations belonging to the same session (multicast tree).
    - Routers identify the session based on the source / destination IP address & ports (usually using Flow field (20-bit) in IPv6).
- What RSVP is not:
  - For reserving resource, it needs scheduling mechanisms (priority, etc.).

RSVP (4)

- RSVP is not a routing protocol, it does not provide the function to find a route from sender to receiver.
  - The route needs to first be found out.
- Heterogeneous Receivers:
  - Ex) In a network, the data rate of some receivers is 28.8Kbps, another is 128Kbps, and the other is 10Mbps.
    - Sender will encode the video in different qualities:
      - Low quality: 28.8Kbps.
      - Middle quality: 128Kbps.
      - High quality: 10Mbps.
    - Using layered encoding.
      - Ex) MPEG encoding:
        - I frame, P frame, B frame.
        - Transmission: IBBPBBPBBPBBIBBPBB……

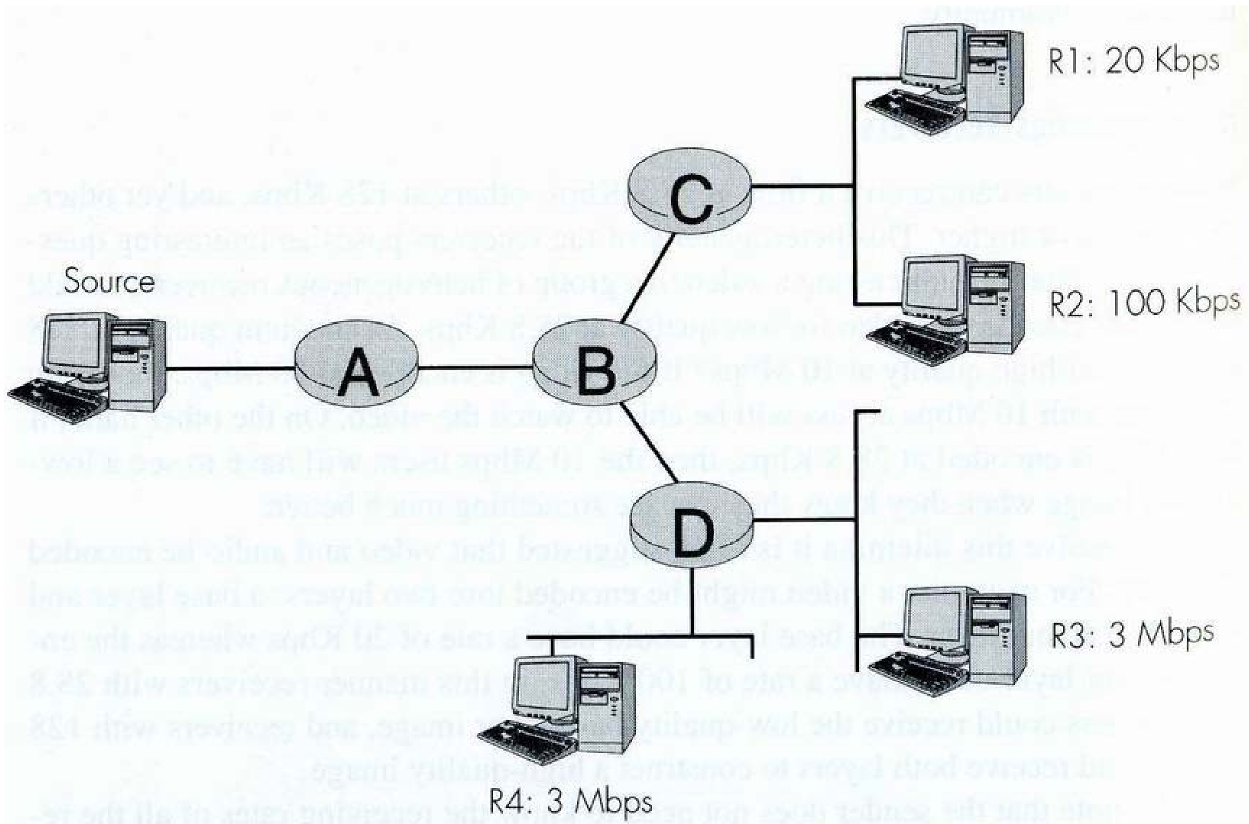
RSVP (5)

- Video can be classified into base layer & enhancement layer.
  - Base layer is 20Kbps for 28.8Kbps receivers.
  - Enhancement layer is 100Kbps for 128Kbps & 10Mbps receivers.
- The sender does not need to know which receiver uses what kind of data rates.
  - It just needs to know the max. data rate, and it will send video streaming with the max. data rate.

- To maintain the reserved bandwidth, using two methods:
  - Soft state method:
    - Using a timer, if the timer is time out, the reserved bandwidth will be release.
    - Require a update message to reset the timer.
  - Hard state method:
    - State release or modification require have the specified messages.

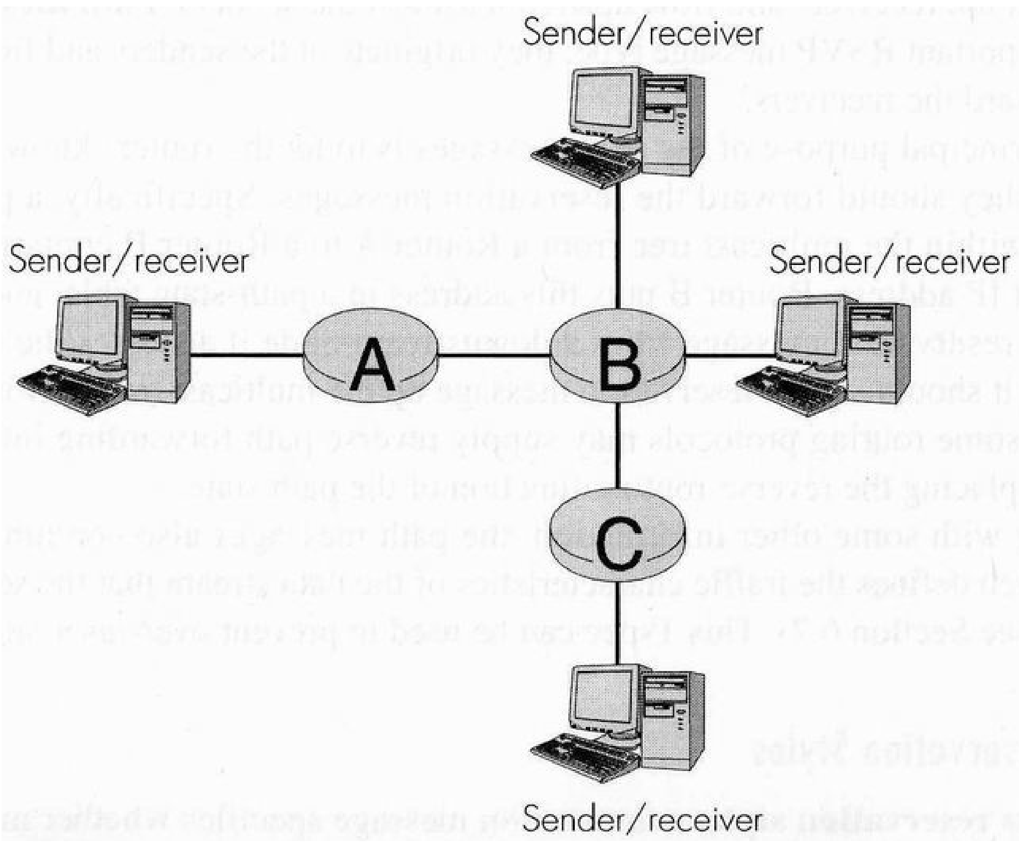
RSVP (6)

- Ex) A session with a multicast tree. Video is from a sender to different receivers (R_1, R_2, R_3, and R_4) with different receiving rates.



RSVP (7)

- Ex) A interactive session (with a video conference). Each hast receives a video streaming from the other host of 3Mbps data rate.



Outline

- Scheduling and Policing Mechanisms.
  - Scheduling Mechanism.
  - Policing: the Leaky Bucket.
- Integrated Services.
  - Guaranteed Quality of Service (QoS).
  - Controlled-load Network Service.
- RSVP.
- Differentiated Services.
  - Traffic Classification and Conditioning.
  - Per-hop Behaviors.

Differentiated Services (1)

- Concerns with Intserv: the per-flow resource reservation has some difficulties.
  - Scalability:
    - Signaling, maintaining per-flow router states are difficult (with large number of flows in core network / backbone routers).
  - Flexible service models:
    - Intserv only provides some pre-defined services.
      - It cannot handle newly generated applications / services.
    - The service classification does not associate with traffic types / classes / properties.
- Diffserv (DS) approach developed by IETF (RFC 2475):
  - To implement simple functions in network core, relatively complex functions at edge routers (or hosts).
  - To provide scalability & flexible service models.

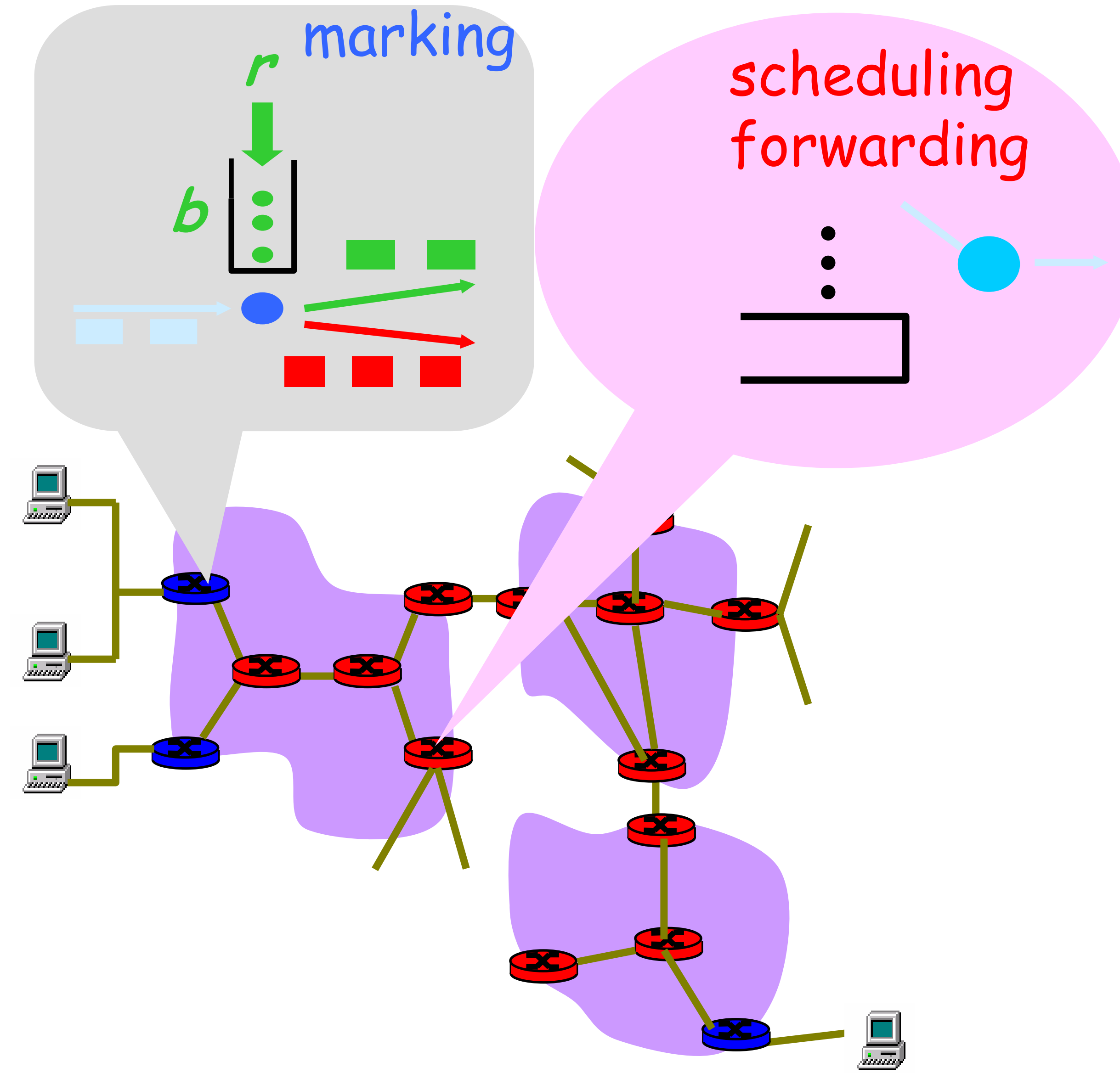
Differentiated Services (2)

- Diffserv approach includes two functions:
  - Edge functions: edge routers.
    - Packet classification.
    - Traffic conditioning.
  - Core function: core routers.
    - Forwarding.
    - Per-hop behavior (PHB).
  - Edge router:
    - Per-flow traffic management (like Intserv).
    - Marks packets as in-profile and out-profile.
  - Core router:
    - Per class traffic management (like Diffserv).
    - Buffering & scheduling based on marking at edge routers.
    - Assured Forwarding.

Differentiated Services (3)

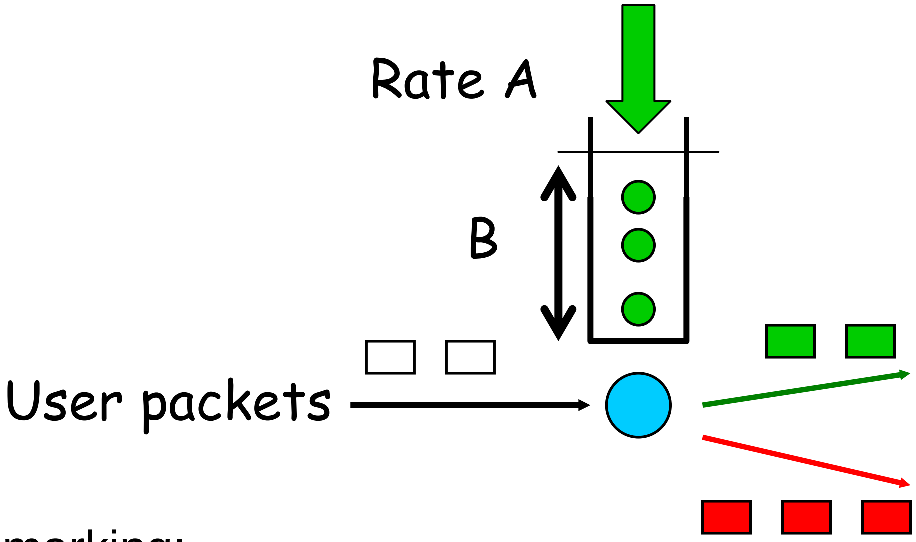
Diffserv architecture:

- Edge router:
- Core router:



Differentiated Services (4)

- Edge-router packet marking:
  - Profile: pre-negotiated rate A, bucket size B.
  - packet marking at edge based on per-flow profile.



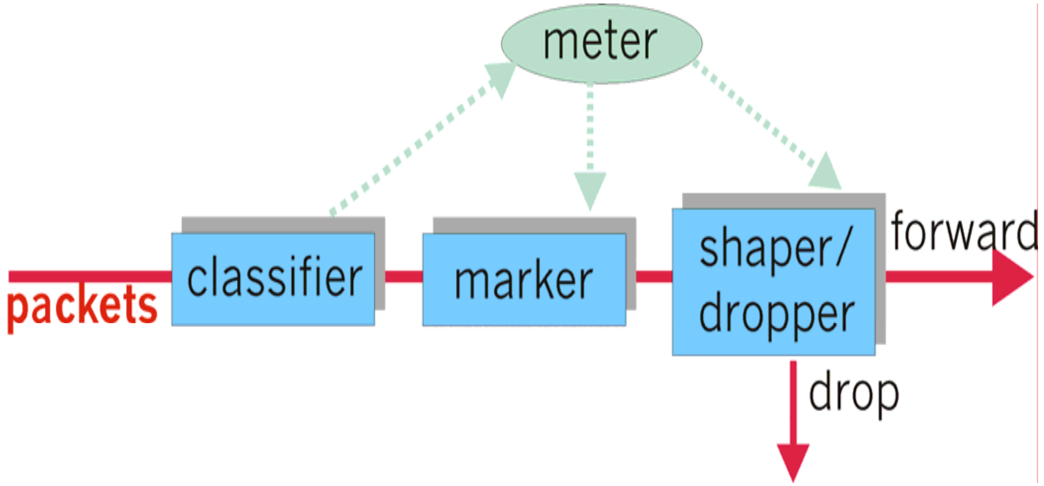
- Possible usage of marking:
- Class-based marking: packets of different classes marked differently.
- Intra-class marking: conforming portion of flow marked differently than non-conforming one.

Differentiated Services (5)

- Traffic classification and conditioning:
  - Packet is marked in the Type of Service (TOS, 8-bit) in IPv4, and Traffic Class (8-bit) in IPv6.
  - Mark (label, 8-bit):
    - Differentiated Service Code Point (DSCP):
      - The left most 6 bits of mark / label: are used to identify different classes. It can determine the PHB that the packet will be processed by the receiving routers.
    - CU: The right most 2 bits of mark / label: are currently unused.

Differentiated Services (6)

- The packet arriving at edge router will be first classified.
  - Based on source / destination IP addresses & ports, etc..
  - Then it is marked in the DS label.
- Some classes may have higher priority, but also allow to limit traffic rate.
- User declares traffic profile (e.g., max rate, burst size).
- Using traffic metering function: to compare the incoming traffic with the negotiation traffic → to shape / drop traffic, if it is non-conforming.



Differentiated Services (7)

- Per-hop behaviors (PHB):
  - It is employed in core routers to forward marked packets.
  - Considerations:
    - Different PHBs may result in a different observable (measurable) forwarding performance behavior.
    - But PHB does not specify what mechanisms to be used to ensure required PHB performance behavior.
    - The PHB must be observable (measurable).
      - Ex) Class A must get x% of outgoing link bandwidth over a specified time interval.
      - Ex) Class A packets must leave first before class B packets.

Differentiated Services (8)

- At present, two PHBs are developing:
  - Expedited Forwarding PHB (RFC 3246):
    - Packet departure rate of a class must equal or exceed specified rate (guarantee min data rate).
    - Logical link with a minimum guaranteed rate, even the network traffic load is heavy.
  - Assured Forwarding PHB (AF, RFC 2597):
    - AF has 4 classes of traffic.
      - Each class is guaranteed with the minimum amount of bandwidth.
    - AF has 3 types of packet drop preference.
      - Each traffic class is also classified into one of these three drop preference.
        - Which needs to be drop first when network is congested.