Networking Technologies and Applications

Rolland Vida
BME TMIT

September 22, 2016

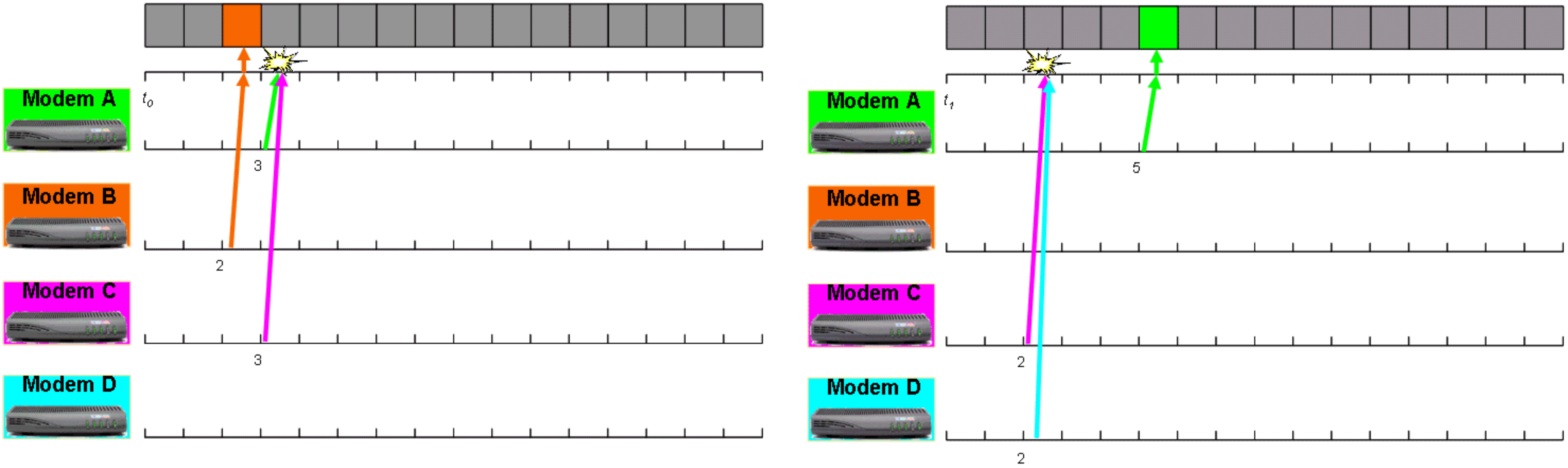
Contention based reservation for upstream traffic

- The upstream channel is divided (in time) into mini-slots -FDD/TDMA
  - Each upstream packet has to fit in one or more mini-slots
    - The length of the mini-slots is different in different networks
    - Typically 8 bytes of user data have to fit in one mini-slot
- The CMTS periodically announces the start of a new group of mini-slots
  - Because of the signal propagation on the cable, the modems do not hear it in the same time
    - Each modem can calculate the beginning of the first mini-slot (using the results of the previous ranging)
  - Each modem is assigned a special mini-slot (**Bandwidth Request Slot**) to ask for upstream bandwidth
    - Several modems on the same mini-slot

Contention based reservation for upstream traffic

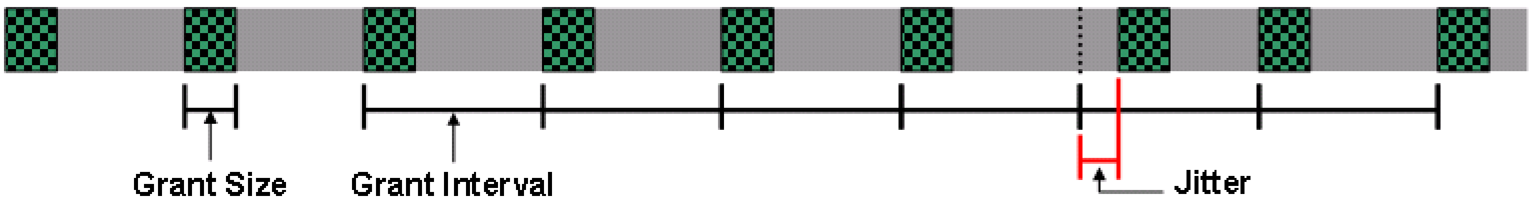
- If a modem wants to send a packet, asks for sufficient mini-slots
  - If the CMTS accepts the request, it sends and acknowledgment with the assigned mini-slots
    - If the modem wants to send further packets, in the headers it can ask for new slots
  - If two modems ask in the same time for slots, collision occurs, no acknowledgment is received
    - The modem waits for a random time interval, and then tries again
      - A timer set to random value chosen from the [0, x] interval
    - If a new collision occurs, the upper limit of the interval is doubled
      - A timer set to random value chosen from the [0, 2x] interval

Contention-based uplink



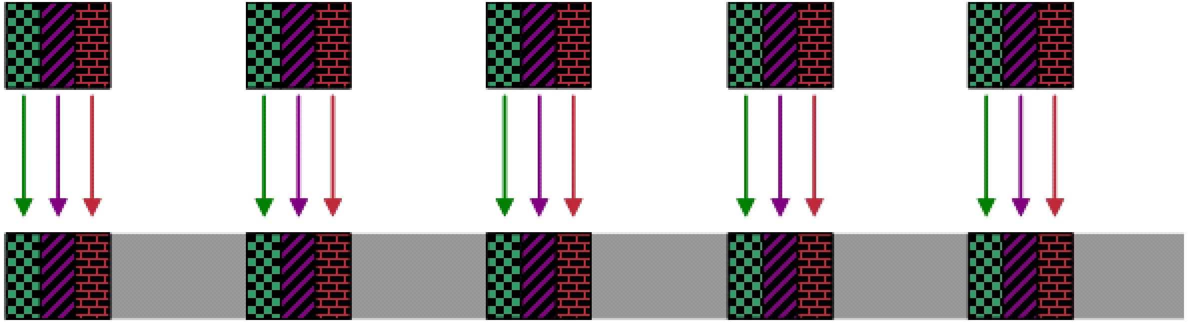
Providing Quality of Service

- Different applications have different QoS requirements
- CBR – Constant Bit Rate (pl. VoIP)
  - **Unsollicited Grant Services (UGS)**
    - No need to sollicit uplink slots all the time



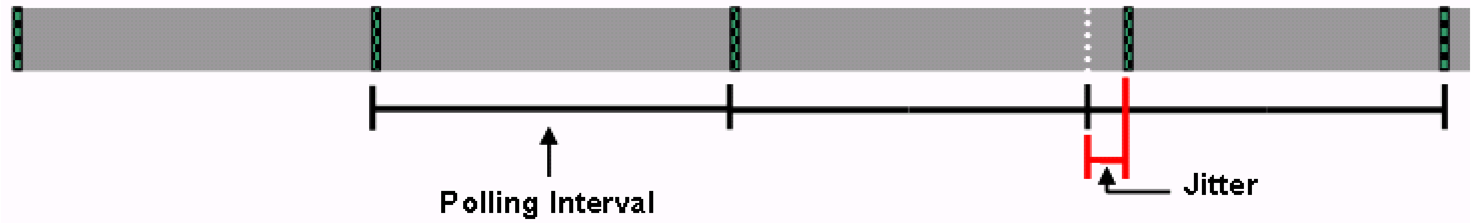
Admission Control

- UGS demands are accepted only in limited number
  - You have to leave room for other traffic types as well



Providing QoS

- rt-VBR (Real Time Variable Bit Rate)
  - E.g., live video stream
  - **Real Time Polling Service (RTPS)**
    - Bandwidth Request Slot dedicated to one specific application / modem
    - Can send his request for sure, no collision

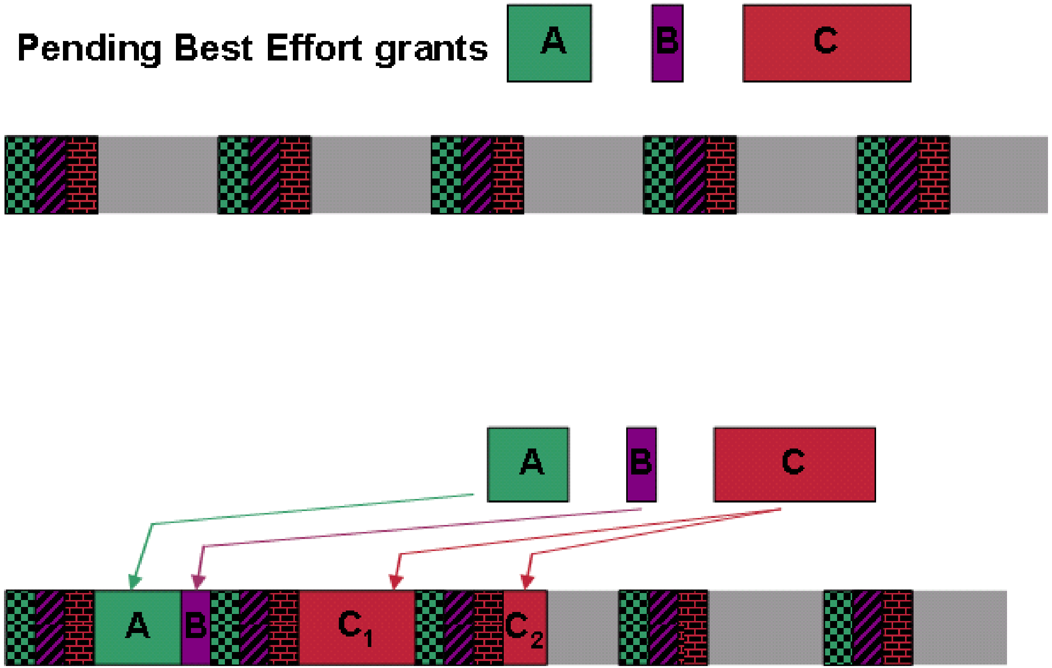


Providing QoS

- **Unsollicited Grant Service with Activity Detection (UGS-AD)**
  - Operates in UGS mode only if it has data to be sent
  - If temporarily no data, switches to RTPS mode
  - If needed, can switch back to UGS mode
  - E.g., VoIP with Voice Activity Detection (VAD)
- **Non-Real Time Polling Service (nRTPS)**
  - For nrt-VBR traffic
  - The polling intervals are not uniform

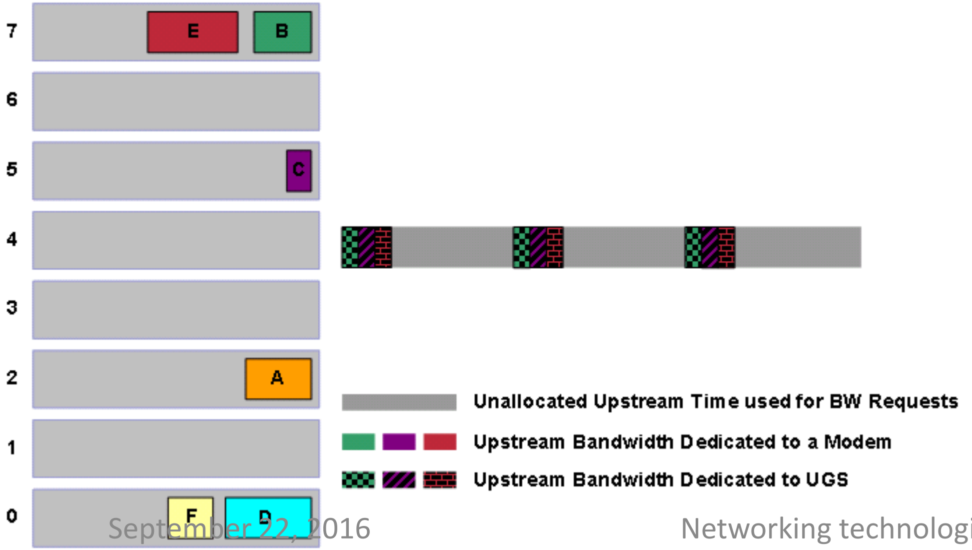
Providing QoS

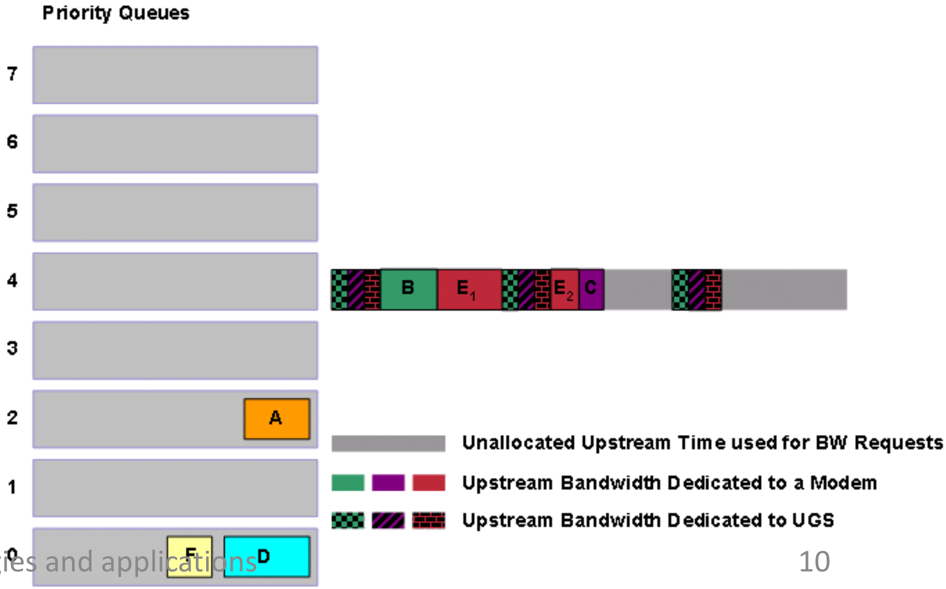
- **Best Effort Grants (BEG)**
  - No strict requirements for delay or jitter
  - Fragmentation – if needed, the slot requests can be split in time
    - More headers, but sometimes it is worth doing it



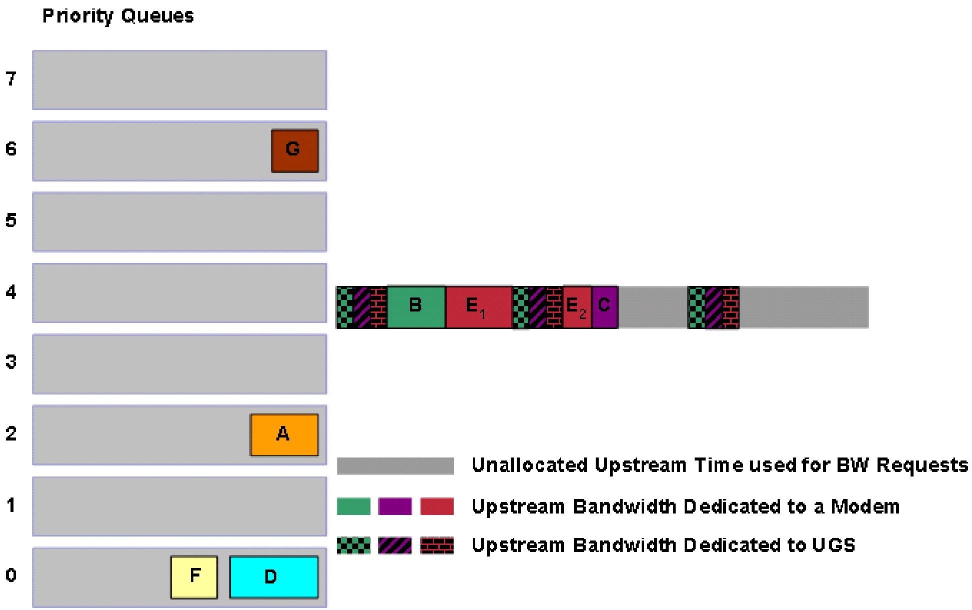
Scheduling

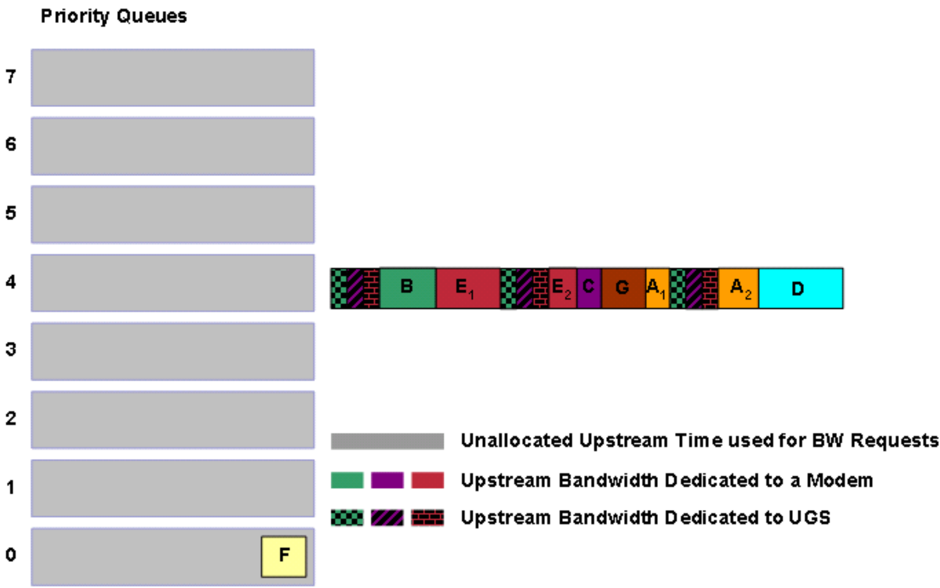
- Priority queues – by default 8 (from 0 to 7)
  - Higher priority queues are served firsti





Scheduling


Priority Queues
7
6
G
5
4
3
2
A
1
0
F
D
B
E1
E2
C
Unallocated Upstream Time used for BW Requests
Upstream Bandwidth Dedicated to a Modem
Upstream Bandwidth Dedicated to UGS


Priority Queues
7
6
5
4
3
2
1
0
F
B
E1
E2
C
G
A1
A2
D
Unallocated Upstream Time used for BW Requests
Upstream Bandwidth Dedicated to a Modem
Upstream Bandwidth Dedicated to UGS

No contention in the downstream traffic

- Downstream traffic is sent only by the CMTS
  - No contention, no need for mini timeslots
    - No collisions, lower probability for bit errors, no need for retransmission
  - Large packets in the downstream traffic
    - Typical packet length: 204 bytes
      - Includes Reed-Solomon error correcting code
      - 184 bytes for user data

Secure communication

- Shared cable
  - Anyone can read the traffic that passes by
- Two way traffic encrypted, to avoid the eavesdropping of the neighbors
  - Agreement between the modem and the CMTS on a common encryption key
    - Between two strangers, on a shared, eavesdropped link
  - Diffie-Hellman algorithm
    - Alice and Bob agree on two large prime numbers n and g
      - Public values, e.g., Alice chooses them, and send them to Bob, without encryption
    - Alice chooses a large (512 bit long) number: x
    - Bob chooses a similar one: y
    - Alice starts the key exchange, and sends the triplet $(n, g, g^x \bmod n)$ to Bob
    - Bob sends back the value $g^y \bmod n$
    - Both of them calculate the shared key:
      - $(g^x \bmod n)^y = (g^{xy} \bmod n) = (g^{yx} \bmod n) = (g^y \bmod n)^x$
    - Carol knows g and n, but cannot obtain x and y
      - It would take too much time, even with a supercomputer

MITM attack

- Diffie-Hellman does not protect against a MITM attack
  - Man-In-the-Middle
  - How do I know that Alice is really Alice?
    - Carol chooses a number z
    - It intercepts the triplet $(n, g, g^x \bmod n)$ sent by Alice, and replaces it with her own triplet $(n, g, g^z \bmod n)$
    - It intercepts Bob's answer $g^y \bmod n$ and replaces it with her own $g^z \bmod n$
    - Carol agrees with Alice in the shared key $(g^{xz} \bmod n)$, and with Bob in a different key $(g^{yz} \bmod n)$
    - Alice and Bob think they talk to each other, but in reality they talk to Carol
- Some authentication scheme is required
  - Digital signature - public/private keys
    - Alice knows Bob's public key
      - Certificate authority – trusted third party
    - Bob attaches a digital signature to its packet, using his private key
    - Alice verifies if the packet was really sent by Bob or not, using his public key