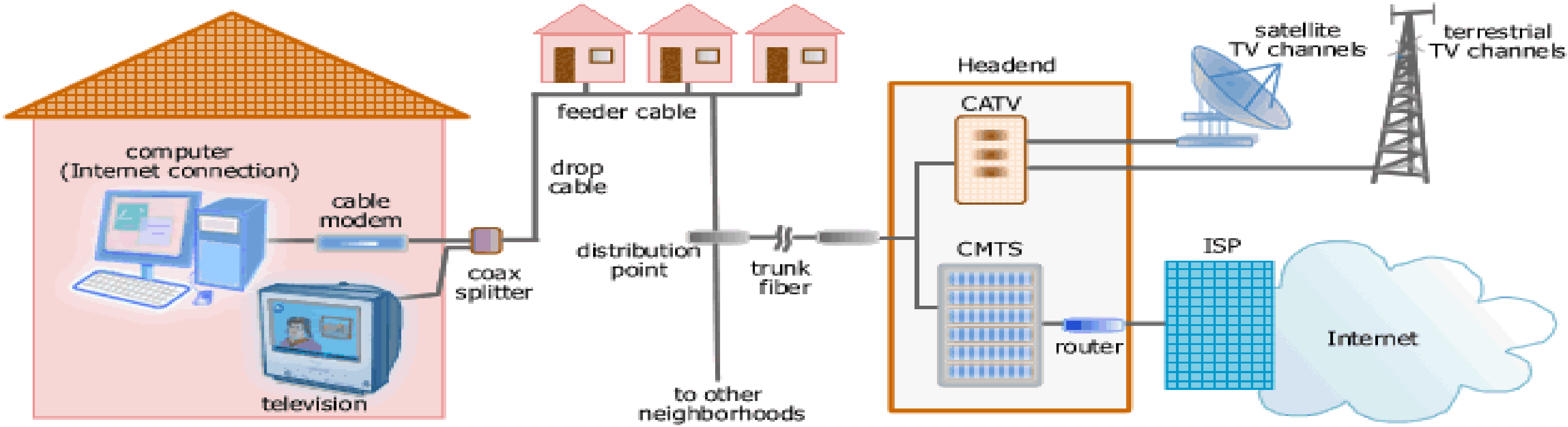
Networking Technologies and Applications

Rolland Vida
BME TMIT

September 12, 2017

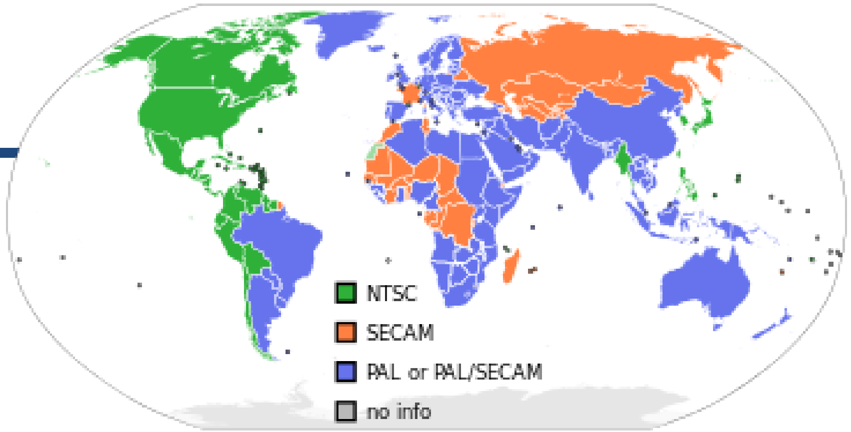
Internet on the cable



Spectrum allocation

- The cable network cannot be used exclusively for internet access (at least not yet…)
  - Many more TV viewers than broadband subscribers
  - The cities regulate what can be offered on the cable, a TV service is mandatory
  - The frequencies should be divided between TV channels and Internet access
- USA, Canada
  - FM radio: 88 – 108 MHz
  - Cable TV channels: 54 – 550 MHz
    - 6 MHz wide channels, with a guard band
      - NTSC - National Television System Committee
      - Resolution: 720 x 480, 29.97 fps

Spectrum allocation

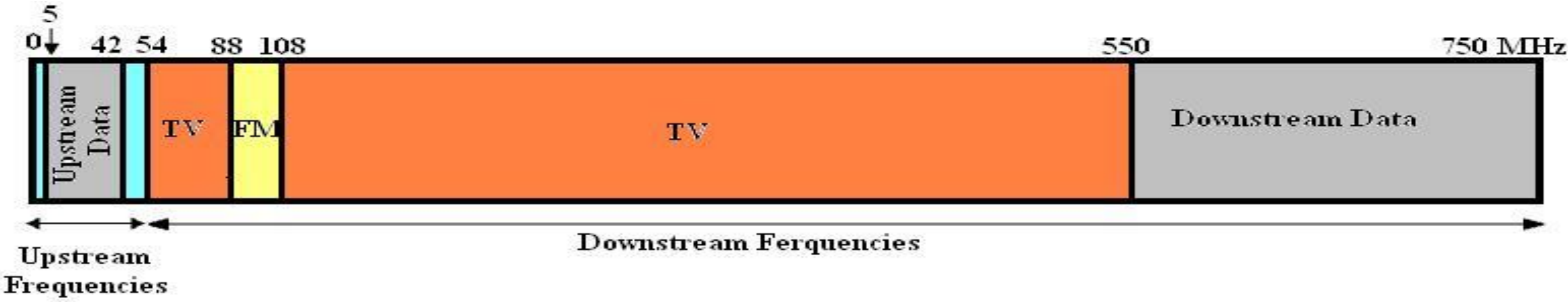


- Europe
  - TV channels above 65 MHz
  - 6-8 MHz wide channels
    - PAL and SECAM systems with higher resolution
      - PAL - Phase Alternating Line
      - SECAM - Système Electronique Couleur Avec Mémoire
      - Resolution: 768 x 576, 25 fps
  - The lower frequencies not used

Spectrum allocation

Modern cables provide good transmission quality above 550 MHz, up to 850 MHz or more

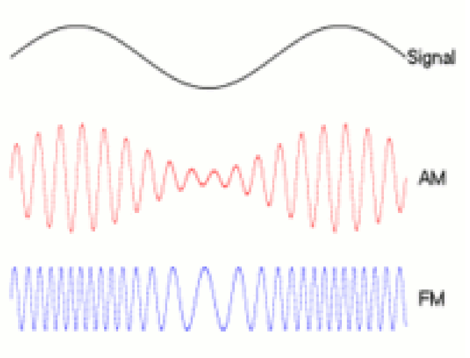
- Solution: uplink traffic between 5 – 42 MHz (5 - 65 MHz in Europe)
- The upper part of the spectrum used for downlink traffic

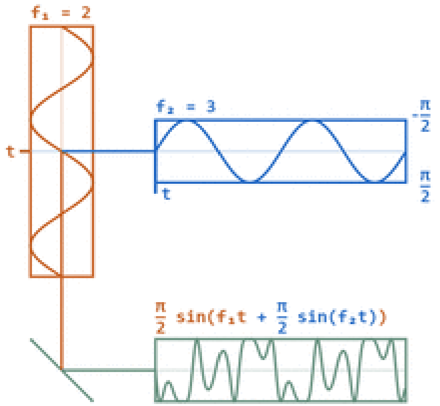


Asymmetric system

- TV and radio downstream
  - From the headend towards the end user
  - In the upstream direction, amplifiers working in the 5-42 MHz frequency range
  - In the downstream direction, amplifiers that work above 54 MHz
  - Larger downstream than upstream
    - Technological reasons, not like in the case of ADSL
    - Not a good solution for P2P traffic
      - Designed for asymmetric web traffic

Modulation



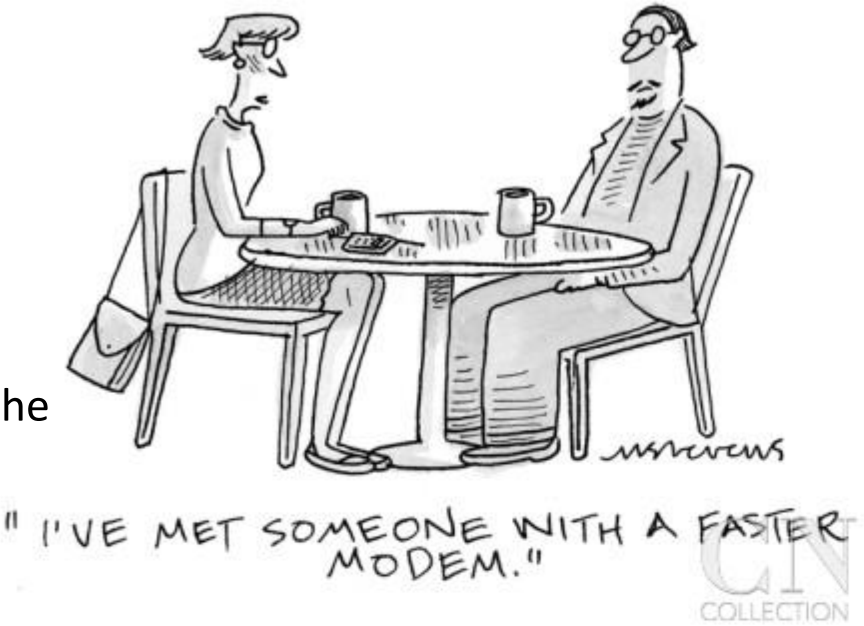


- Each 6-8 MHz is modulated with 64-QAM
  - Quadrature Amplitude Modulation
  - If a good quality cable, 256-QAM
- On a 6 MHz channel with 64-QAM → ~ 36 Mbps
  - Effective bandwidth without headers 27 Mbps
  - With 256-QAM, ~ 39 Mbps
  - In Europe larger bandwidths, because of the 8 MHz channels
- On the upstream channel 64-QAM is not acceptable
  - Too much noise, from microwave systems, CB-radios, etc.
    - Citizen Band – walky-talky
  - QPSK modulation
    - Quadrature Phase Shift Keying, much slower
  - Much larger difference between the upstream and downstream speeds

Cable modem

- Transforms the analog signals coming on the cable to digital data, and vice versa
  - MOdulates és DEModulates

- Two interfaces – one towards the PC, one towards the cable network
  - Ethernet/USB/WLAN connection between the cable modem and the PC



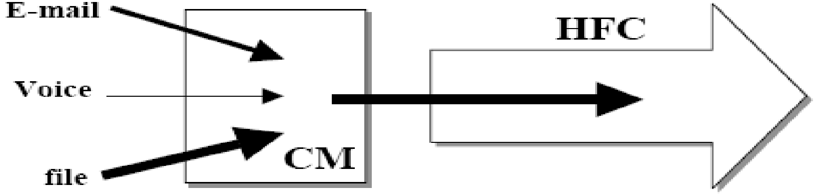
Cable modem

- In the early years each operator had its own modems, installed by a technician
  - An open standard was needed
    - Open the market, lower the prices
    - Contributes to the spread of the technology
    - If the users installs the modem, costs can be cut
- CableLabs
  - Association of the largest cable operators
  - DOCSIS standards
    - Data Over Cable Service Interface Specification
    - EuroDOCSIS – European version
  - Many were not happy about it
    - Could not hire out anymore their expensive modems to the defenseless subscribers

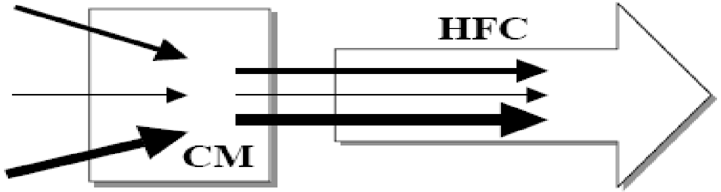
DOCSIS

- DOCSIS 1.0 (1997)
  - RF Return
    - Two-way communication
  - Telco Return
    - Dial-up connection for the upstream traffic
    - No need to modify the infrastructure, one-way communication on the cable
  - Modem prices fall from $300 (1998) to < $30
- DOCSIS 1.1 (1999)
  - VoIP, gaming, streaming
  - Compatible with DOCSIS 1.0
  - QoS

DOCSIS



DOCSIS 1.0



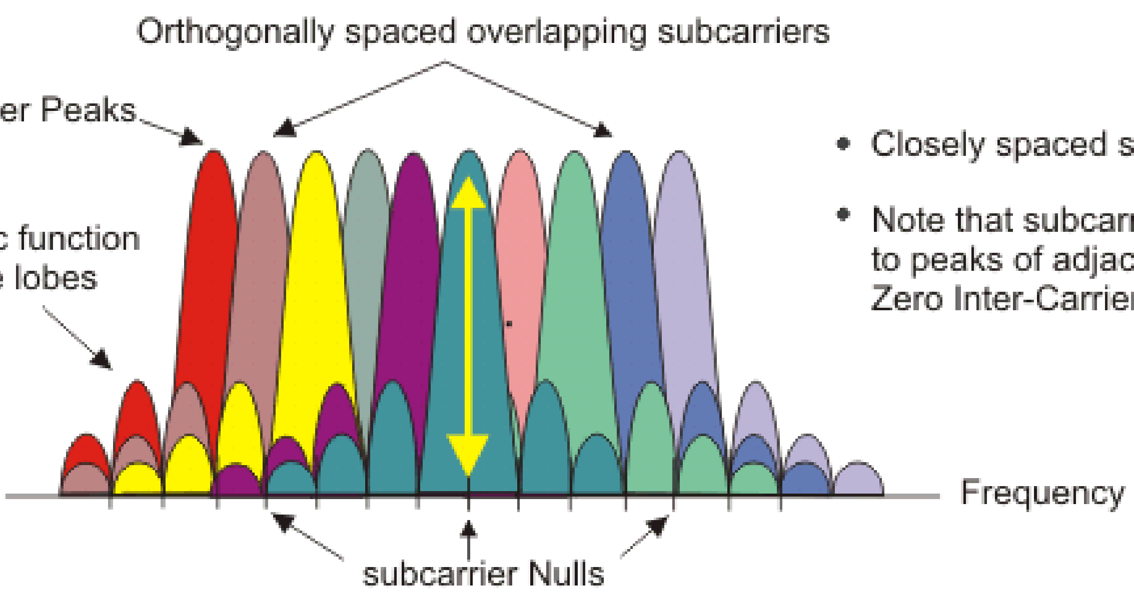
DOCSIS 1.1

- In DOCSIS 1.0 all the services are in contention for upstream bandwidth, on a „best effort" basis
- In DOCSIS 1.1 QoS guarantees can be associated to applications

DOCSIS

- DOCSIS 2.0 (2002)
  - Capacity for symmetric services
    - Larger upstream capacity than for DOCSIS 1.0 (x6) or DOCSIS 1.1 (x3)
    - Instead of QPSK, it uses 32-QAM, 64-QAM or 128-QAM on the upstream part as well
    - TDMA and S-CDMA in the MAC layer, instead of simple TDMA
- DOCSIS 3.0 (2006)
  - 160 Mbps downstream, 120 Mbps upstream
  - Channel bonding
    - Many channels associated in parallel to the same user
- DOCSIS 3.1 (2013)
  - 10 Gbps downstream, 1 Gbps upstream, 4096 QAM modulation
  - Instead of 6-8 MHz wide channels it uses narrow channels of 20-50 KHz, and OFDM (Orthogonal Frequency Division Multiplexing)
  - Channel bonding – spectrum width up to 200 MHz

OFDM



- Closely spaced subcarriers overlap
- Note that subcarrier nulls correspond to peaks of adjacent subcarriers for Zero Inter-Carrier-Interference.

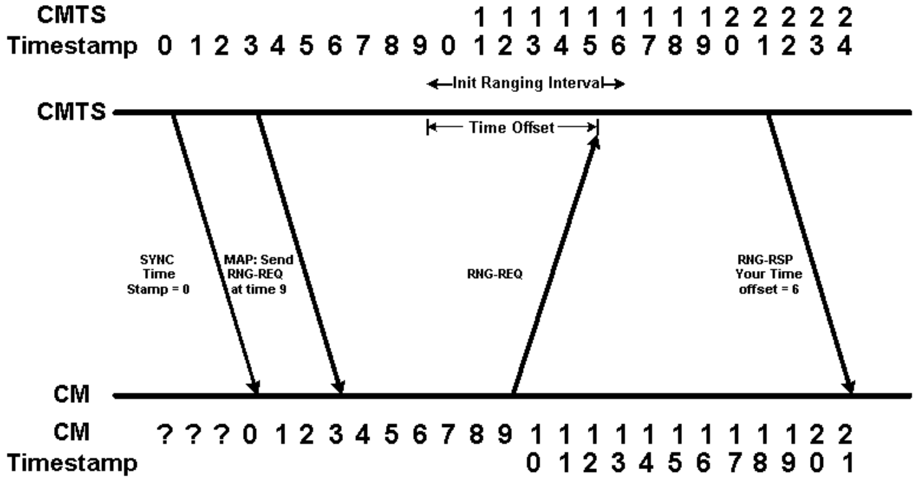
OFDM Signal Frequency Spectra

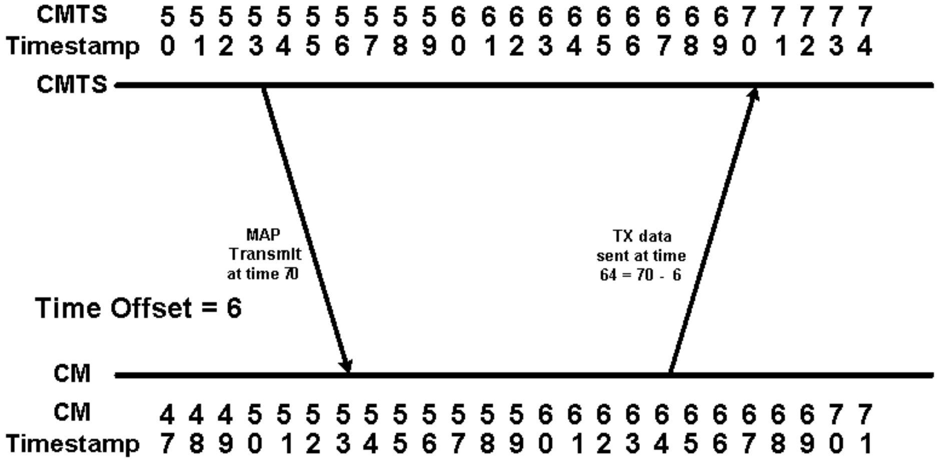
Connection

- When establishing the connection, the modem starts to scan the downlink channels
  - The CMTS periodically sends a special packet, with system parameters to enable new modems to connect
  - The modem register itself at the CMTS
  - The CMTS assigns the uplink and downlink channels of the newcomer
    - This can be changed later, e.g., for load balancing
    - Many modems on the same uplink channel
  - The first packets from the modem to the ISP
    - Ask for an IP address, through the DHCP protocol
      - Dynamic Host Configuration Protocol
    - Time synchronization with the CMTS

Contention based reservation for upstream traffic

- The modem measures its distance to the CMTS
  - Ranging – similar to a ping
  - Necessary to handle time slots correctly





Contention based reservation for upstream traffic

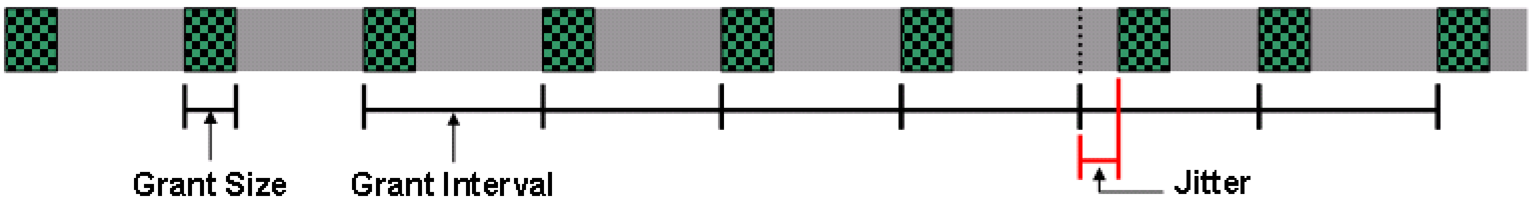
- The upstream channel is divided (in time) into mini-slots -FDD/TDMA
  - Each upstream packet has to fit in one or more mini-slots
    - The length of the mini-slots is different in different networks
    - Typically 8 bytes of user data have to fit in one mini-slot
- The CMTS periodically announces 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

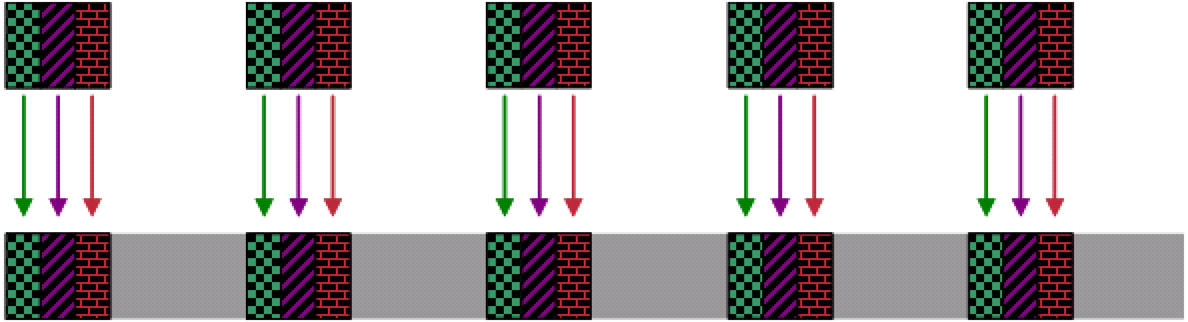
Providing Quality of Service

- 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



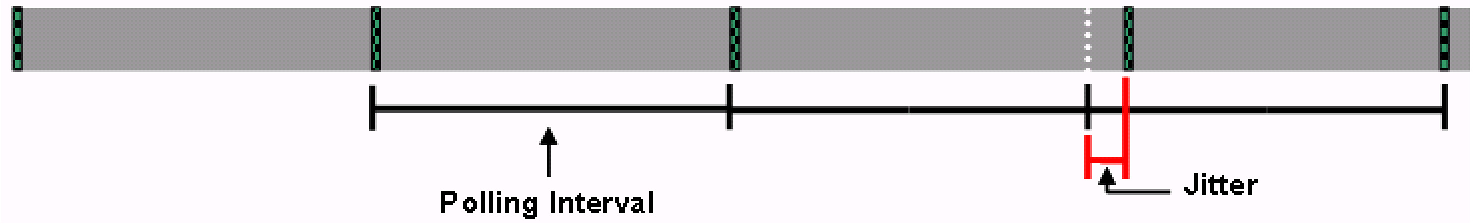
Admission Control

- 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

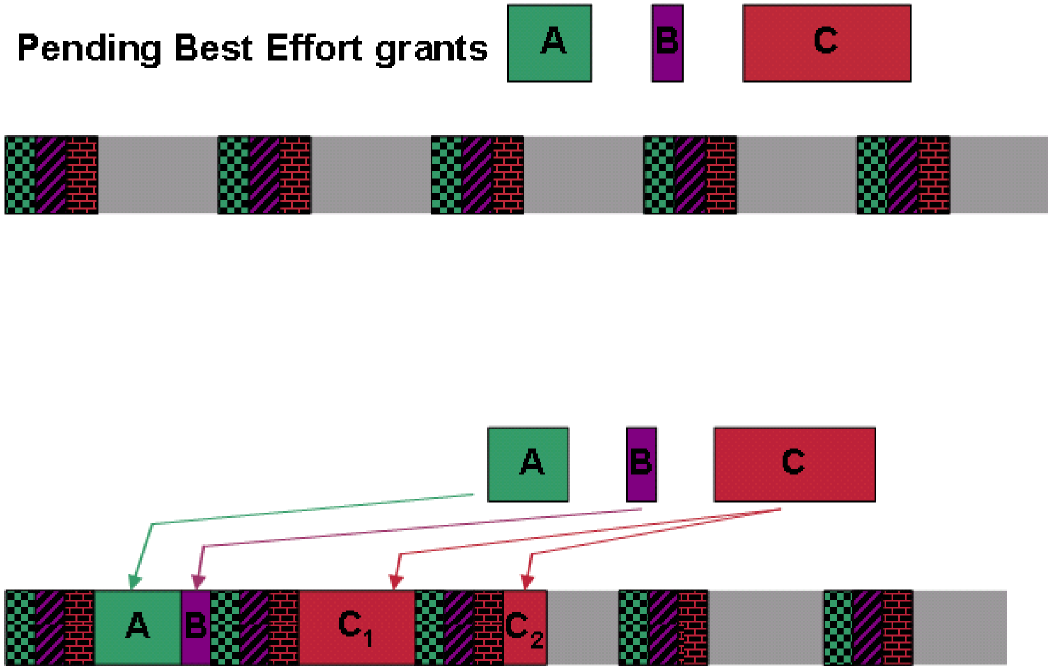


Providing QoS

- **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

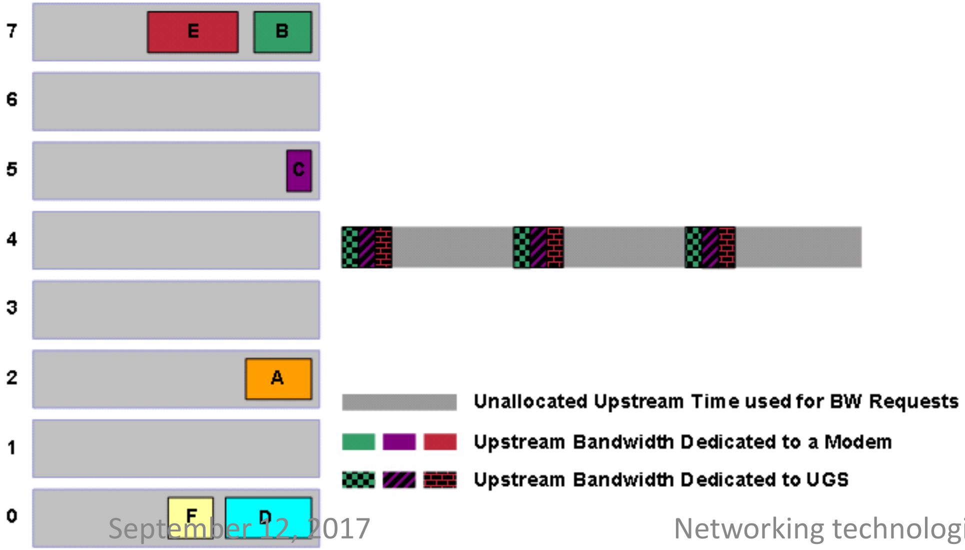
Providing QoS

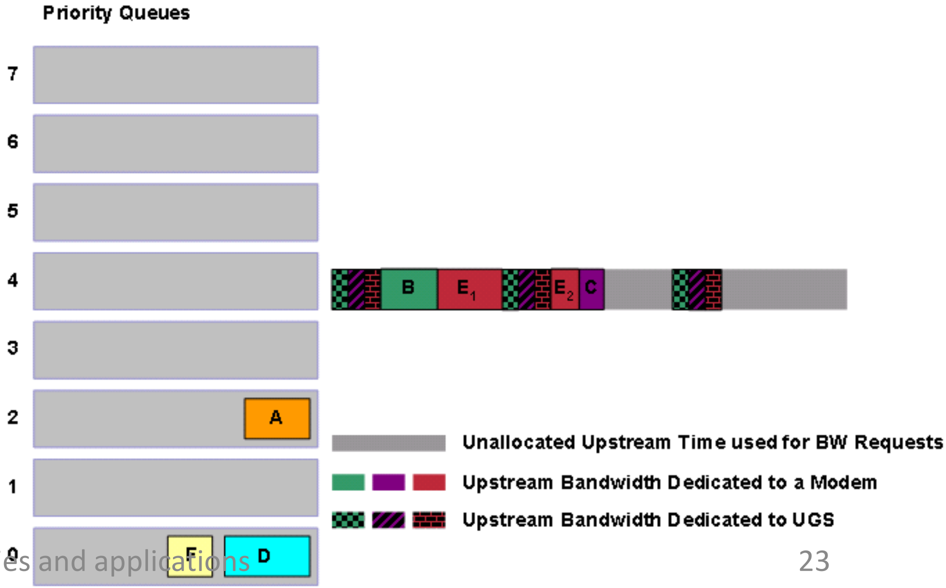
- **Best Effort Grants (BEG)**
  - No strict requirements for delay or jitter
  - Fragmentation – if needed, the slot requests can be split in time
    - More headers, but sometimes it is worth doing it



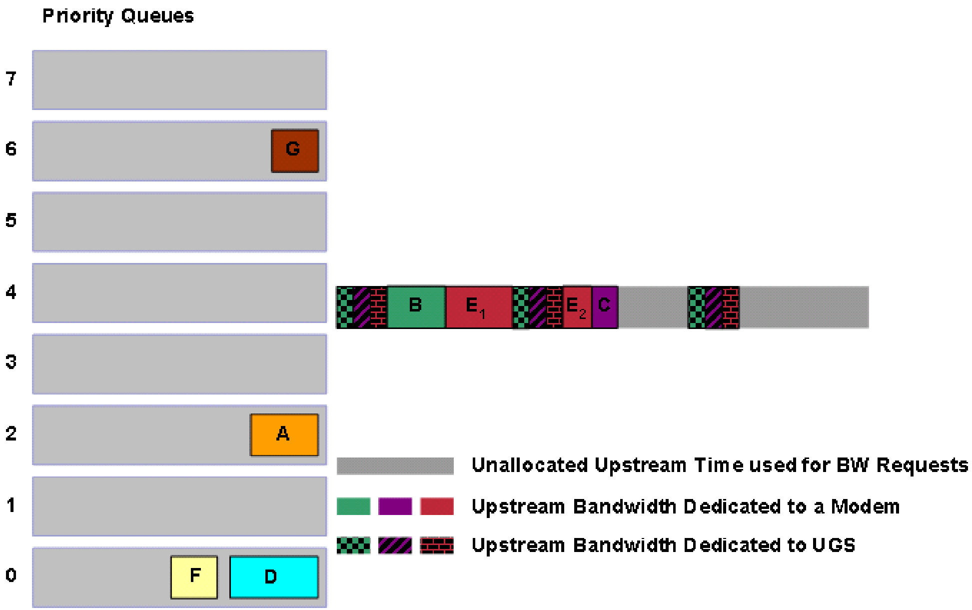
Scheduling

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

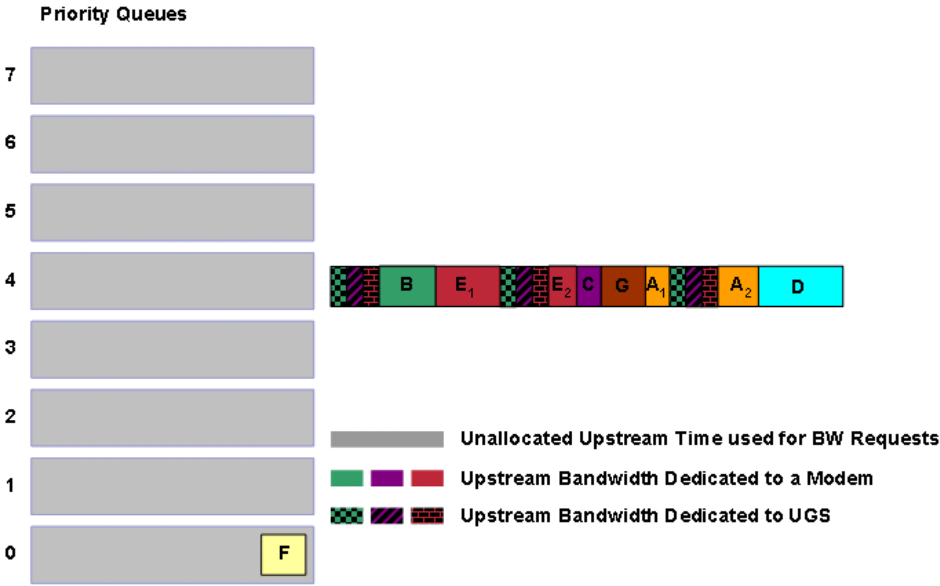




Scheduling



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 mod n) sent by Alice, and replaces it with her own triplet (n, g, g^z mod n)
    - It intercepts Bob's answer g^y mod n and replaces it with her own g^z mod n
    - Carol agrees with Alice in the shared key (g^{xz} mod n), and with Bob in a different key (g^{yz} mod 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