Networking Technologies and Applications

Rolland VIDA, PhD

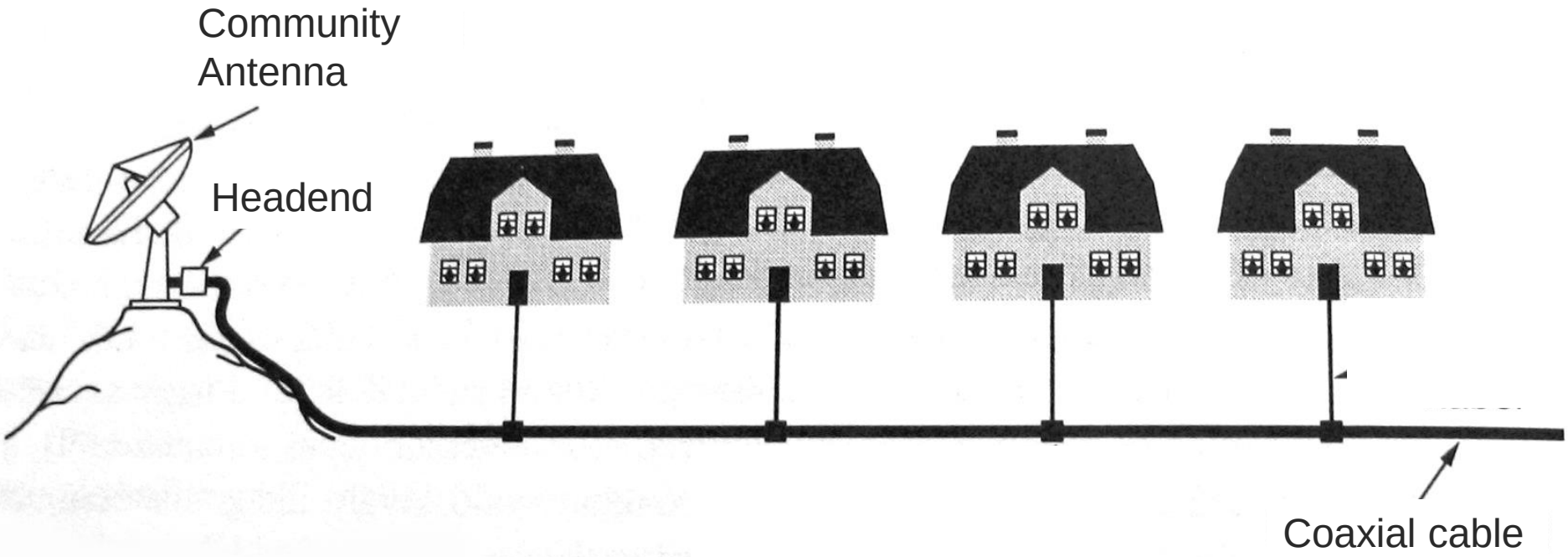
April 1, 2015

Cable TV

Why cable TV?

- The idea appeared at the end of the 40's
  - Better signal quality for people living in suburbs, or in the mountains
- Community Antenna Television – CATV
  - A big antenna on the top of a hill
  - Headend
  - Coaxial cable
- Family business, anyone could deploy its own network
  - If more users, new cables and amplifiers needed
- One-way traffic, only from the head-end towards the subscriber

Early cable TV system



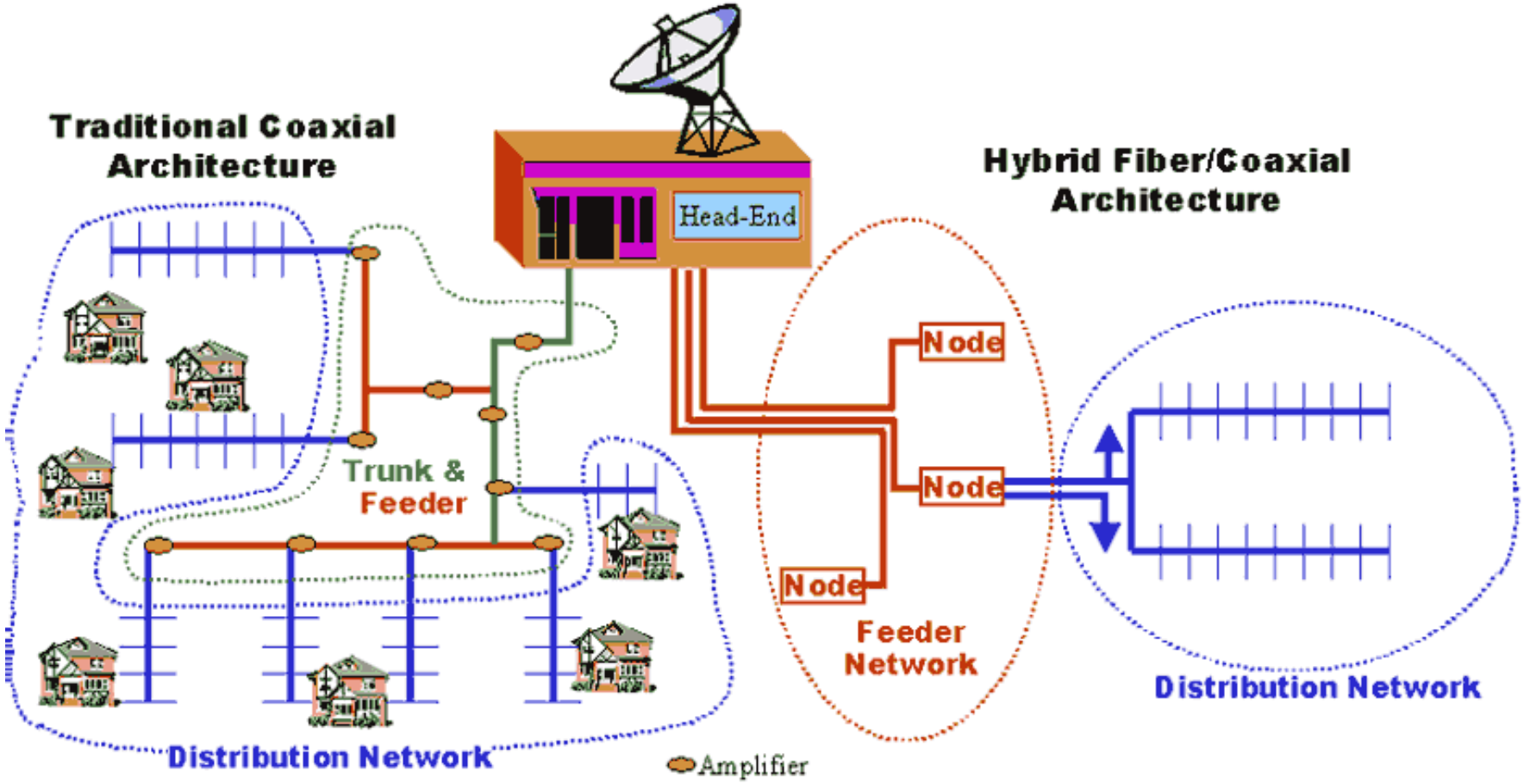
The development of cable TV

- Thousands of independent systems in the 70's
- HBO starts in 1974, as the first TV channel transmitted exclusively on cable
  - Many new thematic cable TV channels – news, sports, cooking, etc.
- Big companies start to buy the small local networks, and extend them with new cables
  - Cables linking the different cities
  - Similar process to the evolution of the PSTN networks
- The inter-city links changed later for optical fiber

HFC system

- HFC - Hybrid Fiber Coax
  - Optical fiber to span large distances
  - Coaxial cable to reach the homes
  - Fiber optic node
    - Electro-optical converter
      - Converts optical signals to electrical ones, and vice-versa
  - One optical cable can feed many coaxial cables
    - Much larger bandwidth

Modern Cable TV system



Internet on the cable

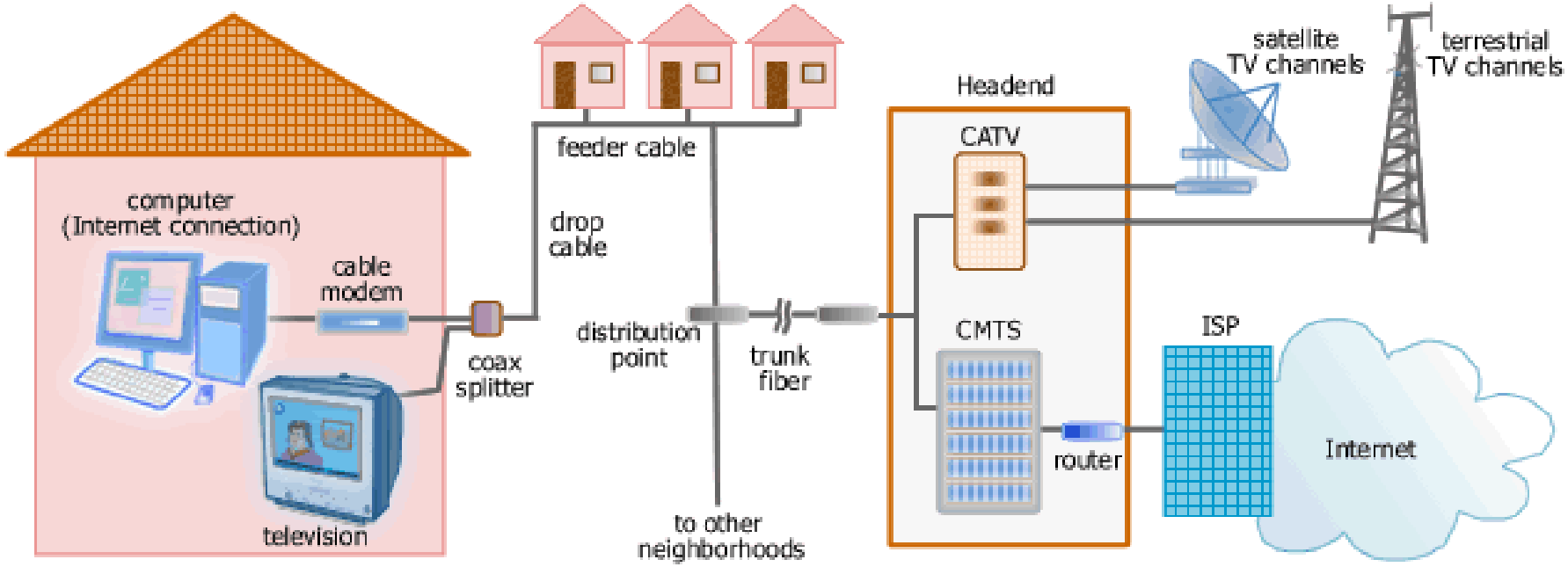
Internet on the cable

- The service providers started to enlarge their services
  - Internet access
  - Telephony
- The network has to be transformed
  - One-way amplifiers changed to two-way amplifiers
  - Upgraded headend
    - The dummy amplifier replaced with an intelligent digital computer system
      - High speed optical connection to an ISP's network
    - Cable-Modem Termination System (CMTS)
  - The coaxial cable a shared medium, many users use it simultaneously
    - In the PSTN network each user has its own twisted pair (local loop)
    - For the broadcast of TV channels this is not important
      - Each program transmitted over the same cable, no matter if there are 10 or 10.000 viewers at the same time
    - In case of internet access, it matters a lot if there are 10 or 10.000 users
      - If someone downloads a large file, no bandwidth for the others
    - On the other hand, much larger bandwidth on a coaxial cable than on a twisted copper pair

Internet on the cable

- Solution: a long cable is divided into many smaller segments
  - Each segment connected directly to the fiber optic node
  - The speed between the headend and the fiber optic nodes basically unlimited
    - If not many homes on a segment, the traffic can be handled
  - Today typically 500-2000 homes on a segment
    - Smaller segments expected if more subscribers and larger speed demands appear

Internet on the cable



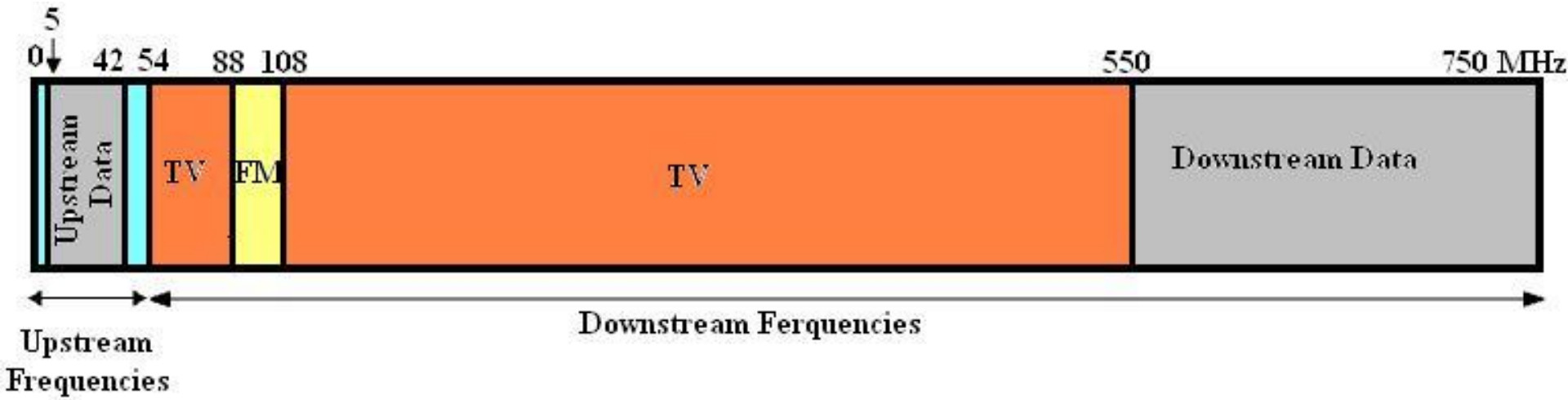
Spectrum allocation

- 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
- 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

Spectrum allocation



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
    - Only two bits per symbol (with 64-QAM 6 bits, with 256-QAM 8 bits)
  - 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
    - Many PCs on the same LAN, if needed
    - Each PC needs an IP address
      - Buy more IP addresses from the ISP
      - NAT (Network Address Translation) – many hosts behind the same IP address

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
- The upstream channel is divided (in time) into mini-slots
  - 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

Contention based reservation for upstream traffic

- 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 to ask for upstream bandwidth
    - Several modems on the same mini-slot
- 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

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

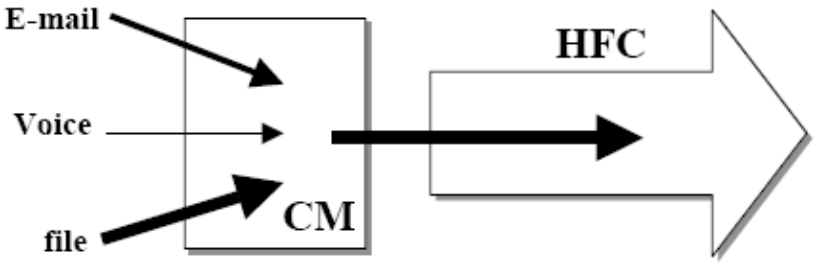
Cable modem

- 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

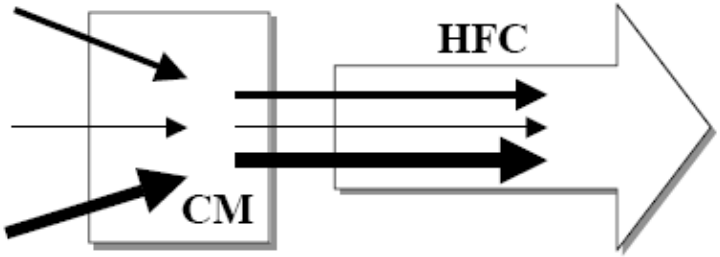
DOCSIS

- 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, CM authentication

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

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