Data Transmission and Home Networks

Gralla: part 2
A Home Network

Roughly from: Gralla pp. 80-81
How the Home Network Works

• The computers are connected by a hub or switch to form one Ethernet segment
  – The Ethernet is a shared medium
  – Ethernet frames can be sent to other computers by attaching the recipient's Ethernet address into the beginning

• Each computer has its own IP address
  – Other computers can be found by their IP address by broadcasting an ARP query to the Ethernet network

• The gateway has two IP addresses
  – One for the inside segment
  – One for the outside interface
• A LAN (lähiverkko) means usually a physical network and the lower layer (1-2) protocols related to it
• Current common standards are Ethernet and WLAN
  – Both standards use 6 byte Medium Access Control (MAC) addresses inside the *network segment*
  – Both require an adapter to the computer and a device driver to translate the signals to data
• Ethernet uses various media, most common is a twisted pair cable
  – IEEE 802.3 defines the protocol behavior. Cabling and capacity differs in versions.
• Wireless LAN uses radio frequencies
  – The most common standard is IEEE 802.11b/g, aka. WLAN or WiFi
A Shared Media

- The traditional Ethernet media is a shared bus,
  - Only one station can send at the same time or signals confuse each other
  - Likewise with WLAN
- Solution: everybody waits until nobody is sending
  - CSMA, Carrier Sense Multiple Access
- Other solutions: have a master controller or give everybody a fair share
  - Many sensor or field bus networks have a master controller
  - Token Ring nodes are organized in a ring and a data pattern called token is passed around in order, whoever has the token has a right to send
Collisions happen, so a strategy is needed to manage them

- Collision Detection and resend: CSMA/CD (Ethernet)
  - When two stations on an Ethernet send simultaneously they recognize the collision, each party stops sending and starts again after a random time
- Collision Avoidance e.g. reservation of the media: CSMA/CA (WLAN)
  - WLAN nodes ask the access point for a permission to send
Current Ethernet Hubs & Switches

**Single collision domain**

(a)

Hub (keskitin):
Star-topology CSMA/CD

Both:
Twisted Pair is cheap
Easy to work with

Switch (kytkin):
Bridging increases scalability
Separate collision domains
Full duplex operation
Star topology

(b)

High-Speed backplane or interconnection fabric
WLAN Hidden Node Problem

(a) A transmits data frame

(b) C transmits data frame & collides with A at B,
   C does not detect the collision

- New MAC algorithm: CSMA with Collision Avoidance
- A and C send Request To Send messages
- B decides who can send with a Clear To Send message
A computer on the network should know its:
- Own IP address
- Gateway (router, firewall) IP address
- Netmask

Own IP address is obvious
Gateway is needed to connect the host to the Internet and is recognized by its IP address

Netmask is a *binary mask* that enables the operating system to recognize which addresses are on the LAN and which can be accessed through the gateway:

- **IP:** 192.168.1.100
- **GW:** 192.168.1.1
- **NM:** 255.255.255.0

This means that all 192.168.1.* addresses are on the LAN
IP Addresses

- IP address identifies a network interface. A host can have several interfaces.
- Current length is 32 bits (IPv4).
  - Future length is 128 bits (IPv6).
- General syntax:
  - 4 components (bytes) separated by dots ("dotted quad")
  - Represented as decimal numbers (0-255)
  - For example: 193.210.18.18
- Addresses have two components, the network id and the host id.
Address Resolution Protocol

- Problem: IP addresses only make sense to the TCP/IP protocol suite, not to the hardware (Ethernet) interface
- Solution: ARP maps IP addresses to hardware addresses

- A host finds other hosts by broadcasting an ARP query for the IP address
- The host with correct IP address replies with its hardware address
- The address pair is added to receiver's dynamic ARP cache
  - See: `arp -a`

- But how to know my own IP address?
• Dynamic Host Configuration Protocol (DHCP)
• Automatic assignment of IP addresses
  – Dynamic assignment for a limited time
  – Or a permanent address tied to the MAC address
• Used when a host enters a new LAN segment
  – At boot time, or a portable computer connects
• A translation between host names (mostly for humans) and IP addresses
• Based on distributed servers
• Each organization can maintain the data for their own zone
  – Zones are delegated from above organizations in the hierarchy
  – E.g. Ficora in Finland maintains the fi zone and they have delegated tkk.fi to TKK
• Thus:

  vipunen kiravuo 56% /usr/sbin/dig www.hut.fi
  www.hut.fi. 3600 IN A 130.233.240.9
  ns1.hut.fi. 3600 IN A 130.233.224.1
What is really happening in the Ethernet network, GSM phones, WLAN etc.

How to send a digital signal over a physical medium?
  - The digital signal can be coded and the coding sampled at the receiving end

How to translate an analog signal to digital?
  - Analog signals can be sampled and translated to a digital representation
How is Digital Voice Transmitted?

1. Sound signal
2. Sampling, Quantifying
3. Coding
4. Transmission

- Mikrophone → A/D → Source coding → Line coding
- Sound → Filtering → Decoding → Receiving
- Loudspeaker → D/A → Sample generation → Line (de)-coding

Transmission channel

1001101 .mp3
Why Digital Transmission?

• In optimal conditions analog transmission provides superior quality

• However conditions over any meaningful transmission path are usually not optimal
  – It is usually impossible to figure out which part of an analog signal is distortion and which is original

• It is easy to recreate an exact replica of a digital signal
  – Digitalization loses a pre-defined amount of detail
Sampling and Quantizing
Line Coding for Transmitting Digital Data

- Line coding is used over high quality media (e.g. Ethernet or optical cabling)
  - Very little noise or other signals
- The coding provides a method to identify 0s and 1s
Transmission Errors

- Original signal
- Attenuated
- Limited bandwidth
- Noise
Modulation for Digital Signals

- A carrier wave can be used to transport the signal
  - amplitude modulation (AM),
    amplitude shift keying (ASK)
  - frequency modulation (FM),
    frequency-shift keying (FSK)
  - phase modulation (PM),
    phase-shift keying (PSK),

- Modulation is used when the media has noise or interference, the receiver can create a reference signal and detect the differences that contain the data
• ADSL (Asymmetric Digital Subscriber Line) uses a single twisted pair, and allows simultaneous transmission of downstream simplex, duplex, base band analogue, ADSL line overhead and framing, error control, operations and maintenance.

• Uses Discrete Multitone (DMT) modulation, where the frequency spectrum is divided in narrow sub bands, each of which can be configured separately

• ADSL transmission is possible simultaneously with POTS, analogue modems, ISDN.

• ADSL has a low speed full-duplex bearer channel and a high speed bearer channel on the downstream direction.

• ADSL version ITU-T G.992.1 supports 6.144Mbps downstream and 640kbps upstream.

• ADSL version ITU-T G.992.2 supports up to 1.563Mbps downstream and 512kbps upstream.

• ADSL provides transport of STM and/or ATM.
Traffic Encapsulation

- Encapsulation allows the use of several techniques at the same time
  - Different layers implement different methods
• LANs are needed to move data over shared local networks
• The Internet Protocol transmits data from LANs to other LANs regardless of the differences in underlaying protocols
  – Otherwise WLAN could no provide access to Ethernet services
• Modulation or line coding is used at the physical layer to transmit bits