Network Hardware

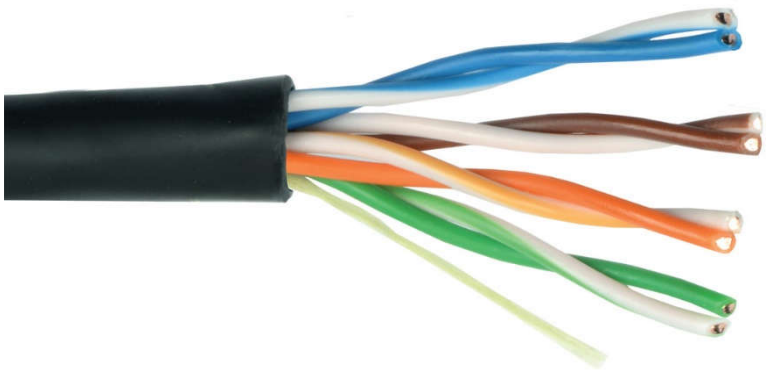
Network hardware comprises all physical parts of the network equipment.

Passive Elements

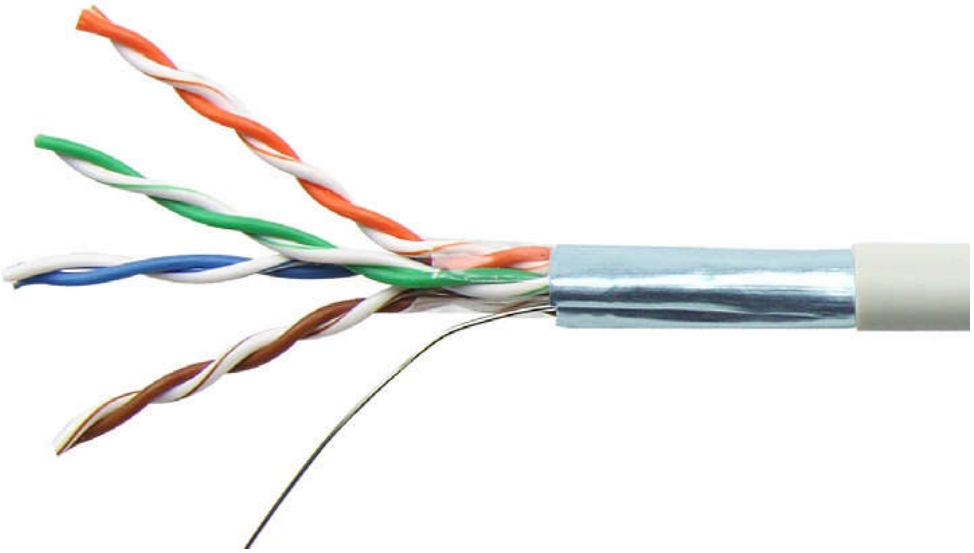
- All of them are defined on the physical layer of OSI/Network Access Layer of the TCP/IP model.

Wired

- **Twisted Pair Cable**
  - 8 copper wires in 4 twisted pairs – reason: twisted wires are relatively immune to electromagnetic noise, which disrupts signal.
  - Types:
    - **Unshielded Twisted Pair** (**UTP**) – wires and plastic insulation only – the cheapest and simplest one



    - **Foiled Twisted Pair** (**FTP**) – there is a metallic foil wrapping wires – additional protection against the electromagnetic noise,



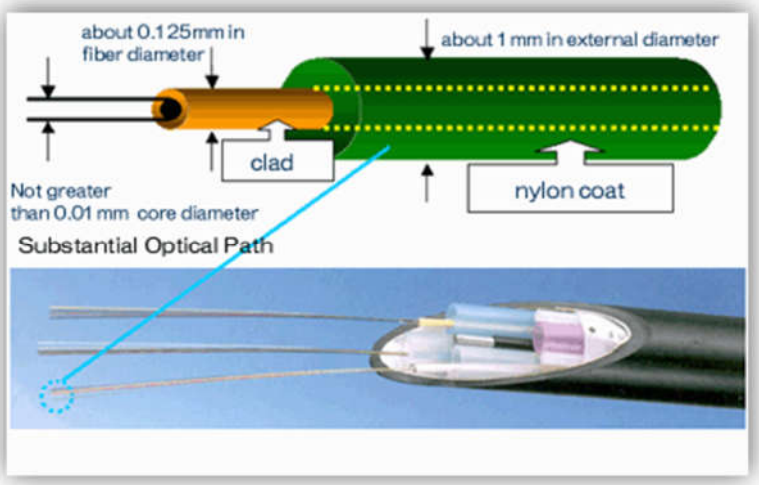
    - Shielded Twisted Pair (**STP**) – all pairs are covered by metallic foil + there is a common metallic shield for all pairs. The STP cable is used in

environments, which are heavily disrupted by the electromagnetic noise (industrial settings mostly), because the cables are expensive and require proper installation, esp. grounding; if the shielding is improperly grounded or damaged, it acts as a antenna that collects noise.

- **Maximal distance**: 100 m – for longer distances there must be used a devices able to amplify the signal (switch, hub)
- **Connector**: RJ-45

- **Speed**: 100 Mbps (Category 5) – 10 Gbps (Category 6A or better)

- **Optical fibres**
  - made of **glass** or **plastic** (cheap, for short distances and low speeds), covered by several protective layers. The fibres are very thin thus flexible.
  - Extremely fast (Gbps to tens of Gbps and more in real use; terabits per second in development).



  - Immune to electromagnetic interference.

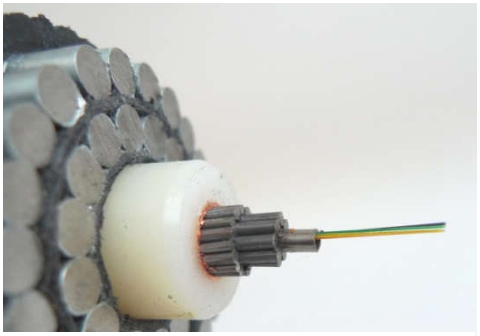


Figure 1: Submarine optical fibre (source: http://fopnews.wordpress.com/2011/03/24/incident-report-hudson-canyon-geologic-city-report-10/)

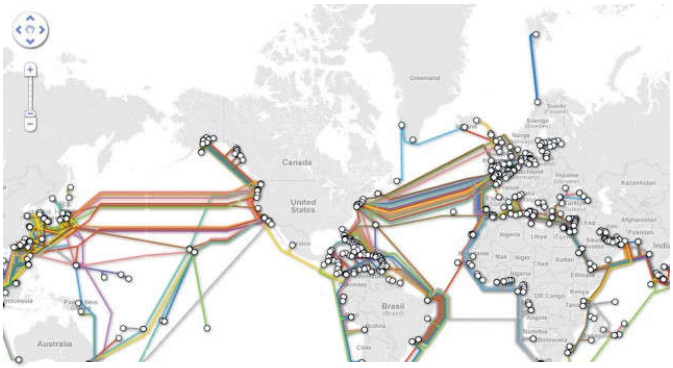
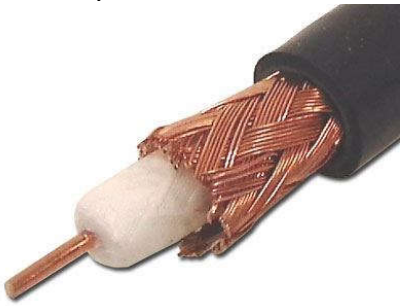


Figure 2: Map of the submarine cables (source: http://www.extremetech.com/computing/96827-the-secret-world-of-submarine-cables)

  - Distance: meters to kilometers – used also for intercontinental links – the cables must contain also **amplifiers**, which regenerate signal.

- **Coaxial**
  - A type of wire that consists of a center wire surrounded by insulation and then a grounded shield of braided wire. The shield minimizes electrical and radio frequency interference.
  - They used to be popular in networks; nowadays they are still used in cable TV networks.



Wireless

- transmission of electromagnetic waves (radiowaves, microwaves, infrared, visible light)
  - *Very-short distance* (several metres usually)
    - Bluetooth
    - WiDi (Wireless Display), Miracast
    - infrared connection
  - *Short distance* – WiFi – protocol 802.11 (up to few kilometres)

    - **802.11b** – speed – up to 11 Mbps; band: 2.4 GHz
    - **802.11g** – speed – up to 54 Mbps, better range than 802.11b; band: 2.4 GHz
    - **802.11n** – speed – up to 450 Mbps, better range than 802.11g; band: 2.4 GHz or 5 GHz
    - **802.11ac** – speed – hundreds of Mbps to several Gbps (6.93 Gbps); band: 5 GHz
    - **802.11ad** – speed similar to 802.11ac; band: 60 GHz
  - *Medium distance* – mobile networks – 2G (GSM, GPRS, EDGE) – up to hundreds of kbps , 3G (UMTS, HSDPA) – up to tens of Mbps, 4G (LTE, WiMAX) – up to Gbps
  - *Long distance* – satellite Internet access – up to 1 Gbps

Active Elements

- They can amplify, transform or process transmitted data

Network Interface Controller (NIC)

- it connects computers to the network
- it works on the physical and data link layer of OSI – each card has its unique MAC address
- NIC
  - **expansion card**
  - **a part of the motherboard**
  - **USB**

Repeater

A repeater is an electronic device that amplifies the signal it receives - a device which receives a signal and retransmits it at a higher level or higher power so that the signal can cover longer distances. It works on the 1st level of the ISO OSI model, therefore it recognizes bits only.

Their purpose is usually to overcome some distance limitations, e.g. in Ethernet over the TP cables the maximum distance for the bare cable is 100 meters. If a part of the network is further apart, the signal has to be amplified.

The amplification can be done by other devices as well, for example by a switch or a bridge.

Switch

- It is a multiport ***bridge*** – a device, which **interconnects** computers of the **same network**
- A connection point in a star network. The switch sends accepted data **only to the final destination** – better than a similar device – **hub**, which sends data to all computers in the network (this behaviour overloads network).
- It works on the 2nd level of the OSI model – it can recognize MAC addresses in order to deliver the data to a proper computer.
- For computers the switch is **transparent** – they are not aware of its existence in the network.
- The switch learns MAC addresses of the connected devices from the incoming frames.

How to display MAC addresses?

1. Start the command prompt
2. In Windows type *getmac*
3. In Linux type *ifconfig –a* or *arp -n*

Router

- A **connector of independent networks** (e.g. home network ↔ Internet). Each network has its own router. If the router connects the network to any other network, it is named **gateway** (**in the route table it is indicated as the route for addresses 0.0.0.0**).
- It works on **the 3rd level of the OSI** model – it can recognize IP addresses and transfer them in a proper direction – the direction is defined by a routing table.
- Home routers are combined with a small switch, which connects computers of a home network.

How to display the routing table?

4. Start the command prompt
5. In Windows type *route PRINT*
6. In Linux type *route*

How hubs, switches, and routers work (do not mind the narrator☺) – WATCH IT!

https://www.youtube.com/watch?v=Ofjsh_E4HFY

Modem

- Short for ***mo****dulator-****dem****odulator.* A modem is a device that enables a computer to transmit data over telephone or cable lines.
- In the early days of networks the modem converted data from digital form to analog = *modulation*, and from analog to digital = *demodulation*).
- Nowadays it converts/translates WAN (used by ISP) and LAN (used by PCs) protocols.

Access Point (AP)

- A device that connects wireless communication devices together to form a wireless network.
- Some of them can be accessed by the public – **public hot spots**.
- AP can act in two ways
  - **Bridge** - the wireless network is a part of the LAN
  - **Router** – the wireless network is an independent network
- **Access to the AP**
  - *Without any authentication* – either fully open (dangerous) or managed by a system behind the AP
  - *WEP* – old system; its access code can be acquired in minutes at most
  - *WPA* – newer system, however some vulnerabilities were detected
  - *WPA2* – the strongest system for personal WiFi networks

Figure 4: Wireless Access Point