Network is a group of devices that can share information and resources with each other, so this devices are connected. The main characteristic of network is the type of connection, it can be wired or wireless:

Wired networks are linked by Ethernet cables such as telephone cables, network cables and fiber-optic cables. Wireless networks, however, use electromagnetic waves, such as radio waves and microwaves, to transmit data.

There is one more classification:

PAN: generally in one flat

LAN : limited by one building

MAN : limited by one city

WAN : limited by one country

A communication channel used to transport information from one network device to another. As I said there two general classifications: wired and wireless. Wired channels transport data through wires and cables, mostly by fiber-optic. It is more secure. Wireless channels transport data from one device to another using RF signals and microwaves. It is less secure.

There are five main network topologies:

1.Full mesh: every device is connected with each other. Data travelling on a mesh network can take any of several possible paths from its source to its destinations.

2.Point-to-point: For example, When peripheral devices connect to a host device using expansion ports, USB cables, or Bluetooth.

3.Star: features a central connection point for all workstation and peripherals. The central connection point is not necessarily a servermore typically it is a network device called a hub. The main disadvantage of this topology is that if the central device fails ,it can take down the entire network

4. A Bus topology uses a common backbone to connect all network devices. The backbone functions as a shared communication link, which carries network data.

5. In partial mesh topology, some of the devices are connected to many devices together, but other devices are connected only to one or two devices.

Devices on a network are classified as DTEs or DCEs. DTE stands for data terminal equipment. A DTE can be any device that stores or generates data. When connected to a network, your laptop is a DTE, as are your smartphone, tablet, and fitness tracker. Your own DTEs are under your controls. DCE stands for data communication equipment. These devices control the speed of data over networks, convert signals, check for corrupted data, and route data from its origin to its destination. The most well-known DCEs are routers and modems.

Network protocol is just a set of rules and standarts for encoding and decoding data and guiding data to its destination. Network use different protocols, for instance the internet uses TCP/IP

Transmition control protocol is responsible for breaking data into packets,

While Internet protocol is responsible for addressing packets, that’s why this protocol sends data.

The Internet is international network, which is not controlled, but nowadays it is generally controlled by countries. World Wide Web makes internet popular.

There are some ways to connect to the Internet:

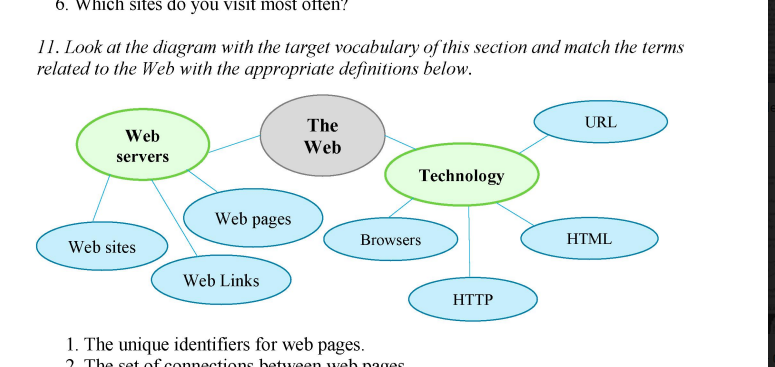
Dial-up: It is much slower than other types. This is a relatively inexpensive service that provides minimal conveniences at a reasonable price.

Digital subscriber line: it plugs into your phone line, it is known as a broad internet connection, that is why it offers much faster speeds.

Cable: uses cable TV connection

3G,4G: it is a wireless internet connection which is often used by smartphones.

WWW is just a system which provides access to interconnected documents, located on different computers, which are connected to the internet



Every process of getting access to the page on the WEB consists of 3 steps

First of all client browser makes request. Then web server sends objects on response to request, as a result client receives displays objects

IOT is a group of devices which are connected and they can discern themselves to other devices

This includes everything from cellphones, coffee makers, washing machiness and almost anything else you can think of. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig. The 10T is a giant network of connected "things' It is big and getting bigger. There are already more connected things than people in the world. Occasionally the benefits of the 10T for business depend on the particular implementation, but the key is that enterprises should have access to more data about their own products and their own internal systems. Manufacturers are adding sensors to the components of their products so that they can transmit back data about how they are performing. Companies can also use the data generated by these sensors to make their systems and their supply chains more efficient, because they will have much more accurate data about what's really going on. The 10T also promises to make our environment — our homes and vehicles smarter, more measurable. IOT can help us to manage public space. Sensors can help us understand

How noisy and pollute our environment. Health checkers will be able to monitor our health 24 hours a day

Problems of IOT: First of all, given that a large amount of data that will run the 10T will be stored in the cloud that why it will be the first target of an informational war. Another problem is that government regulation often takes a long time to catch up with the current state of technology. Finally the real issue is how to increase the ability for people to understand the changes more clearly.

Nowadays The Internet landscape is any device that can be connected to the internet. The list of "smart" devices includes washing machines, robotic vacuum cleaners, door locks, toys, and toasters. Here are several predictions about the future of the IOT.

1. A quick look back shows where 10T devices are going. Consider: in 2016, there were more than 20 billion things connected to the Internet, according to 10T Analytics. Fast-forward to 2020 the market had increased to nearly 50 billion 10T devices.
2. In 2016, the world was introduced to the first "Internet of Things" malware — a set of malicious software that can infect connected devices such as DVRs, security cameras, and more. This malware accessed the devices using default password and usernames. After that it will be possible to create DDOS attack bringing a well known websites and services to a halt for hours.
3. A lot of manufacturers work to get their IoT products to market quickly, so security may be an afterthought. This is where the home router plays a very important role. The router is essentially the entry point of the Internet into your home.

While many of your connected devices cannot be protected, the router has the ability to provide protection at the entry point. A conventional router provides some security, such as password protection, firewalls, and the ability to configure them to only allow certain devices on your network.

Router makers will likely continue to seek new ways to boost security.

1. And the last one is developing 5G networks. 5G — fifthgeneration cellular wireless — promises greater speed and the ability connect more smart devices at the same time. Faster networks mean the data accumulated by your smart devices will be gathered, analysed and managed to a higher degree.