1.1t: Lesson 1: Connectivity

# Connectivity

One of the first things to talk about is how do we connect a computer to another computer or a network? Essentially, we have 3 main types, copper, fibre and wireless.

Yes, the module is about cloud and virtualization, but you still to have some sort of connection to these systems.

1. Copper cable – still a very common way to connect devices, we see this in CAT 5 and CAT 6 cable
2. Optic fibre – now very common for connecting backbones but unusual at the desktop, this is due to the success of the transmission speeds that can be achieved by copper and now wireless.
3. Wireless systems have become increasingly used to connect workstations; it is heavily used in domestic environments but is obviously very popular in a workplace.

# Copper cables

For today’s introduction to networking we will concentrate on the copper cables that connect Local Area Networks (LAN) devices together using the ETHERNET protocol – that is most of the LAN networks in the world today!

Data consists of long sequences of 1s and 0s. These 1s and 0s are represented on the cable by changes in the voltage. It is just like flicking the light switch on and off very quickly – only millions of times a second!

A copper cable is plugged into the NIC (Network Interface Card) on the computer.

The NIC is also called a Network Adaptor or LAN adaptor.

The NIC is connected to the system bus on the PC

It puts those quick voltage changes onto the cable when sending data and interprets them when receiving. In the practical later we’ll be using Wireshark to look at this information, but more on that later.

In modern networking we usually use two types of coper cables, STP and UTP.

We can just consider two types of cable, there are others. The two we are concerned with are call STP and UTP.

# Shielded Twisted Pair

STP stands for Shielded Twisted Pair, the actual copper is shielded to prevent interference, cables like these are of moderate cost but if you’re making your own termination needs care. As you can see from the slide, there is the outer jacket, to give some general protection, then we have the braided shield, this is a wire mesh designed to limit external signal interference, then there is foil shield to add another layer of protection from signal interference and finally the twisted pairs themselves, the actual copper that carries the signals.

# Unshielded Twisted Pair

UTP stands for Unshielded Twisted Pair, the twists help prevent interference. These types of cable are cheap and very common. Again, as you can see in the diagram there is an outer jacket, however as the names implies there is no shielding, we just have the twisted pairs.

If the distance between devices is more than a few feet, permanent cabling is usually installed in trunking. This cabling is connected to sockets at each end and the devices are connected to these with short patch cables. In a workplace environment cabling is normally in a fixed structure, you may have seen this in your own place of work.

# Signals

Let’s have a look at the signals themselves, we’ve already mentioned these rapid changes in electricity in copper cables. These rapid changes represent the 1s and 0s in computer networks, so we can have different voltages in an electric wire  
If we were using optic fibre different intensities of light and if it was wireless, it would be distortions (modulations) of a radio wave.

To understand signals in a copper environment we need to understand a little about electricity. Everything consists of atoms. Atoms consist of a positively charged nucleus and negatively charged electrons.

In some materials (called conductors), the electrons are very loosely attached and can be attracted away. This leaves the atom unbalanced and it tries to attract electrons from somewhere else.  This gives rise to electric current.

Copper has one single electron in its outer shell, this makes copper susceptible to having this electron attracted away fairly easily, so it makes copper an ideal conductor.

I should add that silver and gold are actually better conductors than copper, but if we had silver and gold cables connecting our devices, I’m not sure how long they’d be there before someone stole them!

# Electricity

There are three components of electricity we should be aware of if we’re going to understand signals, they are:

1. Voltage – this is the force pushing the electrons along – it is measured in volts
2. Current – this is the flow of electrons through a conductor – measured in amps
3. Resistance – this is the ability of a material to slow the flow of electrons down – it is measured in ohms.

Electric current flows in closed loops called circuits.

Current will flow when there is a complete circuit and a voltage is applied, the electrons flow from the negative terminal to the positive one when the switch is closed. If this flow is controlled and both ends understand what a 1 or a 0 ‘looks like’ then we have signals.

Signals take a measurable time to travel through a medium:

* 1.9 - 2.4 x 108 m/s in copper
* 2.0 x 108 m/s in glass

The time taken to the end and back is called the round-trip time (RTT)

Delay in the system due to propagation and equipment delay is called “Latency”

# Encoding

Let’s put the information in to the real context of network signals, for digital encoding of digital information, we have to have an agreement by both sides what represents a 1 or a 0, we call these protocols.

One protocol is Non return level to zero, or NRZ-L. As you can see in the slide typically, negative voltage = 1 positive voltage = 0. This protocol would be used for very short connection as it’s unreliable, , Problem with NRZ is no clocking, our receiving end could easily fall out of synchronisation due to delay.

An alternative is Manchester encoding, Manchester encoding also known as biphase. As you can see in the slide, it transmits the clock by sending a mid-transition change every bit time.

Direction of mid-bit transition shows 0 or 1. This system is used in Ethernet.

So far today we’ve discussed cables and signals, this really only deals with the physical connection in a network. I’m sure you’ve guessed there is much more than just sending a signal down a cable.

# Protocols

I mentioned protocols a little earlier, it’s a word you’ll hear lot in computing, particularly in networking.

Protocols are agreements to do things in a particular way; in communication, there are lots of things that both sides need to agree upon.

So, what are some functions of protocols, the things we need to agree upon?

* What medium to use, Copper, fibre, wireless?
* How to represent a bit in the medium, does a positive represent a 1 or does it represent a 0?
* What will an address look like?
* How will we know when the message has finished?
* Will we use encryption?
* And there are many other things to consider…

To overcome these questions we use protocols, we do this so that the receiving node knows exactly how to deal with a message, the sender attaches that information to the front of each part of the message that it sends.

# Protocol data unit

This information is called the header. Header and data together are called a PROTOCOL DATA UNIT or PDU.

Let’s put this in everyday terms, if I want to send a letter to someone. I write the letter, I place in inside an envelope, I write the receiving address on the front and I write my address, the return address on the back.

I have encapsulated the data, my letter, inside an address header, the envelope, with both sender and recipient included. In a network packet we will include a destination address, the senders address, something to indicate the start of the message, the message (data) and something to say this is the end of the message.

The source host breaks a long message into individual pieces or frames that meet both the minimum and maximum size requirements.

Each frame will also have its own addressing information.

At the receiving host, the pieces are reconstructed to be processed and interpreted.

The role of network protocols is to agree on how the message is formatted or structured.

The process by which networking devices share information about pathways with other networks.

How and when error and system messages are passed between devices.

# Next video

In the next video we will discuss the models used for transmission in networks.