Name: Gokhan

Surname: Dilek

SCADA REPORT #2

TERM 1, SEMESTER 1, 2013

Lecturer: Lubo Dimitrov

Table of Contents

1- What is SCADA?

SCADA is an acronym for Supervisory Control and Data Acquisition is used to control applications remotely. It can simplify complicated systems to reduce the labour costs.

Any SCADA system has two elements:

- The application (water pump, bridge, trains)
- The network (set of devices that control and monitor the application)

The network plays a critical role in SCADA systems. For example, if there is a power generator in Kalgoorlie located 600+ kms from Perth, the only way to control this system is to use networked devices to be able to collect data. Satellite communication systems, the internet, fibre cables or any combinations of these can be used to control the power generator however, if there is an issue with the network, it would not be possible to receive any data from the generator.

SCADA systems can control factories, water systems, lighting and entry systems. It can also monitor transport systems as well as traffic lights. [1]

SCADA system has four functions:

1. Sensors and control relays
2. RTUs
3. Data presentation
4. Control

Since SCADA systems can control the whole application, security may be an issue.

Old SCADA systems used non-internet connections however, with the advent of technology to make communications and support easier and faster, SCADA systems now use TCP/IP technologies which make these systems vulnerable to attacks.

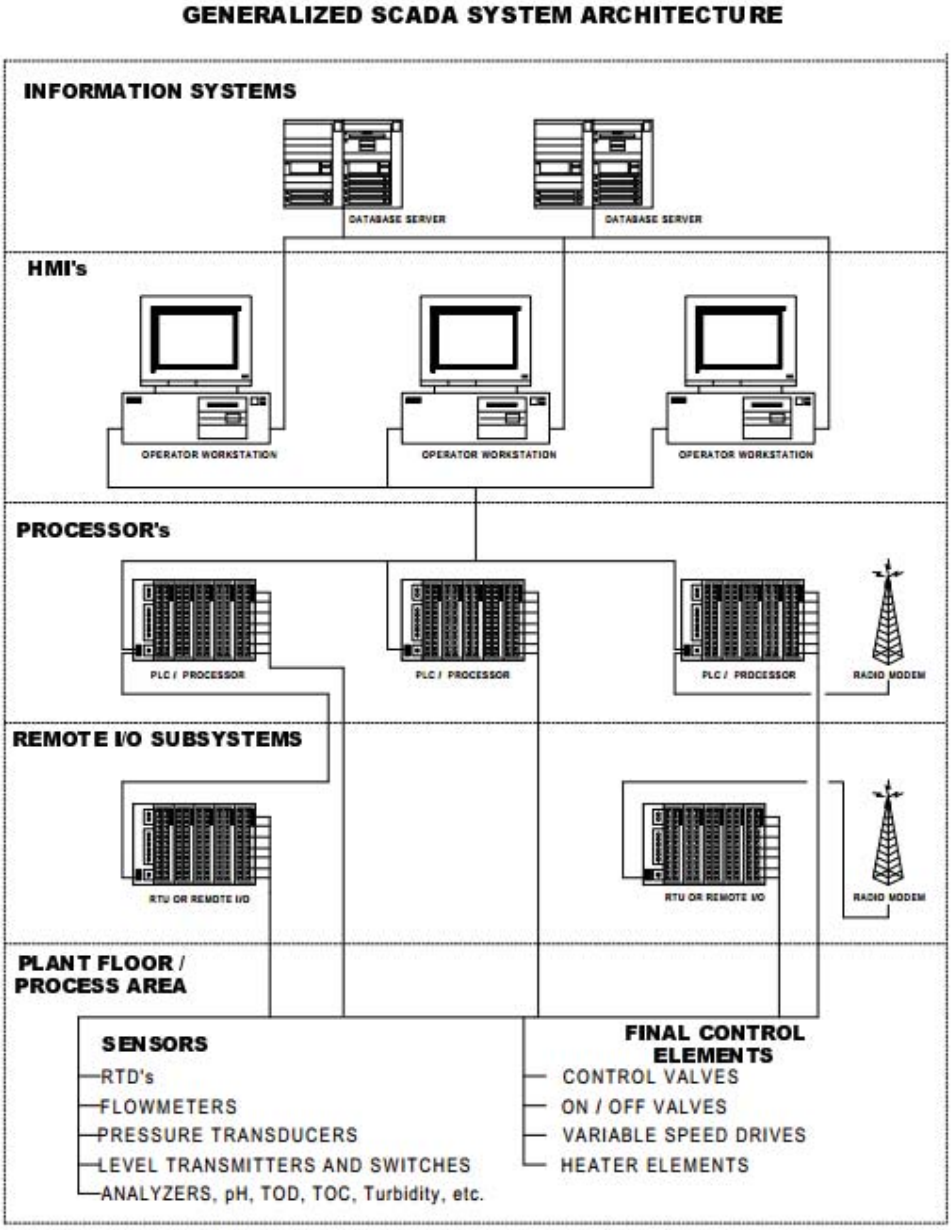


Figure 1 Figure 1 demonstrates the general architecture of a SCADA system [2]

2- What is noise?

Noise is unwanted signals in electrical circuits. It can be reduced by shielding, proper earthing, twisting of the signals in conductors and the separation from the noise source. There are two types of noise:

2.1 Internal Noise

Internal noises are caused by the elements within the circuitry. Internal noises can also be divided into four:

2.1.1 Thermal noise

Thermal noise is caused by random movements of electrons at non-zero temperatures. Thermal noise is only depending on the bandwidth (frequency) and temperature.

According to Neil J. Boucher very small voltages can be lost in the thermal noise. [3]

$$E_{\mathrm{RMS}} = \sqrt{(4 \times 10^{6} \times 1.38 \times 10^{-23} \times 290 \times 10^{6})}$$
$$= 126 \text{ microvolts!}$$

Thermal noise can be reduced if the temperature can be kept closer to zero.

2.1.2 Imperfections

Every component can be designed in a different way by different manufacturers. This could create unexpected noise in circuits. Another reason that may create imperfection is that the contacts between the PCB board and the components.

For example, if the resistor or the microcontroller is not soldered properly, it may create noise. The best way to defend this type of noise is to implement good connectors and interfaces. [4]

2.1.3 Stray signals from oscillators and amplifiers

Just like every other device, oscillators and amplifiers produce noise. This is because they consist of multiple parts.

Amplifiers use transistors to create gain therefore if the emitter current of the transistor is increased, the noise will also be increased. [4] A low noise amplifier needs to have a low NF and a large gain. [5]

On the other hand, oscillators can also result in noise which affects the electrical devices. This is due to the frequencies that are closer to oscillator frequency.

2.1.4 Intermodulation of stray low RF produced by internal circuits

Low RF pulses can affect the internal circuitry. Components like microcontrollers and transistors which need very low voltage to operate, RF can disturb the function of these.

Department of Electrical and Computer Engineering University of Maryland has made an experiment that demonstrates that a simple digital counter circuit can be distracted by low RF signals.

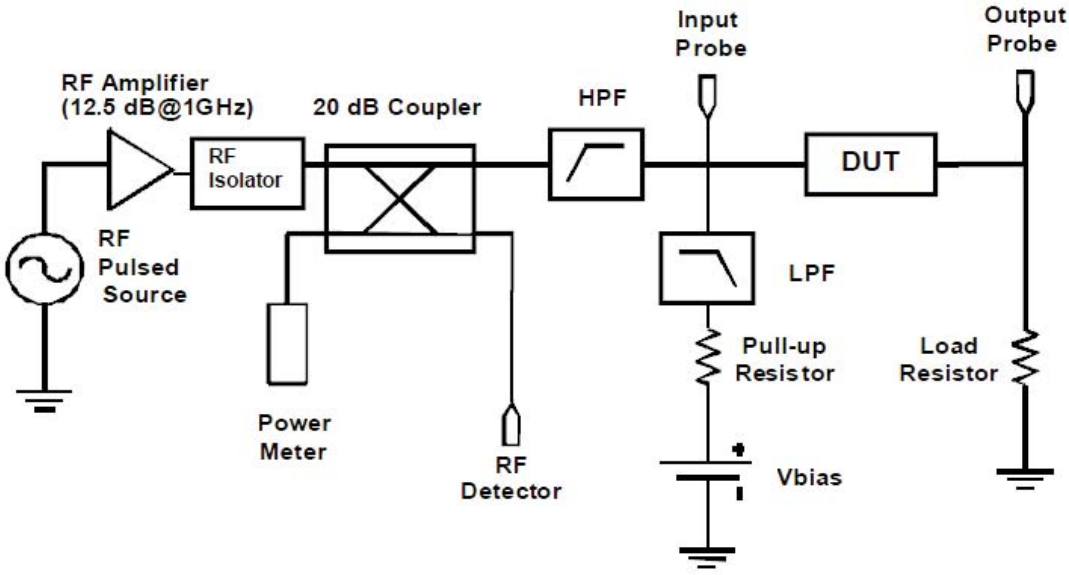


Figure 2 Experimental Setup

This goal of this experiment is to find out the sensitivity level of the counter so that the behaviour of the circuit can be observed. [7]

2.2 External Noise

2.2.1 Natural Origins

2.2.1.1 Electrical Storms

Electrical storms are caused by electrically charged clouds in the sky. This creates electrical field which then cause to leak into the circuitry. [8]

2.2.1.2 Galactic Noise

Galactic noise is known as “Cosmic Noise”exists since the big bang. It also affects electrical circuits. [9]

2.2.1.3 Quantum Noise

Quantum physics states that noise will always exist even in vacuum at zero temperature. [10]

2.2.2 Electromagnetic Interference (EMI)

Electromagnetic interference short for (EMI) is a kind of noise that affects electrical devices due to electromagnetic forces. [11] Every device emits (EMI) especially communication devices.

EMI an affect AM radios as well as smartphones, FM radios and TVs.

There are two types of EMI:

1- Man-Mad EMI

Electromagnetic radiation can be caused by other electrical circuits especially high current electrical devices.

2- Naturally occurring EMI

This type of noise can be caused by many sources like background noise and quantum noise and electrical storms which are explained before.

Australian EMI standards

In Australia, it is manufacturers' responsibility to produce products that do not interfere with other electrical devices.

EMI is important to consider because a smartphone may interfere with your smart TV if they are not designed properly. [12]

How to detect an EMI signal?

A simple way to detect EMI signal is to use an AM radio. Move the AM radio closer to the electrical device or circuit and turn on the volume. A constant voice can be heard on the radio when EMI signals exist. [13]

2.2.3 Radio Frequency Interference (RFI)

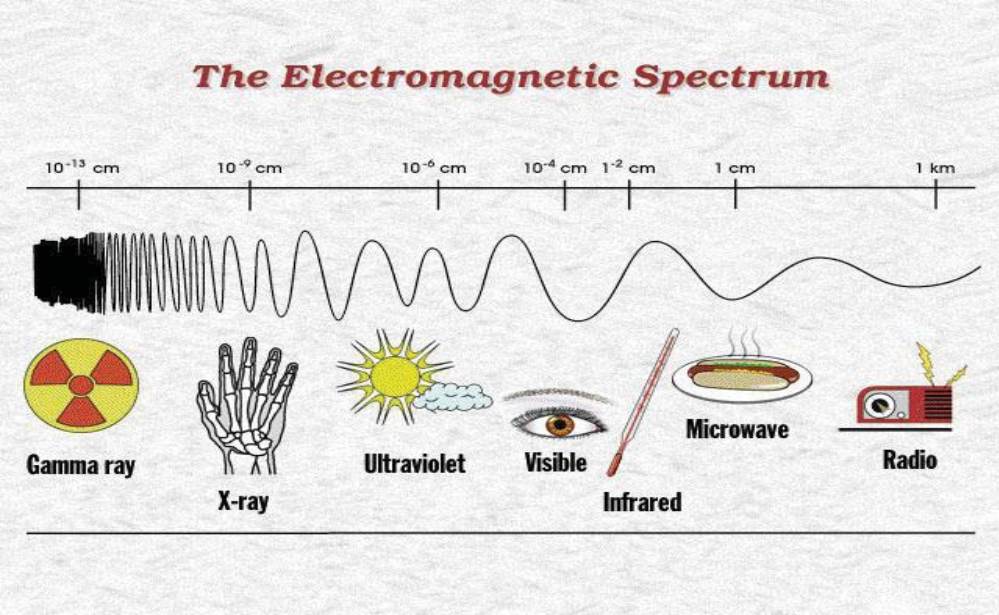


Figure 3

Electromagnetic spectrum: *http://3enscience.files.wordpress.com/2010/06/em-spectrum21.jpg*

Radio frequency is an invisible electromagnetic wave. Radio frequency waves are signals. That all means RF signals must also be based on alternating current. When EMI is in the radio frequency range that is called RFI.

Radio frequency interferences occur on the radio part of the electromagnetic spectrum. RF signals acts as a wave therefore the more distance it propagates, the more noise it may be subject to.

Absorption:

Most objects will absorb RF signals. Water can be a big problem for RF signals. For example, average adult body has 50 to 60 % water. It can absorb most RF signals causing interference for these signals.[14]

Multiple waves:

Multiple waves are created due to refraction and reflection of the RF signals. When an RF signal arrives at the receiving antenna from more than one propagation route is called multipath.[15]

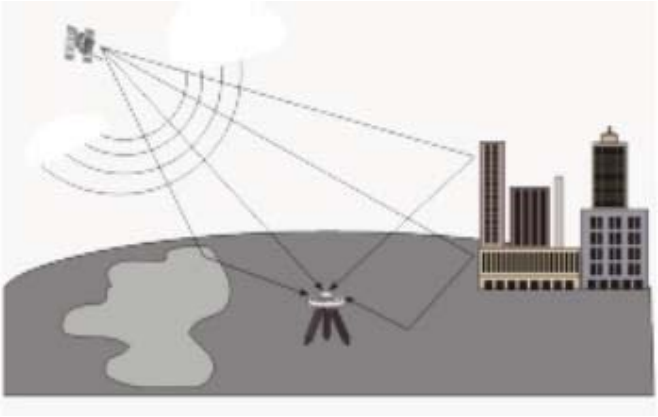


Figure 4

Multipath is shown in figure 4, the source sends the RF signals. The RF signals then travels and hits the buildings as well as the earth. Multiple waves are created. The receiver then gets the waves but it gets confused as to which one is the right message.

Multiple waves can also be produced due to density of the air and the temperature. If the waves are travelling long distances, it needs to be considered to reduce the noise created.

To prevent RF signals, the best gadget is the ability to adapt. That means that if there is an older device that is causing trouble, upgrade it with newer ones. [16]

Multipath may cause downfade, upfade, nulling, and data corruption.[17]

2.2.4 Cross Talk

Cross talk is caused by undesired signals from other electrical circuitry. This could be caused by capacitive, inductive or conductive coupling from another circuit.[19]

It is a known fact that if a current flows through a conductor, it will create a magnetic field. Figure 5 below demonstrates it with blue circles around the wire.

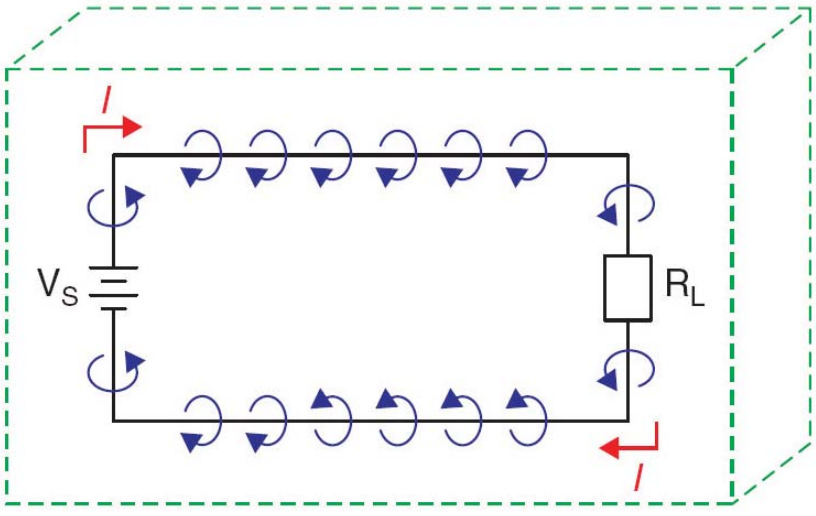
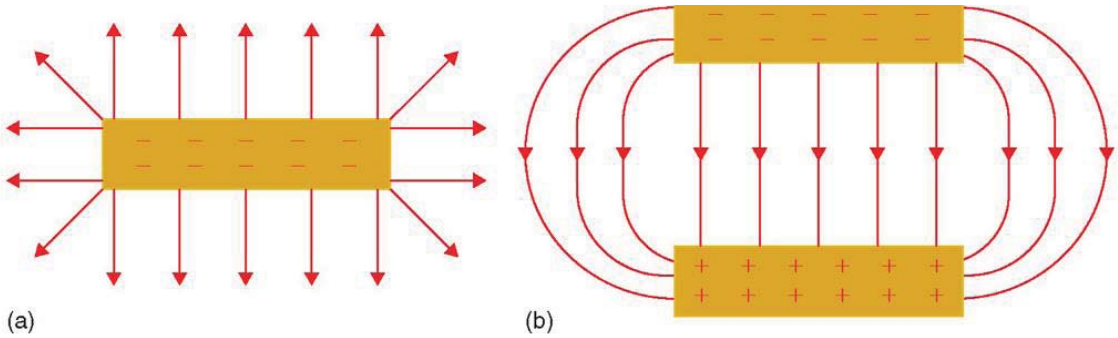
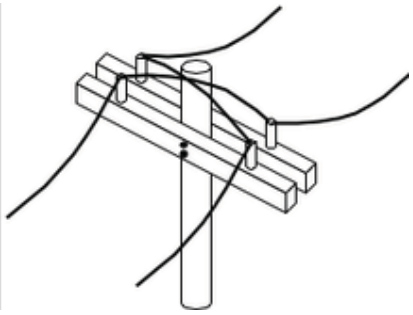


Figure 5





Another example is wire transposition, in the early days of 1900s, the growing energy and communication needs brought interference with it. Figure 6 shows wire transposition to cancel out the interference.

Figure 6 Wire Transposition

3- Cables

Cable is a connector system to join both ends together. This system includes but not limited to shielding, insulation, conductors, terminators and connectors.

3.1 General Cable Characteristics

It is important to know what kind of cables is needed for a particular application. Applications can vary from ceiling installation to across ocean to other geo locations installations.

For example, if there is a critical chemical plant that is very sensitive to high voltages. High voltages or high current must be avoided using industry standard cables.[20]

Another example would be a big induction motor. It produces a great amount of power hence it creates an EMI being a threat to the surrounding devices. Using a fibre optic cable could solve the problem because fibre optic cables are not affected by external interference.

Australian standard for cables and cable installations has also been developed by Communication Alliance under the AustralianCommunications Authority (ACA) and the Australian Communications IndustryForum (ACIF).

It demonstrates the proper earthing methods, combination of electrical cables in a proper way as well as the correct connection to avoid confusion. [21]

3.1.1 Logical Cable Characteristics

Cable Type	Data Transfer	Frequency	Noise	Bandwidth	Data Transmission	Capacity	Security	Distance	Weight
Fiber Optic	1	1	0	Higher	Light	High	Almost impossible to tapping attacks	60+ km	Lighter
Coaxial Cables	1	1	1	0	Electrical Signals	0	0	100 m	1
Twisted Pair	0	0	1	0	Electrical Signals	0	0	100m	1
Shielded Twisted Pair	1	1	0	1	Electrical Signals	0	0	100+m	1

1= Higher

0= Lower

3.1.2 Physical Cable Characteristics

ISO/IEC 11801

International organization for Standardisation has provided different classes for a wide range of electrical applications.

	Cable characteristics	Units	Requirements
1.1	Diameter of conductor[a]	mm	0,4 to 0,8
1.2	Diameter over-insulated conductor[b]	mm	≤1,6
1.3	Outer diameter of backbone cable[c]	mm	≤90
1.4	Temperature range without mechanical or electrical degradation	°C	installation: 0 to +50 operation: –20 to +60
1.5	Minimum bending radius (after installation)[d]	25 mm for four-pair cables with a diameter up to 6 mm 50 mm for four-pair cables with a diameter over 6 mm	

a Conductor diameters below 0,5 mm and above 0,65 mm may not be compatible with all connecting hardware.
b Diameters over the insulated conductor up to 1,7 mm may be used if they meet all other performance requirements. These cables may not be compatible with all connecting hardware.
c Should be minimised to make best use of duct and cross-connect capacity (see Clause 10).
d For minimum bending radius requirements during installation refer to manufacturer's recommendations.

Figure 7 Mechanical Requirements of cables [22]

Cable Classes: [23]

Twisted Pair

- Class A: up to 100 kHz using elements category 1
- Class B: up to 1 MHz using elements category 2
- Class C: up to 16 MHz using elements category 3
- Class D: up to 100 MHz using elements category 5e
- Class E: up to 250 MHz using elements category 6

- Class E_A: up to 500 MHz using elements category 6_A (Amendment 1 and 2 to ISO/IEC 11801, 2nd Ed.)
- Class F: up to 600 MHz using elements category 7
- Class F_A: up to 1000 MHz using elements category 7_A (Amendment 1 and 2 to ISO/IEC 11801, 2nd Ed.)

Fibre Optic Cables

- OM1: Multimode fiber type 62.5 µm core; minimum modal bandwidth of 200 MHz*km at 850 nm
- OM2: Multimode fiber type 50 µm core; minimum modal bandwidth of 500 MHz*km at 850 nm
- OM3: Multimode fiber type 50 µm core; minimum modal bandwidth of 2000 MHz*km at 850 nm
- OM4: Multimode fiber type 50 µm core; minimum modal bandwidth of 4700 MHz*km at 850 nm
- OS1: Singlemode fiber type 1db/km attenuation

3.1.3 Real World Example

Olex is a cable design and manufacturing company in Australia that provides services for commercial applications. Figure 6 demonstrates that they have classified different cables for different applications. This makes entrepreneurs life easier to implement cabling systems. [24]

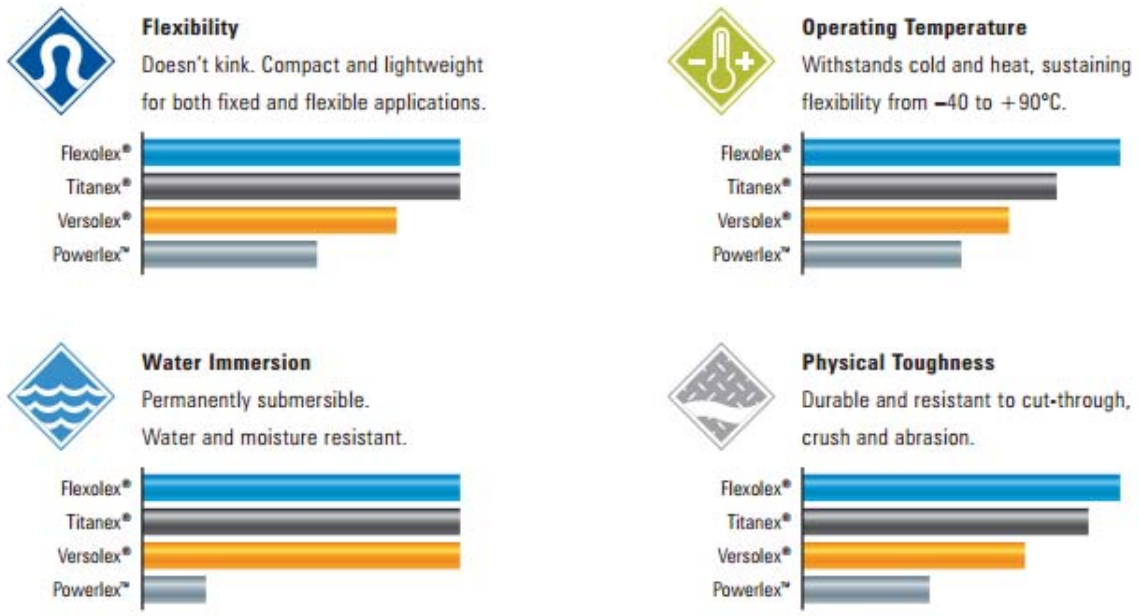


Figure 8 Cable types depending on the external cause

To sum up, cable properties depend on the following elements:

- **Transmission speeds:** 100Mbps or 10Gbps?
- **Distance:** This is a crucial factor for some cases. Twisted pair should have a maximum length of 100 meters
- **Duplex:** Half duplex (coaxial cabe) or full duplex (fiber optic or twisted pair).
- **Noise and security:** Fibre optic cables are much when better in terms of shielding compared to those that use copper.
- **Frequency:** Cat 5e cable=100Mhz while Cat6 is 250MHz.
- **External factors:** For what application will the cables be used?

3.2 Twisted Pair Cables

The demand for data transfer has changed the cabling industry. Not only the data transfer but the early connection standards like rs232 did not support higher speeds.[25]

Twisted pair cables reduce the overall network costs.

3.2.1 UTP – Unshielded Twisted Pair

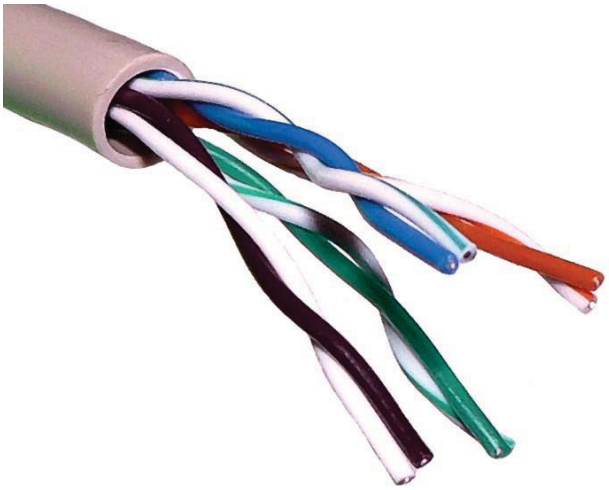


Figure 9

Source: http://upload.wikimedia.org/wikipedia/commons/c/cb/UTP_cable.jpg

The most common cable that is used to infrastructure a network is UTP – Unshielded Twisted Pair. For example Category 5 (Cat 5 for short) and CAT6 cables are commonly used due to its low cost and ease of installation.

3.2.2 STP – Shielded Twisted-Pair

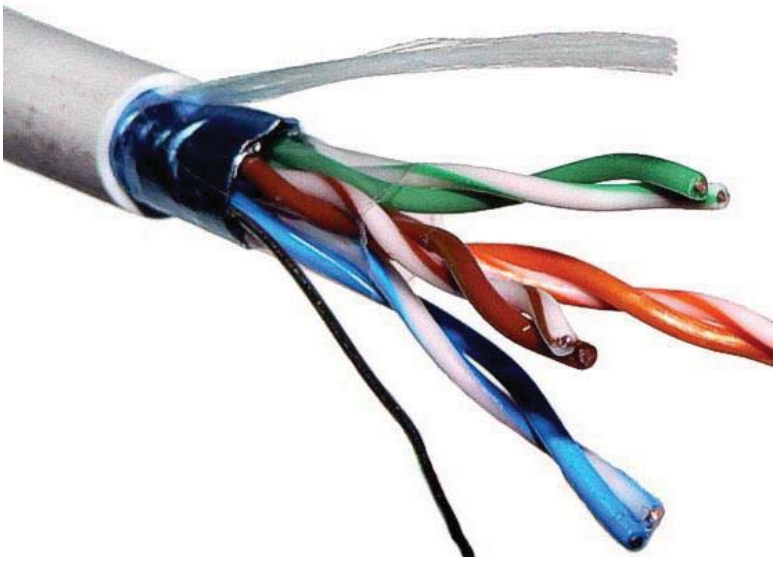


Figure 10

Source: http://packetbyte.com/Images/TwistedPairCabling/STP-L.jpg

Shielded Twisted pair cables protect the system from electromagnetic interferences (EMI).

3.2.3 Screened Twisted-Pair

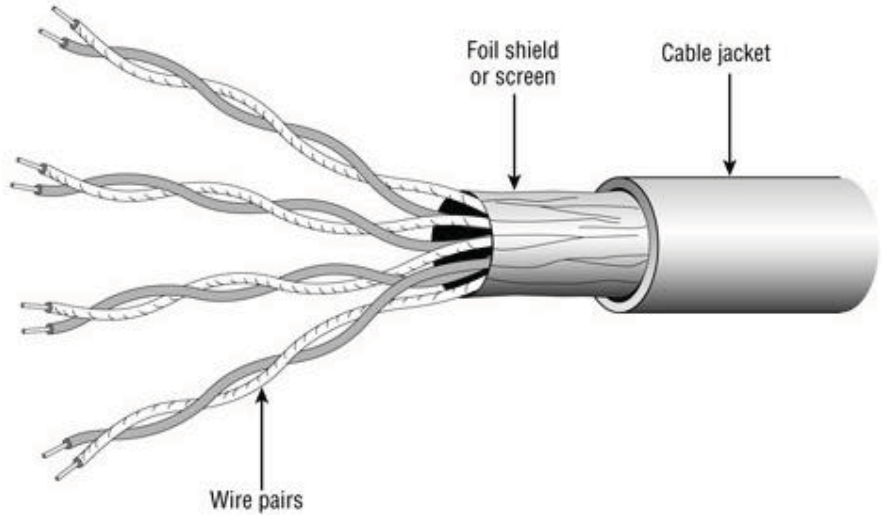


Figure 11

Source: http://www.amazon.com/exec/obidos/ASIN/0470477075/books24x7com

3.2.4 Screened Shielded Twisted-Pair

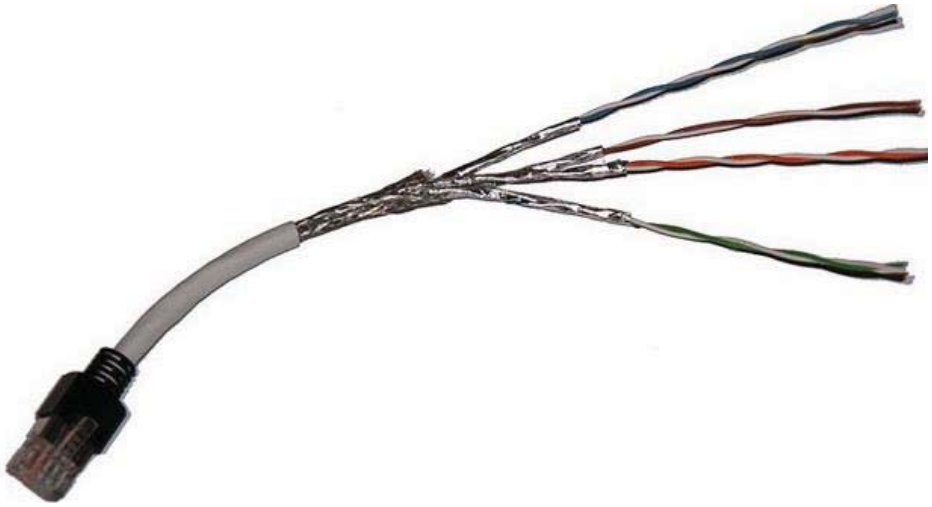


Figure 12

Source: http://packetbyte.com/Images/TwistedPairCabling/S-Twisted%20Pair-L.jpg

3.3- Fibre Optic Cables

Fibre optic cables use a technology to transport light from one place to another. This technology is needed to carry data signals (1s and 0s) across continents up to 500+ kms.[26] This has changed the data communications significantly.

To understand this technology, light needs to be understood first.

3.3.1 What is light?

Light cannot be described as a single term. It has a particle which is called photon. It also acts as a wave. Light can bend, reflect and refract. Speed of light is 299,792,458 m/s at vacuum. [28]

3.3.2 Comparison between copper and fibre optic cables [40]

Cable	Material	Weather	Speed	Bandwidth	Data Transmission	Capacity	Security	Distance	Weight
Fiber Optic	Glass and other elements	Effected very little	Faster up 10.000 MBps	Higher	Light	High	Almost impossible to tapping attacks	60+ km	Lighter
Copper	Coax wire	Easily get affected	Average	Lower	Electrical Signals	Low	Vulnerable to tapping attacks	100 m	Heavy

3.3.3 Mode of Operation

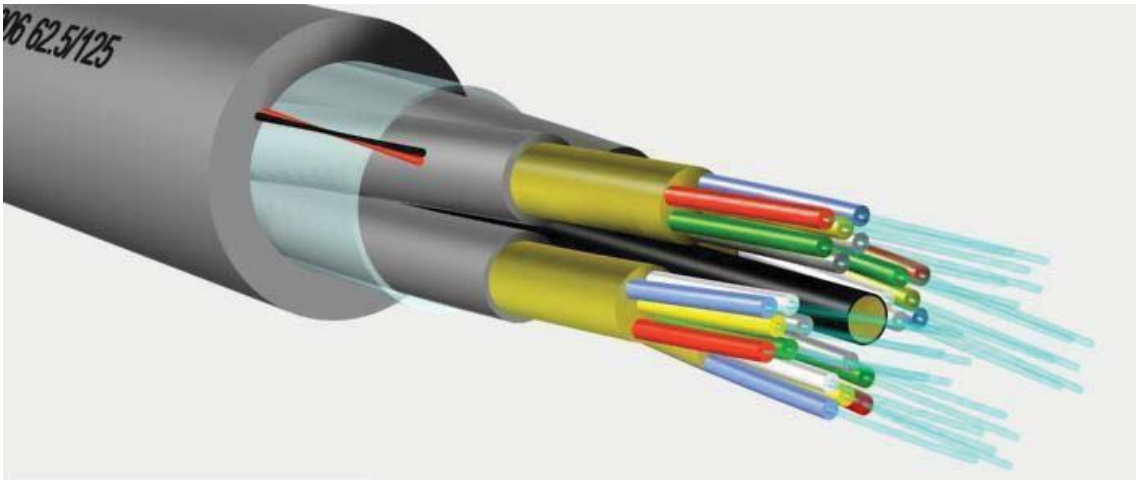


Figure 13

Figure 13 demonstrates the cross section of a fibre optic cable. As it can be seen, the fibre consists of a core surrounded by a cladding layer. To confine the optical signal in the core, the refractive index of the core must be greater than that of the cladding

($n_{core} > n_{cladding}$).[27]

Fibre optic cable transfer data slower than the speed of light due the glass structure. The light can either be LED(light emitting diode) or ILD (injection laser diode) . The light can be amplified using optical amplifier. [29]

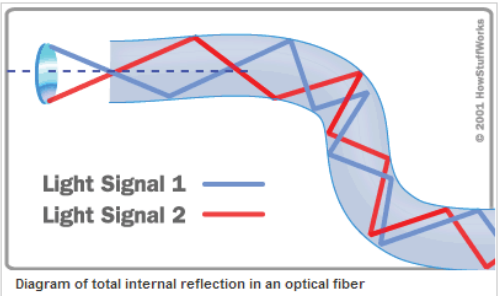


Figure 14 ***How two sources of light travels inside the fibre optic cable (Multimode fiber optic cable)***

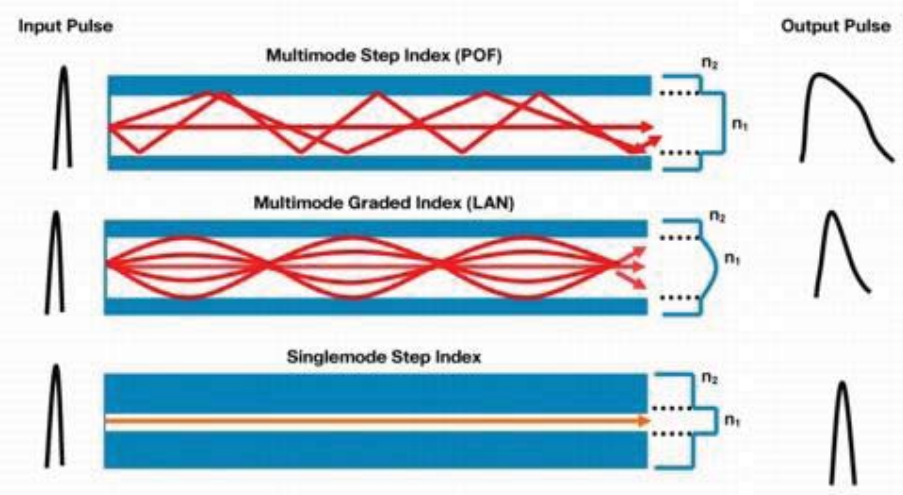


Figure 15 **Single light source propagates through the fibre optic cable (Single Mode fiber optic cable)**

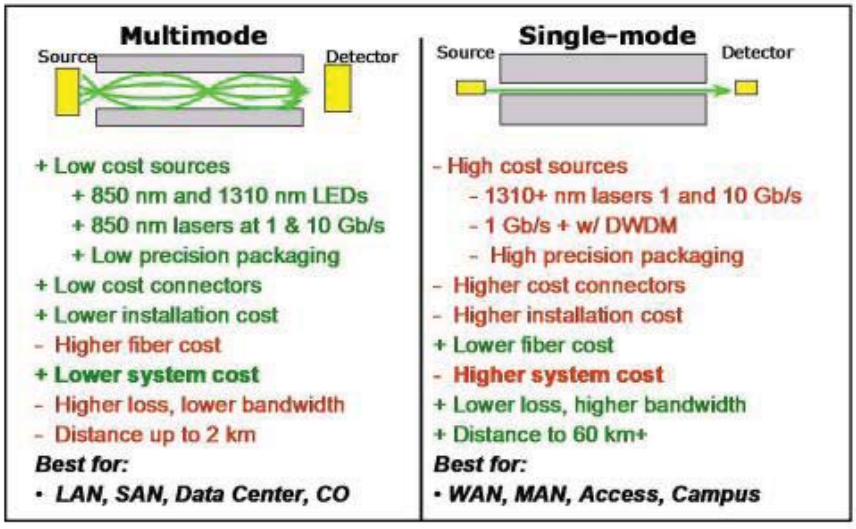


Figure 16 ***Multimode VS Single (Mono) Mode Fiber Optic Cables***

Single light source based fibre optic cable uses expensive light sources therefore they are better than multimode fibre optic cables in terms of bandwidth and data transmission distance(30 times more than multimode)[30]

3.3.4 Current Applications and Future Trends

Current applications:

Unity Cable System: http://en.wikipedia.org/wiki/Unity_(cable_system)

Transatlantic communication cable:
http://en.wikipedia.org/wiki/Transatlantic_communications_cable

Submarine Communication Cable:

http://en.wikipedia.org/wiki/Submarine_communications_cable

Google Fibre: http://fiber.google.com/about/

Google Fibre lets you broadcast HD TV as well as the internet at the speed of light.

Current applications of fibre optic cable are not limited to data communication. There are other uses of fibre optic applications such as Surgery and Dentistry, Lighting and Decorations, Mechanical Inspections, Military and Space Applications and Automotive Industry [32]

Future Trends:

Power over fibre solutions:

It is now possible to transfer very little currents by converting it to light then converting back to current. https://share.sandia.gov/news/resources/news_releases/pof/

Optical Circuit Design:

The problem with fibre optic is that it needs to be converted back to electrical signals to work with current circuit design. Optical circuit design allows http://en.wikipedia.org/wiki/Photonic_integrated_circuit

3.3.5 Security

Even though the security level is higher when it comes to fibre optic technologies, there are still some concerns.

Fibre technology is based on light blinks. If an attacker is planning to read this light blinks, it would be possible to decode the packets that are sent by the users.[34]

3.3.5.1 Vulnerabilities

The cable can be bent allowing light to escape. Attackers then use optical detectors to receive the information. This can be detected easily using attenuation monitoring systems. Over distance, devices lose signals. This loss of signal strength is called attenuation and is typically measured in decibels. [36]

The security problems do not end here. There is a method which does not require any physical connection with the cable. This method is called “non-touching” tempering.

3.3.5.2 Fibre Optic Encryption

As explained before, 100 % security of a system is impossible. This also applies to fibre optic cable technology. It can easily be read by attacker by following various kinds of methods that are explained above.

The key point here is that the data that has been stolen can only mean something if it can be interpreted. When the data is encrypted before the transmission, it can increase the

integrity of the data. Even if the attacker steals the data attacking the fibre connections, it would not make any sense when read.

3.3.6 Health

Just like laser beams, fibre optics has strong light that may cause blindness if looked perpendicularly.

You should never assume that there is no light. No light may also mean there is no data that is being transferred at the time. That does not mean that you will not see any light when you look into it. [37]

Steps to inspect a fibre optic cable:

1. Turn off the equipment (switches, computers etc.)
2. Disconnect the fibre cable from the network
3. Start inspecting the cable using fibre optic cable testers.

3.3.7 Hands on Experience

I used to work as an IT technician for a private school between the years 2010 and 2012. They constructed a new block in 2011 which had a distance more than 100 meters from the main server room.

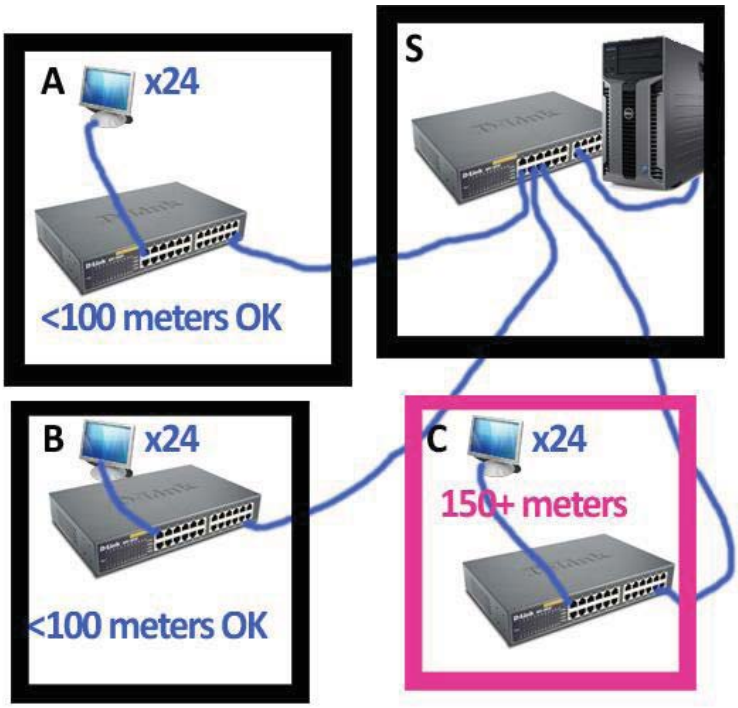


Figure 15

As it can be seen in figure 2, (A) and (B) blocks did not have a problem. However, the newly constructed building (C) could not use copper cable to link due to the distance between the main server room and the C block.

The existing switch did not support to uplink using fibre optic cable so I have required them to change the main switch which was located in the server room (S). I have also bought a transceiver on ebay to complete the set up. (Qualified LAN cable installer came in and finalised the fibre optic cable installation)

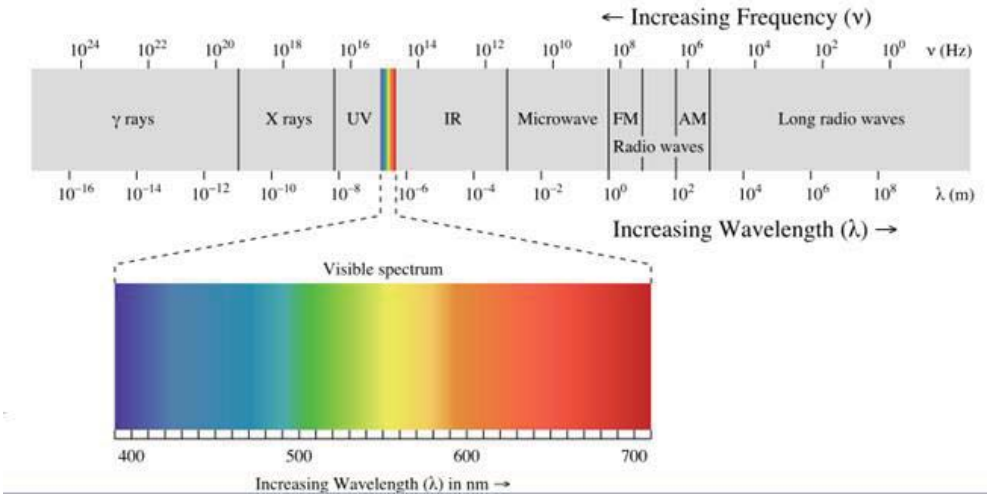
With this system, (C) block was able to connect to schools internal network without any problem.

3.3.8 Interesting Facts

Sharks have attacked the fibre optic cables in the past. It was a test fibre optic cable that was laid by AT&T in 1985. [38]

After further research, it has been found that sharks have electroreceptor organs called Ampullae of Lorenzini. These organs can sense the electromagnetic forces.

Visible light is an electromagnetic wave that was found by Sharks. Sharks thought that it was a living creature therefore they have attacked the fibre optic cables.[39]



4 - Network

A network is a system of electrical devices that are linked together by a transmission protocol.

4.1 Network Components

Node

A node is an electrical device that can communicate on the network. Examples include but not limited to printers, computers, phones, laptops, network hard drives.

Transmission Media

Data needs to be transferred to electrical devices (nodes) in order to enable communication between the devices. This can be done using a cable or radio transmission also called wireless (wifi).

Intranetwork Devices

Instead of connecting the nodes together directly, a third party device is used to connect all the nodes together. A switch or a hub can be one of the examples of intranetwork devices.

-Unmanaged switches and Managed switches [41]

Figure 16 below is an example of a switch that is very simple. It is not costly therefore it is suitable for home users as well as small business owners.

Figure 16 Unmanaged Switch

Figure 17 Dell Managed Switch

However, a managed switch is more intelligent. Big corporations and companies use managed switches. It can create virtual network to connect devices to other large networks. It can offer traffic prioritization and filtering. A managed switch can be controlled via SNMP user interface. Figure 17 shows a managed switch from DELL which costs up to $2500. Network administrators can perform advanced administration on these switches using a familiar and intuitive command-line interface (CLI) or an easy-to-use, web-based graphical user interface (GUI). [42]

Other feautures include:

• Monitor network traffic using sFlow or Simple Network Management Protocol (SNMP) capabilities. • Help ensure network security with features such as access control lists (ACLs), 802.1x and denial-of-service (DoS) attack prevention.

-Hubs

Compared to switches hubs are dummy devices that connect nodes directly to each other.

Backbones

Backbones are links between larger networks. They usually need to be faster to carry so much data.

Protocol

Protocol is a system that has rules and formats for network devices. If there is no protocol, the devices may not be able to talk to each other. Protocols include authentication, signalling and collision correction and detection. [43]

Some real world protocols include SNMP and Arcnet.

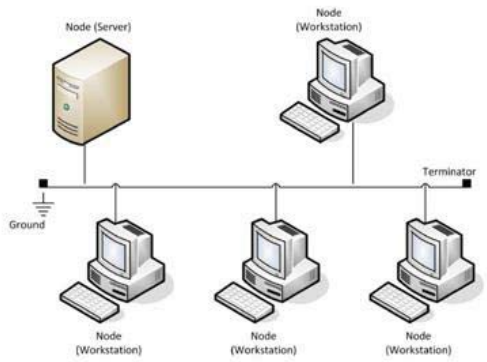
4.2 Network Topologies [44]

4.2.1 Physical Topologies

Physical topology describes the actual appearance or layout of the network. It can also refer to as wiring of the particular network.

4.2.1.1 Bus Topology:

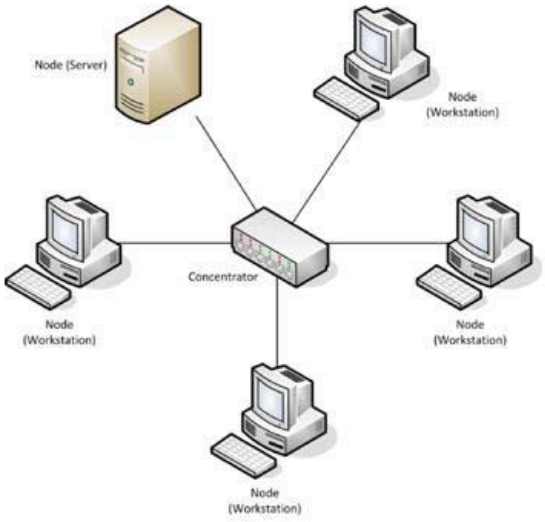
In this topology, devices are connected on a single transmission media.



Bus topology simulation: https://www.youtube.com/watch?v=r-aMKWr-NbM

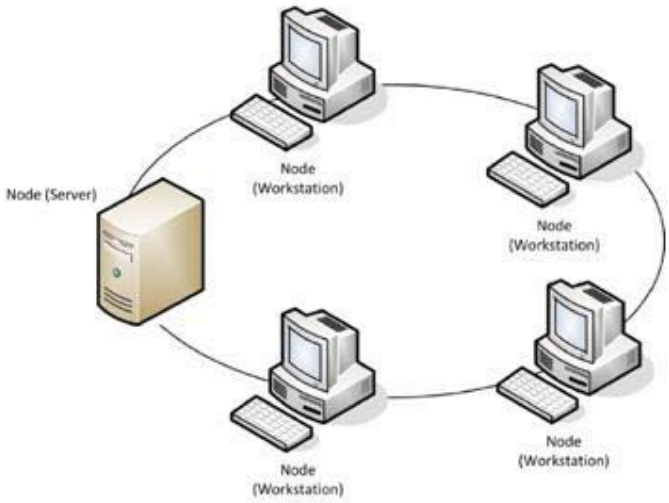
4.2.1.2 Star Topology

In a star topology, each node is connected to a central point. This can be a switch or a server.



4.2.1.3 Ring Topology

A ring topology enables the data to be sent from one node to another until it reaches its correct destination.



4.2.1.4 Mesh Topology

This topology links every node with each other. The idea behind this is, if one node fails to communicate to another node via a transmission way. It can use an alternative route to find its destination.

The number of connections depends on the nodes:

C= Number of connections

N= Nodes

$$\mathbf{C} = \frac{\mathbf{n(n-1)}}{\mathbf{2}}$$

Figure 18 below demonstrates the mesh topology also known as fully connected network. [45]

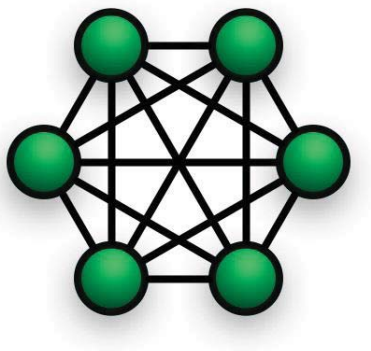


Figure 18 fully connected nodes

4.2.1.5 Advantages and Disadvantages [46]

Topology Type	Advantages	Disadvantages
Bus	➢ Simple to implement ➢ Inexpensive ➢ Easy to add/remove devices	❖ Communication may be a problem ❖ Collision can occur easily ❖ Security problem ❖ Not easy to troubleshoot ❖ Cable size is limited ❖ Limited number of nodes
Star	➢ Easy to add/remove devices ➢ Monitoring traffic is easy ➢ Troubleshooting is easy	❖ Central device is critical ❖ Central device is usually expensive ❖ More cables are needed ❖ Faults do not affect other devices.
Ring	➢ A central device is not required ➢ Less cabling ➢ Same priority for each node to talk	❖ Harder to add/remove devices ❖ One way communication either clock or anti-clock wise. ❖ Failure of a single node can cause a network failure

Mesh	➢ Data can be transferred to each node simultaneously ➢ If one of the nodes fail, there is an alternative route to take ➢ Adding/removing nodes do not disrupt the network	❖ Security problem because each node is connected to every node ❖ Expensive ❖ Troubleshooting and administration is very hard

4.2.2 Logical Topologies

Each node on the network sends data to other nodes. In order to police this data logical topologies are put in place. This enables how electrical devices can gain access to the network. This is also called media (medium) access methods.

4.2.2.1 Deterministic Methods

Token Passing:

Tokens are 3 bytes of data frame that move around the network. Nodes can only start transmitting data once this token is received. Nodes wait for the token to broadcast.[47]

Token passing is standardised with protocol IEEE 802.5.

Log of events

1. The sending node creates a token followed by the actual data
2. Token starts to travel around the network
3. Token touches every node on the network
4. Every node reads the header file of the token
5. If the token is not for them, they ignore the message
6. Finally an intended node discovers the header and copies the message
7. The sender then receives the token back to see if the message has been sent correctly.
8. It then sends out the token back to the network for other nodes to use.

Master and Slave:

Master/Slave method is a simple model to send data to other nodes known as slaves in unidirectional way. One of the examples would be a sensor or a closed-source system. [48]

4.2.2.2 Probabilistic (Random) Methods

CSMA/CD:

CS (Carrier Sense) listens to the transmission line and finds out if any node is using the line. If no node is using the transmission line, it then starts send the message to the desired node. If someone is using the line, it waits random amount of time and tries again.

MA (Multiple Access) refers to multiple nodes using the transmission line. Nodes share the capacity of the transmission line. [49]

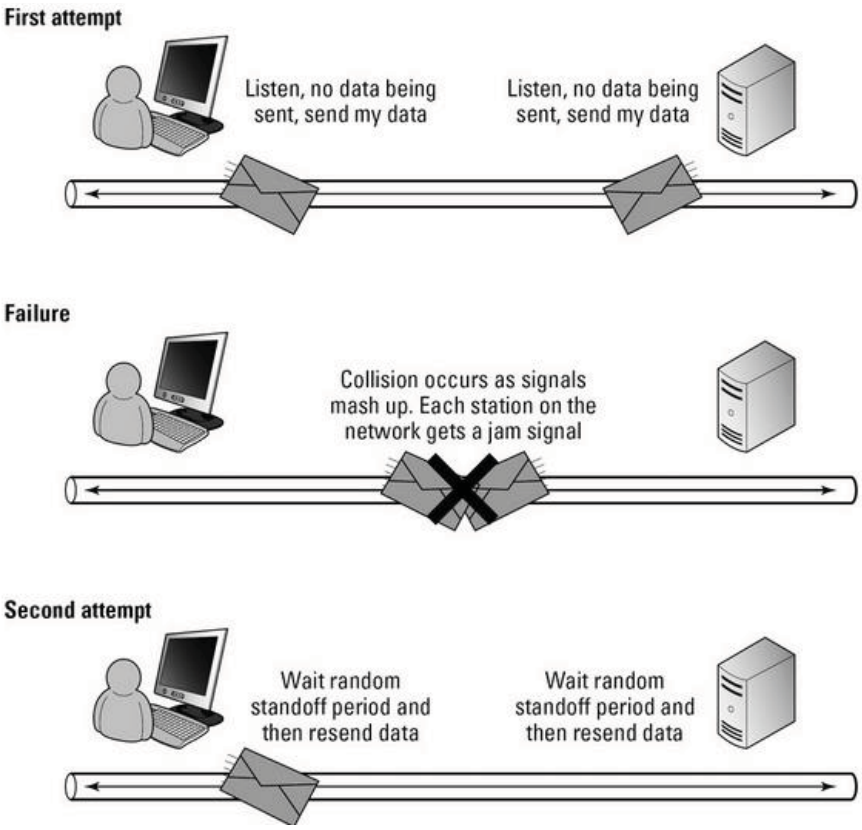
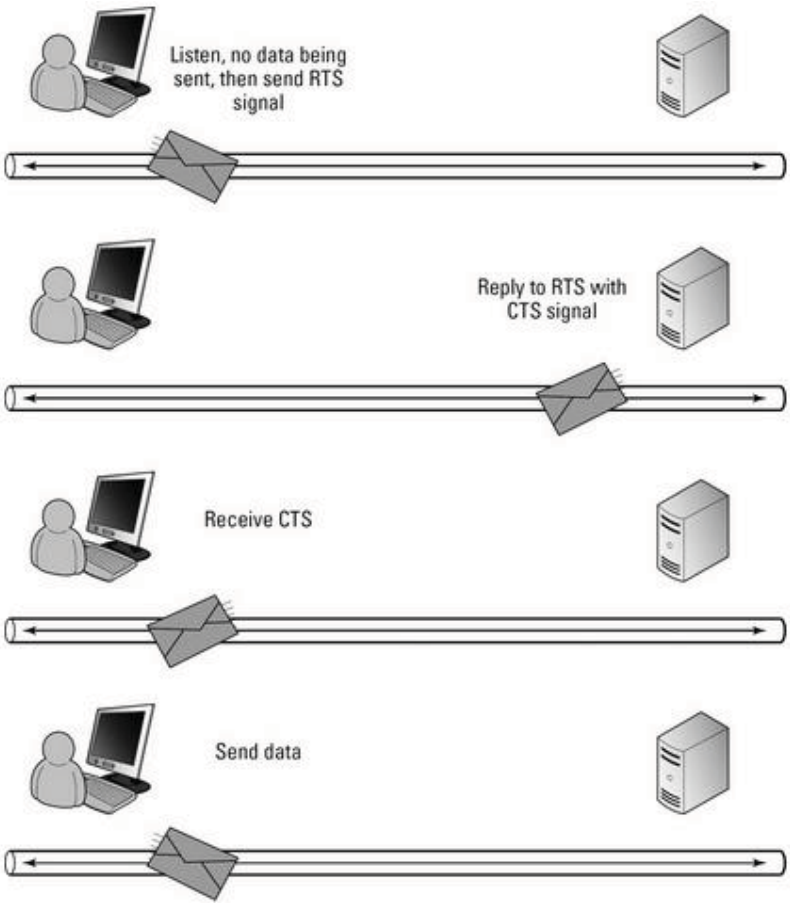


Figure 19 Steps to how collusion on a bus network occurs

CSMA/CA:

Nowadays almost every Ethernet uses this method to enable communication between different nodes. It works just like CSMA/CD except that it has an algorithm to solve collision problems more efficiently. Notice the CA which stands for collision avoidance.

The IEEE 802.11-2007 standard defines a function called Distributed Coordination Function (DCF) [50] to avoid collisions.



4.4 Network Types

4.4.1 LAN

LAN (Local Area Network) is a network consisting of network-enabled electrical devices in fairly close proximity to each other. Ethernet protocol is used widely for LANs. It is standardized in 1985 as IEEE 802.3.[51].

Figure 20 demonstrates a typical LAN wiring for a building. It consists of fibre optic distribution for longer distances. It can also be seen the cabling management for each floor does not exceed the 100 meter distance. [52]

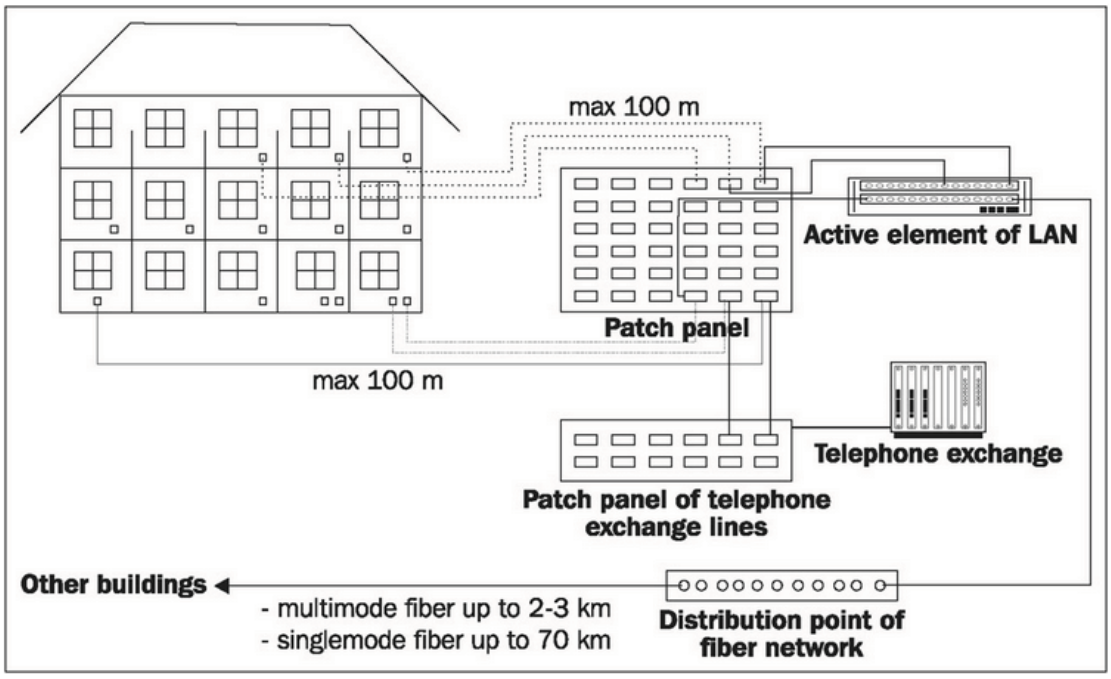


Figure 20 LAN Cabling in a building

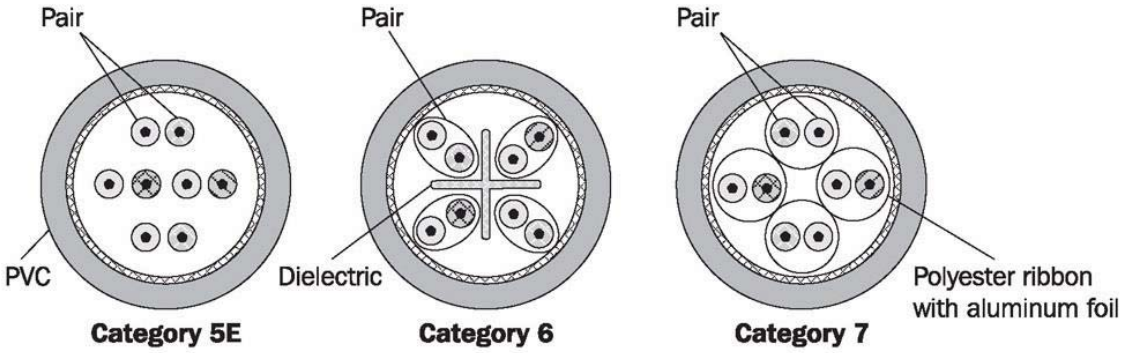


Figure 21 Twisted Pairs are used for shorter distances

Depending on the bandwidth choice, cables may vary for a LAN.

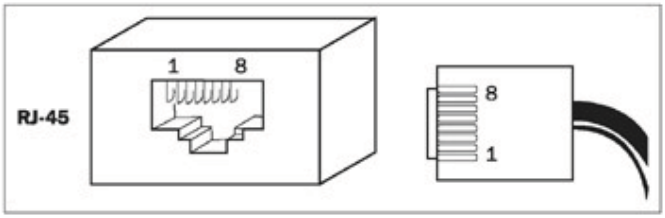


Figure 22 RJ45 wall socket and connector

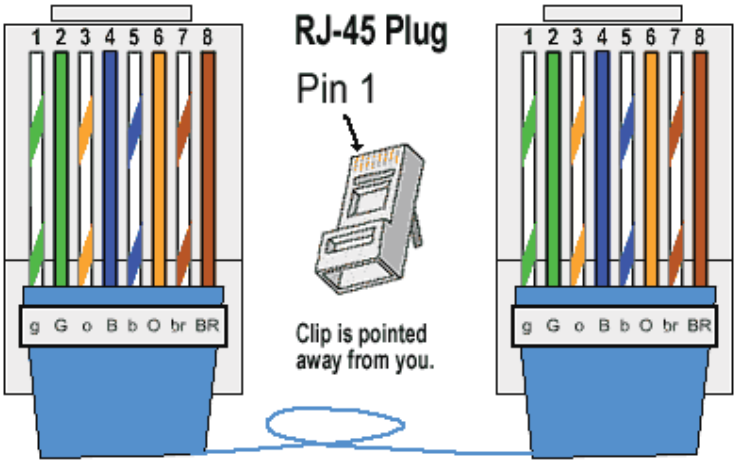


Figure 23 Straight connection

Straight connection is used if there is a communication between a switch, hub or a modem (router). The colour code needs to be followed according to the Figure 23 otherwise it will not function properly. A LAN cable tester can be used to test after the cable connection has been finalised. [53]

- Green white
- Green
- Orange white
- Blue
- Blue white
- Orange
- Brown white
- Brown

When the distance is greater than 100 meters in LAN systems, fibre optic cables are chosen. This is due to its perfection of carrying data using light without losing any of the data. Multimode is used to carry the data to shorter distances up to 3kms. Single mode however can be used to carry the data up to 60+kms.

It is important to understand that some of the applications may require longer than 60kms. In such cases, connectors (figure 24) can be used. If the data is crucial, splicing method can also be used to weld the fibre optic cables together. This ensures the data is not lost on the way to its destination [54]

Figure 24 some of the most common fibre optic mechanical connectors [55]

Ethernet

Ethernet is a combination of computer networking technologies for local area network.

AUI 10Mbps

AUI is the Cannon 15 connector. It is also known as 10BASE-5.

BNC 10Mbps

BNC is known as 10BASE-2.

Twisted-Pair

Twisted-pair as it is called TP or 10BASE-T is connected via the RJ-45 connector as mentioned before. It is possible to use twisted-pair cables as a telephone connection as well.[56]

Optical Fiber

Optical fibers on a LAN is called 10BASE-F.

Fast Ethernet (100 Mbps)

Fast ethernet speed achieved by twisted pair cables called 100BASE-TX. Optical fibre connector is called 100BASE-FX. The difference between Ethernet and faster Ethernet is that the faster Ethernet uses quality cables.

Gigabyte Ethernet (1000Mbps=1 Gbps)

Gigabyte Ethernet needs to use Cat6 twisted cables to avoid network problems. Optical fibres can also be used as a single mode called 1000BASE-LX. Multimode fibres on Ethernet called 100BASE-SX.[57]

Commercial Name	Standard Name	IEEE	Cabling	Range	Max. Bandwidth
Ethernet	10BASE2	802.3	Thin coaxial	185m	10 Mbps
	10BASE5		Thick coaxial	500m	
	10BASE-T		**UTP Cat3, Cat5**	**100m**	
Fast Ethernet	100BASE-T4	802.3u	UTP Cat3	100m	100 Mbps
	100BASE-TX		**UTP Cat5**	**100m**	
	100BASE-FX		MM fiber	2000m	
Gigabit Ethernet	**1000BASE-T**	802.3ab	**UTP Cat5, 5e**	**100m**	1000 Mbps
	1000BASE-SX		SM/MM fiber	550m	
	1000BASE-LX		SM/MM fiber	5000m	
10 Gigabit Ethernet	**10GBASE-T**	802.3an	**UTP Cat6, 6e**	**100m**	10000 Mbps
	1000BASE-SR		SM/MM fiber	300m	
	1000BASE-LR		SM/MM fiber	25000m	

Figure 25 Quick summary of Ethernet standards [58]

Network Simulators

When the network gets complicated, some tools may become handy to manage and troubleshoot networks. GNS3 is a network simulator that allows network administrators to create and simulate networks using Linux or Windows operating system. It is an open source software and free. It can be downloaded and installed within seconds. [59]

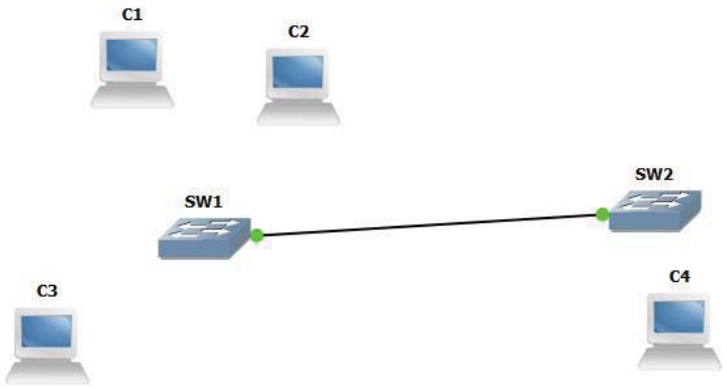


Figure 26 GNS3 - creating a simulation of a LAN network

4.4.2 VLAN

VLAN (Virtual LAN) is used for larger networks. It separates the devices using IP addresses. It can control the traffic within the network. Therefore it can increase the security of a particular LAN network.

Let us say there are different people working for a SCADA system. It would be impossible to locate the different people in the same building. This is because SCADA systems always

control remote locations. In such case, VLAN allows network administrators to group different departments.

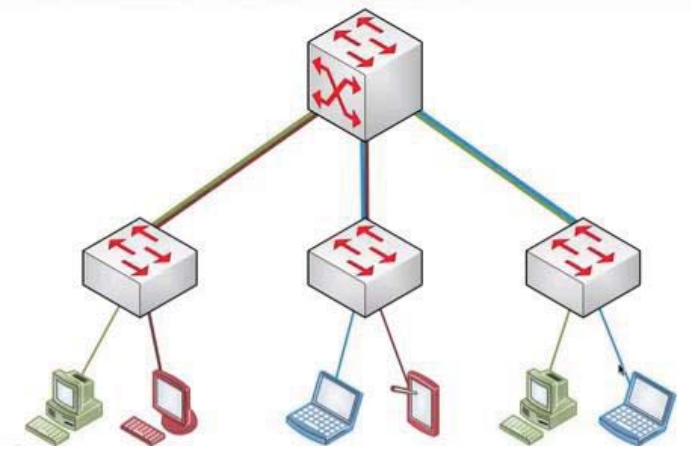


Figure 27 Red, blue and green devices connect the main switch using VLAN [60]

4.4.3 CAN

CAN (Controller Area Network) is designed for vehicle communication systems [61]. It is a serial connection to control different modules in a vehicle. CSMA/CD is used in case if two or more modules want to transmit data at the same time. [62]

4.4.4 WAN

WAN stands for Wide Area Network is a data communication system for broader areas. It is between two or more Local Area networks. WAN uses telephone companies to establish this link between different networks in different remote locations. The purpose of the WAN is to share data between authorised users no matter where they are located.[63]

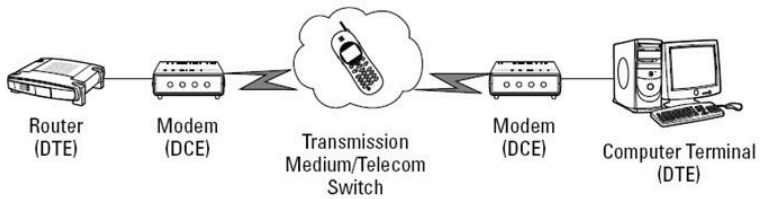


Figure 28 Establishing a WAN network

As figure 28 shows, a router and a modem needs to be used to be able to connect the telephone company provider. However, these devices nowadays are combined.

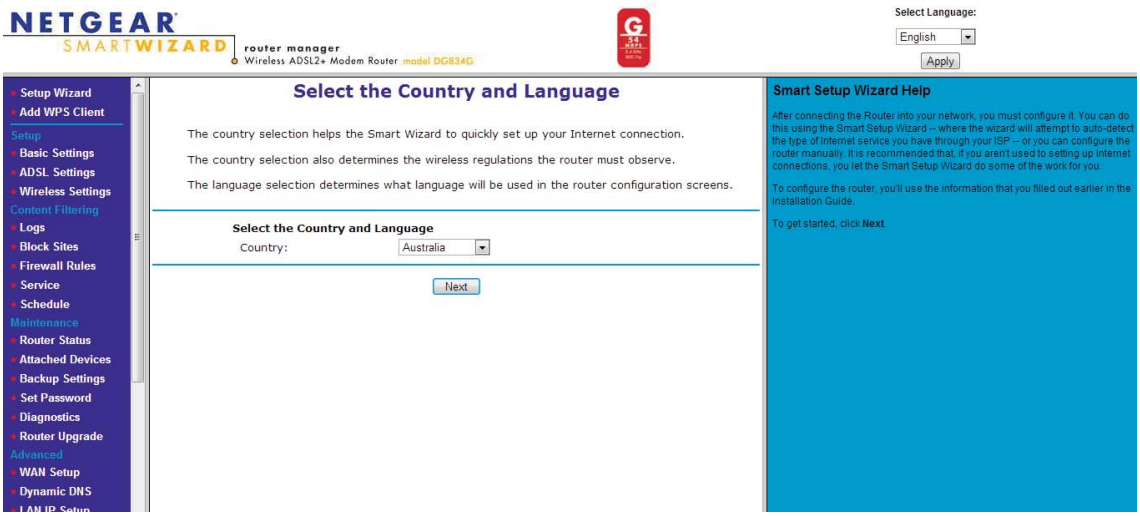


Figure 29 Netgear Modem and Router

Figure 29 shows the Netgear device, the router, wireless access point and the modem are all combined in one device.

4.4.5 Intranet

Intranet is an internal private network which is not available to anyone that is outside this private area. It is an internal internet within a network. Users will not be able to reach this network from another outside network.

4.4.6 Extranet

Extranet is between the internet and the intranet. It can serve the users who are not under the private network. It can also serve for the private network users.

4.4.7 Internet

Internet uses a protocol called TCP/IP. TCP was published by IEEE (Industrial of Electrical and Electronic Engineers) in 1974 [64]. TCP/IP protocol enabled the networks to interconnect across a gateway. Gateway also known as proxy was created because it knew what messages the networks were sending. [65]

Common TCP and UDP default ports

- SMTP – 25
- HTTP – 80
- HTTPS – 443
- FTP – 20, 21
- TELNET – 23
- IMAP – 143
- RDP – 3389
- SSH – 22
- DNS – 53
- DHCP – 67, 68

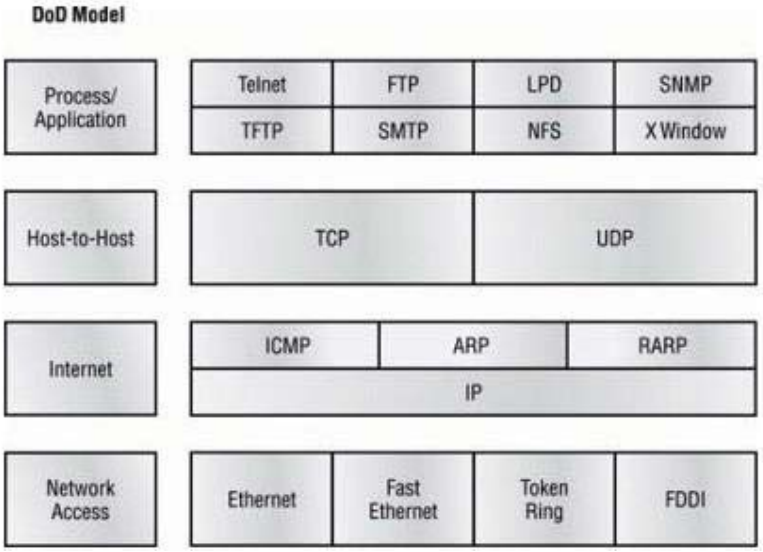


*Figure 30 Different layers of TCP/*IP protocol

Process Application

Telnet is used to access the other electrical devices on different networks via a telnet server. Telnet software is available and it has a text based user interface. One of the common telnet server is PuTTY. [66]

FTP is called File Transfer Protocol is the protocol as well as software that allows authenticated users to transfer files from one device to another. The file size is not a concern because even files in big size can be transmitted via FTP. Filezilla is the most popular FTP software. [67] Dropbox is also a cloud version of a FTP application. [68]

SMTP and POP3 are used for receiving and sending emails. Outlook is Microsoft's proprietary email application. On the other hand Thunderbird is an open source email application. [69]

RDP is a proprietary protocol that was developed by Microsoft which allows users to access the remote computer using graphic based interface. [70] Teamviewer is a remote management software that can also manage this. It is installed on the remote device as well as the client device [71]

VoIP is a protocol that is used for voice and video calls. [72] The best example for VoIP is the Skype application.

HTTP and HTTPS are protocol links between the web server and web browser. Some common web servers are Apache (open source) and IIS (Internet Information Services). According to W3schools, one of the most common web browser worldwide is now Google Chrome which is built by Google.[73]

HTTPS is the secure link between the web server and web browser. Notice the https in the address bar below in figure 31. This ensures the data is encrypted between the web browser and a web server.

Figure 31 Secure Connection to Googel.com.au

Host to Host

TCP (Transmission Control Protocol) is used to receive and prepare the data to be sent to the receiver. [64]

Internet Layer

Internet Protocol IP has a responsibility to transport(route) data through an internetwork. [74]

Summary of how the internet works

1. User types in a web address in their web browser (Google Chrome)
2. The request then goes to their router/modem.
3. The request then goes to ISP (Internet service provider) like Telstra or TPG
4. ISP then takes a look at the request and redirects it to a device that identifies the request by
5. Is it a website? It is a telnet access? It is an email? Is it RDP access?
6. It is a website in this case, it then forwards the request to the hosting company that has the website data
7. The hosting company computer then takes this request, authenticates it then returns to the user.

References

1- http://dpstele.com/pdfs/white_papers/scada.pdf

2- http://www.process-logic.com/content/images/SCADA.pdf

3- http://au.wiley.com/WileyCDA/WileyTitle/productCd-0471387258.html

4- http://www.amazon.com/exec/obidos/ASIN/0750682140/books24x7com

5- http://users.tpg.com.au/users/ldbutler/AmpNoise.htm

6- http://en.wikipedia.org/wiki/Low-noise_amplifier

7- https://docs.google.com/viewer?a=v&q=cache:KXzCVYCXTk0J:citeseerx.ist.psu.edu/viewdoc/download?doi%3D10.1.1.77.1554%26rep%3Drep1%26type%3Dpdf+&hl=en&gl=au&pid=bl&srcid=ADGEEShl9a3gM09CaePZ4lWrMmL_RXi3dfwRqx82ILDFKhKj3QVE9kAfNfSzdr-_Nduhc0_jP0XJNt1l5_80J5Y-A8FxvID7Bmkrn7VbUFYrphiYwEly0jBDnW2e8prMr7pc4qZ9vc-f&sig=AHIEtbTe3RD8IApQRxuFsmv4Hg_rHl0JgQ

8- http://science.howstuffworks.com/nature/natural-disasters/lightning1.htm

9- http://radiojove.gsfc.nasa.gov/library/sci_briefs/galactic.html

10- http://en.wikipedia.org/wiki/Quantum_noise

11- http://en.wikipedia.org/wiki/Electromagnetic_interference

12- http://www.acma.gov.au/scripts/nc.dll?WEB/STANDARD/1001/pc=PC_310704#arrangements

13- http://www.ehow.com/how_6825974_simple-way-detect-emi_.html

14- http://au.wiley.com/WileyCDA/WileyTitle/productCd-111812779X,descCd-DOWNLOAD.html

15- http://www.techrepublic.com/blog/networking/rf-interference-just-how-important-are-antennas/548

16- http://www.popularmechanics.com/technology/how-to/tips/how-to-fight-rf-interference-with-your-gadgets

17- http://www.novatel.com/assets/Documents/Bulletins/apn008.pdf

18- http://www.articlesfactory.com/articles/business/crosstalk-in-electronics.html

19- http://en.wikipedia.org/wiki/Crosstalk_(electronics)

20- http://www.cablesplususa.com/pdf/nec-cable-fire-ratings-guide.pdf

21- http://commsalliance.com.au/__data/assets/pdf_file/0008/2420/S008_2010.pdf

22- https://www.google.com.au/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&ved=0CEEQFjAB&url=http%3A%2F%2Fiiti.it%2Fhome%2Findex.php%2FDownload-document%2F6-

Generic-cabling-for-customer-premises.html&ei=F7NTUfNFzdCQBfLugagB&usg=AFQjCNH8vD5y-naevWtL9cXuD3cI6BIFVw&sig2=KBl2vhVZGIYI668xp8dEjA&bvm=bv.44442042,d.dGI

23- http://en.wikipedia.org/wiki/ISO/IEC_11801

24- http://www.olex.com.au/eservice/Australia-en_AU/fileLibrary/Download_540224625/Australasia/files/Industrial%20Catalogue.pdf

25- http://packetbyte.com/Content/TwistedPair.html

26- http://www.amazon.com/exec/obidos/ASIN/0470477075/books24x7com

27- http://en.wikipedia.org/wiki/Optical_fiber_cable

28- http://en.wikipedia.org/wiki/Speed_of_light

29- http://en.wikipedia.org/wiki/Optical_amplifier

30- http://www.ofsoptics.com/resources/MultimodeorSingle-Mode.pdf

31- http://www.abc.net.au/science/articles/2010/10/21/3044463.htm

32- http://www.doityourself.com/stry/9-uses-of-fiber-optic-cables#b

33- http://www.ad-net.com.tw/index.php?id=46

34- http://www.itnews.com.au/News/79213,analysis-hackers-eye-up-fibre-optic-data-networks.aspx

35- http://en.wikipedia.org/wiki/Rayleigh_scattering

36- http://www.telecomadvisors.org/dcl1.6/index.php?infoguardpaper.pdf

37- http://technet.microsoft.com/en-us/library/cc700841.aspx

38- http://www.ehow.com/facts_6850844_fiber-cable-laid-ocean-floor_.html

39- http://www.oafrica.com/broadband/sharks/

40- http://www.cabledepot.com/05DTFIBVSCOP.html

41- http://www.automation.com/library/articles-white-papers/industrial-ethernet/when-do-you-consider-using-a-managed-switch

42- http://www.dell.com/us/business/p/powerconnect-6200-series/pd

43- http://en.wikipedia.org/wiki/Communications_protocol

44- http://www.gtslearning.com/comptia-network-certification-2012-student-edition-courseware/

45- http://en.wikipedia.org/wiki/Fully_connected_network

46- http://www.buzzle.com/articles/advantages-and-disadvantages-of-different-network-topologies.html

47- http://iveeng.tripod.com/cn0203.pdff

48- http://www.samson.de/pdf_en/l155en.pdf

49- http://www.amazon.com/exec/obidos/ASIN/0470945583/books24x7com

50- http://en.wikipedia.org/wiki/Distributed_coordination_function

51- http://en.wikipedia.org/wiki/Ethernet

52- http://www.packtpub.com/TCP-IP/book?utm_source=Book24x7&utm_medium=UnderstandingTCP%2FIP&utm_term=Networking%26Telephony&utm_campaign=May2006

53- http://www.groundcontrol.com/galileo/ch5-ethernet.htm

54- http://www.wisegeek.com/what-is-a-fiber-optic-splicer.htm

55- http://www.thefoa.org/tech/connID.htm

56- http://en.wikipedia.org/wiki/Ethernet_over_twisted_pair

57- http://en.wikipedia.org/wiki/Gigabit_Ethernet

58- http://www.amazon.com/exec/obidos/ASIN/0470489626/books24x7com

59- http://www.gns3.net/

60- http://www.youtube.com/watch?v=7lriho8Su5Q

61- http://www.igi-global.com/book/advances-vehicular-hoc-networks/37323

62- http://en.wikipedia.org/wiki/CAN_bus

63- http://www.amazon.com/exec/obidos/ASIN/0470944986/books24x7com

64- http://en.wikipedia.org/wiki/Transmission_Control_Protocol

65- http://www.youtube.com/watch?v=MdMo5k-f1aw

66- http://www.chiark.greenend.org.uk/~sgtatham/putty/

67- http://filezilla-project.org/

68- https://www.dropbox.com/

69- https://www.mozilla.org/EN/thunderbird/

70- http://www.microsoft.com/en-us/legal/intellectualproperty/IPLicensing/Programs/RemoteDesktopProtocol.aspx

71- http://www.teamviewer.com/en/index.aspx

72- http://en.wikipedia.org/wiki/Voice_over_IP

73- http://www.w3schools.com/browsers/browsers_stats.asp

74- http://en.wikipedia.org/wiki/Internet_Protocol