- ## Network Devices

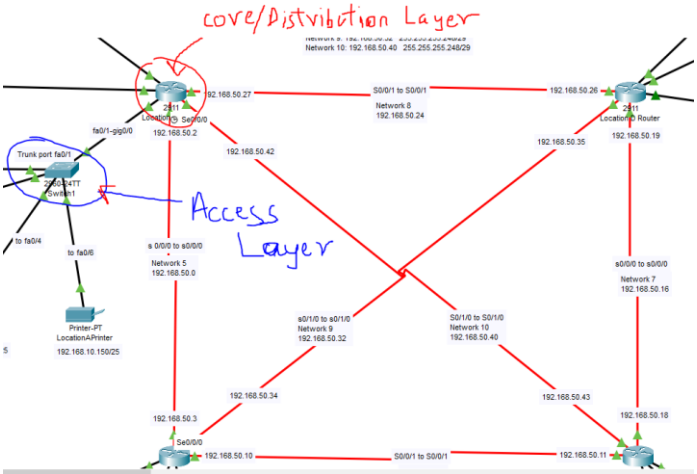
  Router: Router is a network device that receives data, filters it, accepts the data that is intended for it and the rest it forwards based on the IP address. Routers were used to connect the 4 locations by forming a mesh network that allowed the nodes from each location to talk to each other. If one of the networks fails since they are connected in a mesh, the chances of the whole network going down are very slim.

  Switch: Is an intelligent network device that allows users to expand the network by providing Ethernet ports where devices can be plugged in. Each port has a unique MAC address that directs incoming data packets. The networks had more computers than could be supported by the router. Multiple switches were connected to the Gigabit port on the router, and the switches in turn connected to all the peripheral devices at the location. Virtual LAN was also implemented on the switches to separate the traffic of all the different departments.

  Wireless access point: Allows users to connect their devices to the network using the 2.4GHz or 5GHz band. It also has a password that users need to enter to be able to connect to the wireless LAN. Employee devices and phones that need to connect have to select the SSID of the WAP and are assigned IP's using DHCP. In the network design, there is 1 WAP at each location to allow employees to connect their BYOD and Mobile phone.

- ## Choice of Network Design Model

  The network model used is a **hierarchical, tier-two network design model** has been used in the network implementation. The core/ distribution layers include the main routers in the mesh that connect all 4 locations. This will make the network more resilient if one of the networks in the mesh goes offline.
  The distribution layer is also linked with the core layer here because the routers in the mesh network are the ones that carry the data to the internal switches in the access layer of every location
  Every location has it's own three to four switches that are directly connected to the PC's and other devices, therefore, they are at the access layer in the network.



The core layer with the mesh network is very important in the networks because it provides reliability since each router is connected to all others independently in the case one smaller network in the mesh goes down the whole network won't go offline. The router mesh network carries the majority of the data packets by providing high-performance routing on the Serial interface.

- **IP addressing scheme devised for the network**

  In the network, there are 4 locations with 30+ nodes, each needs their unique IP's, therefore, subnetting is the best way to make sure that all of them will have enough IP addresses to go around. For each location, the main IP for each was split into 4 or 5 subnets depending on how many departments were present there. The main IP for each location was split into number of departments, this saved IP address from being wasted. For example, if there were 3 management department computers present at location-A then, the max allocated IP's for that department would be 6.
  Splitting IP address will also help with the performance of the network overall as there will be fewer hosts per subnet.
  Also, each department at every location has its VLAN implemented and this requires subnetting to operate smoothly. Each VLAN needs to be on different IP address so that they don't interact. (Example like 192.168.1.x vs 192.168.2.x)

- **How Network Segmentation has been implemented**

  Network segmentation is achieved by dividing the network to control the flow of traffic between branches or departments. For the 4 location the traffic was isolated by their Departments and the firewalls were also used between the network and the server in each location. Also, between the network and the Internet.
  At each location, DMZ's were implemented by having a firewall present between the internal network and the server present at that location. The physical firewall between the internet and Location-A router stops unauthorized sources from sending traffic into the network.
  VLAN's were implemented in all 4 locations by using Switches. On the switches across the 4 locations, each department was allotted a certain number of ports with the VLAN number (unique to each department across all location. E.g. Sales department has VLAN port 10) that allowed only hosts for that department to be connected to the reserved ports. For example, this makes sure that the traffic from or for the Management department is not accessed by some from the Administration department. It was the best way to isolate traffic from each department, it helps in saving resources and bring down costs.
  ACL's can also be implemented in the network that allows the user to filter network traffic. ACL can be configured on network devices such as routers and firewalls that have packet filtering capabilities. Here using Access lists we can get the router to only allow traffic arriving and departing to pass through and unwanted traffic can be denied access. The two types of access lists are standard and extended access lists.

- **Protocols used**

  Protocols are a set of rules that make the transmission data between devices possible by setting up pre-existing rules that decide how the information is structured and the way to send and receive it. The simulation uses Routing which selects which path the data takes across different networks, this is

important in the network because it allows the Packets to take the shortest path to its destination with the help of routers. Which, decide the route the packet will take. In the network, simulation Routing will ensure packet sent from one location will get to the other location which is its destination. The data packets might take the shortest path depending on the number of networks and their speeds en-route.
TCP/IP is a routing protocol and the evolution of OSI-7-layer model. In TCP/IP. TCP is responsible for the delivery of data when the IP finds where the data is supposed to go. IP is responsible for obtaining the IP address where the data is supposed to be sent, they both work together to make data transfer possible. TCP/IP packs the data into layers when sending the data and on the receiving end it unpacks the layers to extract the data. In the simulation, TCP/IP makes communication possible between all the devices.
EGIRP is a routing protocol used to send help packets to the other routers in the assignment networks, the neighbor will then send a response hello packet and add it to the topology table. Thus, finding the best path for data to travel between two points. It makes exchanging information between routers more efficient compared to other protocols. EIGRP uses DUAL algorithm to determine the most efficient route to the destination.
The network simulation used IPv4 IP addressing protocol. When the data is sent to a host the network address identifies which network it's in, there each host has is the unique address that identifies it. All the devices in the assignment networks have a network address part in the IPv4 address which identifies the location and which sub-network its in- at that location.
ICMP is a transport-level protocol which is used for communicating info about network connectivity problems back to the source. It allows devices such as routers to send control messages (e.g. source route failed) to the data source device.
ICMP made it easy to constantly test the connection between 2 devices and diagnosing problems and solving them on the spot. It will display the control message if a problem is encountered.

How Standards relate to the network technologies

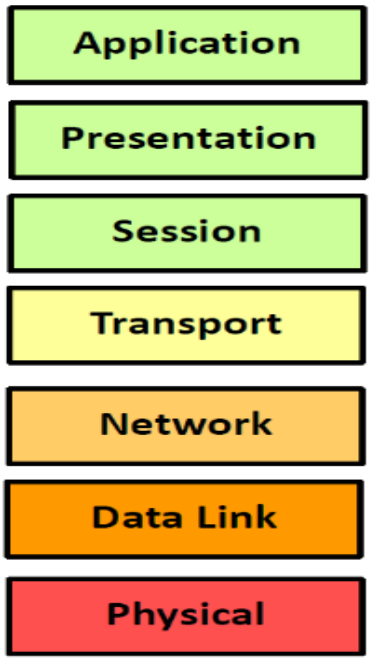
IEEE is a standards organisation that issues standard specification for different technology sectors including networking. They have released standards for networking devices, networking interfaces, connectors and cables.
IEEE 802.1: is a protocol that provides tools for network management and network monitoring. It handles the security and internetworking of LAN's, media access control, and data encryption and network traffic management. All these standards have improved security and network capacity
IEEE 802.3: This is the specification for Ethernet, this was the supported 10Mb/s connection speed paving way for the improved 1GB/s connection speed
Similarly, the IEEE 802.11 wireless standards specify the 2.5 and 5 GHz bands for wireless connection and all devices in the simulation that utilize Wi-Fi are capable of operating at both or one these bands.
RFC was published by IETF to describes methods, research, and innovation involved the working of the internet

- 802.1 Bridging and Architecture
  – generally the top of the link layer
- 802.3 Ethernet
- 802.11 Wireless LAN (WLAN)
- 802.15 Wireless Personal Area Network (WPAN)
- 802.16 Broadband Wireless Access (BWA)
- 802.18 Radio Regulatory TAG
- 802.19 Coexistence TAG
- 802.21 Media Independent Handover
- 802.22 Wireless Regional Area Networks (WRAN)
- 802.24 Smart Grid TAG

Some of IEEE standards

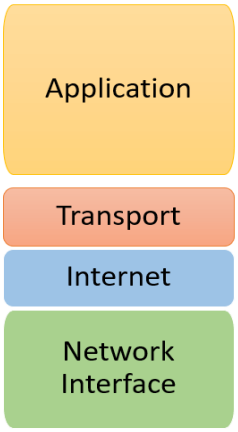
- **How theoretical models such as TCP or OSI model are key to understanding data transmission**

OSI 7-Layer model

Activity	Example	Layers
Provides interface for the data to be displayed to the user	Chrome, HTML	
Formats data between the Application and Session layer converting it allows it to be displayed in ASCII format	HTTP	
Responsible for Initiating and terminating communication between given devices	HTTP	
Used to manage end-to-end communication in the network, also resends and failed data segments	TCP	
Breaks the data into network packets and routes the packets by finding the best path in the network	IP	
Provides a link between two directly connected nodes and handles error correction for the physical layer	MAC	
Transports the data bits onto the medium	CSMA/CD	

TCP/IP model is the replacement for the OSI model but has 4 layers only with error checking. The four layers in it are:

- Datalink layer
- Internet layer
- Transport layer
- Application layer



- **Security implemented for the network**

Firewalls are used at each location in the DMZ which holds the server that could be vulnerable to attacks. The firewall will block unwanted traffic reaching the server. The main firewall connecting Location-A router to the internet also blocks unwanted traffic from getting into the whole network.

All routers and wireless access points have been given passwords to secure the network from physical threats where unauthorized users could try to connect to the network. Now every wireless device that connects to the network needs to have the password to connect to the network. Also, routers in all locations have passwords enabled. This means unauthorized people cannot gain access to the router controls and compromise the security of the network.

DMZ's are used in the network to isolate servers at each location to create a security barrier. That will protect them from untrusted traffic. DMZ was also intended to be present between Location-A router and the internet, for the same purpose this allows the devices on the network to access the internet but block the untrusted data coming in from there.

VLAN's and networks segmentation play a major part in the company's security policy. In the network simulation, each department's devices were logically separated using VLAN's so that others cannot access it. VLAN's create their own logical separate networks by carrying the data of each given department device on the VLAN port assigned to that department. This creates a logical bubble for the data of each department on the network.

Network segmentation has been implemented by giving each location its own IP address, this is important to isolate the locations network in case it is being attacked from the outside, making it easier to deal with the attack and still have the other locations operational. Also, every department at each location is operating on different subnets, making it difficult to attack all of them together or in case of a malware attack only targeted department will be affected.

References

Computing, H., 2021. *What Are Network Devices And What Do They Do?*. [online] WhatIsMyIPAddress.com. Available at: <https://whatismyipaddress.com/network-devices> [Accessed 12 January 2021].

Encyclopedia.com. 2021. *Network Design | Encyclopedia.Com*. [online] Available at: <https://www.encyclopedia.com/computing/news-wires-white-papers-and-books/network-design> [Accessed 12 January 2021].

Network Computing. 2021. *Campus Network Design Models*. [online] Available at: <https://www.networkcomputing.com/data-centers/campus-network-design-models> [Accessed 12 January 2021].

Operations, I. and Explained, N., 2021. *Network Devices Explained*. [online] Blog.netwrix.com. Available at: <https://blog.netwrix.com/2019/01/08/network-devices-explained/> [Accessed 12 January 2021].

Techopedia.com. 2021. *What Is Network Design? - Definition From Techopedia*. [online] Available at: <https://www.techopedia.com/definition/30186/network-design> [Accessed 12 January 2021].

Nuggets, C., 2021. *5 Subnetting Benefits*. [online] Network Computing. Available at: <https://www.networkcomputing.com/data-centers/5-subnetting-benefits> [Accessed 14 January 2021].

Palo Alto Networks. 2021. *What Is Network Segmentation?*. [online] Available at: <https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation> [Accessed 14 January 2021].

Reddy, A., 2021. *Network Standardization*. [online] Tutorialspoint.com. Available at: <https://www.tutorialspoint.com/Network-Standardization> [Accessed 14 January 2021].

University, G., 2021. *What Is ACL (Access Control List)? | CCNA*. [online] Geek University. Available at: <https://geek-university.com/ccna/what-is-acl-access-control-list/> [Accessed 14 January 2021].

Encyclopedia Britannica. 2021. *Protocol | Computer Science*. [online] Available at: <https://www.britannica.com/technology/protocol-computer-science> [Accessed 14 January 2021].

Extrahop.co.uk. 2021. *ICMP: Definition & How It Works | Protocol Support Library | Extrahop*. [online] Available at: <https://www.extrahop.co.uk/resources/protocols/icmp/#:~:text=ICMP%20is%20a%20transport%20level,route%20failed%2C%20and%20source%20quench.> [Accessed 14 January 2021].

Rouse, M., 2021. *What Is EIGRP (Enhanced Interior Gateway Routing Protocol)? - Definition From Whatis.Com*. [online] SearchNetworking. Available at: <https://searchnetworking.techtarget.com/definition/EIGRP> [Accessed 14 January 2021].

Services, P., 2021. *What Is Network Segmentation?*. [online] Cisco. Available at: <https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html> [Accessed 14 January 2021].

Us.norton.com. 2021. *What Is A Firewall And Do You Need One?*. [online] Available at: <https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html#:~:text=A%20firewall%20is%20a%20security,private%20data%20on%20your%20computer.&text=Firewalls%20can%20provide%20different%20levels%20of%20protection.> [Accessed 14 January 2021].

What is TCP/IP and How Does it Work?. 2021. *What Is TCP/IP And How Does It Work?*. [online] Available at: <https://www.avast.com/c-what-is-tcp-ip#:~:text=TCP%2FIP%20stands%20for%20Transmission,network%20such%20as%20the%20internet.> [Accessed 14 January 2021].

Tutorialspoint.com. 2021. *Network Standardization*. [online] Available at: <https://www.tutorialspoint.com/Network-Standardization#:~:text=Network%20Standards%20Networking%20standards%20define%20the%20rules%20for,needed%20for%20interoperability%20of%20networking%20technologies%20and%20processes> [Accessed 15 January 2021].

Techopedia.com. 2021. *What Is The IEEE 802.1 Working Group (IEEE 802.1)? - Definition From Techopedia*. [online] Available at: <https://www.techopedia.com/definition/19936/ieee-8021-working-group-ieee-8021> [Accessed 18 January 2021].