Introduction

This paper aims to design a university security system network that satisfy the confidentiality , integrate and availability triad with maximum usability. The system is required to handle four types of users which are university students ,campus guests ,Admins and academic employee. Each system user can access different package of network resources . for example, Admins can access security cameras ,Students can access the E-learning , Academic Staff can access the university’s network and guest can only access the admission website. so, the network security system must deny the access of unauthorized users to network resources to keep data’s confidentiality and integrity . Also, the paper will provide a detailed description to the used network topology and network architecture along with all the used network devices. And finally, the paper will discusses security solutions and recommendation for the network.

**Topology :**

The choice of network topology will determine the efficiency of the whole network in terms usability, security ,cost and whither the network has a single point of failure or not. There are many types of network topologies that fits different types of network requirements and needs but the most commonly used network topologies are bus,ring,hyprid,mesh and star which one of them might be a suitable option for the project requirements.

**Star network topology:**

Star network topology is the a suitable option for this project as it is fast and do not cause buttle neck like the bus topology. also , it is tolerant towards failures unlike the ring topology as if one of the wired cables failed for some reasons , the network will continue to run despite the defects.

The star topology design mainly consists of multiple different end devices that can be computers, laptops or phone which all are connected directly to a switch or a hub that is called a core switch, the switch main job is to establish the network or the connection between the end devices and help in exchanging data between them [1].

The star topology has some more advantages that satisfies the project requirements like good performance ,reliability, robustness and scalability as the network can be extended very easily by only plugin new devices to the core switch or the core hub.it is also easy to detect fault in the system as the devices are not all fully connected and if one device is failed , it will not affect the other as long as the core switch is not the failed device.

Some of the disadvantage the star topology have is the fact that the design is totally dependent on the core switch making it a single point of failure, but the problem can be solved by implementing multiple redundant core switches as if one failed the other will work fine. Also, it is more expansive than other network topologies as it requires more network devices like switches or hubs.

**Tree Topology:**

Another suitable solution is the tree topology design. the tree topology is basically a combination between bus topology and the star topology without the down sides like bottle neck ,single point of failure and security weakness that both bus and star topology have , it also called expanded bus topology.

The design of the tree topology adopts the idea of parent child hierarchical concept as every child node (switch or other network device) must be connected to a parent node(another network device) in a hierarchical structure. Basically, every two nodes that are related in someway can be connected with a route node that acts as a parent node in parent-child hierarchical concept [2].

The tree topology is also a suitable topology for the university network design as some of its advantages is reliability , robustness, and flexibility as it is very easy to detect faults in the system since the network nodes are not fully connected with each other and connected with core switch or hub that can detect which node is not working and as a result the maintenance process is sample since technicians only fix the defected nodes and not the whole system. Also , the tree topology supports scalability as new child nodes can be incremented without configuring the core nodes in the system because the topology adopts the hierarchical structure which also supports scalability and expansion friendliness. Finally , one of the most important advantages is the topology ability to evade single point of failures since defected nodes can not affect other nodes because there are not fully connected.

But also, the tree topology has critical disadvantages like the difficulty of installing the network design in real life because the topology is very complicated as it is the result of the combination of two different topologies which is bus and star topologies. And as a result, it is very expansive to install the network design because it requires expert technicians, also the topology requires a decent number of switches and hub which might be really expansive for small to medium companies.

**The hybrid topology approach (tree and star combined ) FINAL CHOICE :**

one topology is not enough to satisfies the requirements of huge network like the university campus design. due to these circumstances , The hybrid approach is recommended to satisfies these requirements. The hybrid topology is mainly a combination of multiple different topologies together in one design. so ,as both the tree and star it is advised to be combined into one topology to achieve maximum efficiency with as less downsides as possible.

The star topology will be used to connect all end devices with the switches in the access layer to lower the complexity and bottle neck of the system. And the tree topology will be used to connect the access layer switches with the distribution layer switches in a parent-child hierarchical structure in order for the departments expansion process to be easy and flexible.

**Network architecture :**

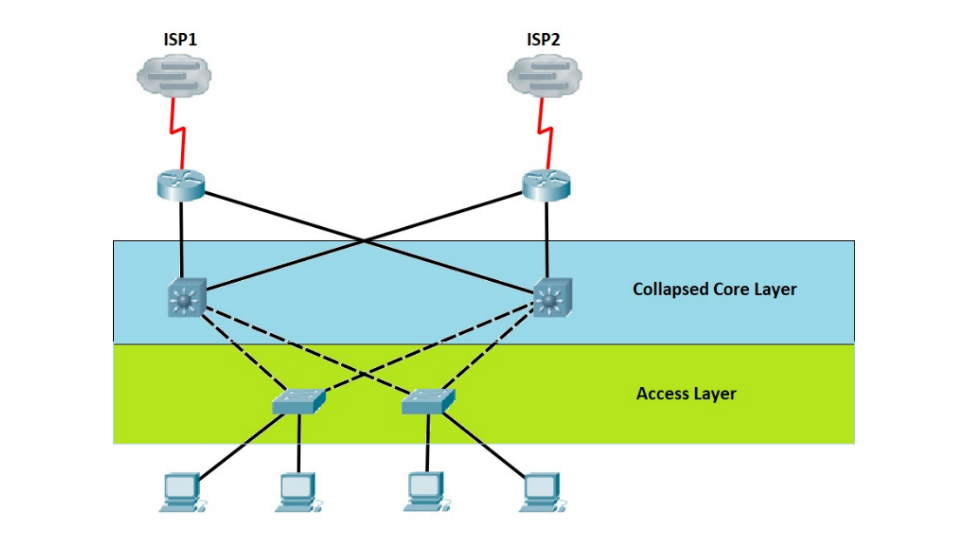
The use of collapsed core network architecture will prevent the occurrence of single point of failure since the redundant implementation and distribution of core multi-layer switches and ISP serves will be a great solution as if one device is failed the other redundant device will take its place without defecting the system which will eliminate vulnerability towards single point of failures.

Collapsed core is a two-tier architecture design which consists of two layers ,one is the distribution layer and the second is the access layer.

**The core layer** core switches are responsible for transmitting large packets to the system internal network **The distribution layer** core switches are responsible for routing and switching packets between the core layer and access layer, finally **the access layer** switches is responsible for distributing the shared data among the end devices creating a small internal subnets or networks.

The concept behind two-tier core collapsed network architecture is concatenating the core distribution into one layer called **collapsed core layer [3]**.

collapsed core layer core switches is responsible for transmitting large packets and route it to the **access layer switches** which lower the cost of the whole network since the network architecture requires less hardware devices , coper, and fiber Caples to install the network.



Devices :

In this part, all of the used network devices will be described in details along with why it was used in the network

**ISP:**

ISP stands for internet serves providers which is basically is an internet subscription provider company like Telecom Egypt or Vodaphone. ISP is an essential tool in the network as the designed network is required to provide Wi-Fi network for students ,visitors and academic staff and. also ,an access to websites like E-learning , SRS and admission website mainly requires internet access.

**Router :**

router is devices that connects to computer networks to deliver packages and control the traffic of the packets being sent by the network. The router is needed to connect all the switches with ISP and route the internet packets . Cisco 2911 Routers is an excellent option as it provides high speed WAN environment.it also offers a power consumption control feature.

**Switch:**

Switch is a device that connects the end devices like computers , tablets ,phones or servers with each other and allow the communications between these devices by transmitting packets between them. The switch is needed to connect the campus computers with the university resources and other computers

Through the university network. the cisco 2960-24TT switch is the best option as it has some great security advantages like Identity based Networking services and access control features than prevents unauthorized network user from accessing private resources which achieves the confidentiality of the network data.

**Multilayer switch :**

it Is a high-performance switch that is used in much complicated system due to its high speed and incredible performance.it is mainly used in higher OSI layers. The chosen Multilayer switch is cisco catalyst 3560-24PS

**Servers :**

Server is the component that provides hardware and the software resources of the network that is shared among different end devices through the network. Multiple instances of this component are needed like web server , DNS server and E-mail server.

**Computer:**

Computers are the end devices provided by the university that is used by the system actors to communicate with each other’s or to access the network resources.

**Smart phones:**

Students might use their personal smart phones as an end device to access the university network to obtain some of the resources that the network host like SRS and E-learning vie the wireless network established by the access point devices

**Security cameras :**

Since the security network is being designed for a university campus area. One of the necessities is to provide a full surveillance system in order to detects abnormal behavior. The network design includes security cameras around the campus area that is connected to the university networks where only the Administrative Branch users can access theses security cameras to observe the current state of the campus area

**Wireless network device (access point):**

Basically, Wireless network device allows the connectivity of end devices like computers , phones and tablets to the system network without the need of ethernet cable or any wires .in order to satisfy this requirement an access point router is implemented in the system so the end devices can establish a wireless connection to the network.

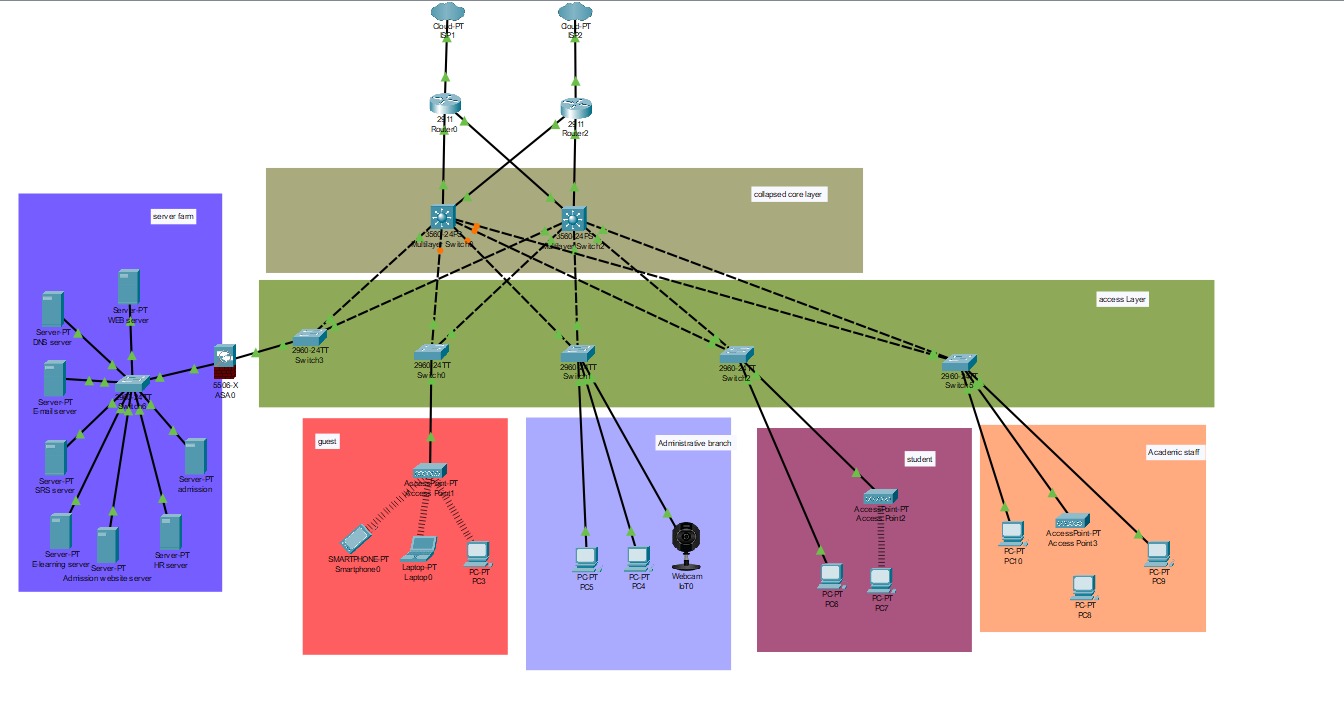
**Laptop:**

Students might use their personal computers as an end device to access the university network to obtain some of the resources that the network host like SRS and E-learning vie the wireless network established by the access point devices

**Design:**

The system design requires two internet serves providers as if one is failed the other will carry on the work, each one of the two internet serves providers are connected to a cisco 2911 Routers to transmit the packets to the rest of the network. Each one of The routers are connected to two cisco catalyst 3560-24PS multilayer layer switches in the collapse core layer that is responsible to communicate with the access layer. Every multilayer switch is connected to a five non-programmable cisco 2960-24TT switch in the access layer. Every switch is dealing with a number of end device like computers and security cameras forming a subnet or small network. The system contains five small networks or campus area.

1. **Campus Students :**  switch is connected to the campus computers that acts like end devices which can access the network resources , also the switch is connected to access point device in order to provide wireless connection to the network .
2. **Servers** **farm** switch is connected to hardware firewall device that ensures the safety of the shared data. The fire wall device is connected to servers that hosts the network shared recourses which is WEB server ,DNS server ,E-mail server ,SRS server, E-learning server, Admission website server, Finance server ,University administration server , HR server AND department server.
3. **Academic staff** switch which is also connected to the campus computers that acts like end devices which can access the network resources , also the switch is connected to access point devices in order to provide wireless connection to the network .
4. **Administrative department** switch is connected to campus computers and security surveillance cameras that covers and records the campus areas .
5. **Visitors** switch is only connected to an access point device that provides a wireless service that connects end devices like smart phones , laptops, tablets, and computers to the university network as one of the project requirements is that guests are only allowed to access the admission website through Wi-Fi connection.



**Network design and security principles and CIA triad :**

Security principles and CIA triad is a basic set of rules or principles that must be met by any network security system design in order to protect the shared data and resources from getting breached, manipulated, and stolen.

Availability:

availability principle is the term which states that network system must be available to deliver a store and exchange data all the time and any failed data exchange process at any time might be critical enough to declare emergency state that will cost the business a lot off many.There are some common approaches to address the availability principles like network redundant structure, data backups and restore , servers duplications [4].

1. **network redundant structure:**

as shown in the provided network design, the redundant implementation of hard-ware and software devices like switches hubs internet service providers and multi layer switches not only will prevent a single point of failure occurrence ,but also if any hardware or software devices failed for any given its redundant implementation will take place and keep the system running with zero down time.

1. **backup and restore data:**

one of the oldest techniques to keep the data preserved and available at any given is the backup and restore method which is basically having server backups and data replication on regular bases every month as if some pieces of data got lost or corrupted the replication will be restored.

1. **servers duplications.**

Server replication is very similar to data backup and restoration but instead of replicating the data the whole server will be replicated with the same configuration , connection and purposes. And the work load will be balanced among the server and the replicant so if the server failed the replicant will take over the work load leaving the system with no down time and maximum availability.

Integrity :

The integrity principle states that if the data sent by the end user got manipulated or altered in the way by some hacker or breach, the data Integrity is lost.so , the data sent by the end user must be secured from data manipulation so that the data integrity is preserved. Some of the solution provided by the network deign is

1. **Access control :**

Access control is a concept states that no one can access data but the authorized members which means

If unauthorized user tried to access sensitive data, the access control system will prevent him in order to keep him from manipulating the data. The access control can be implemented by inserting an access control list that contains the IP address for authorized devices into the programmable multilayer switch in the distribution layer.

1. **Hashing:**

Hashing is a software algorithm used to keep the data Integrity by preventing or detecting data manipulation or altering by third parties. The way hashing techniques works is providing a secret key that consist of a random binary value to any connection between two parties in the network. Then, applies the MD5 hashing algorithm on the data that needs to be sent to obtain the digest which a series of random vales. The digest value will not be changed if the data did not get altered no matter how many times the algorithm is applied on the data.in the final step the sender pass the secret key along with digest and the message to the receiver if the secret key and the digest matched then ones with the receiver, then data is not altered and Integrity is not lost.

Confidentaiality :

Confidentaiality is basically the data between sender and receiver must be as private as possible and not to be accessible or breached by unauthorized third-party hackers or malware since data is extremely sensitive. And even if a third party managed to access the data must be encrypted so it cannot be observed.

1. Encrypting sensitive data:

Encryption is the act of manipulating the data or resources in a way that it is readable for only for the authorized users and it will be unreadable for unauthorized parties.by Encrypting sensitive data the data will keep its Confidentaiality since no unauthorized party will be able to access the readable content of the data. The way encryption works that ,before the data get exchanged between sender and receiver ,the encryption algorithm will be applied the plaintext to convert it into non-readable ciphertext using an encryption key , then the ciphertext is sent to the receiver, from there the ciphertext is decrypted using the decryption key to be convert to the original plain text. What makes the exchanged private and confidential is the decryption and encryption keys that the sender and receiver have ,without keys the data will unreadable ciphertext.

1. Firewall:

by firewalling the network and the servers farm will protect the end devices from getting defected and leak data.

**Authentication :**

Authentication is the mechanism of differentiating between authorized and unauthorized network users. Mostly the Authentication process an IP address , token or username and passer word in order to identify the authorized system users and allow them to access the network resources. There are two applications of Authentication integrated in the designed network security system, one is the user access list which is a list of all authorized IP addresses devices that can access the network resources. The access list is integrated on the multilayer switches and firewalls.it is also proposed to integrate a **network access server** to handle login and connection authentication from network users. Also, encryption and hashing are sorts of Authentication.

**PART 2: Trojan Horse virus**

Trojan Horse virus idea came from a historic myth which stated that there was a giant wooden horse present as gift for the people of troy city , but the hidden truth is the fact that the giant wooden horse was stuffed with armored warriors waiting to conquer the city at night so the people of the city would be ungraded.The Trojan Horse virus adopted this strategy .as also, the Trojan Horse appears as an ordinary .exe file that might help the user in some tasks waiting to be downloaded and run, after being run the trojan horse virus start to not only steal sensitive data from the computer like E-mails , passwords , credit cards info and even phone numbers but also starts to noticeably lower the performance of the infected pc and spread other computers.

There are a lot of types of trojan, for example the **backdoor trojan** which upon activation allows the hacker to fully control the infected computer. Or the **banker trojan** that is designed to target bank account user to steal bank account information and credit cards info. And the **game-thief** trojan which is specifically designed to steal online gamers money. And the **spy trojan** that stay on infected computers to records computer user behavers and action in order to steal his personal data. **Mail finder trojan** is designed to steal email address and password stored in a computer. **Fake anti-virus trojan** that acts like a real antivirus to infect the pc upon download. **The rootkit trojan** which its only purpose is to stop the infected computer from detecting other viruses and trojan. And finally, **infostealer trojan** which is similar to the rootkit trojan as it is also prevents the infected computer from detecting other trojans, but it also helps on installing other trojans on the computer. The trojan can be detected by human if noticed some changes on the windows setting, lack of performance or also, trojan can be detected trojan scanner and removal applications [5].

How to protect the network devices from trojan attacks:

Since most of the trojans comes from internet and targets the end devices through downloading the exe file. The proposed solution is to configure the fire wall to prevent the access to untrusted site vie DNS based restriction and prevent downloading exe applications on campus end devices unless the user is an authorized admin. Also, the campus devices must be provided with Trojan scanner and remover applications. Also, the website server must be configured to a trusteed list that contains the trusted website that the student can access form the campus end devices. Pack up and restore process must be done regular as if the network got infected the reboot and restore will be the only solution [6-7].

Conclusion :

In summary , this project aimed to design a secured network system for the BUE university ,the hybrid mix between tree topology and star topology were proposed, the core collapse architected were chosen because of its ability to eliminate single point of failure which makes it reliable and efficient. The network devices used in the designer were described briefly. Also, the paper demonstrated how the designed system will accomplish the CIA principles which is confidentailty,availability ,integrity and authentications. And finally, the trojan horse attached were explained in detail with mentioning different types of trojans and how the designed system will stop these attacks.

References

[1] Bisht, N., & Singh, S. (2015). Analytical study of different network topologies. *International Research Journal of Engineering and Technology (IRJET)*, *2*(01), 88-90.

[2] Tree Topology Advantages and Disadvantages | What is Tree Topology? Advantages and Disadvantages of Tree Topology. (2022). Retrieved 25 January 2022, from <https://www.aplustopper.com/tree-topology-advantages-and-disadvantages/#Advantages_of_Tree_Topology>.

[3] Collapsed Core and Three-Tier Network Architectures - Study CCNA. (2022). Retrieved 26 August 2022, from <https://study-ccna.com/collapsed-core-and-three-tier-architectures/>.

[4] Otto, R. (2016). Security System Availability: Managing Risk - Security Coverage. Retrieved 27 October 2016, from <https://www.facilitiesnet.com/security/contributed/Security-System-Availability-Managing-Risk--38068>.

[5] What Is a Trojan Horse? Trojan Virus and Malware Explained | Fortinet. (2017). Retrieved 22 October 2017, from https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus.

[6] Atamaniuk, M. (2022). What Is a Trojan Virus and How To Prevent It. Retrieved 3 August 2021, from <https://clario.co/blog/what-is-trojan-horse/>.

[7] What is a Trojan Virus & How to Protect. (2022). Retrieved from https://www.webroot.com/us/en/resources/tips-articles/what-is-trojan-virus