# Introduction

I have been tasked with designing and developing a network infrastructure for ABC University to improve there current network. I have to use the universities business and technical requirements in accordance to designing an efficient and effective network that will seamlessly interface across multiple campuses.

The following screenshots are of ABC Universities network design in Cisco Packet Tracer:

CAMPUS A

A computer network diagram with many different colors

Description automatically generated with medium confidence

CAMPUS B

A screenshot of a computer

Description automatically generated

CAMPUS C

A screenshot of a computer

Description automatically generated

# Seamless Connectivity

My current network design for ABC University enables seamless connectivity across all three campuses by introducing one singular router that controls both internal and external network access. This allows the servers inside the campus to be access internally and externally from any location in the world.

Effective communication between various sites in a network depends on a strong infrastructure that incorporates hardware, software, and protocols. Redundancy plays a vital role in reducing the risk of system failures by utilizing duplicate hardware and failover mechanisms. Routing protocols such as BGP and OSPF dynamically select the most efficient data paths, adjusting to changes in the network.

Quality of Service (QoS) guarantees that important applications receive priority bandwidth and minimal latency, ensuring a consistent user experience. Security measures, such as encryption and firewalls, safeguard data while it is being transmitted over public internet connections.

Centralized management tools empower administrators to monitor network infrastructure across all sites through a single interface, promoting uniformity and simplifying management tasks. Scalability is crucial for accommodating growth, which can be achieved through scalable architectures like cloud-based services.

This comprehensive approach allows organizations to enhance collaboration, access essential resources, and align with business goals seamlessly across dispersed locations.

# Scalability

My network design provides excellent scalability by allowing additional devices to be added to the network at any time. I am able to do this by calculating the subnet so that there is flexibility in the assigned IP addresses whilst also insuring minimal cost and work for the network configuration of newly added devices and features.

Scalability is a crucial element in the design of a network, guaranteeing that the infrastructure can adapt and expand seamlessly as the organization progresses. In my network design, I achieve scalability through meticulous subnet calculation, which enables the allocation of IP addresses with flexibility while minimizing costs and configuration efforts when incorporating new devices or features.

By accurately defining subnets, I efficiently assign IP addresses, ensuring that there are ample available addresses to accommodate future expansions without necessitating significant reconfiguration. This method reduces the intricacy of managing IP addresses and simplifies the integration of new devices into the network.

Furthermore, the design emphasizes cost-effectiveness by minimizing the requirement for additional hardware or software licenses when scaling up the network. By optimizing resource utilization and leveraging existing infrastructure, I guarantee that scalability is attained without incurring unnecessary expenses.

Moreover, the scalability of the network design extends beyond the mere addition of devices. It also encompasses the capability to accommodate new features or services without disrupting existing operations. This flexibility empowers the organization to innovate and deploy new technologies as needed without overhauling the entire network architecture.

In conclusion, my network design prioritizes scalability by providing a flexible and cost-effective framework for accommodating growth and evolution. This approach ensures that the network can support the changing requirements of the organization while minimizing complexity and maximizing efficiency.

# Security

The network offers robust security measures by providing a firewall between internal and external access of the servers which allows the network to reject or allow connections externally depending on if the connection is authorized.

Security is of utmost importance in any network infrastructure, and in this particular design, strong measures have been put in place to safeguard against unauthorized access and potential threats. A firewall plays a crucial role by acting as a barrier between internal resources, such as servers, and external entities like the internet.

By implementing a firewall, the network ensures that only authorized connections are allowed to access internal servers and resources. Incoming traffic is thoroughly examined, with the firewall utilizing predefined rules and policies to determine whether a connection request should be accepted or rejected.

This proactive approach to security helps mitigate various risks, including unauthorized access attempts, malware infections, and data breaches. The firewall acts as a gatekeeper, effectively filtering out potentially harmful traffic while enabling legitimate users and services to communicate with internal resources without any hindrance.

Moreover, the firewall configuration is regularly reviewed and updated to address emerging threats and vulnerabilities. This proactive maintenance ensures that the network remains resilient against evolving security challenges and maintains a strong defense posture.

In addition to firewall protection, other security measures such as intrusion detection systems (IDS) and intrusion prevention systems (IPS) may be employed to further enhance the security posture. These systems monitor network traffic for suspicious activity and can automatically take action to block or mitigate potential threats in real-time.

Overall, the network's security architecture, with a robust firewall at its core, provides effective protection against unauthorized access and potential security breaches. By implementing these measures, the network ensures the integrity, confidentiality, and availability of critical resources, offering peace of mind to both users and stakeholders.

# Quality of Service

My design provides a great priority of service because it enables usage of local or external servers depending on availability which provides the university with prioritization of services such as email, data, etc.

Quality of Service (QoS) plays a vital role in network design by prioritizing critical services to maintain optimal performance and user experience. QoS implementation ensures that services like email, data access, and other essential applications used by the university community receive priority treatment.

One important aspect of QoS implementation is the dynamic allocation of resources based on availability. This involves utilizing both local servers within the university's network infrastructure and external servers or resources accessible via the internet. By intelligently routing traffic to the most suitable and available resources, the network enhances performance and guarantees reliable access to crucial services.

For instance, during peak demand or localized network congestion, the system may prioritize access to local servers to reduce latency and provide a responsive user experience. Conversely, if local resources are inadequate, the network can redirect traffic to external servers or cloud-based services to ensure uninterrupted service.

Moreover, QoS mechanisms are configured to prioritize specific types of traffic, such as email or data transfers, over less critical activities. This prioritization ensures that essential services receive the necessary bandwidth and resources, maintaining consistent performance levels even during peak usage or resource constraints.

Regular monitoring and analysis of network traffic patterns enable administrators to adjust QoS parameters and respond to changing conditions effectively. This ensures that the network meets the university's requirements for reliability, performance, and accessibility of critical services.

In conclusion, the QoS implementation in this network design offers the university community reliable and responsive access to essential services, regardless of fluctuations in demand or resource availability.

# Centralized Management

The network includes detailed logging systems built in to the devices and are monitoring and logging every incoming and outgoing connection to the device whilst also any errors or success messages are also being logged for specialists to go back and monitor if needed.

Centralized management plays a crucial role in efficient network administration by enabling streamlined monitoring, configuration, and troubleshooting across all network devices through a unified interface. Detailed logging systems integrated into each device facilitate this centralized management in the network architecture.

The logging systems meticulously document all incoming and outgoing connections to the network devices, capturing not only connection attempts but also errors and successful connections. This comprehensive logging provides network administrators with valuable insights into network activity and performance, allowing them to proactively address potential issues.

A significant benefit of centralized logging is its role as a centralized repository for all network-related data. This repository simplifies the monitoring and analysis of network activity, providing administrators with a single source of truth for troubleshooting and performance evaluation. Moreover, centralized logging aids in compliance with regulatory requirements and internal policies by ensuring thorough documentation and auditability of network activity.

Additionally, the logged data serves as a valuable resource for post-incident analysis and forensic investigation. In the event of a security breach or network outage, administrators can refer to the logs to reconstruct events, identify root causes, and implement preventive measures to prevent future occurrences.

In conclusion, the integration of detailed logging systems into each network device enhances centralized management capabilities by offering comprehensive visibility into network activity and performance. Centralized logging empowers administrators to maintain a secure, efficient, and resilient network infrastructure.

# Campus Connectivity

The network connects all three campuses together as if they are backups of each other whilst also sharing data and resources to ensure that people in campus a can access required data that are in other campuses if needed from campus A servers. If campus A server go down they can switch over to campus B or C to continue with the work they need to do with no issues.

The network design implemented in this context establishes a seamless and resilient environment within the campuses, enabling them to function as backups for one another. This interconnectedness not only facilitates the sharing of data and resources but also guarantees uninterrupted operations in the event of a server failure or outage.

To achieve this, each campus is connected through redundant links, which offer multiple paths for data transmission between them. This redundancy significantly reduces the risk of single points of failure and enhances the network's ability to tolerate faults. Consequently, if a server failure or network outage occurs in one campus, users can seamlessly switch to accessing data and resources from servers located in other campuses.

For instance, if a server in Campus A experiences downtime, users can swiftly redirect their requests to servers situated in Campus B or C without any disruption to their workflow. This failover mechanism ensures continuous access to critical data and resources, thereby maintaining productivity and minimizing downtime for users across all campuses.

Furthermore, efficient data replication and synchronization mechanisms facilitate data sharing between campuses. These mechanisms ensure that important data and resources are consistently updated and available across all campuses, thereby promoting collaboration and productivity among users.

The campus connectivity architecture also incorporates centralized management tools and monitoring systems. These tools and systems enable network administrators to proactively identify and address potential issues before they impact users. Additionally, regular testing and simulation of failover scenarios are conducted to validate the effectiveness of the network's redundancy and failover mechanisms, ensuring preparedness to handle any unexpected events.

In conclusion, the campus connectivity architecture establishes a robust and resilient network infrastructure that fosters collaboration, data accessibility, and continuity of operations across all campuses.

# Wireless Infrastructure

The network contains multiple WIFI access points to ensure that students and staff both have the capabilities to use Wi-Fi enabled devices on the network without security risk as the WIFI access points are positioned deep inside of the network for internal usage only so that external factors or connections cannot directly interact with the WIFI network as this would be a security risk due to the lack of security WIFI has compared to wired networks.

The network design strategically deploys the wireless infrastructure to ensure reliable Wi-Fi connectivity for students and staff, while also implementing robust security measures. Multiple Wi-Fi access points are strategically positioned throughout the campus to ensure comprehensive coverage and reliable connectivity for users with Wi-Fi-enabled devices.

A key aspect of the wireless infrastructure design is the placement of Wi-Fi access points deep within the network, limiting access to internal users only. This internal positioning serves two important purposes. Firstly, it optimizes Wi-Fi coverage within campus buildings and facilities, minimizing areas with poor connectivity and ensuring consistent access throughout the campus. Secondly, it mitigates security risks associated with external access to the Wi-Fi network.

By placing Wi-Fi access points deep within the network infrastructure, external factors and unauthorized connections from outside the campus perimeter are unable to directly interact with the Wi-Fi network. This provides protection against potential security threats and unauthorized access attempts that could compromise sensitive data or disrupt network operations.

Additionally, the network incorporates robust security measures to address the inherent risks of wireless communication. These measures may include encryption protocols, authentication mechanisms, and intrusion detection systems, among others. By enforcing strict security policies and protocols, the network ensures that only authorized users can access the Wi-Fi network, safeguarding the integrity and confidentiality of network resources and data.

In conclusion, the wireless infrastructure design prioritizes both connectivity and security, offering students and staff reliable Wi-Fi access while effectively safeguarding against potential security threats.

# Network Security

The network contains a firewall to control incoming and outgoing traffic of the network to ensure the best possible security of the ABC Universities network infrastructure and data. The network also includes software that is able to protect data such as encryption and access control systems so that not just anyone can access important and confidential data stored on the network.

The protection of network security is of utmost importance in ensuring the integrity, confidentiality, and availability of data within the infrastructure of ABC University. To enhance its resilience against potential threats, the network incorporates multiple layers of security measures, with a firewall serving as the primary line of defense.

The firewall diligently regulates both incoming and outgoing traffic, acting as a barrier between the university's internal network and the external internet. By enforcing predefined rules and policies, the firewall meticulously examines each connection request, permitting authorized traffic to pass through while obstructing or filtering out potentially harmful or unauthorized access attempts. This proactive approach to traffic management effectively mitigates a wide range of security risks, including unauthorized access, malware infections, and denial-of-service attacks.

In addition to the firewall, the network employs advanced software solutions to safeguard sensitive data stored within its infrastructure. Encryption technologies are utilized to encode data, making it incomprehensible to unauthorized users or malicious individuals who may attempt to intercept or eavesdrop on network communications. This ensures that even if data is intercepted, it remains secure and confidential, safeguarding sensitive information such as student records, research data, and administrative documents.

Furthermore, access control systems play a crucial role in reinforcing network security by regulating user permissions and privileges. Through robust authentication mechanisms, such as username/password credentials or multi-factor authentication, access to critical data and network resources is strictly limited to authorized personnel only. This stringent control helps prevent unauthorized access and unauthorized modifications to data, thereby reducing the risk of data breaches and insider threats.

In conclusion, the network's comprehensive security architecture, which encompasses firewalls, encryption, and access control systems, provides a robust defense against a multitude of cyber threats. By implementing these measures, ABC University ensures the protection of its network infrastructure and the confidentiality of its valuable data.

# Bandwidth Management

Due to issues with the software there was no way to configure bandwidth correctly therefore after several attempts to overcome the technical issues I had to move on to other parts of the network as I had a deadline for the work to be done. In the future I will implement bandwidth management by setting min and max values on the network of what devices can use what amount of bandwidth and monitor what devices are using the most bandwidth and what for to help better improve and adjust the bandwidth manager over time of usage.

Bandwidth management is essential for enhancing network performance and ensuring fair access to resources. Despite facing technical obstacles related to software configuration, proactive measures were taken to tackle the issue within a limited timeframe.

Although immediate resolution was not possible due to time constraints, a forward-looking strategy was implemented to enforce efficient bandwidth management practices. This involves establishing minimum and maximum bandwidth limits for devices connected to the network, promoting equitable resource distribution and preventing any single device from monopolizing bandwidth at the expense of others.

The utilization of monitoring tools will be crucial in this initiative, offering valuable insights into bandwidth consumption patterns and identifying devices that are using an excessive amount of bandwidth. By identifying the devices consuming the most bandwidth and the reasons behind it, adjustments can be made to optimize resource allocation and alleviate network congestion.

Continuous monitoring and analysis of network traffic will allow for the fine-tuning of the bandwidth management system over time. By continuously refining policies and thresholds based on actual usage data, the network can adapt to changing demands and ensure optimal performance for all users.

Despite initial setbacks that may have delayed implementation, the proactive approach to bandwidth management showcases a dedication to improving network efficiency and user satisfaction. Looking ahead, ongoing adjustments and adaptations will be essential in maintaining a balanced and responsive network environment.

# Technical Issues

Bandwidth management and IP/network configuration play a crucial role in network administration, contributing significantly to performance optimization and seamless connectivity. Nevertheless, challenges arose when configuring the network simulation software, leading to the need for alternative solutions within strict time constraints.

The software's limitations affected bandwidth management, hindering the direct configuration of bandwidth parameters and the implementation of targeted control measures. Despite efforts to overcome these obstacles, the urgency of the deadline necessitated a shift in focus to other network components.

Similarly, IP and network configuration encountered difficulties due to the software's constraints. The inability to adjust IP settings and network configurations in the simulation environment impeded efforts to achieve optimal network performance. Tasks such as subnetting, routing configuration, and IP address allocation were impacted, requiring innovative approaches to maintain functionality within the specified timeframe.

To address these issues, a practical approach was adopted, prioritizing tasks that could be completed within the given limitations. While bandwidth management and IP/network configuration faced challenges, attention was redirected to other network elements to ensure the project's timely completion.

Looking ahead, the lessons learned from these obstacles will guide future strategies for network configuration and management. Proactive measures will be implemented to anticipate and address technical challenges, facilitating smoother implementation of bandwidth management and IP/network configuration in upcoming projects.

Despite the constraints posed by software limitations and time constraints, the experience highlights the significance of adaptability and resourcefulness in network administration.

# Conclusion

The network design outlined above adopts a comprehensive approach to connectivity, security, scalability, and management, establishing a strong and resilient infrastructure. By seamlessly linking various locations, the design guarantees uninterrupted communication and data transfer, while also reducing the risk of failures through redundancy and failover mechanisms.

Security is a key focus, with the inclusion of firewalls, encryption, and access control measures to prevent unauthorized access and potential threats, safeguarding sensitive data's confidentiality and integrity. Centralized management tools further enhance efficiency by allowing streamlined administration and monitoring of all network components, ensuring consistency in policies and configurations.

Scalability is another crucial aspect, enabling the network to expand and adapt as organizational requirements change. Through meticulous subnet calculations and scalable architectures, the design accommodates future growth without compromising performance or reliability.

Quality of Service mechanisms play a vital role in prioritizing critical applications, guaranteeing optimal performance and user experience even during peak usage times. This, combined with campus connectivity efforts and a robust wireless infrastructure, promotes collaboration and accessibility while upholding security and reliability.

Despite potential challenges like bandwidth management issues and network simulation software limitations, proactive measures and adaptive strategies are implemented to overcome obstacles and drive progress.

In summary, this network design reflects a dedication to innovation, reliability, and adaptability, ready to meet ABC University's diverse user base's evolving needs in a secure, seamless, and scalable networking environment.