ASIA PACIFIC UNIVERSITY OF TECHNOLOGY & INNOVATION

GROUP ASSIGNMENT

NAME (TP NUMBER)	**:**	Androjuniko (TP081988) Tung Jean San (TP082276) Koo Wai Kit (TP081761)
INTAKE CODE	**:**	APUMF2406CYS
MODULE TITLE	**:**	Network Design and Performance (072024-KRV)
MODULE LECTURER	**:**	Dr. Kuruvikulam Chandrasekaran Arun
PROJECT TITLE	**:**	Assignment Task 1: Network Development Life Cycle (NDLC) Part 1
DATE ASSIGNED	**:**	1/8/2024
DATE COMPLETED	**:**	4/9/2024

Table of Contents

List of Figures

List of Tables

1.0 Introduction

National Technological University (NTU) is a renowned institution in Malaysia, widely known for its commitment to academic quality, advanced and latest research, as well as providing a lively studying environment. The university, which was established in 1992, stretches 50 acres wide, equipped with the newest facilities, including research centres, libraries, and dedicated recreational areas to support the students' needs. Among its wide array of research departments, the Internet of Things Research Centre (IoTRC) has been faced with continuous issues with its Local Area Network (LAN). A recent performance test carried out by NTU's Information and Communication Technology (ICT) team suggested that the current LAN at the IoTRC did not result in a desired performance, causing a noticeable disruption for faculty and students involved in research activities, especially in the cyber security field.

The unsatisfactory performance of the LAN has been a major obstacle, obstructing the centre's ability to assist high-demand research tasks productively. This problem highlighted the demand for a reliable and responsive network that lines up with the university's dedication to promote innovation and supporting its academic and research goals. Recognising the urgent need, the ICT team, in cooperation with the university senate, academic staff, and students, came to an agreement to embark on a project to remodel and reconstruct the IoTRC's LAN. The main objective of this initiative is to build a dedicated high-speed LAN specially made for research purposes, therefore warranting that faculty and students can carry out their research without having to worry about network-induced delays.

Given NTU's priority on academic excellence and technological development, it is assumed that the university prioritises network reliability and performance as crucial goals in this redesign effort. This report examines various network design approaches, including top-down and bottom-up approaches, to identify the best suited model for addressing NTU's network problems. Additionally, the analysis will take into account the alignment of technical specifications with NTU's wider strategic objectives, eventually providing a thorough solution that improves the LAN's reliability, performance, and scalability to meet existing and upcoming demands.

Additionally, this report focuses on addressing the network challenges faced by NTU's IoTRC by evaluating various network models and simulation tools. The report explores different network models to identify the most suitable design for the centre's needs, considering factors such as scalability, reliability, and security. Several network simulation tools will also be examined to determine which one best supports the implementation and testing of the selected network design. This allows network to be designed from the ground up to support the expected growth in high-bandwidth applications and intensive research activities, leading to enhanced ability of the research centre to remain prominent in terms of technological advancements. Ultimately, the redesigned network will serve as a robust foundation that aligns with NTU's goals, supporting both present needs and future demands as the IoTRC continues to grow its research capabilities.

2.0 Network Design Approaches

2.1 Network Design Approach

A network design approach is an organised procedure used to design a network that satisfies the communication needs of an organisation or environment (Petryschuk, 2024). The action meticulous planning and applying network elements such as access points, switches, routers, and the protocols required for the network to provide efficient and reliable operation. Network design approaches help in addressing a wide array of technical needs, such as scalability, security, and performance, by providing a clear structure that controls the design and implementation of network infrastructure. The choice of approach is essential, as it has a direct impact on how well the network orients with organisational goals, adapts to upcoming needs, and addresses prospective challenges.

There are two main network design approaches: the top-down approach and the bottom-up approach. The top-down approach begins with a detailed analysis of the organisation's goals, demands, and advanced needs. It emphasises understanding the operational goals before selecting the suitable technologies that align most with the determined objectives (Petryschuk, 2024). This approach is comprehensive, ensuring that the network infrastructure is designed to meet the specific requirements of the organisation, making it perfect for sophisticated environments such as universities or large businesses.

On the contrary, the bottom-up approach focuses on leveraging existing network components and setups to build or grow the scale of a network. This method is normally faster and more flexible, as it depends on accessible technologies and standard configurations that can be implemented at high speed. While the bottom-up approach can be efficient for smaller-sized projects or environments with narrowly defined requirements, it lacks in the detail of planning and customisation that the top-down approach provides. Selecting the proper network design approach depends on various aspects, such as the size of the organisation, the complexity of the network requirements, and the priority that is being put on performance, scalability, and future growth.

2.2 Top-Down Approach

The top-down approach starts with identifying the operational goals and the technology that is best suited with them. For instance, a default or widely used commercial router would be perfectly fine for a small office that has five to ten staffs in it. It would be different if it were a big organisation such as NTU in the given case, in which it would need a more reliable router with the latest WIFI standard and the necessary network routing throughout different floors or buildings to ensure peak performance. So instead of a one-size-fits-all solution, the top-down approach is more detailed in planning and more time consuming. As a result, it is widely agreed upon that the top-down approach is the better and more careful approach especially for businesses because its primary concern is the long-term usage of the network.

2.3 Bottom-Up Approach

While the top-down approach begins with identifying the important areas of an organisation and apply the most suitable network design, the bottom-up approach uses existing network configurations that are versatile, therefore ready to be implemented at any time. The readily available configurations have the necessary hardware specifications, bandwidth allocation, and other components prepared for a network to work. This is best used in instances where a user is short on time or is already familiar with the business needs and simply need to focus on refinements in some areas of the network such as expanding the coverage of a network or increase the bandwidth. As for NTU's situation, this would not be the best option since it does not prioritise performance and reliability in the network design process, which will create more problems in the future as the network demand grows. Unless there is a time constraint, which in this case is not indicated and assumed to have no sense of urgency at all, it would be best to avoid the bottom-up approach.

2.4 Comparative Analysis of Both Approaches

The top-down and bottom-up network design approaches offer different methodologies that serve different organisational needs, especially in terms of performance, scalability, cost, and deployment speed. The top-down approach starts with a focus on the organisation’s goals and makes sure that the chosen technologies match with the objectives (Crespi, 2005). By starting with a high-level study of the organisation's requirements, this approach reduces potential issues related to the network performance and reliability. This detailed planning procedure ensures that the network is built based on the specific operational requirements, making it a more solid option for environments where network reliability is crucial, such as in large organisations like universities or corporations.

Scalability is another important consideration that sets apart the two approaches. In a top-down design, scalability is integrated into the early planning stages, ensuring that the network is adaptable against future growth without having to go through significant reconfigurations or disruptions. This anticipation is essential for organisations that may consider expansion, which includes adding new devices, users, or services. On the other hand, the bottom-up approach often prioritises swift deployment over long-term flexibility. While it may offer a fast and cost-effective solution, its drawback starts to show in situations where scalability is a priority. Reconfigurations in a bottom-up design can result in new problems in other areas of the network, potentially causing increased maintenance, operational challenges, and additional financial costs over time (McClure, 2024).

That being said, the comprehensive nature of the top-down approach also brings certain disadvantages, especially in terms of cost and time. Since meticulous planning, detailed analysis, and prolonged testing are involved, the top-down approach requires a demanding investment of both financial and human resources. This makes it a rather costly option, which may not seem as valid of an option for smaller organisations with a limited budget or less complicated network requirements. In contrast, the bottom-up approach is naturally less time-consuming and therefore a budget friendly option. By utilising existing configurations and emphasising quick deployment, it reduces the financial costs and implementation time, making it best for smaller organisations where speed and budget limitations are notable considerations.

In addition, if an organisation is unlikely to expand significantly in the near future, the simple and less costly nature of the bottom-up approach can be worthwhile. It provides a quick solution that meets the urgent needs without having to over-engineer. This simplicity, however, comes at the cost of the network being more rigid and increased potential challenges in adapting to future growth or demand changes.

In summary, the choice between top-down and bottom-up approaches lies on the specific needs and constraints of the organisation. The top-down approach offers a meticulous and scalable solution, while being more expensive and takes longer to implement, making it ideal for massive and more complex environments. Meanwhile, the bottom-up approach is a faster and more economical option suited for smaller organisations with less focus on scalability and long-term resilience. Understanding these trade-offs is important for selecting the appropriate network design approach for a specific situation.

2.5 Selected Approach and Justification

Since the redesign was carried out to fix the issues of the university LAN for research purposes, it is assumed that the performance and reliability of the network would be the top concern instead of time constraints, if there were any. With that in mind, the appropriate network design choice would be the top-down approach as opposed to the bottom-up approach.

The top-down approach goes through an in-depth analysis of the organisation's requirements, which includes the scale and the organisation's daily operation. This practice considers the extensive size of the university with multiple buildings, broad availability of faculties, and student bodies, making sure that the network can handle a large number of devices and users at any given time. It also analyses the types and the amount of data traffic that the network has to handle, enhancing the network to manage research activities that are high in demand without making any sacrifice to the performance.

In addition, the top-down approach assesses the hardware compatibility with a wide array of devices to ensure that the technologies used can integrate with the current infrastructure. This is important for a large organisation such as NTU where there is a demand for a wide list of research tools, computers, and IoT to work well in tandem. Prioritising hardware compatibility lowers the risk of network issues that can get in the way of the workflow of research.

Moreover, the detailed nature of the top-down approach takes into account the scalability and adaptability aspect of the network in the future, which would be important as the organisation grows and adopt more advanced technologies. This involves predicting potential issues such as increased number of users, evolving security threats, and higher bandwidth. At the end of the day, they provide a reliable foundation for current and future research strategies.

To sum up, the top-down approach is more appropriate for situations where network performance is the main goal, such as the assumption made for the case above. However, due to the nature of the top-down approach being meticulous, it goes without saying that the process takes a lot of time before the network is ready for use. On the contrary, the bottom-up approach emphasises the speed at which a network can be deployed in an environment, eliminating the need for processes that are overly detailed.

3.0 Analysis of Business and Technical Goals

When designing a network, it is crucial to understand both the business and technical goals in order to create a solution that caters to the customer's requirements effectively (Oppenheimer, 2019). Business goals focuses on how the network can enhance the organisation's ability to deliver better products and services, ultimately supporting the mission and vision of NTU. On the other hand, technical goals are essential for ensuring that the network infrastructure meets the demands of users while remaining manageable and affordable. By catering to both business and technical goals, NTU can create a network that supports both current and future needs, fostering a culture of innovation and excellence in the IoT research environment. The following sections discusses on the business and technical goals of the NTU's IoTRC network redesign project.

3.1 Business Goals

Business goals are crucial in a network design project as they ensure that the network infrastructure aligns with the institution's overall mission and objectives. Additionally, understanding the business goals helps the team to prioritise network requirements based on the impact on the NTU's operations. This can ensure the optimisation of resource allocation as well as providing a good return on investment, contributing to the organisaiton's long-term success. This section provides a discussion on the business goal for the current network design project.

Firstly, the project aims improve the efficiency and effectiveness of research activities in the IoTRC's by ensuring a high network performance and availability. The older unoptimized network caused delays and interruptions in research tasks, leading to decreased productivity. The new high-speed LAN for the IoTRC will ensure a reliable network performance which supports high-bandwidth applications and large-scale data processing, allowing faculty and students to focus on their research activities. This aligns with Cisco's principle of ensuring that network design directly supports business productivity (Oppenheimer, 2010).

Next, this project also aims to reinforce NTU's reputation as a premier higher education and research institution. As an institution known for its state-of-the-art facilities, the redesign will include a cutting-edge network infrastructure equipped with the latest networking technology. This will also improve its ability to support high-demand research and academic activities, producing higher quality research. Overall, this helps to bolster the institution's brand and reputation in the academic community.

Thirdly, the new network redesign must be able to adapt to future technological advancements and research needs. This is supported by Oppenheimer (2010), who highlighted on the importance for future-proofing network infrastructures. As a research centre focused on IoT devices and applications, the research and technology landscape will continue to evolve and advance over the years. Thus, an adaptable and scalable network ensures that NTU can continue to incorporate the new technologies without the need for an overhaul. Long-term adaptability and scalability will ensure that NTU can maintain its technological edge and support innovative researches effectively.

An improved operational efficiency is also crucial to reduce administrative overhead and operational costs. The network redesign should incorporate centralised network management tools and automation, which allows for a simplified and more efficient network management process. A manageable and usable network design helps to reduce the resources needed for network administration as well as lowering the operational cost of the network.

Lastly, it is important for the network redesign to be cost-effective in both initial investment and long-term operational costs. This means that there must be a balance between the network performance and the costs associated with the network, providing valuable returns to the organisation. A cost-benefit analysis can be performed to evaluate the different design options and ensure that the chosen solution provides the best value for investment. Cost-effectiveness also ensures that the network redesign project remains within the budget constraint while delivering the required performance needed to support the business and technical goals.

3.2 Technical Goals

The following section analyses the technical goals that are pivotal to the success of this project, ensuring that the new LAN infrastructure meets the demands and requirements of the NTU's IoTRC and aligns with the network design best practices. There are eight technical goals which will be discussed and analysed in this section, which are scalability, availability, network performance, security, manageability, usability, adaptability and affordability (Oppenheimer, 2010).

Availability should be the primary technical goal for most network projects. It refers to the continuous uptime of the network, with minimal downtime. Designing the network with redundancy can help minimise downtime and ensure availability. This includes backup links, failover mechanisms and redundant hardware that can ensure that the network remains operational even in the event of hardware failures (Oppenheimer, 2010). High availability is essential for maintaining productivity for the IoTRC, where research activities are often time-sensitive and any network downtime may significantly impact the research outcomes. According to F5 (n.d.), the goal of network availability should ideally be 99.999%, which is equivalent to only a few minutes of downtime annually.

Scalability refers to ensuring the network can accommodate future growth in users, devices and data traffic (Oppenheimer, 2019). This means that the redesigned LAN should be planned with future expansions in mind, and must be able to handle increasing numbers of researchers and students, as well as a growth in the number of IoT devices and sensors. This is especially crucial for NTU's IoTRC, as IoT applications commonly involve connecting a large number of devices simultaneously (GTCSYS, n.d.). Scalability can be achieved through various methods, such as utilising modular network architecture and scalable network hardware that allows for easy upgrades. In addition, technologies such as Virtual LANs (VLANs) and network virtualisation allow for network segmentation and assists in managing network traffic efficiently.

The third technical goal analysed is the network performance, which involves an optimised network speed to support high-demand IoT applications and data-intensive research. There are several metrics to measure the performance of a network (Oppenheimer, 2019). In the case of NTU's IoTRC, the important network performance metrics are the bandwidth and latency. IoT devices may vary in their bandwidth requirements depending on the type of data they transmit. For a research centre, the network should be able to handle high bandwidth demands for IoT devices that have data-heavy transmissions, such as videos and real-time analytics data. Low latency is crucial in IoT networks, especially for IoT applications that involve real-time processing (GTCSYS, n.d.). Nabto (n.d.) further explains that low latency is required to unlock the potential of IoT devices, which is crucial for a IoT research centre that focuses on innovation and creating new possibilities for IoT applications. Hence, a network design with high performance will support the efficiency of research tasks and experiments in the IoTRC, contributing to improved productivity, innovation and faster search results.

Affordability refers to a network design that is cost-effective, within the specified budget of the organisation, and provides value for investment (Oppenheimer, 2019). Affordability can involve both upfront costs as well as long-term operational costs. Affordability is crucial for NTU, which is an education institution where resources may be limited. Hence, the design must find a balance between cost and performance. Several methods can help to ensure the affordability of the network. For instance, a cost-benefit analysis can be performed to evaluate the various network component and solution options, avoiding unnecessary expenditures while meeting the technical requirements. In addition, the team can also leverage existing infrastructure from the old network if possible, as well as opting for open-source solutions provided that the design will still align with the other business and technical goals.

Security is one of the most important goal in a network design. It involves protecting network data and resources from unauthorised access and cyber threats. GTCSYS (n.d.) explains that security is a common concern in IoT devices as they often deal with sensitive data. Furthermore, an IoT network consists of a large amount of connected devices, where each device serve as a potential point of vulnerability. Hence, it is important to secure the network to safeguard sensitive research data, prevent unauthorised access to the IoT devices and maintain the integrity of the research environment. To ensure a secure network, the network assets must first be identified and risk assessment should be performed. Organisations must also ensure security by implementing strict access control policies, encryption, and network security tools such as firewalls, intrusion detection systems (IDS) and intrusion protection systems (IPS).

A manageable network is crucial to ensure the network runs smoothly and efficiently (Oppenheimer, 2019). FCAPS is a popular network management framework, which breaks down network management functions as fault management, configuration management, accounting management, performance management and security management. Ensuring that the network is easy to maintain and troubleshoot can also help reduce human error and minimise administrative overhead. Additionally, a manageable network also ensures that any issues can be identified and resolved immediately, reducing any disruptions to the research activities carried out in the IoTRC.

Usability refers to a network that is user-friendly and meets the requirements of its users (Oppenheimer, 2019). A network that prioritises on the user experience allow for easy access to network resources and network management interface that is simple with low learning curve. Additionally, compatibility with a wide range of devices is crucial in a IoT research centre where many different types of IoT devices and sensors may be tested and used. Usability is crucial for the research centre to support research activities without unnecessary complexities. However, it should be noted that usability is often sacrificed for increase network security. For instance, strict password policies that require frequent changes may not be user friendly, but ensures a highly secure network. Hence, it is important to balance between the usability of the network without compromising its security and performance.

Lastly, the adaptability of a network involves designing a network that can accommodate future changes in technology (Oppenheimer, 2019). The rapid evolution of IoT technology means that adaptability is a necessity for the IoTRC. This includes adaptability to new IoT devices, protocols as well as research requirements. Network adaptability can be achieved by implementing a flexible and modular network architecture that enables the integration of new and upgraded technologies without disrupting the network. Adaptability ensures that the network can evolve with technological advancements and changing research requirements, maintaining its relevance and effectiveness without the need to for a complete overhaul.

4.0 Network Models

First of all, network models define the arrangement and connections of network nodes, such as switches and routers, as well as the data flow between them (Cisco, n.d.).

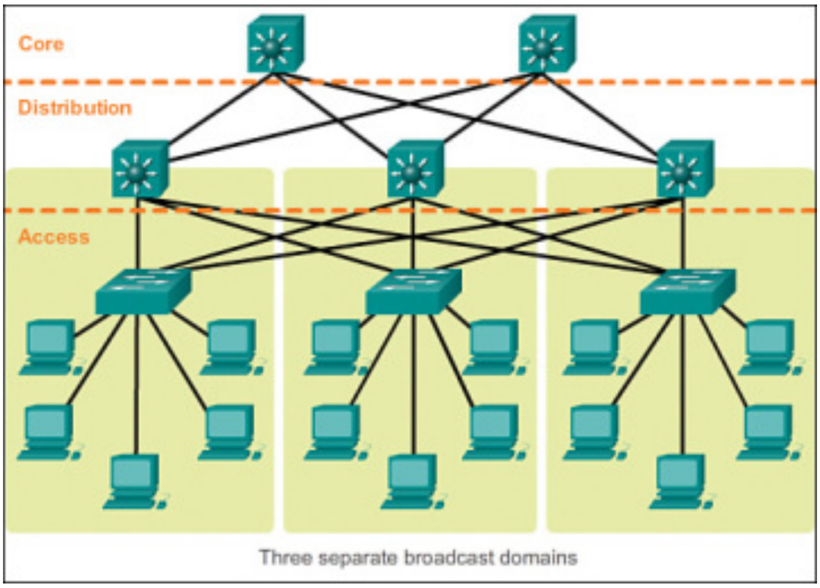
In order to design an efficient and high-performing LAN for NTU's IoT Research Center (IoTRC), selecting the appropriate network model is crucial. The chosen model will determine how well the network can meet the centre’s technical and research needs. This section will explore three key network design models, which consists of the Cisco Hierarchical Internetworking Model, the Spine-Leaf Architecture, and the Mesh Network Design. Each of these models is particularly suitable for large LAN networks, offering different advantages depending on the specific requirements of the infrastructure. The models will be assessed for their suitability in improving the centre's network infrastructure.

4.1 CISCO Hierarchical Internetworking Model

4.1.1 Design

The Cisco Hierarchical Internetworking Model is a standard framework used for designing networks that are scalable, reliable, and cost-effective (Cisco Press, 2014). This model is also known as the traditional three-tier hierarchical model. In this model, network is organised into three distinct layers: Access, Distribution, and Core, each serving a specific function. An illustration of this model can be found under Figure 1.

Figure 1: Hierarchical Network (Cisco Press, 2014)



According to Cisco Press (2014), the Core Layer acts as the network backbone, providing high-speed data transport across the network. It interconnects various distribution devices and connects to external networks such as WAN and the Internet. This layer is designed for high-speed switching and redundancy to support fast and reliable data forwarding. It ensures that data can traverse the network quickly and efficiently, connecting different network segments and maintaining high performance.

In addition, the Distribution Layer acts as an intermediary between the Access and Core layers (Cisco Press, 2014). It aggregates data from the Access Layer and routes it to the Core Layer. This layer often uses routers or multilayer switches to manage policy-based security, handle routing between VLANs, and provide redundancy. It also serves as a boundary between Layer 2 and Layer 3 network segments, helping to segment and manage network traffic effectively.

Furthermore, the Access Layer is responsible for connecting end devices to the network (Cisco Press, 2014). It typically includes Layer 2 switches and access points that facilitate device connectivity. This layer handles essential functions like Layer 2 switching, port security, Quality of Service (QoS), and Power over Ethernet (PoE), ensuring that devices can access network resources efficiently.

4.1.2 Benefits

This model is widely adopted for its numerous benefits, including improved performance, reliability, scalability, security, manageability, and cost-efficiency (Popa, 2024).

Popa (2024) explains that it improves performance by utilising high-speed switches in the distribution and core layers, which ensures that data travels quickly and efficiently, minimising latency and bandwidth issues. Reliability is increased due to the network's modular structure, allowing faults to be isolated and rerouted while redundancy in the distribution and core layers supports continuous operation. Scalability is facilitated by the design's modular nature, which makes expanding the network straightforward and minimally disruptive. In terms of security, the separation of network functions allows for precise control over traffic and effective implementation of access policies. Manageability is enhanced because each network layer serves a specific function, simplifying management and troubleshooting. Finally, cost efficiency is achieved by optimizing equipment use and avoiding unnecessary expenses, with incremental expansion which enables cost-effective scaling.

4.1.3 Limitations

One significant issue for this model is when the core layer device fails, it can cause a network outage, impacting all connected devices and disrupting network operations (Jain, 2023). Additionally, Jain (2023) also states that the hierarchical topology can be challenging to configure. The complexity of setting up multiple layers requires careful planning and skilled configuration, which can be time-consuming and prone to errors. These factors can complicate network management and increase the risk of disruptions.

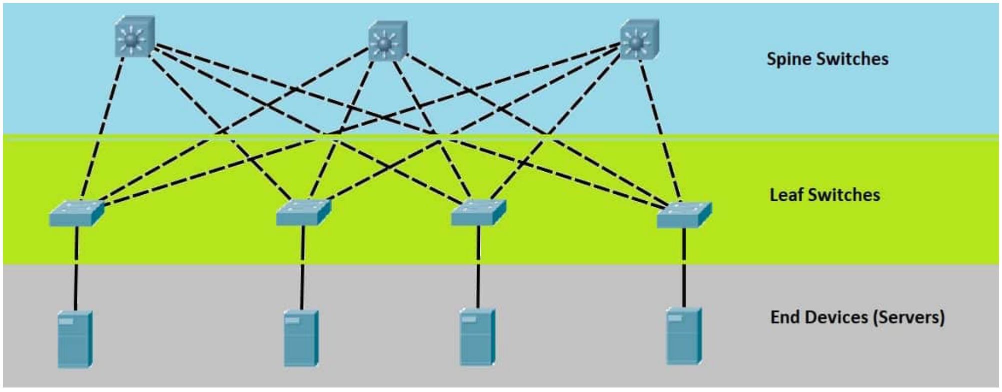
Additionally, a limitation of the three-layer hierarchical design is its focus on north-south traffic and reliance on Spanning Tree Protocol (STP), which supports up to 100 switches (Moore, 2023). As network traffic increases, this structure can lead to port blockages and scalability issues, potentially affecting performance and efficiency.

4.2 Spine-Leaf Architecture

4.2.1 Design

The Spine-Leaf Architecture is a two-layer, full-mesh network design used primarily in data centres to address the limitations of traditional three-tier architectures (Study CCNA, n.d.). Unlike the three-tier model, which is optimized for north-south traffic, the Spine-Leaf model is designed to efficiently handle east-west traffic, which involves server-to-server communication within the same data centre, as illustrated under Figure 2.

Figure 2: Leaf-spine network topology (Study CCNA, n.d.)



In this architecture, the spine layer acts as the network's backbone, similar to the core layer in a three-tier design. Spine switches, which are typically Layer 3 switches, connect to each leaf switch, ensuring that traffic can be quickly routed through the network without excessive hops or bottlenecks.

Moreover, the leaf layer functions like the access layer in the three-tier model, connecting directly to end devices such as servers. Leaf switches are interconnected with all spine switches, facilitating efficient communication between servers and other devices within the data centre. This setup supports various types of servers, including web, application, database, and storage servers.

4.2.2 Benefits

According to Study CCNA (n.d.), this architecture offers several significant benefits for network design. Firstly, it enhances redundancy by connecting every leaf switch to all spine switches, utilizing technologies like Shortest Path Bridging (SPB) and Transparent Interconnection of Lots of Links (TRILL) instead of STP. This full-mesh approach ensures that traffic can flow across multiple active links, reducing the risk of network failures and providing improved redundancy. By allowing all available links to be used, it also boosts bandwidth, as opposed to STP, which limits the use of active links. Additionally, the architecture supports increased scalability, enabling easy expansion by adding more spine or leaf switches as needed to accommodate higher traffic volumes or port density concerns.

Another advantage of the Spine-Leaf Architecture is its cost efficiency and performance benefits (Study CCNA, n.d.). Fixed-configuration switches, commonly used in this setup, are generally more cost-effective and energy-efficient compared to modular switches. With a maximum of two hops between any source and destination, the architecture minimizes latency and avoids congestion, leading to improved network performance. This efficient design reduces power consumption and operational costs, making it a practical choice for modern data centres where high performance and scalability are essential.

4.2.3 Limitations

One major drawback for this architecture is the increased cabling requirement, as every leaf switch must be connected to all spine switches, leading to a higher demand for copper or fibre cables (Study CCNA, n.d.). Additionally, the architecture can face limitations on the number of hosts supported, as the spine's port count can restrict the number of connections to leaf switches. This can impose constraints on the scalability of the network, particularly in environments with a large number of devices.

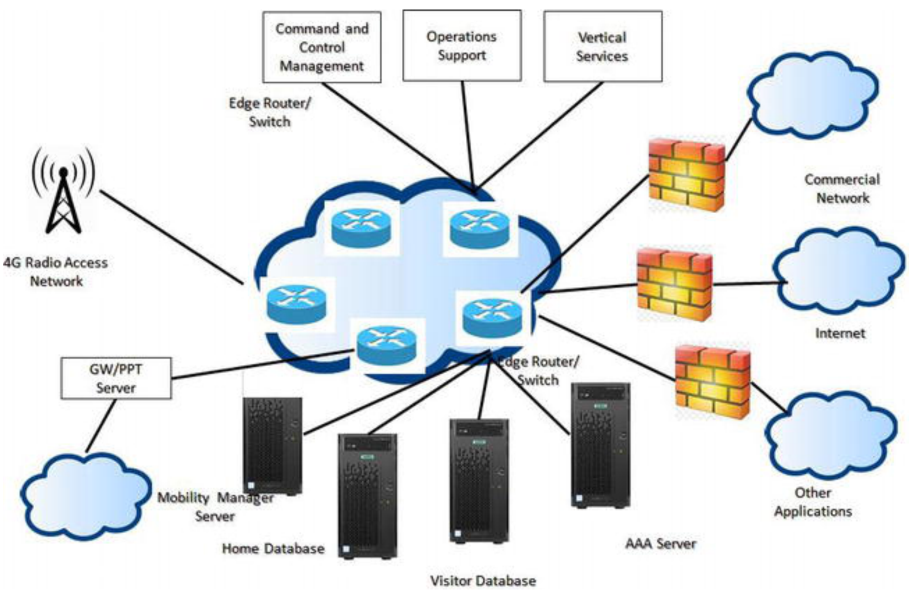
4.3 Mesh Network Model

4.3.1 Design

A mesh network is a LAN topology where devices, or nodes, connect in a non-hierarchical, fully interconnected manner (BasuMallick, 2022). This design allows nodes to work together to extend network coverage and enhance reliability compared to single-router systems. In a mesh network, each device communicates directly with others, creating multiple paths for data to travel. BasuMallick (2022) explains that this structure is often referred to as "self-configuring" because new nodes automatically integrate into the existing network. Mesh networks can be wired or wireless, and they are designed to improve coverage in large areas or complex environments, such as homes with poor Wi-Fi signals or public infrastructure needing widespread connectivity.

Mesh networks are particularly effective in extending Wi-Fi coverage across large spaces or eliminating dead zones (BasuMallick, 2022). They work by using multiple nodes, each of which connects to every other node, ensuring robust and reliable connections. This design contrasts with traditional Wi-Fi extenders, which create new access points and may still suffer from performance issues. In addition to providing enhanced coverage, mesh networks often come with mobile apps for network management, allowing users to prioritize devices, monitor speeds, and manage connectivity from anywhere (BasuMallick, 2022). An illustration of a mesh network can be found under Figure 3.

Figure 3: Mesh network representation (Parvin, 2019)



4.3.2 Benefits

According to Javatpoint (n.d.), mesh topology offers several notable advantages for network design. One of its key benefits is its resilience to failures; if one node fails, the network continues to function normally, thanks to its numerous redundant connections. This robustness ensures that data transmission remains consistent, as multiple paths are available for routing information, reducing the risk of interruptions even if several nodes experience issues. Additionally, mesh networks allow for easy scalability and flexibility. New devices can be added seamlessly without disrupting existing network traffic, and each node operates as an individual router, facilitating straightforward expansion.

Furthermore, mesh networks do not require centralized control, which enhances privacy and security by allowing for anonymous communication without the need for a centralized authority (Javatpoint, n.d.). The decentralized nature of mesh topology also makes it highly adaptable, enabling efficient management of large volumes of data and maintaining performance as the network grows. This adaptability, combined with the network's ability to handle data through multiple nodes simultaneously, makes mesh topology an excellent choice for large or dynamic environments where consistent, reliable connectivity is essential.

4.3.3 Limitations

This model presents several notable challenges (Javatpoint, n.d.). One significant drawback is its high cost, as the implementation requires extensive hardware, cabling, and bandwidth, making it more expensive compared to other network topologies. Additionally, the initial setup and maintenance of a mesh network can be complex and time-consuming, despite the ease of adding new nodes once it becomes operational. The topology can also suffer from redundant connections due to its extensive network structure, which can increase complexity and workload on each node (Javatpoint, n.d.). Furthermore, mesh networks may experience latency issues because each node is tasked with routing and handling multiple responsibilities, potentially affecting overall network performance.

4.4 Comparative Analysis

Table 1 provides a comparative analysis of the Cisco Hierarchical Internetworking Model, Spine-Leaf Architecture, and Mesh Network Model. The information in the table is obtained from the discussion of the models above. It highlights key aspects of each model to help evaluate each model's suitability for different network requirements.

Table 1: Comparison between network models

Model	Hierarchical	Spine-Leaf	Mesh
Design	Organized into three layers. The Core Layer handles high-speed data transport, the Distribution Layer aggregates and routes data, and the Access Layer connects end devices.	Consists of two layers—Spine and Leaf. Spine switches form the network backbone, connecting to every Leaf switch, which connects to end devices.	Features a fully interconnected structure where each node communicates directly with others. This design can be wired or wireless.
Traffic handling	Optimized for north-south traffic, involving data flow between clients and servers or external networks.	Designed to handle east-west traffic, focusing on server-to-server communication within data centres.	Supports general coverage and dynamic traffic routing, enhancing connectivity and reliability across large areas.
Scalability	Scalable with a modular design that allows for straightforward network expansion.	Highly scalable, with easy expansion by adding more Spine or Leaf switches as needed to handle increased traffic or port density.	Allows for easy scalability by integrating new nodes without disrupting existing traffic, though cabling and hardware constraints may limit scalability.

Redundancy and Fault Tolerance	Provides redundancy through the modular structure of the Distribution and Core Layers.	Offers high redundancy with every Leaf switch connected to all Spine switches, reducing the risk of network failures and improving fault tolerance.	Highly resilient to failures due to multiple redundant connections; if one node fails, data can be rerouted through alternative paths.
Performance	Performance is enhanced by high-speed switches in the Core and Distribution Layers.	Minimizes latency with a maximum of two hops between any source and destination, improving network performance and avoiding congestion.	Performance can be affected by latency due to each node handling multiple responsibilities; however, robust connectivity helps maintain consistent data transmission.
Cost	Cost-efficient in terms of incremental expansion and optimized equipment use, though the initial setup can be expensive.	Generally cost-effective with fixed-configuration switches and energy-efficient design, though the initial cabling requirements can be high.	High implementation cost due to extensive hardware and cabling requirements, though operational costs may be lower due to decentralized management.
Complexity	Complex to configure and manage due to multiple layers, requiring skilled configuration and careful planning.	Relatively straightforward to set up and manage, with less complexity compared to three-tier models.	High complexity in setup and maintenance due to extensive hardware and cabling, though adding new nodes is relatively simple.

Flexibility	Modular design provides flexibility in expanding and adapting network segments.	Flexible and easily expandable, accommodating increased traffic and port density by adding switches as needed.	Highly adaptable with seamless integration of new nodes, making it suitable for large and dynamic environments.
Security	Provides robust security through segmented layers, enabling precise control over traffic and effective access policy implementation.	Enhances security with redundancy and full-mesh connectivity, but security measures depend on the implementation of technologies like SPB and TRILL.	Enhances privacy and security by avoiding centralized control, which allows for anonymous communication and decentralized management.

4.5 Selected Model and Justification

Based on our analysis and the technical goals outlined for NTU's IoT Research Center (IoTRC), the Cisco Hierarchical Internetworking Model has been selected as the most suitable framework for the new LAN infrastructure. This choice aligns with the technical requirements of scalability, reliability, network performance, security, manageability, and affordability.

Scalability is a critical requirement for the IoTRC, given the anticipated growth in the number of IoT devices and research activities. The hierarchical model's modular design, with its distinct Core, Distribution, and Access layers, supports scalability by allowing for incremental network expansion. The model facilitates straightforward upgrades and additions without major disruptions, accommodating future increases in network traffic and device count effectively.

Reliability is another key goal, crucial for ensuring continuous operation in the research environment. The hierarchical model enhances reliability through its modular structure, which isolates faults within specific layers. This isolation minimizes the impact of any single failure and maintains overall network operation. Redundancy built into both the Distribution and Core layers further supports high availability, aligning with the goal of achieving near 99.999% uptime, which is essential for maintaining productivity and ensuring minimal disruptions to research activities.

Network performance is addressed by the Core layer's role as the network backbone, providing high-speed data transport across the network. The use of high-speed switches and efficient routing at the Core and Distribution layers ensures that data is transmitted quickly and efficiently, meeting the high-bandwidth demands of IoT applications and data-intensive research. This setup minimizes latency and optimizes bandwidth usage, which is crucial for supporting real-time processing and high data throughput.

Security is integral to the IoTRC's operations, particularly in safeguarding sensitive research data and IoT devices. The hierarchical model's separation of network functions allows for precise traffic management and the implementation of robust access control policies. The Distribution layer's role in handling policy-based security and routing between VLANs helps to protect the network from unauthorized access and cyber threats, ensuring the integrity and confidentiality of research data.

Manageability is enhanced by the hierarchical structure, which simplifies network management and troubleshooting. Each layer of the model serves a specific function, making it easier to monitor and maintain the network. This clear separation of responsibilities reduces administrative overhead and helps in quickly identifying and resolving issues, thus supporting efficient network operations.

Affordability is also considered, as the hierarchical model's modular approach allows for cost-effective scaling. By optimizing the use of network equipment and enabling incremental expansion, the model helps to manage both upfront and long-term operational costs. This cost-efficiency is crucial for NTU, where budget constraints are a consideration.

In summary, the Cisco Hierarchical Internetworking Model provides a balanced solution that aligns with the technical goals of the IoTRC. Its scalability, reliability, performance, security, manageability, and cost-efficiency make it the most appropriate choice for rebuilding the LAN network, ensuring that the IoTRC can effectively support its research activities and adapt to future technological advancements.

5.0 Network Simulation Tools

For NTU's IoT Research Center (IoTRC), effective network design is crucial to improving the current LAN infrastructure. According to PyNetLabs (2024), network simulation tools are software applications that mimic real network operations using mathematical models and algorithms. These tools play a vital role in this process by allowing the ICT team to create virtual models of the network, test various configurations, and analyze performance without the need for physical hardware (PyNetLabs, 2024). In addition, these tools help in understanding the potential impacts of different network designs and ensure that the chosen model meets the centre's research needs. In this section, we will explore three popular network design tools, highlighting their key features. After analysing the tools, we will decide on the most suitable tool to be used in the IoTRC's network upgrade

5.1 NetSim

NetSim is a comprehensive network simulation and emulation tool designed for modeling communication networks in a virtual environment (TrustRadius, n.d.). NetSim is used by professionals in industry, defense, and academia to design, simulate, analyze, and verify the performance of various networks (Tetcos, n.d.). It enables users to explore the performance and behavior of new network protocols and devices before deploying them in real-world scenarios. NetSim is available in three versions: Academic, Standard, and Pro. The Academic version is focused on lab experiments and teaching, the Standard version is used for research and development in educational institutions, and the Pro version addresses the advanced needs of defense organizations and industrial applications (Tetcos, n.d.).

One of NetSim's standout features is its user-friendly interface, which allows even those with limited experience in network simulation to easily set up and run simulations (Tetcos, n.d.). The tool supports a wide variety of networks and protocols, including cutting-edge technologies like 5G NR, Ethernet, LTE, Wi-Fi, TCP/IP, IoT and software-defined networks. This versatility ensures that NetSim can model a broad range of network environments, making it adaptable to different simulation needs.

NetSim also offers flexible licensing options, catering to diverse user requirements. Users can choose between perpetual or annual licenses, node-locked or floating licenses, or even cloud-based or on-premise setups (Tetcos, n.d.). NetSim provides the necessary flexibility to meet specific organizational needs. Additionally, NetSim can be connected to external hardware running live applications, allowing users to test their network configurations in a realistic, live environment.

Furthermore, it allows custom algorithms to be developed. NetSim Pro includes protocol source code in C, which can be modified using the integrated MS Visual Studio environment (Tetcos, n.d.). Apart from that, NetSim provides advanced utilities like batch execution of multiple simulations, multi-parameter sweepers, and large-size network scenario generators, all aimed at enhancing productivity and efficiency.

The tool's compatibility with external analysis and visualization tools, such as MATLAB, Simulink, SUMO, Wireshark, and Python, further enhances its utility (Tetcos, n.d.). This integration allows users to leverage the specialized capabilities of these tools for deeper analysis and richer visualizations. NetSim also generates detailed output files in an easy-to-analyze CSV format, which can be opened in Excel or Python Pandas for further examination (Tetcos, n.d.).

To support users in getting started, NetSim includes an extensive library of built-in examples and use-cases (Tetcos, n.d.). These pre-configured scenarios save time and provide a solid foundation for users to build upon, streamlining the process of creating complex network simulations. Lastly, NetSim Pro also provides specialized services, including synthetic data generation for machine learning, custom protocol development, and tailored network modeling and simulation services (Tetcos, n.d.).

5.2 EVE-NG

EVE-NG, which stands for Emulated Virtual Environment - Next Generation, is a network simulation tool that enables users to run and interconnect various virtual and physical devices (Kaushik, 2024). It is available in two editions, which includes a free Community edition, which can be downloaded and used by anyone, and a paid Professional edition that requires a license.

Kaushik (2024) mentions that EVE-NG supports a range of multivendor devices, including Juniper, Cisco, FortiGate, and Palo Alto, offering a comprehensive Cisco platform for network simulation and learning. The simulator is accessible through modern web browsers, featuring an interactive GUI that simplifies topology design and network learning. Kaushik (2024) also highlighted that EVE-NG is particularly valuable for those pursuing network and network security certifications, such as Cisco and NSE, providing an effective environment for practical training and certification preparation.

Based on the documentation provided in its website, EVE-NG offers a range of advanced features across its Community and Professional Editions, enhancing its capabilities for network simulation and emulation (EVE-NG, n.d.). Key features include KVM hardware acceleration, a user-friendly "click and play" topology designer, and robust memory optimization through Kernel Samepage Merging (KSM). The platform supports detailed network design with custom kernel support for Layer 2 protocols, and it features a full HTML5 user interface that eliminates the need for additional tools. Users can create and import lab topologies, interact with real networks, and benefit from simultaneous lab instances.

The Community Edition focuses on improving user interface functionality, enabling easier sharing of designs and configuration files, and providing clientless access to network services through HTML5 (EVE-NG, n.d.). It supports local Wireshark captures and offers options for importing and exporting configurations.

The Professional Edition expands on these features with dynamic console porting, support for up to 1024 nodes per lab, and integration with Docker containers (EVE-NG, n.d.). It includes advanced options like multi-user support with administrator roles, NAT cloud integration, and HTML desktop console management. The platform also supports lab timers for self-training and allows for the simultaneous operation of multiple labs, enhancing its flexibility for complex network simulations (EVE-NG, n.d.). Overall, it streamlines network design and testing, providing detailed control over lab setups and node management (Zawalnyski, 2024).

5.3 GNS3

GNS3, or Graphical Network Simulator-3, is an open-source network simulation tool that supports cross-platform use (Kaushik, 2024). Zawalnyski (2024) states that professionals are able to emulate, configure, and troubleshoot virtual and physical networks using this tool. As an open-source and freely available platform, GNS3 is continuously developed and supported, ensuring it meets the evolving needs of network engineers (Zawalnyski, 2024).

Additionally, GNS3 supports an unlimited number of devices, the only limiting factor is the user's hardware capabilities (GNS3, n.d.). It is able to accommodate multiple switching options and it supports all VIRL images, which includes IOSv and NX-OSv. GNS3 is versatile since it can operate with or without hypervisors, and it supports both free and paid hypervisors like VirtualBox and VMware (GNS3, n.d.). Users can also leverage pre-configured, optimized appliances to simplify deployment.

Besides, GNS3 offers real-time network simulation, enabling precise pre-deployment testing without requiring physical hardware (GNS3, n.d.). It supports testing across more than 20 network vendors in a secure virtual environment, allowing for the creation of dynamic network maps that aid in troubleshooting and proof of concept (POC) evaluations. The platform also allows for the connection of GNS3 topologies to real networks, expanding the functionality of existing hardware. It also supports customised topologies and labs, making it an efficient tool for network design and validation.

5.4 Selected Tool and Justification

After evaluating the network simulation tools, NetSim has been selected as the most suitable tool for NTU's IoT Research Center (IoTRC). This decision is based on NetSim's robust feature set, which aligns closely with the technical goals of the network upgrade project, making it an ideal tool for the centre's needs.

One of the primary reasons for selecting NetSim is its capability to handle complex and large-scale network environments, which is essential for the IoTRC's scalability and network performance requirements. The tool supports a broad range of network protocols and technologies, including advanced options like 5G NR and IoT. Its features for batch simulation and multi-parameter sweeps facilitate the efficient analysis of different network configurations. This supports the technical goal of scalability by allowing the IoTRC to plan for future growth in users, devices, and data traffic, ensuring that the network can handle increased demands effectively.

NetSim also excels in enhancing network availability and reliability, which are critical aspects for the IoTRC since uninterrupted operations are vital for research activities. The tool's ability to integrate with external hardware and run live applications allows for real-time testing and analysis of network configurations. This capability helps in identifying potential issues and optimizing the network design to minimize downtime, thereby supporting the technical goal of high availability. Ensuring that the network remains operational and reliable is crucial for maintaining productivity and research continuity at the IoTRC.

In terms of security, NetSim provides valuable support for developing and testing security measures. Its features for custom algorithm development and protocol testing allow for thorough evaluation of network security in a simulated environment. The tool's detailed output files and compatibility with external analysis tools like Wireshark facilitate comprehensive traffic analysis. These features align with the technical goal of securing sensitive research data and implementing effective network security strategies.

NetSim's user-friendly interface and extensive library of built-in examples contribute to both manageability and usability. The tool's ease of setup and operation enhances network management and troubleshooting. Furthermore, its compatibility with external analysis and visualization tools, such as MATLAB and Python, supports effective network management. This aligns with the technical goal of creating a manageable network design that is easy to maintain and optimize.

Affordability is another key factor in the selection of NetSim. The tool offers flexible licensing options, including perpetual, annual, and cloud-based licenses, which allows the IoTRC to select a plan that fits its budget. This flexibility, along with NetSim's comprehensive features, ensures that it provides good value for investment while adhering to budget constraints. Additionally, the availability of pre-configured scenarios and the option to leverage existing infrastructure contribute to cost-effective network simulation and design.

Overall, NetSim's robust simulation capabilities, combined with its alignment with the IoTRC's technical goals of scalability, performance, availability, security, manageability, usability, and affordability, make it the ideal choice for upgrading the LAN infrastructure. Its extensive features will support effective network design and optimization, ensuring that the network meets the centre's current and future needs.

6.0 Conclusion

The redesign performed on NTU's IoT Research Centre (IoTRC) LAN network is a project aimed at overcoming current performance issues and a form of anticipation for future needs. Through a thorough analysis of various network design approaches, the top-down approach was selected because of its alignment with NTU's goals of reliability, performance, and scalability. This approach shapes the network in such a way that it is tailored to the specific needs of the IoTRC, allowing for a detailed and customised design that can support high bandwidth research and mass data processing. By setting network performance and reliability as priorities, NTU desires to enhance the productivity of its research and strengthen its reputation as a major institution in the field of IoT research.

The evaluation of network models strengthens the decision to implement the Cisco Hierarchical Internetworking Model even further. This model offers a robust and scalable network design with well-defined layers that facilitate efficient data transfer, redundancy, and security. Its adjustable design supports network expansion, ensuring that the network architecture can keep up with the increasing needs of the research centre without causing issues along the way. Additionally, the hierarchical model's emphasis on high-speed data transfer and fault tolerance addresses the IoTRC's need for a reliable and high-performance network, which is important for sustaining the demanding research activities.

In choosing the most suitable network simulation tool, NetSim was selected due to its advanced features and alignment with the main goals of the project. NetSim's ability to simulate complex network scenarios and its compatibility with third-party analysis tools allows for detailed testing and optimisation of network settings. This allows the network to meet both existing and future demands while also maintaining availability and security. Through NetSim, proactive planning and testing are made possible, which is needed for addressing potential challenges and maintaining resiliency in the face of advancing technological field.

Altogether, the combination of the top-down design approach, the Cisco Hierarchical Internetworking Model, and the NetSim simulation tool provides a complete solution that addresses the performance issues of the IoTRC's LAN and prepares it for future growth. The significance placed on scalability, adaptability, and security ensures that the network will not only meet the current demands but also accommodate advancing technologies and expanding research demands. This strategic alignment with NTU's broader objective of promoting innovation and quality in research places the IoTRC to maintain its prominent position in the field of IoT.

In summary, the network redesign initiative directly supports the university's mission of upgrading research efficiency, maintaining high network availability, and future-proofing the network. By implementing a network design that is made specifically for NTU and leveraging enhanced simulation tools, NTU can address its network issues while also building a scalable and reliable network design for future developments. This project not only solves the current challenges but also sets the direction for sustained innovation and expansion.

7.0 References

BasuMallick, C. (2022, August 12). *What Is a Mesh Network? Meaning, Types Working, and Applications in 2022*. Spiceworks. Retrieved from https://www.spiceworks.com/tech/networking/articles/what-is-mesh-network/

Cisco. (n.d.). *What Is Network Topology?*. Retrieved from https://www.cisco.com/c/en/us/solutions/automation/network-topology.html

Cisco Press. (2014, May 9). *Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design*. Retrieved from https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4

Cisco Press. (2014, May 9). *Hierarchical network [Diagram]*. Retrieved from https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4

Crespi, V., Lerman, K., & Galstyan, A. (2005, July). *Comparative analysis of top-down and bottom-up methodologies for multi-agent system design*. ResearchGate. Retrieved from https://www.researchgate.net/publication/221455935_Comparative_analysis_of_top-down_and_bottom-up_methodologies_for_multi-agent_system_design

Dhanraj, P. (2023, February 21). *Top-down approach vs. bottom-up approach*. Simplilearn. Retrieved from https://www.simplilearn.com/top-down-approach-vs-bottom-up-approach-article

EVE-NG. (n.d.). *Key Features*. Retrieved from https://www.eve-ng.net/index.php/features/

F5. (n.d.). *What is network availability?* Retrieved from https://www.f5.com/glossary/network-availability

GNS3. (n.d.). *Getting Started with GNS3*. Retrieved from https://docs.gns3.com/docs/

GTCSYS. (n.d.) *What are the network requirements for IoT applications?* Retrieved from https://gtcsys.com/faq/what-are-the-network-requirements-for-iot-applications/

Jain, A. (2023, April 26). *Network Topologies: Types, Advantages, and Disadvantages*. IncludeHelp. Retrieved from https://www.includehelp.com/computer-networks/network-topologies-its-types-advantages-and-disadvantages.aspx

Javatpoint. (n.d.). *Mesh Topology Advantages and Disadvantages*. Retrieved from https://www.javatpoint.com/mesh-topology-advantages-and-disadvantages

Kaushik, V. (2024, January 13). *Best Network Simulation Tools for Network & Network Security [2023]*. GNS3 Network. Retrieved from https://www.gns3network.com/best-network-simulation-tools/

McClure, M. (2024, January 31). *Top-down vs. bottom-up network design*. CBT Nuggets. Retrieved from https://www.cbtnuggets.com/blog/technology/networking/top-down-vs-bottom-up-network-design

Moore. (2023, September 28). *What is Spine-Leaf Architecture and How Does It Work?*. QSFPTEK. Retrieved from https://www.qsfptek.com/qt-news/what-is-spine-leaf-architecture-and-how-does-it-work?srsltid=AfmBOopBqjBeJVusJRozvgATB3bAQ3jptud1-WoOoA3rAkRiCU8tyunZ

Oppenheimer, P. (2010). *Top-down network design* (3rd ed.). Cisco Press.

Parvin, J. R. (2019, June 10). *Wireless Mesh Networks - Security, Architectures and Protocols*. IntechOpen. https://doi.org/10.5772/intechopen.83414

Popa, L. (2024, May 28). *What is Hierarchical Network Design?*. Auvik. Retrieved from https://www.auvik.com/franklyit/blog/hierarchical-network-design/

PyNetLabs. (2024, January 11). *Top 10 Most Popular Network Simulation Tools*. Retrieved from https://www.pynetlabs.com/top-most-popular-network-simulation-tools/

Petryschuk, S. (2024, July 18). *Network design best practices*. Auvik. Retrieved from https://www.auvik.com/franklyit/blog/network-design-best-practices/

Simplilearn. (2024, August 31). *Top Down and Bottom Up Approaches: Effective Management*. Simplilearn. Retrieved from https://www.simplilearn.com/top-down-approach-vs-bottom-up-approach-article

Study CCNA. (n.d.). *What is Spine and Leaf Network Architecture?*. Retrieved from https://study-ccna.com/spine-and-leaf-architecture/

Tetcos (n.d.). *NetSim Introduction*. Retrieved from https://tetcos.com/help/v13.2/User-Manual/01.%20NetSim-Introduction.html

TrustRadius. (n.d.). *Pros and Cons of NetSim 2024*. Retrieved from https://www.trustradius.com/products/netsim/reviews?qs=pros-and-cons#overview

Zawalnyski, A. (2024, February 13). *The Top 5 Network Simulation Solutions*. Expert Insights. Retrieved from https://expertinsights.com/insights/the-top-network-simulation-solutions/