



INDIVIDUAL ASSIGNMENT

NAME (TP NUMBER)	:	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 2: Network Development Life Cycle (NDLC) Part 2
DATE ASSIGNED	:	1/8/2024
DATE COMPLETED	:	20/9/2024

Table of Contents

1. Introduction.....	4
1.1 Assumptions Made.....	4
1.2 Selected Network Design Approach and Network Model.....	4
2. Floor Plan and NetSim Network Design	5
2.1 Overview of IoT Research Centre Floor Plan.....	5
2.2 Floor Plan Layout Visualisation	5
2.3 NetSim Network Design	7
3. Routing Protocols.....	8
3.1 Open Shortest Path First (OSPF)	8
3.2 Routing Information Protocol (RIP)	9
3.3. Network Metrics Comparison Between OSPF and RIP	9
3.4 Protocol Selected and Justification	10
4. Wireless Local Area Network (WLAN) Standards	11
4.1 IEEE 802.11 a/b/g/n.....	11
4.2 IEEE 802.11 ac/p	12
4.3 Network Metrics Comparison Between IEEE 802.11ac and IEEE 802.11p	12
4.4 Standard Selected and Justification	14
5. Infrastructure Connectivity	14
5.1 Wired connectivity.....	14
5.2 Wireless connectivity.....	14
5.2.1 Transmitter Power.....	15
5.2.2 Antenna Gain	16
5.2.3 Bandwidth	16
6. Data Security.....	17
6.1 Impact of Encryption on Network Traffic Speed	18
6.2 Discussion of NetSim's Encryption Algorithms.....	18

6.2.1 Advanced Encryption Standard (AES)	18
6.2.2 Data Encryption Standard (DES).....	19
6.2.3 XOR Cipher	19
6.2.4 Tiny Encryption Algorithm (TEA)	20
6.3 Encryption Algorithm Selected and Justification	21
7. Network Management Strategies	21
7.1 Fault Management	21
7.2 Configuration Management	22
7.3 Accounting Management	22
7.4 Performance Management	23
7.5 Security Management	23
7.6 FCAPS Application in the IoTRC	23
8. Conclusion	24
9. References	25

List of Figures

Figure 1: 2D layout of floor plan	6
Figure 2: 3D layout of floor plan	7
Figure 3: IoTRC NetSim network design	7
Figure 4: Routing protocol configuration	10
Figure 5: WLAN standard configuration.....	13
Figure 6: Physical type configuration.....	13
Figure 7: Configuration for transmitter power, antenna gain, bandwidth	15

List of Tables

Table 1: 2D layout symbol description.....	5
Table 2: Throughput and delay of OSPF and RIP	10
Table 3: Throughput and delay of IEEE 802.11ac and IEEE 802.11p	13
Table 4: Comparison between different values of transmitter power.....	15
Table 5: Comparison between different values of antenna gain.....	16
Table 6: Comparison between different values of bandwidth	17

1. Introduction

The design and configuration of an effective network for the IoT Research Centre (IoTRC) at NTU requires a comprehensive approach that incorporates various critical elements. This report outlines the network design project, leveraging NetSim for simulation and configuration.

The network design will address several key aspects, including the floor plan layout, and the selection of appropriate routing protocol and wireless network standard. It will also discuss infrastructure connectivity, both wired and wireless, to support diverse research activities. Additionally, this report provides a comparison between the encryption algorithms available in NetSim, and the most suitable algorithm for data security will be selected for the network design. Finally, effective network management strategies will be proposed to streamline administration and enhance performance. Through this detailed analysis and design, the goal is to provide a well-rounded network solution that supports the IoTRC's mission and operational needs.

1.1 Assumptions Made

Given that the entire NTU campus spans only 50 acres and there are only 2 buildings dedicated for research purposes, it is reasonable to expect that the IoT Research Centre, as a specific facility, would be located within a single building, with all devices and research equipment concentrated within this limited space.

1.2 Selected Network Design Approach and Network Model

For redesigning the NTU IoT Research Centre's LAN, the top-down approach was chosen to ensure optimal performance and reliability. This method involves a thorough assessment of the centre's needs, including data traffic and hardware compatibility, to support numerous devices and high-demand research activities. It also addresses future scalability and adaptability to accommodate growth and technological advancements.

The Cisco Hierarchical Internetworking Model was selected for its suitability to NTU's technical goals. Its modular design supports scalable and incremental expansion, while its layered structure enhances reliability and performance. Security is managed through robust access controls, and the model simplifies network management and cost-effectively balances initial and operational expenses, ensuring a robust foundation for current and future research.

2. Floor Plan and NetSim Network Design

The floor plan layout for the NTU IoTRC is critical in ensuring an optimised network design tailored to the centre's specific needs. This section begins with an overview of the floor plan, detailing the centre's spatial arrangement and its implications for network infrastructure. Following this, the floor plan visualisation provides a graphical representation of the network layout, offering a clear depiction of equipment placement and connectivity. This visual guide aids in effectively planning and implementing the network setup. The network design in NetSim will be created based on the floor layout, aligning the virtual configuration with the physical setup.


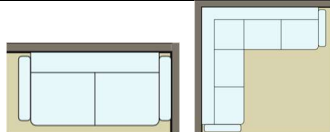
2.1 Overview of IoT Research Centre Floor Plan

The IoT Research Centre is structured across two floors, where both floors follows the same layout and covers an approximate area of 3000 square feet each. There are ten workstations set up for daily tasks, along with two printers for general use. A dedicated room is available for meetings and demonstrations, promoting collaboration and discussions. The general testing area features four workbenches, providing ample space for experimentation. Additionally, the specialised lab is equipped with three experiment stations and a discussion table, designed to facilitate focused research and development efforts.

2.2 Floor Plan Layout Visualisation

This section presents the floor plan of the IoTRC using both 2D and 3D layout figures to illustrate the spatial design. The 2D layout under Figure 1 provides a clear top-down view of the floor arrangement, while the 3D layouts under Figure 2 offer a more realistic perspective of how various areas and workstations are positioned within the centre. Additionally, a brief description of each symbol used in the 2d layout will be provided under Table 1.

Table 1: 2D layout symbol description

Symbol	Description
	Chair
	Sofa

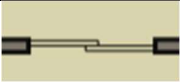


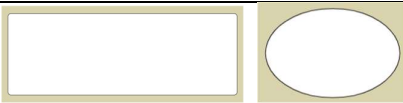



	Sliding door
	Window
	Printer
	Table
	IOT Device
	Computer/Workstation
	TV

Figure 1: 2D layout of floor plan

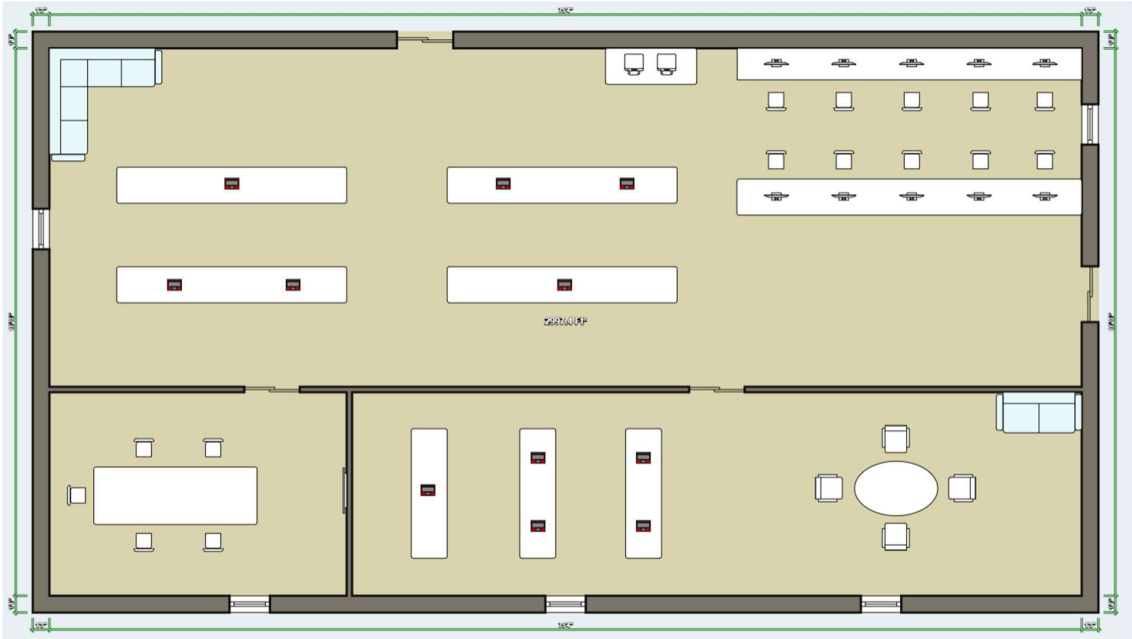


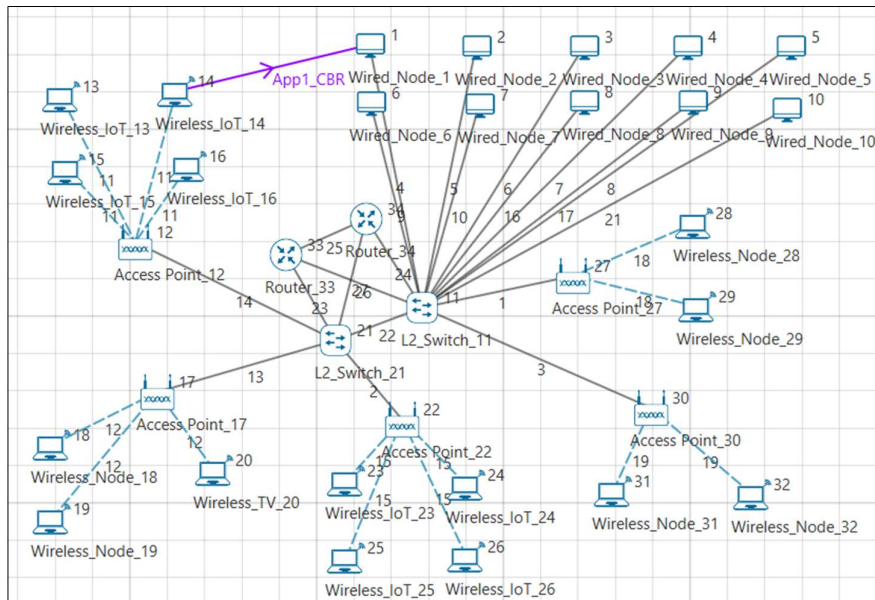
Figure 2: 3D layout of floor plan



2.3 NetSim Network Design

The network design includes five wireless access points (WAPs), two switches, and two routers, all interconnected. The WAPs are strategically positioned to cover two sides of the general area and two sides of the dedicated lab, ensuring comprehensive wireless coverage. All IoT devices are assumed to connect wirelessly to the WAPs, enabling efficient communication within the network. This design is illustrated under Figure 3.

Figure 3: IoTRC NetSim network design



3. Routing Protocols

Routing protocols are rules that guide routers in transferring data between source and destination devices (Yau & Arun, 2021). Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) routing protocols are particularly prominent, playing key roles in optimising data transfer and selecting efficient communication paths within networks (Yau & Arun, 2021).

Selecting the appropriate protocol is essential for determining the most efficient paths for data to travel across a network, ensuring optimal performance and connectivity within the IoTRC. While RIP and OSPF both have their strengths and weaknesses, they remain popular choices for network routing (Arvey, 2023). This section examines OSPF and RIP to determine which protocol is better in supporting the centre's network infrastructure.

3.1 Open Shortest Path First (OSPF)

According to Yau and Arun (2021), OSPF is a dynamic, link-state routing protocol that uses the Dijkstra algorithm to calculate the shortest path for data transmission in large TCP/IP networks. OSPF forms neighbour relationships between routers, advertising the status of directly connected links through Link-State Advertisements (LSAs). Additionally, it maintains neighbour, topology, and routing tables to determine the best routes, allowing efficient management of network changes and ensuring optimal data flow (Yau & Arun, 2021). Sheldon (2021) mentions that OSPF is the most commonly used interior gateway protocol (IGP) for large enterprise networks.

OSPF offers several advantages for network routing (Sheldon, 2021). It provides comprehensive knowledge of the network topology, enabling routers to accurately calculate routes based on current network conditions. Unlike RIP, which is limited to a maximum of 15 hops, OSPF does not have such constraints, leading to faster convergence and improved load balancing. In addition, OSPF efficiently manages network updates by multicasting link-state updates only when network changes occur, reducing unnecessary traffic.

However, OSPF also has some drawbacks (Sheldon, 2021). It requires a deeper understanding of complex network structures, making it more challenging to learn compared to simpler protocols. Scalability can become an issue as the number of routers in the network increases, which may limit its effectiveness for large-scale internet routing. Furthermore,

OSPF maintains multiple copies of routing information, which can lead to higher memory usage.

3.2 Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a distance-vector protocol suited for small networks (Yau & Arun, 2021). Yau and Arun (2021) explains that it uses hop count to determine route values, with a maximum limit of 15 hops to avoid loops. RIP updates its routing information every 30 seconds, broadcasting the full routing table to ensure all routers have current data. RIP has two versions: RIPv1, which is classful and broadcasts updates without subnet masks, and RIPv2, which is classless and uses multicast updates with subnet masks, supporting more complex network configurations (Yau & Arun, 2021). Both versions use the Bellman-Ford algorithm to determine the best route.

An advantage of RIP is that this protocol is ideal for small networks due to its simplicity in configuration and widespread router support (Sheldon, 2021). Since it updates its routing tables every 30 seconds, it does not require constant updates for network topology changes, which makes it easy to manage.

However, RIP has notable drawbacks (Sheldon, 2021). Its periodic broadcasts can create traffic bottlenecks, consuming significant bandwidth. The protocol's maximum hop count of 15 limits its scalability, making routers beyond this range unreachable. Additionally, RIP has a slow convergence rate, leading to delays in route adjustments when network changes occur. It also lacks support for multiple paths, which can result in routing loops and inefficiencies in route selection.

3.3. Network Metrics Comparison Between OSPF and RIP

Simulations are performed in NetSim using both protocols to obtain and compare the network throughput and delay. In the simulation, data is transferred from an IoT device to a wired workstation, where all configurations remains constant except for the routing protocol. The routing protocols are configured in the window shown under Figure 4. Simulation results are summarised in Table 2.

Figure 4: Routing protocol configuration

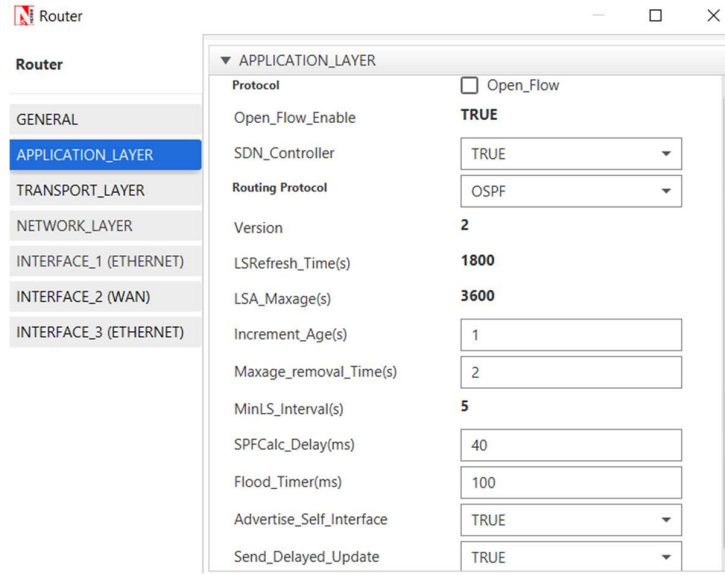


Table 2: Throughput and delay of OSPF and RIP

Routing protocol	Throughput (microsec)	Delay (microsec)
OSPF	0.5840	25805.2347
RIP	0.5840	24486.5649

Additionally, based on the conclusion of the simulation results in the paper presented by Yau and Arun (2021), OSPF surpasses RIP in performance within a wired LAN by providing better throughput and reduced packet delay, due to its efficient link and coverage adjustments. However, RIP performs more effectively than OSPF when used in networks with a limited number of nodes. This statement is aligned with the results in Table 2 as the amount of nodes in the simulation is limited, which results in RIP having a slightly lower delay compared to OSPF.

3.4 Protocol Selected and Justification

For the IoTRC, OSPF is the preferred routing protocol over RIP. The reason is that OSPF is designed for larger and more complex networks, offering superior performance in terms of throughput and packet delay. Besides, OSPF efficiently manages network changes and only send updates when there are changes in the network topology, thus minimising

unnecessary traffic. This capability ensures that OSPF maintains optimal data flow and supports efficient routing in a dynamic environment.

Although RIP performs slightly better in networks with a limited number of nodes, the IoTRC's requirements extend beyond the constraints of small networks. Given that the centre involves a range of research activities and a potentially growing network infrastructure, OSPF's ability to handle larger and more complex networks, along with its lack of hop count limitations, makes it a more suitable choice. Additionally, OSPF's faster convergence time and better load balancing further contribute to its appropriateness for the centre's operational needs.

4. Wireless Local Area Network (WLAN) Standards

Wireless Local Area Network (WLAN) standards, commonly known as "Wi-Fi standards," establish the foundation for wireless networking technologies (Buenning, 2024). Buenning (2024) explains that these standards guarantee interoperability between wireless devices from various manufacturers by specifying the technical aspects of radio frequency communication used in wireless networks. The most common standard is IEEE 802.11, which outlines the specifications for wireless LAN technology.

This section will cover several IEEE 802.11 standards, followed by a discussion on the selection of the most appropriate standard for the IoTRC.

4.1 IEEE 802.11 a/b/g/n

According to Philips (2023), the 802.11a standard, introduced in 1999, operates on the 5GHz band and offers up to 54Mbps but has a shorter range due to signal attenuation. The same year saw the release of 802.11b, which uses the 2.4GHz band and provides speeds of up to 11Mbps, contributing to Wi-Fi's early popularity. In 2003, 802.11g increased data rates to 54Mbps while retaining the 2.4GHz band, leading to widespread adoption. The 2009 802.11n standard supports both 2.4GHz and 5GHz bands, featuring multi-channel usage and offering up to 600Mbps, although its initial adoption was gradual.

However, these standards will not be considered for the centre's wireless network design due to their limitations in performance and features compared to newer technologies.

4.2 IEEE 802.11 ac/p

The IEEE 802.11ac standard, released in 2014, offers very high throughput (VHT) with several key advancements (Felemban, 2020). It enhances the service set to support up to eight spatial streams and employs multi-user MIMO (MU-MIMO) to aggregate frames for multiple receivers. Felemban (2020) further explains that data rates are significantly improved, reaching up to 6.93 Gbps, by increasing the number of bits per symbol and using 256 QAM modulation. The standard also expands bandwidth by providing wider 80 MHz and 160 MHz channels, compared to the 20 MHz and 40 MHz channels of IEEE 802.11n. IEEE 802.11ac operates in the 5 GHz band and includes a complex MAC frame format with multiple protocol data units to support its high-speed capabilities.

The IEEE 802.11p standard, published in 2010, enhances 802.11 technology to support Wireless Access in Vehicular Environments (WAVE) (Sharma & Singh, 2016). Felemban (2020) states that it employs Orthogonal Frequency-Division Multiplexing (OFDM) to address signal fading and enhance data transmission rates. The standard incorporates Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) to manage channel access and reduce collisions, supported by MAC and PHY layer management entities (Felemban, 2020). It uses the Enhanced Distributed Channel Access (EDCA) mechanism from IEEE 802.11e to prioritize traffic across four access categories, ensuring fair access based on priority levels. The IEEE 802.11p standard utilizes 16 Quadrature Amplitude Modulation (16-QAM) and includes a frame format with preamble, signal, and data sections for efficient communication (Felemban, 2020).

4.3 Network Metrics Comparison Between IEEE 802.11ac and IEEE 802.11p

Simulations are performed in NetSim using both standards to obtain and compare the network throughput and delay. In the simulation, data is transferred from an IoT device to a workstation, where all configurations remain constant except for the WLAN standard and the physical type in the datalink layer of each wireless device to match the type required by the standard. The standards are configured in the window shown under Figure 5, and the configuration for physical type is shown under Figure 6. Simulation results are summarised in Table 3.

Figure 5: WLAN standard configuration

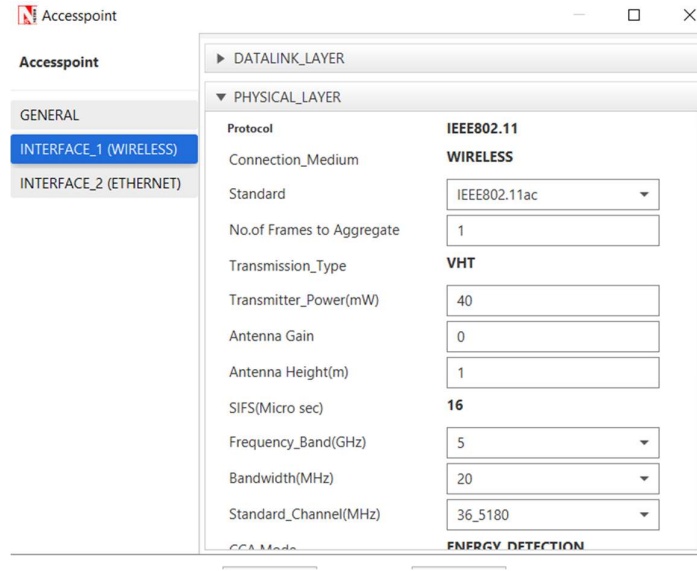


Figure 6: Physical type configuration

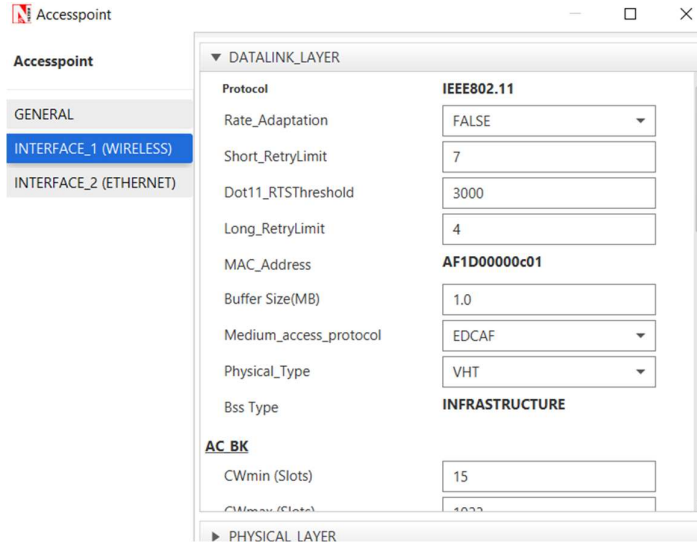


Table 3: Throughput and delay of IEEE 802.11ac and IEEE 802.11p

WLAN standard	Throughput (microsec)	Delay (microsec)
IEEE 802.11ac	0.5840	20875.5016
IEEE 802.11p	0.5840	30969.9327

4.4 Standard Selected and Justification

For the centre's needs, IEEE 802.11ac is the optimal choice due to its superior performance compared to IEEE 802.11p. IEEE 802.11ac supports very high throughput of up to 6.93 Gbps and operates efficiently with wider bandwidth channels, making it ideal for high-demand environments. Its advanced features, such as multi-user MIMO and high-density modulation, ensure reliable and fast wireless communication, which aligns with the centre's requirement for robust and high-speed network connectivity.

5. Infrastructure Connectivity

This section outlines wired and wireless connectivity options for the centre, focusing on ensuring reliable and efficient network performance to support its operations.

5.1 Wired connectivity

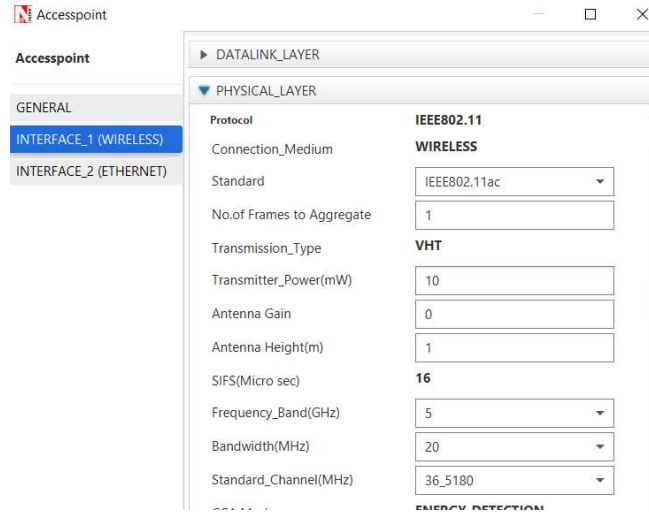
The wired connectivity in the centre utilises Ethernet connections to provide stable and high-speed communication. Wired workstations connect to switches, while wireless access points are also linked to switches to bridge wired and wireless networks. Switches connect with each other and to routers, ensuring a reliable network backbone. Notably, Ethernet configurations in NetSim cannot be modified, which limits any adjustments to the wired connection during the simulation. Overall, this setup supports the centre's need for consistent and uninterrupted data flow.

5.2 Wireless connectivity

Wireless connectivity within the centre relies on WLAN, connecting various wireless devices, such as IoT devices, mobile phones, and laptops, through wireless access points. In NetSim, some key configurations in the physical layer, including transmitter power, antenna gain, and bandwidth, will be examined and adjusted to optimise network performance.

Simulations will be performed to compare the results of different configuration values. The simulation scenario will be a wireless node transferring data to another wireless node. The configuration settings of transmitter power, antenna gain, and bandwidth can be changed in the same window, as shown under Figure 7.

Figure 7: Configuration for transmitter power, antenna gain, bandwidth



5.2.1 Transmitter Power

Transmit power refers to the amount of radio frequency energy emitted by a wireless transmitter (The Network Guys, 2022). The default transmitter power in NetSim is set at 40 milliwatt. According to The Network Guys (2022), a good Wi-Fi transmit power for 5 GHz band ranges from 10 to 17 decibel milliwatts, or equivalently, 10 to 50 milliwatts.

Four distinct values will be compared in the simulations. The transmitter power is changed for both wireless nodes and wireless access points. The simulation results are summarised under Table 4.

Table 4: Comparison between different values of transmitter power

Transmitter power (mW)	Throughput (microsec)	Delay (microsec)
10	0.5840	22145.42
25	0.5840	26290.04
40	0.5840	22041.27
50	0.5840	22041.27

The 40 mW transmitter power is selected for the centre's LAN implementation as it achieved the lowest delay, matching the performance of 50 mW but without exceeding the recommended range. Additionally, being the default setting in NetSim, it indicates that this value is well-calibrated and suitable for optimal performance.

5.2.2 Antenna Gain

According to TP-Link (2024), antenna gain is a measure of how efficiently an antenna converts electricity into radio waves. It affects the antenna's directionality, with higher gain resulting in a more focused beam. For every 3 dBi increase in gain, the antenna's power doubles. In NetSim, the default value for antenna gain is 0dBi. However, TP-Link (2024) mentions that 0 dBi is a theoretical reference point for an isotropic antenna that emits a signal uniformly in all directions, but it's practically impossible to achieve.

Many current wireless routers typically have antenna gains of 3, 5, or 7 dBi (Four-Faith, 2022). Simulations will be done based on these values. The antenna gain will be changed for both wireless nodes and wireless access points. The results are summarised under Table 5.

Table 5: Comparison between different values of antenna gain

Antenna gain (dBi)	Throughput (microsec)	Delay (microsec)
0	0.5840	22041.27
3	0.5840	34855.11
5	0.5840	34855.11
7	0.5840	39003.30

Based on the results above, 5 dBi is the most suitable antenna gain for the LAN implementation as it offers the same performance as 3 dBi but provides better signal directionality, which is beneficial for maintaining strong and stable connections within the centre. Since 0 dBi is theoretically impossible, 5 dBi is the practical choice for optimised performance.

5.2.3 Bandwidth

A Wi-Fi band frequency is partitioned into smaller segments called channels, and bandwidth refers to the range or extent of each channel (Interline, n.d.). Interline (n.d.) explains that while wider channels can increase data transfer rates, their effectiveness depends on having a fast internet connection. Additionally, increasing channel width can lead to interference and potentially degrade performance.

The default bandwidth value in NetSim is 20 MHz. According to Intel (2021), IEEE 802.11ac can support four channel width, which includes 20, 40, 80, 160 MHz. Simulations will be done based on these values. The bandwidth will be changed for both wireless nodes and wireless access points. The results are summarised under Table 6.

Table 6: Comparison between different values of bandwidth

Bandwidth (MHz)	Throughput (microsec)	Delay (microsec)
20	0.5840	34855.11
40	0.5840	25527.31
80	0.5840	26490.42
160	0.5840	24869.63

The throughput remains the same because it is capped by the simulation's configurations, while the delay decreases significantly with increased bandwidth (from 20 MHz to 40 MHz) as it reduces channel congestion.

For the LAN implementation, the 40 MHz bandwidth is chosen as it provides a good balance between performance and stability, significantly reducing delay compared to 20 MHz without introducing the higher interference risks associated with wider channels like 80 MHz and 160 MHz. This makes it suitable for the centre's network, where maintaining consistent performance is crucial.

6. Data Security

This section evaluates various encryption algorithms to determine the most suitable option for data security in the IoTRC. There are four algorithms available for application packet payload encryption in NetSim, namely AES, DES, XOR and TEA.

It is crucial to note that using different encryption methods won't affect the network performance metrics NetSim generates, since NetSim doesn't change packet size during encryption (Tetcos, 2019). It is also mentioned that NetSim skips decryption at the receiver end because it doesn't impact performance measurement. Therefore, no simulations will be conducted since variations in performance cannot be observed.

6.1 Impact of Encryption on Network Traffic Speed

Red Hat (2024) explains the speed of network traffic can be affected by the choice of encryption algorithms and their strength. Different algorithms, such as AES for symmetric encryption and RSA or ECC for asymmetric encryption, have varying computational requirements. While AES is generally faster, longer key lengths enhance security but may slow processing. Hardware acceleration in modern devices, such as CPUs with dedicated support for encryption, can significantly improve performance. Additionally, optimised software and parallel processing capabilities of multi-core processors can enhance encryption speed.

Other factors also play a role in encryption's impact on traffic speed. Red Hat (2024) states that network speed and bandwidth affect how noticeable encryption overhead is, while latency introduced by encryption can lead to slower response times in high-throughput applications. Protocol overhead, such as that from HTTPS, adds additional processing demands, and Quality of Service settings may prioritize certain traffic types, influencing overall speed. Finally, the volume of data being encrypted can also affect performance, making it important to balance security needs with network efficiency.

Therefore, balancing the choice of encryption algorithms with network performance is crucial for maintaining both security and efficient data transmission.

6.2 Discussion of NetSim's Encryption Algorithms

6.2.1 *Advanced Encryption Standard (AES)*

According to Zenarmor (n.d.), the Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm designed to secure sensitive data through varying key lengths: AES-128, AES-192, and AES-256. It operates using a substitution-permutation network and consists of multiple rounds of encryption, where the number of rounds depends on the key length. Its encryption process includes four main operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey, efficiently transforming plaintext into ciphertext while maintaining strong security.

This algorithm offers several advantages. AES is one of the most secure encryption protocols, available for both hardware and software implementation (Zenarmor, n.d.). Its straightforward processes and support for key sizes of 128, 192, and 256 bits enhance

resistance to unauthorized access. Additionally, AES is easy to implement, offers fast encryption and decryption, consumes minimal resources, and can be integrated with other security measures. The vast number of possible combinations makes it extremely difficult to breach.

However, Zenarmor (n.d.) mentions that AES has some drawbacks, including vulnerability to cryptanalysis if keys are not managed properly, thus requiring careful key scheduling. The algorithm encrypts each block with the same method, which may introduce predictability. Its simplistic algebraic structure and the complexity of implementing counter mode can also present challenges, especially in software applications.

6.2.2 Data Encryption Standard (DES)

The Data Encryption Standard (DES) is an encryption algorithm that operates with a 56-bit key to convert a 64-bit block of plaintext into a 64-bit block of ciphertext (Simplilearn, 2024). The encryption process consists of multiple rounds, with the number of rounds varying based on the key size. For instance, a 128-bit key would require 10 rounds and a 192-bit key would require 12 rounds.

Simplilearn (2024) states that this algorithm has some notable strengths, including its status as a government-standardized encryption method in the U.S. It is known for its efficiency, especially when implemented in hardware, where it outperforms software solutions. Additionally, the enhanced version known as Triple DES, which utilises a 168-bit key, significantly increases security and is much more difficult to break.

However, DES has significant disadvantages (Simplilearn, 2024). Its security is considered weak by modern standards, making it susceptible to brute force attacks. Furthermore, specialised hardware, such as the Deep Crack machine, is commercially available and capable of cracking DES encryption, highlighting its vulnerabilities in the current cybersecurity landscape.

6.2.3 XOR Cipher

XOR operations are essential in symmetric key encryption, where plaintext is combined with a secret key using the XOR (exclusive OR) operation to produce ciphertext (Blue Goat Cyber, n.d.). This method is efficient and straightforward, allowing for easy decryption by applying the same operation with the same key. However, the security of XOR

encryption relies heavily on the strength of the key, making secure key management critical for protecting sensitive data.

Its primary strengths include computational efficiency and ease of implementation (Blue Goat Cyber, n.d.). The XOR operation is simple and fast, requiring minimal processing power, making it suitable for resource-limited devices. This simplicity allows even those with limited cryptographic knowledge to understand and implement XOR encryption quickly.

However, XOR encryption has major limitations (Blue Goat Cyber, n.d.). It is vulnerable to known-plaintext attacks, where an adversary can deduce the secret key if they obtain both the original plaintext and its corresponding ciphertext. Additionally, XOR lacks diffusion, which means small changes in the plaintext lead to predictable changes in the ciphertext. This predictability can make the encryption susceptible to pattern analysis and statistical attacks, compromising its security.

6.2.4 Tiny Encryption Algorithm (TEA)

The Tiny Encryption Algorithm (TEA) is a fast and efficient Feistel cipher (Tayloredge, n.d.). It encrypts 64 bits of data with a 128-bit key using operations like XOR, addition, and shifting to ensure security. TEA achieves complete diffusion after six rounds and is considered secure, with no known successful cryptanalyses. Its lightweight design makes it suitable for various applications, including as a random number generator.

TEA can serve as a replacement for DES in software applications due to its compact design, making it easily implementable across various platforms (Tayloredge, n.d.). While speed is not its primary focus, TEA can perform up to three times faster than software implementations of DES, which operates with 16 rounds. TEA supports multiple modes of use similar to DES, and its cycle count can be adjusted, potentially enhancing security through increased iterations.

However, TEA has significant weaknesses, such as the existence of equivalent keys that effectively reduce its key size to 126 bits (Kelsey et al., 1996). Additionally, it is susceptible to related-key attacks, which necessitate a specific number of chosen plaintexts for exploitation. These vulnerabilities led to the development of the XTEA cipher as a more secure alternative.

6.3 Encryption Algorithm Selected and Justification

After evaluating the available encryption algorithms, the Advanced Encryption Standard (AES) has been selected as the most suitable option for securing data in the IoTRC due to its strong security and efficiency. AES provides robust protection against unauthorised access while maintaining high performance, crucial for the centre's operational needs. Its compatibility with modern hardware acceleration further enhances processing speed, making it suitable for the IoTRC's data-intensive applications. Despite some limitations in key management, the overall benefits of AES make it the ideal choice for securing sensitive data within the centre, ensuring confidentiality and integrity without hindering network performance.

7. Network Management Strategies

Network management involves the processes and activities necessary to ensure that a network operates effectively, delivering traffic according to established performance parameters such as maximum delay and minimum throughput (Fulber-Garcia, 2024). Given the complexity of modern networks, effective management is essential for maintaining service quality and reliability.

The FCAPS model will be employed, which consists of five key categories: Fault, Configuration, Accounting, Performance, and Security, to guide the discussion on network management strategies (Fulber-Garcia, 2024). Each level addresses specific aspects crucial for maintaining network functionality.

7.1 Fault Management

Faults are an inevitable part of network operations, even when preventive measures are in place (Fulber-Garcia, 2024). Fault management in the FCAPS model focuses on detecting these issues, minimising their impact, and restoring normal network functionality. The process involves a structured, five-step workflow designed to effectively manage faults and maintain network stability.

The first step in fault management is detection, which involves identifying when something goes wrong within the system (Fulber-Garcia, 2024). Once a fault is detected, the next step is diagnosis and isolation, where the specific part of the system affected by the fault is identified. Following this, correlation and aggregation are performed to assess potential

problems and the consequences of the detected fault. Restoration then involves mitigating and resolving the issue to make the system operational again. Finally, the resolution step confirms that the fault has been fully fixed, ensuring the network returns to its intended performance levels.

7.2 Configuration Management

Configuration management ensures that networked systems operate as intended throughout their lifecycle, even when updates, upgrades, or scaling processes occur (Fulber-Garcia, 2024). This aspect of network management addresses both hardware and software components, ensuring optimal performance and adaptability to changes.

On the hardware side, configuration management includes inventory management, which involves keeping track of all the devices and equipment used in the network (Fulber-Garcia, 2024). It also addresses allocation management, which determines the best physical placement of hardware resources, and upgrading or scaling management to ensure that the network has sufficient computational capacity to handle its workload.

For software, configuration management focuses on selecting the most suitable hardware to support software execution and optimize performance (Fulber-Garcia, 2024). It also involves managing software versioning, ensuring that all programs are up-to-date to prevent vulnerabilities and maintain functionality. Additionally, configuration management defines access controls, specifying which operators can access different parts of the system to maintain security and operational integrity.

7.3 Accounting Management

Accounting management focuses on optimising the distribution of network resources among clients by managing administrative tasks involving network managers, operators, and users (Fulber-Garcia, 2024). One key task is maintaining an updated inventory of all available network resources, which includes integrating updates from configuration management.

Another important aspect is billing management, where statistics are generated on client registrations, network usage, and varying usage profiles to monitor and control resource consumption (Fulber-Garcia, 2024). Accounting management also determines

access rights and permissions, defining what each client is allowed to do within the network, ensuring appropriate resource utilization and security.

7.4 Performance Management

Performance management involves monitoring and enhancing the overall performance of a network by maximising throughput, minimising latency, and avoiding bottlenecks (Fulber-Garcia, 2024). Key monitoring routines include tracking network traffic, identifying performance trends, and pinpointing areas needing optimization.

The primary goal is to improve the quality of service and user experience for clients (Fulber-Garcia, 2024). Beyond that, performance management provides insights into network demands as the number of clients fluctuates or service level agreements evolve, enabling managers and operators to make informed adjustments that maintain efficient operations and meet performance expectations. Additionally, proactive analysis of historical performance data is necessary as it helps to identify and address potential capacity or reliability issues before they impact service quality (Gandhi, 2021).

7.5 Security Management

Security management focuses on safeguarding network resources and equipment by controlling access and preventing unauthorised modifications (Fulber-Garcia, 2024). This approach helps keep the network operational while protecting clients from security breaches. Common threats include denial of service (DoS), man-in-the-middle attacks, and DNS poisoning.

Effective security management begins at the core of the network, deploying various security functions such as firewalls, intrusion detection and prevention systems (IDPS), and antivirus solutions to identify and counteract attacks (Fulber-Garcia, 2024). Additionally, encrypting sensitive network traffic is a crucial security measure, further ensuring that data remains protected from unauthorized access during transmission. These actions collectively help maintain a secure and resilient network environment.

7.6 FCAPS Application in the IoTRC

The FCAPS model plays a vital role in the IoTRC network management, where each component addresses specific challenges. Fault Management is crucial for quickly detecting and resolving issues, ensuring high network uptime essential for ongoing research activities.

Configuration Management helps maintain oversight of both hardware and software configurations, allowing for scalability and updates as the centre's needs evolve. Accounting Management optimises resource allocation among users, promoting efficient network usage and fair billing practices. Performance Management focuses on enhancing service quality by monitoring network efficiency, which is vital for maintaining reliable connectivity for IoT devices. Lastly, Security Management safeguards sensitive data through robust access controls and threat mitigation strategies.

Together, these functions ensure the IoTRC operates effectively, meeting the demands of innovative research while maintaining a secure environment.

8. Conclusion

In conclusion, the design and configuration of the network for the IoT Research Centre (IoTRC) at NTU are carefully tailored to meet its operational needs. By leveraging tools like NetSim, the project incorporates a comprehensive approach that includes a well-planned floor layout, appropriate routing protocols, and robust wireless standards. The selection of OSPF for routing ensures efficient data transfer within the centre's dynamic environment, while IEEE 802.11ac supports high-speed wireless connectivity essential for research activities.

The wired infrastructure relies on Ethernet for stable connections, while wireless connectivity is facilitated through various access points to support IoT devices and other mobile technologies. To optimise wireless performance, configurations such as transmitter power, antenna gain, and bandwidth are tested to determine the most suitable values.

Data security is prioritised through the implementation of the Advanced Encryption Standard (AES), providing strong protection for sensitive information. Finally, employing the FCAPS model enhances network management, ensuring reliability and performance in the face of evolving demands. This strategic design ultimately positions the IoTRC for successful and secure research endeavours.

9. References

- Arvey, S. (2023, March 17). *OSPF vs RIP: Comparing Two of the Most Popular Routing Protocols*. Orhan Ergun. Retrieved from <https://orhanergun.net/ospf-vs-rip#:~:text=OSPF%20is%20a%20link%2Dstate,widely%20used%20in%20today's%20networks>.
- Blue Goat Cyber. (n.d.). *How XOR is Used in Encryption*. Retrieved from <https://bluegoatcyber.com/blog/how-is-xor-used-in-encryption/>
- Buenning, M. (2024, September 13). *What Are 802.11 IEEE Wireless LAN Standards?*. NinjaOne. Retrieved from <https://www.ninjaone.com/it-hub/it-service-management/what-are-802-11-ieee-wireless-lan-standards/>
- Felemban, E. (2020). A comparative study of IEEE 802.11 family protocols. *International Journal of Computer Science and Network Security*, 20(7), 98.
- Four-Faith. (2022, June 7). *What does DBI mean? Detailed Introduction of DBI in Wireless Routers*. Retrieved from <https://www.fourfaith.com/industry-news/what-does-dbi-mean.html>
- Fulber-Garcia, V. (2024, March 18). *Network Management: The FCAPS Model*. Retrieved from <https://www.baeldung.com/cs/network-management-fcaps-model>
- Gandhi, Y. (2021, December 8). *What is FCAPS (Fault, Configuration, Accounting, Performance and Security)?*. Retrieved from <https://analyticssteps.com/blogs/what-fcaps-fault-configuration-accounting-performance-and-security>
- Interline. (n.d.). *Channel Bandwidth Explained 20/40/80/160 MHz*. Retrieved from <https://interline.pl/Information-and-Tips/Channel-Bandwidth-Explained-20-40-80-160-MHz>
- Kelsey, J., Schneier, B., & Wagner, D. (1996). Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. In N. Koblitz (Ed.), *Advances in cryptology — CRYPTO '96* (Vol. 1109, pp. 237–251). Lecture Notes in Computer Science. Springer. https://doi.org/10.1007/3-540-68697-5_19
- Red Hat. (2024, June 3). *Key factors that contribute to encryption traffic speed differences*.

Retrieved from <https://access.redhat.com/solutions/7029269>

- Sharma, P., & Singh, G. (2016). Comparison of Wi-Fi IEEE 802.11 standards relating to media access control protocols. *International Journal of Computer Science and Information Security*, 14(10), 856-862.
- Sheldon. (2021, December 15). *RIP vs OSPF: What Is the Difference?*. FS.com. Retrieved from <https://community.fs.com/article/rip-vs-ospf-what-is-the-difference.html>
- Simplilearn. (2024, August 31). *How the DES Algorithm Works: Basics of Data Encryption*. Retrieved from <https://www.simplilearn.com/what-is-des-article>
- Taylor & Francis. (n.d.). *The Tiny Encryption Algorithm (TEA)*. Retrieved from <https://www.taylorandfrancis.com/reference/Mathematics/TEA-XTEA.pdf>
- Tetcos. (2019). *NetSim User Manual*. Retrieved from https://www.tetcos.com/downloads/v12/NetSim_User_Manual.pdf
- The Network Guys. (2022, November 10). *What is Transmit Power & Transmit Power Control in Wi-Fi? (2023)*. Retrieved from <https://thenetworkguys.wordpress.com/2022/11/10/what-is-transmit-power-transmit-power-control-in-wi-fi/>
- TP-Link. (2024). *Antenna gain explained*. Retrieved from <https://www.tp-link.com/us/support/faq/3/>
- Yau, Z. A., & Arun, K. C. (2021). Comparative performance evaluation of RIP with OSPF routing protocol. *Journal of Applied Technology and Innovation*, 5(3), 67.