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 3: Network Simulation
DATE ASSIGNED	:	1/8/2024
DATE COMPLETED	:	4/10/2024

Table of Contents

List of Tables

List of Figures

1.0 Introduction

This report details the implementation and performance testing of the IoT Research Centre (IoTRC) network design at NTU using a network simulator. The primary goal is to collect, analyse, and interpret performance data from simulations to evaluate the network's effectiveness. By simulating real-world conditions, the assessment will determine whether the IoTRC network meets the requirements for high-speed connectivity, efficient data transfer, and reliable performance. The simulation will focus on key metrics such as throughput and delay, essential for identifying potential bottlenecks and assessing the network's capacity to handle data traffic. Data visualisation techniques will be employed to enhance the analysis and interpretation of results.

Furthermore, the evaluation will examine critical network configurations, including the routing protocol and wireless standard, which are vital for supporting IoT research demands. The findings will provide insights for optimising the network, preparing it to meet the increasing demands of innovative research and secure data handling. This structured approach aims to validate the design choices and demonstrate the IoTRC network's capability to meet current and future needs.

1.1 Overview of the Network Design

The network design for NTU’s IoTRC addresses the performance limitations of the existing LAN. It prioritises high-speed connectivity, efficient data transfer, and robust security. A top-down approach was taken to assess the centre’s current needs while allowing for future scalability. The design uses the Cisco Hierarchical Internetworking Model for its modularity, reliability, and cost-effectiveness.

Ethernet provides reliable, high-speed connections to the wired workstations, while wireless access points support devices like printers and laptops. Each meeting room has a dedicated access point for seamless connectivity during discussions. The general testing area and the lab are each equipped with two access points to ensure comprehensive coverage and minimise dead zones. This combination of wireless and wired connectivity ensures stable network access throughout the center, balancing performance with convenience. Additionally, AES encryption secures data transmission, and the FCAPS model manages network performance and security.

The network is simulated using NetSim, as illustrated in Figure 1, which was designed based on the floor plan of the IoTRC shown in Figure 2. The categorisation of the network devices based on the different layers in Cisco Hierarchical Internetworking Model is shown in Figure 3.

Figure 1: NetSim network design

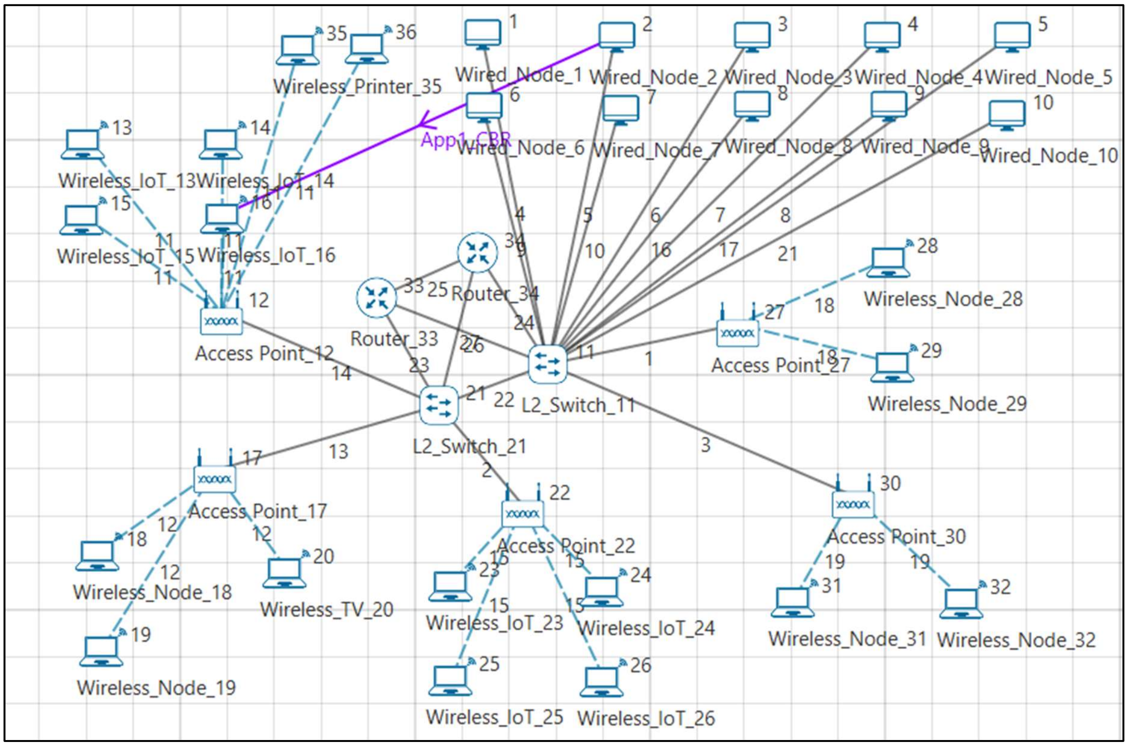


Figure 2: IoTRC floor plan

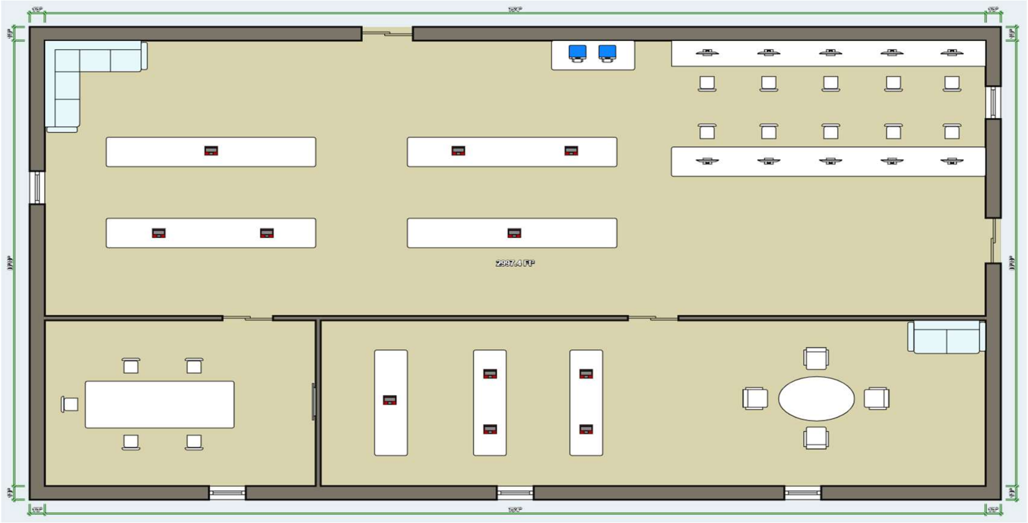
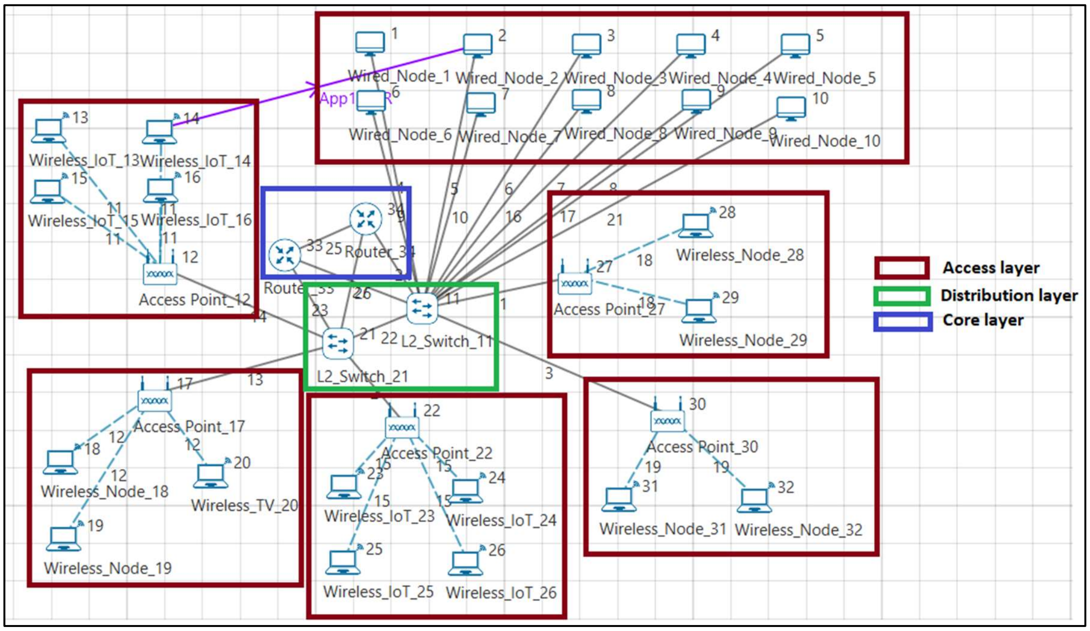


Figure 3: Categorisation of the network devices based on the hierarchical network model



1.2 Simulation Scenarios

The simulation for NTU's IoTRC will include four scenarios, each designed to test data transfers between IoT devices, wired workstations, and wireless devices across different wireless access points (WAPs) in the general testing area and specialised lab:

a. **Scenario 1: IoT Device (General Testing Area) to Wired Workstation**

- In this scenario, an IoT device located in the general testing area transfers data to a wired workstation.
  - IoT Device 14 → Wired Node 2

b. **Scenario 2: IoT Device (Specialised Lab) to Wired Workstation**

- This scenario involves an IoT device in the specialised lab sending data to a wired workstation.
  - IoT Device 24 → Wired Node 2

c. **Scenario 3: Wireless Device to IoT Device (General Testing Area – Different WAPs)**

- A wireless device in the right side of the general testing area transmits data to an IoT device in the left side, each connected to different WAPs.
  - Wireless Node 28 → IoT Device 16

d. **Scenario 4: Wireless Device to IoT Device (Specialised Lab – Different WAPs)**
    - In this final scenario, a wireless device in the right side of the specialised lab transfers data to an IoT device in the left side, each connected to different WAPs.
        - Wireless Node 31 → IoT Device 25

These four scenarios will assess the key network metrics, providing insights into the performance of different configurations within the IoTRC.

1.3 Selection of Encryption Algorithm and Justification

This section evaluates various encryption algorithms to determine the most suitable option for securing data within the IoTRC. The algorithms considered include AES, DES, XOR, and TEA. Notably, the performance metrics generated by NetSim will not be influenced by the choice of encryption methods, as the simulator does not alter packet size during encryption and skips decryption at the receiver end, rendering any simulation tests unnecessary (Tetcos, 2019). Therefore, simulations will not be performed and the evaluation will not be discussed in depth, as it has already been conducted in Task 2.

Among the available options, the Advanced Encryption Standard (AES) has been selected as the optimal choice for the IoTRC due to its strong security features and efficiency (Zenarmor, n.d.). AES is a widely adopted symmetric encryption algorithm that operates with varying key lengths (AES-128, AES-192, AES-256) and employs a substitution-permutation network for data transformation. It is highly secure, easy to implement, and offers fast encryption and decryption while consuming minimal resources.

In contrast, other algorithms present notable weaknesses. The Data Encryption Standard (DES) is considered insecure by modern standards, vulnerable to brute-force attacks, and inefficient in software implementations (Simplilearn, 2024). XOR encryption, while simple and efficient, is susceptible to known-plaintext attacks and lacks diffusion, making it less secure (Blue Goat Cipher, n.d.). The Tiny Encryption Algorithm (TEA), although efficient, has weaknesses related to its key size and vulnerability to specific attacks (Kelsey et al, 1996).

Overall, the advantages of AES, including robust protection against unauthorised access, compatibility with hardware acceleration, and high performance, make it the most suitable option for the IoTRC. This ensures the confidentiality and integrity of sensitive data without hindering network performance.

1.4 Additional Configurations for Wireless Connectivity

In addition to selecting the wireless standard, the network design for the IoTRC incorporates several modifications to enhance wireless connectivity and performance. In Task 2, various parameters were evaluated to enhance wireless connectivity in the IoTRC network design. The selected values based on those simulations will be utilised in Task 3. Key configurations include:

a. **Transmitter Power**: This parameter determines the strength of the signal emitted by wireless devices (The Network Guys, 2022). Four transmitter power levels (10 mW, 25 mW, 40 mW, and 50 mW) were tested. While 50 mW might seem optimal, 40 mW delivers comparable performance with lower delay and aligns with the recommended range for the 5 GHz band. Therefore, a transmitter power of 40 mW will be implemented.

b. **Antenna Gain**: This measures the ability of an antenna to direct the signal, affecting both strength and range (TP-Link, 2024). Simulations were conducted with antenna gains of 0, 3, 5, and 7 dBi. Although 0 dBi has the best performance, it only serves as a theoretical reference. An antenna gain of 5 dBi offers a good balance between signal strength and directionality, resulting in more stable connections. Hence, an antenna gain of 5 dBi will be adopted.

c. **Bandwidth**: The analysis examined bandwidth values of 20 MHz, 40 MHz, 80 MHz, and 160 MHz. It was found that while wider bandwidths can enhance speed, they may also lead to increased interference (Interline, n.d.). The simulations indicated a notable reduction in delay when increasing from 20 MHz to 40 MHz. Therefore, a bandwidth of 40 MHz will be used to optimise performance while minimising delay and interference.

These configurations, chosen based on previous evaluations, will support the overall performance of the network simulations.

2.0 Data Collection and Assimilation

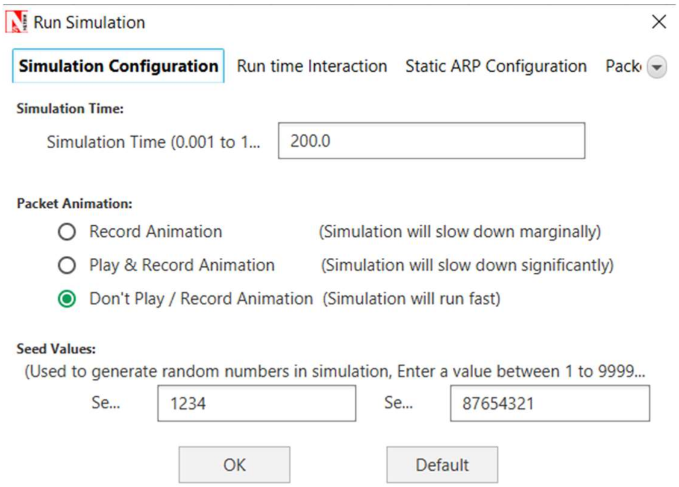
This section outlines the data collection process for evaluating the performance of the network design. The focus will be on four key configurations involving a fixed encryption algorithm, but different routing protocols and wireless standards. The configurations to be assessed include:

- IEEE 802.11ac – OSPF – AES
- IEEE 802.11ac – RIP – AES
- IEEE 802.11p – OSPF – AES
- IEEE 802.11p – RIP – AES

The decision to exclude testing for older wireless standards such as 802.11a, 802.11b, and 802.11g is based on their inadequate performance for the IoTRC's high-speed connectivity requirements. Instead, this evaluation will utilise the latest standards, 802.11ac and 802.11p, to ensure optimal data transfer and reliability.

For each configuration, the four simulation scenarios previously described will be utilised to gather performance metrics. This approach will enable a comprehensive comparison of the various combinations, allowing for a thorough evaluation of how each configuration impacts network performance, particularly in terms of throughput and delay. In addition to throughput and delay, the results will also include the number of packets generated and received to assess any potential packet loss during the simulations. The simulation configuration and application configuration are fixed across all the simulations, which are shown under Figure 4 and Figure 5 accordingly.

Figure 4: Simulation configuration



Simulation Time:

Simulation Time (0.001 to 1... 200.0

Packet Animation:

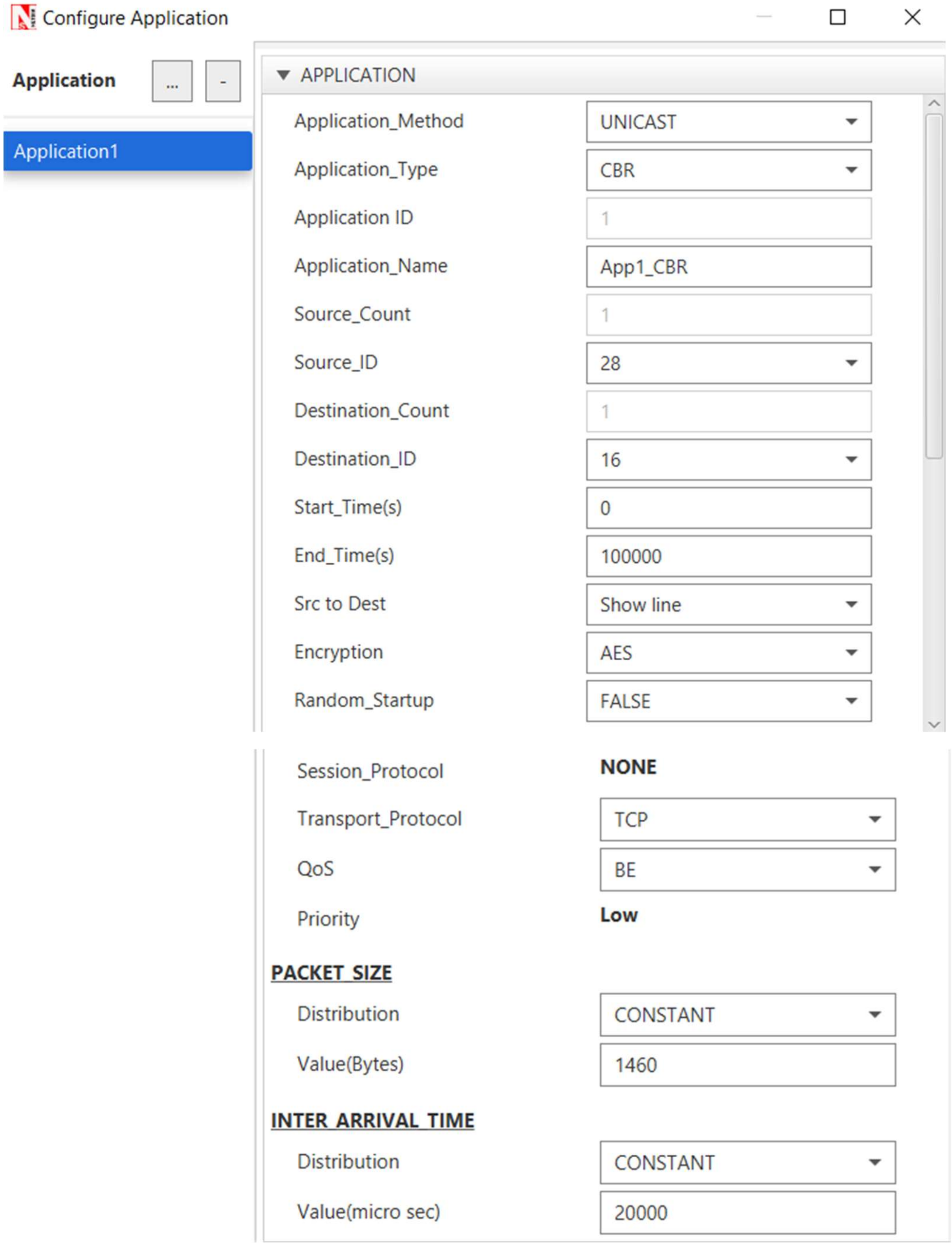
○ Record Animation (Simulation will slow down marginally)
○ Play & Record Animation (Simulation will slow down significantly)
● Don't Play / Record Animation (Simulation will run fast)

Seed Values:

(Used to generate random numbers in simulation, Enter a value between 1 to 9999...

Se... 1234 Se... 87654321

Figure 5: Application configuration



Configure Application

Application

Application1

APPLICATION

Application_Method	UNICAST
Application_Type	CBR
Application ID	1
Application_Name	App1_CBR
Source_Count	1
Source_ID	28
Destination_Count	1
Destination_ID	16
Start_Time(s)	0
End_Time(s)	100000
Src to Dest	Show line
Encryption	AES
Random_Startup	FALSE
Session_Protocol	NONE
Transport_Protocol	TCP
QoS	BE
Priority	Low

PACKET SIZE

Distribution	CONSTANT
Value(Bytes)	1460

INTER ARRIVAL TIME

Distribution	CONSTANT
Value(micro sec)	20000

2.1 Simulation Results

The simulation results for each configuration are summarised under Table 1 below:

Table 1: Data collected for the simulations

Scenario	Packet generated	Packet Received	Throughput (Mbps)	Delay (microsec)
IEEE 802.11ac – OSPF – AES				
1	10000	10000	0.5840	22013.35
2	10000	10000	0.5840	19827.10
3	10000	10000	0.5840	27163.86
4	10000	10000	0.5840	26839.33
IEEE 802.11ac – RIP – AES				
1	10000	10000	0.5840	24252.65
2	10000	10000	0.5840	21161.46
3	10000	9990	0.5834	33638.20
4	10000	9991	0.5835	31689.03
IEEE 802.11p – OSPF – AES				
1	10000	10000	0.5840	30349.48
2	10000	10000	0.5840	30354.49
3	10000	10000	0.5840	24841.21
4	10000	10000	0.5840	40188.62
IEEE 802.11p – RIP – AES				
1	10000	10000	0.5840	30349.48
2	10000	10000	0.5840	22034.30
3	10000	9993	0.5836	27674.81
4	10000	9995	0.5837	25565.17

2.2 Mean Throughput and Delay

Based on the results collected, a mean value is calculated for both throughput and delay, which can provide more insights when visualising and interpreting the results. The mean throughput is summarised in Table 2, while the mean delay is summarised in Table 3.

Table 2: Mean throughput of each configuration

Configuration	Mean Throughput (Mbps)
IEEE 802.11ac – OSPF – AES	0.5840
IEEE 802.11ac – RIP – AES	0.5837
IEEE 802.11p – OSPF – AES	0.5840
IEEE 802.11p – RIP – AES	0.5838

Table 3: Mean delay of each configuration

Configuration	Mean Delay (Microsec)
IEEE 802.11ac – OSPF – AES	23960.91
IEEE 802.11ac – RIP – AES	27685.34
IEEE 802.11p – OSPF – AES	31433.45
IEEE 802.11p – RIP – AES	26405.94

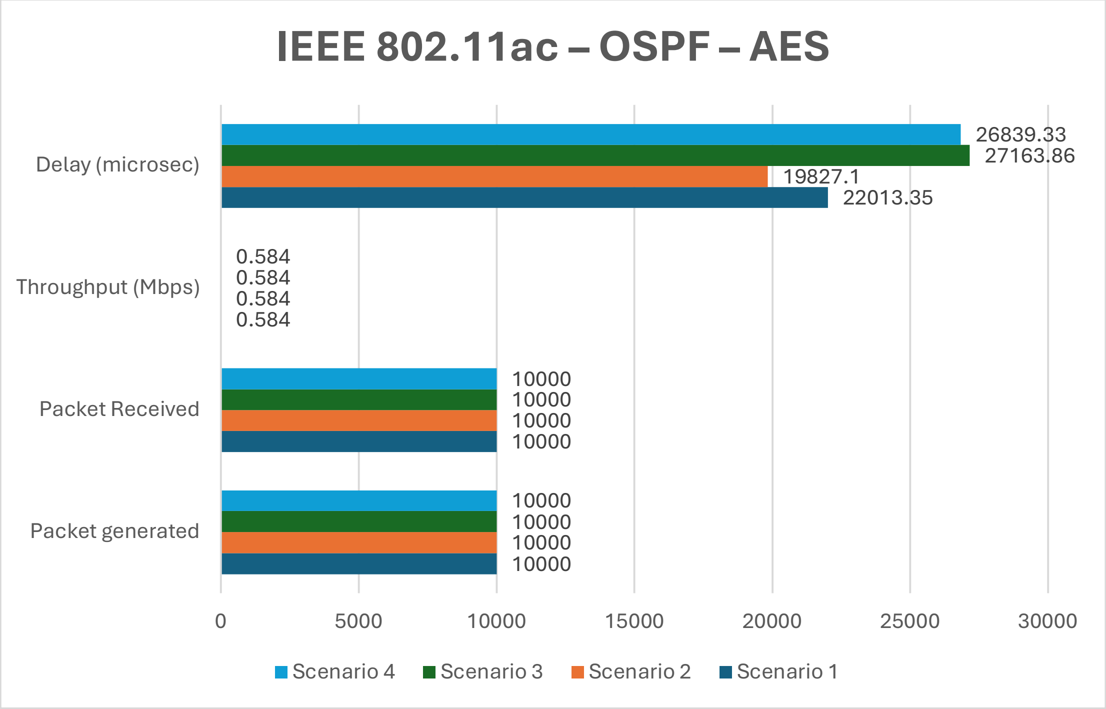
3.0 Data Visualisations

This section will present the performance metrics collected from the network simulations using a variety of graphical representations, offering a clear and intuitive analysis of the results. Each configuration will be visualised using clustered bar graphs. These graphs will display key metrics such as the number of packets generated and received, throughput, and delay for each of the four simulation scenarios.

In addition to the individual configuration graphs, two comparative bar graphs will be developed. The first will focus on mean throughput, highlighting the efficiency and data transfer rates of each configuration. The second will focus on mean delay, allowing for a detailed comparison of latency across the different routing protocols and wireless standards. These comparative graphs will help visualise the broader trends and patterns across all configurations, making it easier to assess which combination provides the most reliable and efficient network performance.

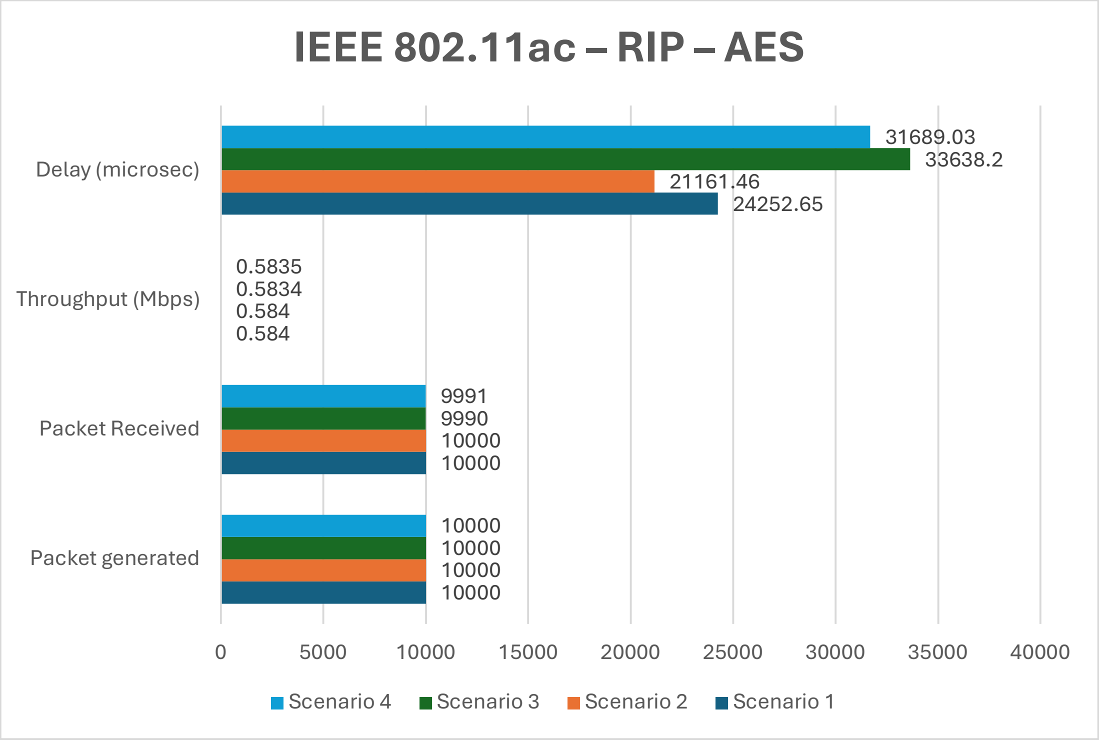
3.1 IEEE 802.11ac – OSPF – AES

Figure 6: Graph for the simulation results of IEEE 802.11ac – OSPF – AES



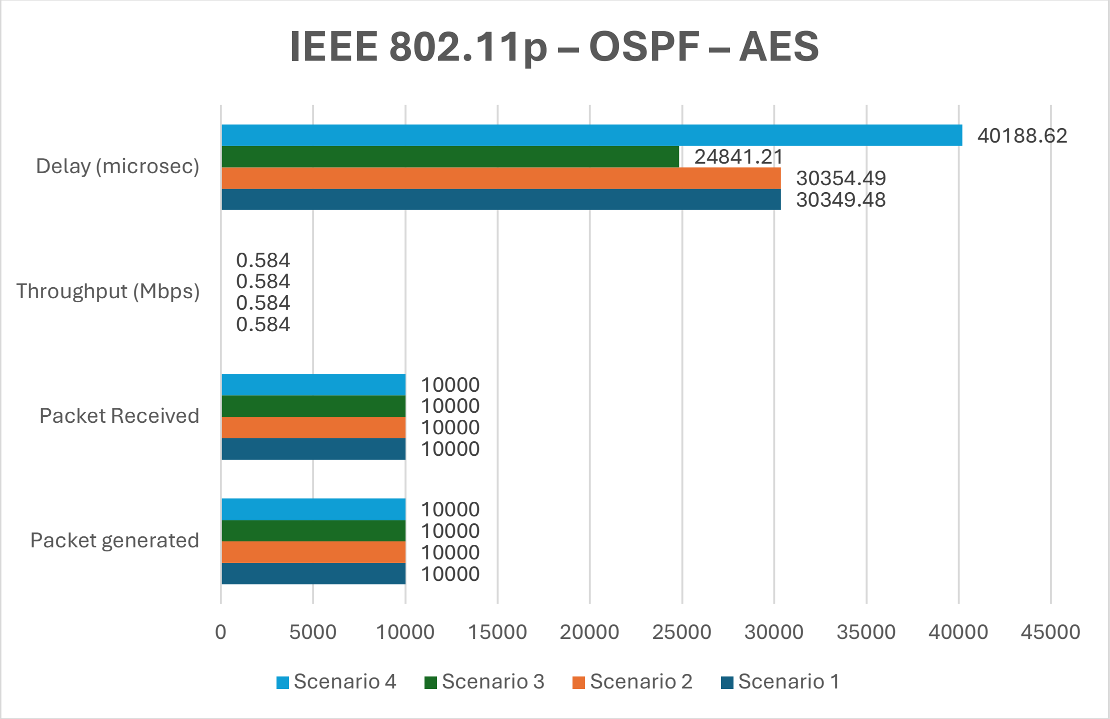
3.2 IEEE 802.11ac – RIP – AES

Figure 7: Graph for the simulation results of IEEE 802.11ac – RIP – AES



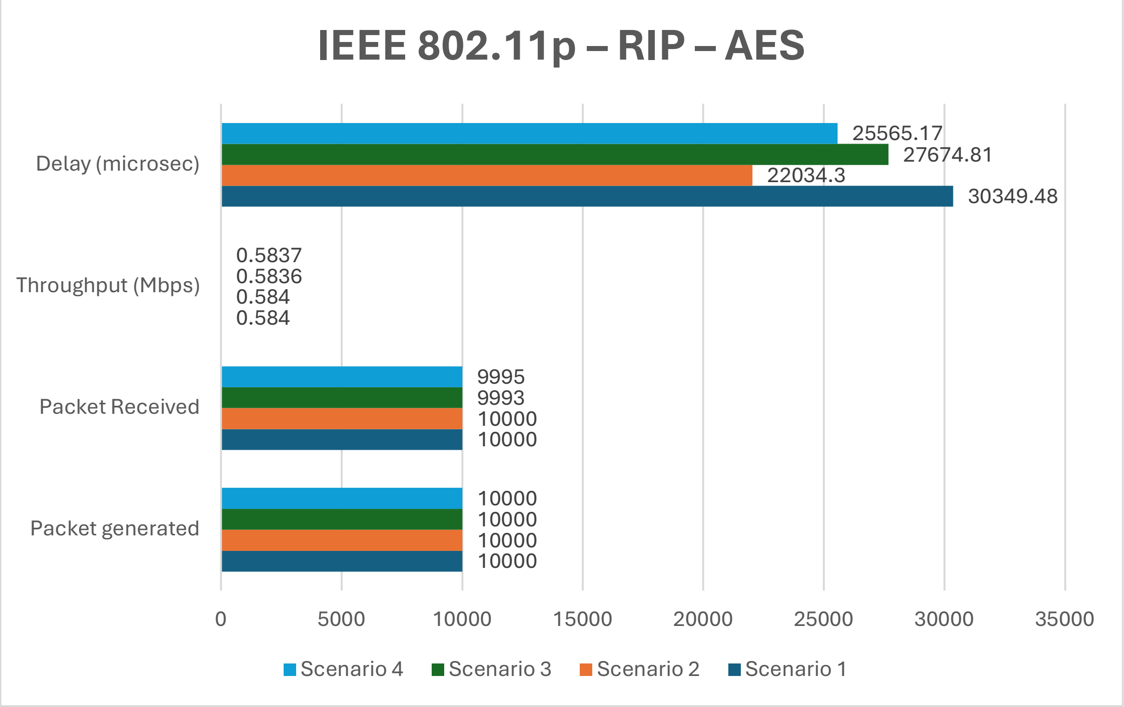
3.3 IEEE 802.11p – OSPF – AES

Figure 8: Graph for the simulation results of IEEE 802.11p – OSPF – AES



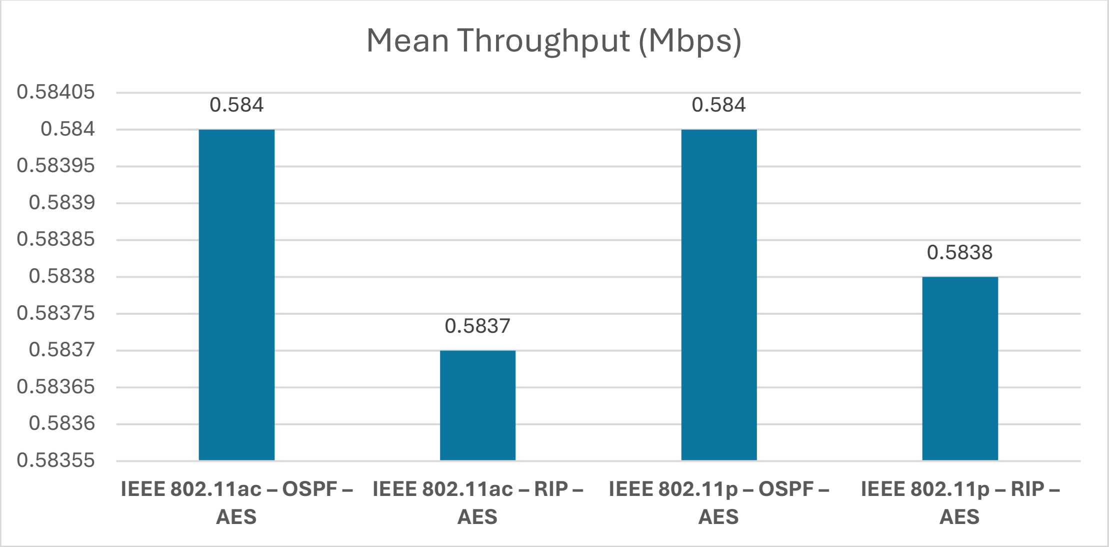
3.4 IEEE 802.11p – RIP – AES

Figure 9: Graph for the simulation results of IEEE 802.11p – RIP – AES



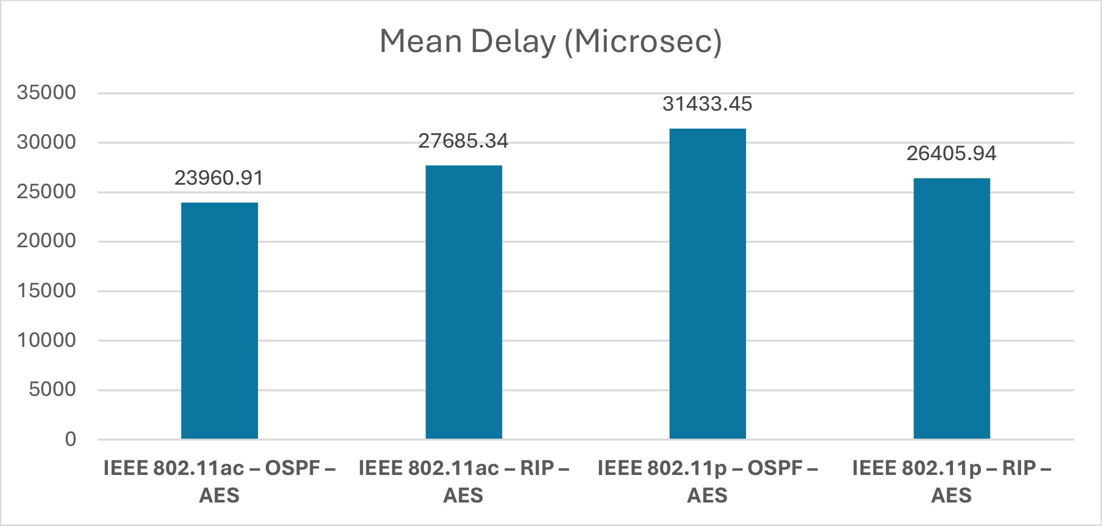
3.5 Mean Throughput of All Configurations

Figure 10: Graph for mean throughput



3.6 Mean Delay of All Configurations

Figure 11: Graph for mean delay



4.0 Data Evaluation and Interpretations

This section presents the analysis and interpretation of the network performance data collected from the simulations of the IoTRC network design. The evaluation focuses on key metrics such as packet generation, packet reception, throughput, and delay across four different configurations. The performance of these configurations is examined to assess the network's reliability, efficiency, and suitability for handling the research center's data traffic.

4.1 IEEE 802.11ac – OSPF – AES

a. **Packet Generated and Received**: Across all scenarios, 10,000 packets were generated and fully received, indicating zero packet loss. This demonstrates the reliability and efficiency of the OSPF routing protocol combined with the 802.11ac standard.

b. **Throughput**: The throughput remains consistent at 0.584 Mbps across all scenarios. This suggests stable data transfer rates under the OSPF protocol with no significant bottlenecks.

c. **Delay**: Delay values fluctuate between 19,827.10 microseconds (Scenario 2) and 27,163.86 microseconds (Scenario 3). These moderate variations suggest that network delay may depend on specific network conditions, such as routing paths and wireless access point congestion.

4.2 IEEE 802.11ac – RIP – AES

a. **Packet Generated and Received**: While Scenarios 1 and 2 show no packet loss, slight losses occur in Scenarios 3 and 4, with 10 and 9 packets lost respectively. This indicates a marginal decrease in reliability when using the RIP protocol.

b. **Throughput**: Throughput remains steady at around 0.584 Mbps, but the minor packet loss in Scenarios 3 and 4 results in a very slight drop to 0.5834 Mbps and 0.5835 Mbps, respectively.

c. **Delay**: Delay is noticeably higher compared to the OSPF configuration, ranging from 21,161.46 microseconds (Scenario 2) to 33,638.20 microseconds (Scenario 3). This indicates that the RIP protocol may introduce additional latency in high-demand scenarios.

4.3 IEEE 802.11p – OSPF – AES

a. **Packet Generated and Received**: As with the previous configurations, there is no packet loss across all scenarios, reflecting the reliability of OSPF with the 802.11p standard.

b. **Throughput**: Throughput is consistent at 0.584 Mbps, mirroring the stability observed in other configurations.

c. **Delay**: The delay values in this configuration are higher, ranging from 24,841.21 microseconds (Scenario 3) to 40,188.62 microseconds (Scenario 4). This indicates that the 802.11p standard may introduce additional latency when compared to 802.11ac, especially in more demanding scenarios.

4.4 IEEE 802.11p – RIP – AES

a. **Packet Generated and Received**: Similar to the 802.11ac-RIP configuration, there is slight packet loss in Scenarios 3 and 4, with 7 and 5 packets lost respectively.

b. **Throughput**: Slightly reduced throughput is observed in these scenarios due to the packet loss, with values dipping to 0.5836 Mbps and 0.5837 Mbps.

c. **Delay**: Delay varies from 22,034.30 microseconds (Scenario 2) to 30,349.48 microseconds (Scenario 1), though it is generally lower than the delay seen with the 802.11ac-RIP configuration. Despite the packet loss, the latency appears more manageable in this setup.

4.5 Summary of Packet Generated and Packet Received

Across all configurations and scenarios, 10,000 packets were generated. Most configurations successfully delivered close to 10,000 packets, indicating minimal packet loss. However, slight packet loss is observed in certain scenarios for configurations using the RIP protocol:

- **IEEE 802.11ac – RIP – AES**: Scenario 3 (9,990 packets received) and Scenario 4 (9,991 packets received)
- **IEEE 802.11p – RIP – AES**: Scenario 3 (9,993 packets received) and Scenario 4 (9,995 packets received)

This minor packet loss suggests that the RIP protocol, particularly when combined with either IEEE 802.11ac or IEEE 802.11p, may be slightly less reliable in maintaining packet delivery compared to OSPF.

4.6 Mean Throughput Evaluation

The mean throughput for all configurations was relatively stable, with only minor differences across scenarios:

- **IEEE 802.11ac – OSPF – AES**: Consistently achieved a throughput of 0.5840 Mbps across all scenarios, indicating high stability and efficiency.
- **IEEE 802.11ac – RIP – AES**: Slightly lower mean throughput (0.5837 Mbps) due to minor packet loss, but the performance remains comparable.
- **IEEE 802.11p – OSPF – AES**: Maintained a throughput of 0.5840 Mbps, showing consistent performance.
- **IEEE 802.11p – RIP – AES**: Despite minor packet loss, throughput remained high at 0.5838 Mbps.

Overall, the difference in throughput between the configurations is negligible, indicating that both wireless standards and both routing protocols can handle the network's data transfer needs effectively.

4.7 Mean Delay Evaluation

Significant differences were observed in the mean delay between the configurations:

- **IEEE 802.11ac – OSPF – AES**: Exhibited the lowest mean delay (23,960.91 microseconds), indicating that this configuration offers the best performance in terms of minimising latency.
- **IEEE 802.11ac – RIP – AES**: Higher mean delay (27,685.34 microseconds), suggesting that RIP introduces additional latency compared to OSPF when using IEEE 802.11ac.
- **IEEE 802.11p – OSPF – AES**: Showed the highest mean delay (31,433.45 microseconds), indicating that the 802.11p standard has a greater impact on increasing delay, likely due to its design for vehicular communication and higher mobility support (Sharma & Singh, 2016).
- **IEEE 802.11p – RIP – AES**: Recorded a mean delay of 26,405.94 microseconds, which is lower than 802.11p with OSPF but higher than any 802.11ac configuration, reflecting a trade-off between mobility support and delay.

4.8 Result Interpretations

a. **Routing Protocols**: OSPF consistently outperforms RIP in terms of packet delivery, with no packet loss in all scenarios. RIP introduces minor packet loss and slightly higher delay, suggesting that OSPF may be better suited for applications requiring high reliability and low latency.

b. **Wireless Standards**: IEEE 802.11ac performs more efficiently in terms of delay than IEEE 802.11p, especially under OSPF. The lower delays with 802.11ac indicate it is more suitable for high-speed data transfers, whereas 802.11p may result in higher latencies, though its stability is comparable to 802.11ac.

c. **Overall Network Performance**: Both OSPF and RIP can provide stable throughput across configurations, but OSPF delivers better overall reliability and lower delay. The combination of OSPF with IEEE 802.11ac stands out as the optimal configuration for ensuring high-speed, low-latency data transfers in the IoTRC network.

5.0 Conclusion

The performance evaluation of NTU's IoT Research Centre (IoTRC) network design has demonstrated the importance of selecting the right combination of routing protocols, wireless standards, and encryption algorithms to ensure reliable, high-speed, and secure data transmission. The network simulations, which tested four different configurations across multiple scenarios, provided key insights into the impact of various protocols and standards on throughput, delay, and packet loss.

The results show that the combination of the IEEE 802.11ac wireless standard, OSPF routing protocol, and AES encryption algorithm delivers the most optimal performance. OSPF consistently demonstrated its superiority over RIP by achieving zero packet loss across all scenarios, along with lower delays. The choice of IEEE 802.11ac over IEEE 802.11p significantly reduced latency, making it more suitable for high-speed data transfers, which are critical for the IoTRC’s research activities. AES encryption was selected for its robust security features without compromising network performance.

The minor variations in throughput between the configurations indicate that both routing protocols and wireless standards are capable of maintaining high data transfer rates.

However, OSPF and IEEE 802.11ac outperformed their counterparts in terms of delay, making them the most efficient configuration for the IoTRC's network. The evaluation underscores the importance of selecting the right protocols and standards for specific network environments to achieve optimal performance and reliability.

In conclusion, the combination of IEEE 802.11ac, OSPF, and AES encryption provides the best balance of speed, reliability, and security for NTU's IoT Research Centre. This design ensures that the network can meet the current demands of data-intensive research while remaining scalable for future needs.

6.0 References

Blue Goat Cyber. (n.d.). *How XOR is used in encryption*. https://bluegoatcyber.com/blog/how-is-xor-used-in-encryption/

Interline. (n.d.). *Channel bandwidth explained 20/40/80/160 MHz*. 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

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.

Simplilearn. (2024, August 31). *How the DES algorithm works: basics of data encryption*. https://www.simplilearn.com/what-is-des-article

Tetcos. (2019). *NetSim User Manual*. https://www.tetcos.com/downloads/v12/NetSim_User_Manual.pdf

The Network Guys. (2022, November 10). W*hat is transmit power & transmit power control in Wi-Fi? (2023)*. https://thenetworkguys.wordpress.com/2022/11/10/what-is-transmit-power-transmit-power-control-in-wi-fi/

TP-Link. (2024). *Antenna gain explained*. https://www.tp-link.com/us/support/faq

Zenarmor. (2023, October 9). *What is the Advanced Encryption Standard (AES)?*. https://www.zenarmor.com/docs/network-security-tutorials/what-is-advanced-encryption-standard-aes