

# **802.11 WLAN Design and Performance Evaluation**

**Name:** Srinithi Anand Prem Anand

**Email:** [srinuanand.p@gmail.com](mailto:srinuanand.p@gmail.com)

## TABLE OF CONTENTS

Abstract .....	3
Task 1: Introduction .....	4
Design Requirements .....	4
Detailed Implementation Plan .....	7
Conclusion .....	9
Task 2: Introduction .....	10
Simulation procedure .....	10
Model of Traffic .....	12
Throughout Analysis-Graph .....	12
Procedures of Simulation .....	13
Throughput Analysis-Table .....	13
Results .....	14
Discussion .....	14
Recommendations for performance enhancement .....	15
Conclusion .....	15
References .....	16

## **Abstract:**

This document contains two thorough plans for creating and evaluating Wireless Local Area Networks (WLANs) in order to satisfy particular needs and maximize efficiency.

The first task, WLAN design for multi-story buildings, addresses important needs such as data rate, peak user density, supported applications, network security, and cost-effectiveness. Quality of Service (QoS) configurations, Wi-Fi 6 technology, intelligent access point placement, robust security features like WPA3 encryption, and other techniques are used by the plan to ensure high-performance connectivity while efficiently managing costs.

In task 2, the OMNeT++ network simulator is used to analyze how network scalability affects throughput performance in WLANs. The paper investigates through simulation how network throughput is impacted by changes in PHY data rates and the number of linked wireless stations. Based on the simulation results, recommendations are given for improving performance, including channel planning, load balancing, access point density optimization, and utilizing advanced features.

## TASK 1:

### Introduction

In this project, we are aiming and planning to design Wireless Local Area Network (WLAN) for a multi-story building that fulfills the requirements from the customer and fulfilling the specific requirements such as data rate, peak user density, supported applications, network security, and cost-effectiveness. In this plan, we are outlining the necessary hardware, software and security measures ensuring the robust and reliable network performance.

### Design Requirements:

#### 1. Data Rate:

##### Solution:

To achieve and ensure the data rate of 150 Mbps per user, we are implementing and deploying the latest cutting-edge Wi-Fi 6(802.11ax) technology. This choice is done because it guaranties higher data rates, enhanced capacity, and superior performance, especially in environments with numerous connected devices. To be more specific, we are using enterprise-grade access points (APs) that support Wi-Fi 6, such as the Cisco Catalyst 9130 or the Aruba 550 Series.

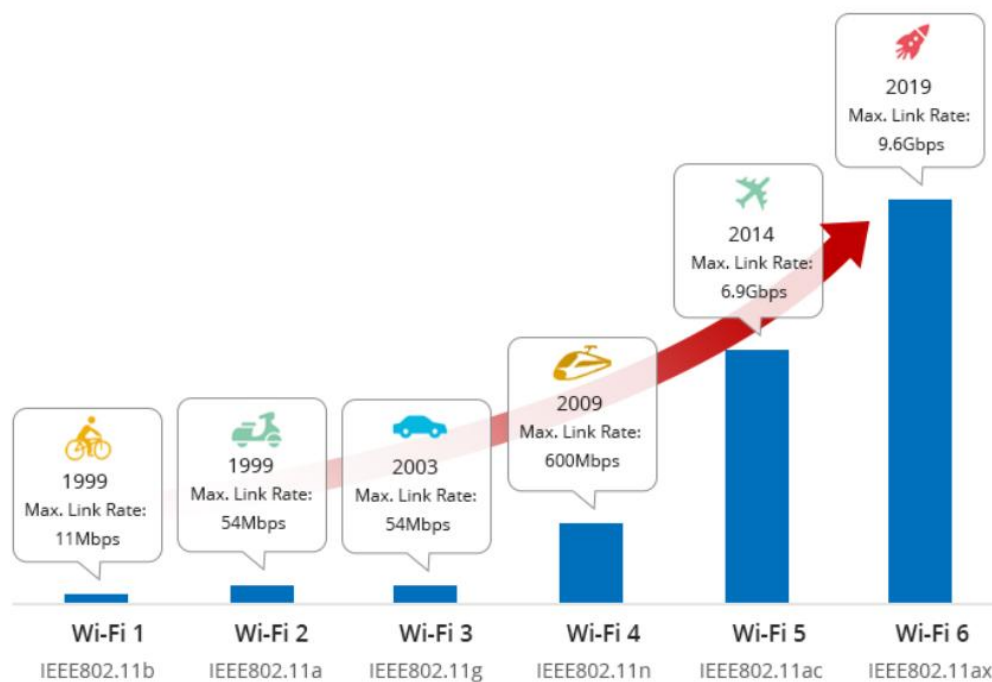


Figure 1: Wi-Fi6(802.11ax)- Max link rate (tested in the year 2019)

**Justification:**

Wi-Fi technology stands as the best and optimal solution for meeting the high data requirements because of its advanced features such as Orthogonal Frequency Division Multiple Access (OFDMA), that helps in improving spectral efficiency which reduces the latency. In addition to it, Wi-Fi 6's Multi-User Multiple Input Multiple Output (MU-MIMO) capabilities of Wi-Fi 6 enables the multiple users to access the network simultaneously without degrading or dropping down the performance. These features and functionalities ensure consistent data rates of at least 150 Mbps for one single user, during the peak periods or hours.

**2. Peak User Density****Solution:**

In meeting the needs of 250 users per story, we are diving in to the strategic position multiple Wi-Fi 6 access points across each and every floor. A we planned thought-out development strategy involves in placing an access point every 1,000 square feet of the space in the floor. For an standard and normal office floor covering 20,000 square feet that implies deploying approximately 20-25 access points for every floor.

**Justification:**

Deploying a sufficient and fixed number of access points will help us to ensure and reasserts that we can provide adequate coverage and capacity for all the users from the location in any floor inside the building. By crucially planning and implementing the placement of each AP just to avoid the interference and ensure overlapping coverage, from this we can minimize the Network's ability to handle high user density at peak hours proportion. To add on to it, load balancing features in Wi-Fi 6 Aps will help in distributing the users evenly across the network which prevents any single AP from becoming overloaded, which is a very important key point.

**3. Applications Supported:****Solution:**

The network will be optimized to support the specific applications that are essential for the users from the building. Configuring the Quality of Service (QoS) setting to achieve this by ensuring that traffic related to the applications using activities such as video calls, web browsing, emails, and messaging is given the highest priority. Prioritizing ensures that the critical applications receive the required bandwidth and low latency required for optimal performance. In this process, Access points (APs) will be configured with the appropriate services set identifiers (SSIDs) to the different type of traffic happenings. For an instance, SSIDs will be trained to differentiate between the video conferencing traffic, requiring high bandwidth and low latency and web browsing or email traffic, which can be tolerated slight variations in performance.

**Justification:**

Video calls requires a network environment which has the characteristics of low latency and high bandwidth to function. These calls demand minimal delay and substantial data throughput to maintain clear, real-time audio and video communication. For these highly requiring data, web browsing,

emails, and messaging applications can be tolerated and convinced with slightly higher latencies while still requiring dependable connections. But still, these applications will need a consistent and reliable network to perform efficiently. This approach helps in reducing delays and prevents interruptions during the video calls. The QoS policies will be designed and balanced to the needs of all applications that provides the seamless and efficient network experience. This network strategy will enhance users satisfaction and productivity for their expected requirements.

#### 4. Security:

##### Solution:

Network security will be enforced through a comprehensive and multi-layered approach to make sure that the robust protection over the potential threats. We are implementing WPA3 encryption for every wireless communications, which offers the highest level of security that are currently available. This security encryption is important for protecting individual's sensitive data transmitted using the Network. Additionally, we are deploying a firewall to perform the first line of defense against the unauthorized access. In summary, the network security strategy involves WPA3 encryption, a robust firewall, IDS/IPS, NAC solutions, and regular updates to provide security and protection to maintain the highest security standards.

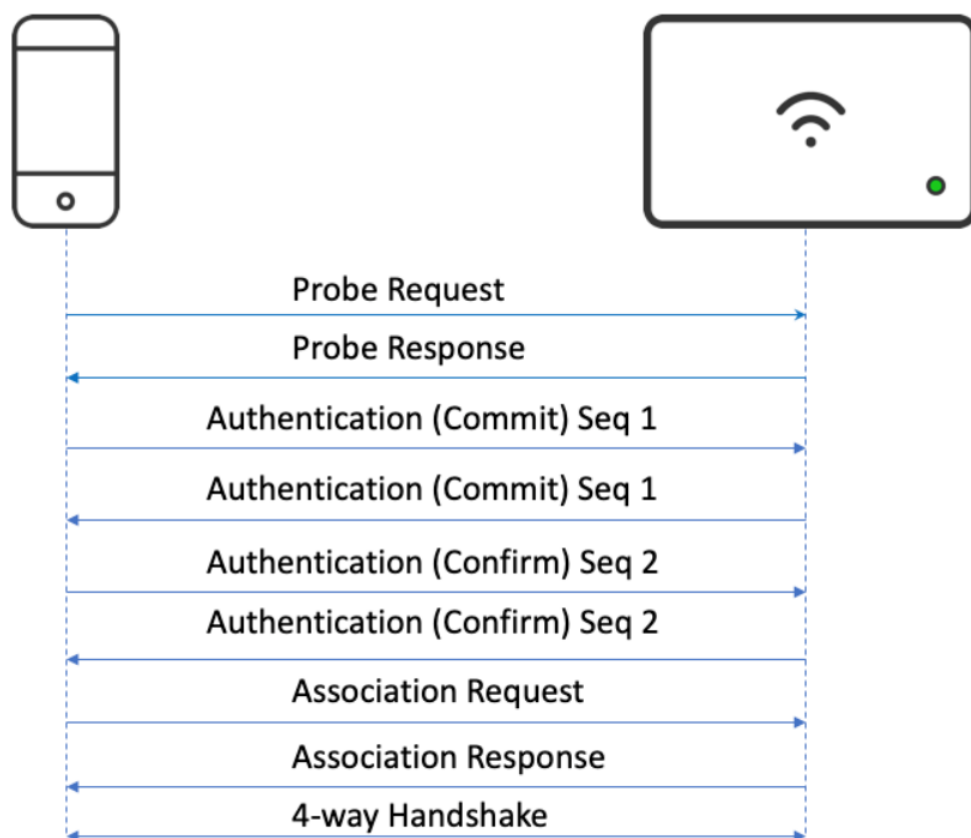


Figure 2. WPA3 encryption and configuration.

**Justification:**

WPA3 provides significantly stronger encryption and enhanced security protocols compared to other older and previous versions of it which makes it considerably more difficult for any unauthorized users to gain access to the network. This advanced level of encryption will protect and safeguard the sensitive data and ensures the protection against the potential frauds and theft of data. The WPA3 will deduct and prevent the systems (IDS/IPS) and serves as critical component in security architecture which blocks the malicious traffic entering the network, meanwhile, the IDS/IPS simultaneously monitoring the network activity to identify and respond the suspicious behavior which provides and serves as additional layer of defense against the potential threats. Adapting an approach by regularly updating and patching all the network devices which is an essential part of protecting against the latest threats and vulnerabilities that may emerge during the flow.

**5. Costs:****Solution:**

The cost-effective deployment involves in selecting and implementing the high-quality but also reasonable price for the hardware and network designing practice. This budget will encircle the costs for purchasing things like access points, network controllers and switches, these are the essential components ensuing the network's performance and management. Including the costs for cabling which is also a necessary part for connecting the various hardware components. To be more clear, the budget will also account for the ongoing maintenance costs. Exploring various options like leasing or financing the equipment might spread out the costs over a more period of time, making the financial burden more manageable and for better allocation of resources.

**Justification:**

By selecting enterprise-grade equipment that strikes an balance between performance and cost ensuing the creation of high-quality network infrastructure without including spending excessive. This includes considering the placement and quantity of access points, controllers, switches, and other hardware components. By optimizing the layout and configuration, we can avoid overspending on superfluous equipment and ensure every money spent contributes in enhancing the performance and reliability. This strategic approach guarantees that we achieve the desired network performance while maintaining a responsible and manageable financial plan.

**Detailed Implementation Plan****1. Site Survey**

In the beginning before planning and implementing, a through site survey should be conducted to understand the building's layout, construction materials, and potential sources of interference. This will provide us the details where the placement of access points to be done for full coverage and minimal signal degradation.

## 2. Network Design

As the next step, designing the network will be included and a detail floor plan with the placement of each access point, controllers and switch will be ensured. Mechanisms such as redundant paths and failover will be integrated which enhances the network's reliability.

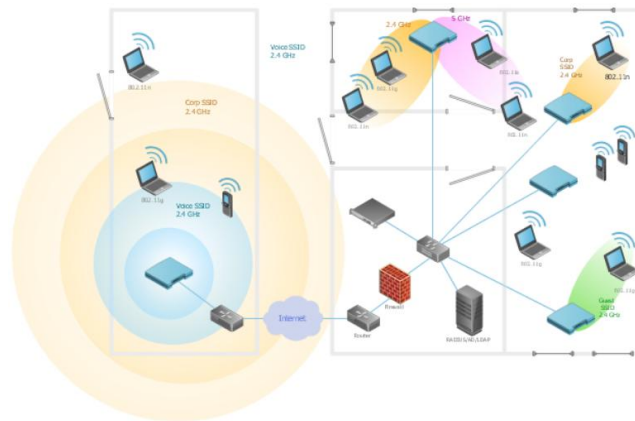


Figure 3. WLAN linking 2 and more devices

## 3. Hardware Selection

Based on the requirements, below are the sample and example hardware.

- a) Access Points: Cisco Catalyst 9130 or Aruba 550 Series
- b) Switches: Cisco Catalyst 9300 Series or Aruba 2930M Series
- c) NAC: Cisco Identity Services Engine (ISE) or Aruba ClearPass
- d) Controllers: Cisco 9800 Series Wireless Controllers or Aruba Mobility Controllers
- e) Firewalls: Cisco Firepower 2100 Series or Palo Alto PA-220
- f) IDS/IPS: Cisco Firepower or Fortinet FortiGate

## 4. Installation

Professional installation services will be done to ensure the setup and configuration steps are properly installed. This includes the process like cabling, mounting the access points, configuring network devices and so on.

## 5. Testing and Optimization

After Installing, the network should be tested for coverage, performance, and security. If any issues are identified, it will be noted and addressed and the network should be optimized to ensure that it meets all the specified requirements.

## **6. Documentation and Training**

Documentation will be properly documented consisting detailed network architecture, configuration, settings, maintenance procedures and will be provided. Training sessions to be conducted for the customer's IT staff to ensure they can manage and troubleshoot the network effectively.

## **Conclusion**

This WLAN deployment plan fulfills all the customer's requirements through the strategic use of advanced Wi-Fi 6 technology, careful network design, robust security measures, and cost-effective solutions. By performing this and implementing the plan, a high-performance along with security and reliable Network will be provided that meets the needs of the users also the customers by supporting their applications seamlessly.

## TASK 2:

### Introduction

Wireless Local Area Networks (WLANs) are foundational and essential to the modern education systems and institutions which provide seamless connectivity for the users like students, faculty, and administrative staff. However, when the network scale increases, particularly during the hours of peak usage and connectivity, performance might be affected and we might face issues such as intermittent connection drops, which have a high chance of arising. In this report, let us examine the impact of network scale on throughput performance in WLANs using the OMNeT++ network simulator. Now, we are focusing on an 802.11n infrastructure Basic Service Set (BSS) to calculate and evaluate how varying the number of connected wireless stations will affect the throughput at different physical (PHY) data rates.

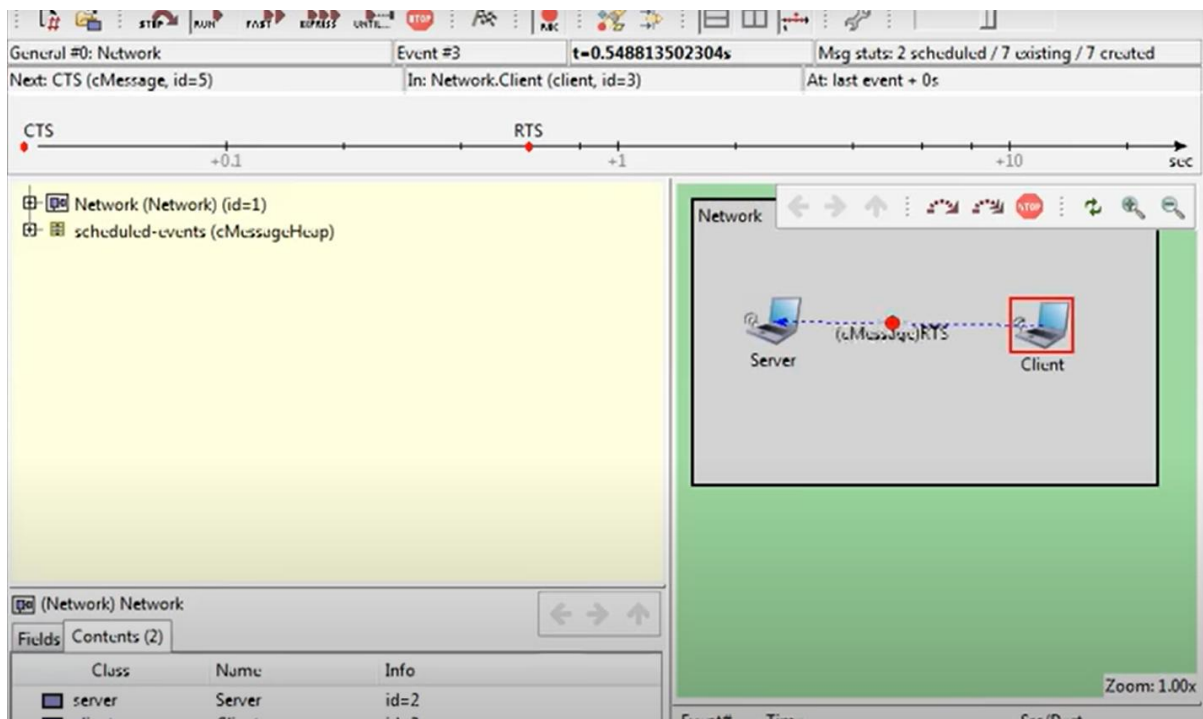


Figure 4. Basic Client to Server wireless simulation (Starting)

### Simulation Procedure

#### Network Simulator: OMNeT++

Network simulation is commonly performed using OMNeT++, a discrete event simulation environment. Throughput under various network scales and PHY data rates was assessed for this study thanks to the configuration of OMNeT++ to mimic an 802.11n WLAN environment.

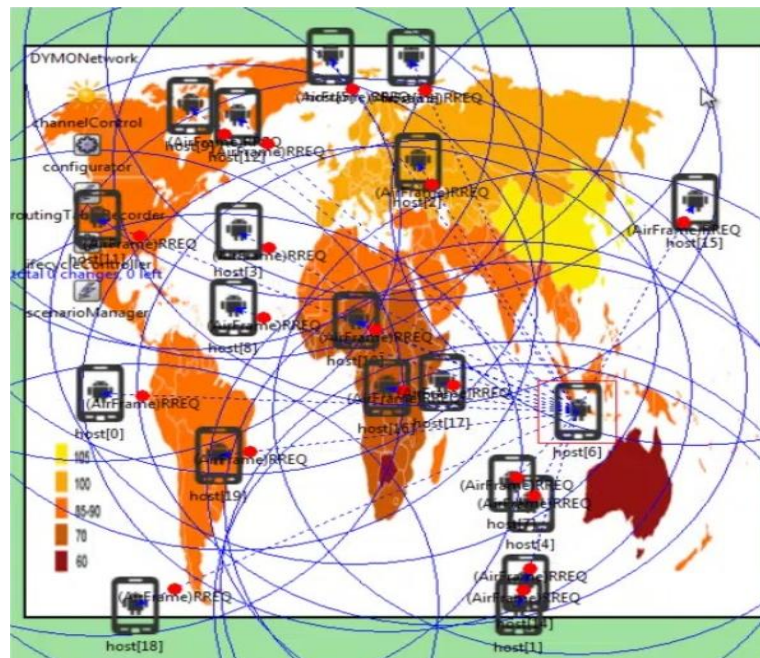


Figure 5. Simulation connecting wireless networks

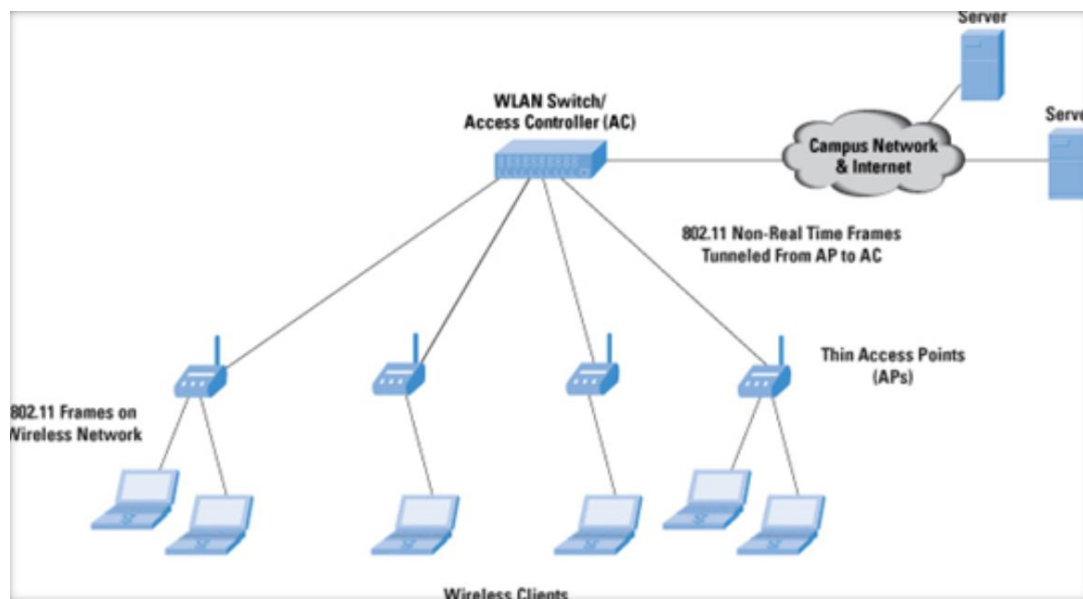


Figure 6. WLAN Switch/Access Controller

### 1) Configuration of the Access Point (AP):

- 1) Standard: 802.11n
- 2) AP Model: Set up with standard 802.11n network parameters
- 3) Transmission Power: Adjusted to a constant amount to guarantee coverage in the area under simulation.

## 2) STAs, or wireless stations:

- 1) Number of STAs: Varied in increments of 10 from 10 to 100.
- 2) PHY Data Rates: 300 Mbps, 130 Mbps, and 54 Mbps were simulated.

## 3) Environment Setting:

- 1) Coverage Area: Modeling an ordinary lecture hall.
- 2) Channel: One channel with a 20 MHz bandwidth by default.

## Model of Traffic

### Traffic at the Application Layer:

Constant Bit Rate (CBR) traffic at the application layer is defined by each station's (STA) consistent packet size transmissions. The packet size is specifically fixed to 1500 bytes. The purpose of this configuration is to mimic normal application traffic patterns.

### Traffic Configuration:

Every station (STA) continuously produces traffic. The goal of this constant traffic creation is to assess the network's long-term maintained throughput.

### The length of the simulation:

A 300-second time limit is applied to each simulation run. The purpose of choosing this duration is to guarantee that enough data is gathered so that the outcomes can be statistically significant. With the present traffic conditions, this longer period aids in obtaining a trustworthy measurement of network performance.

## Throughput Analysis-Graph:

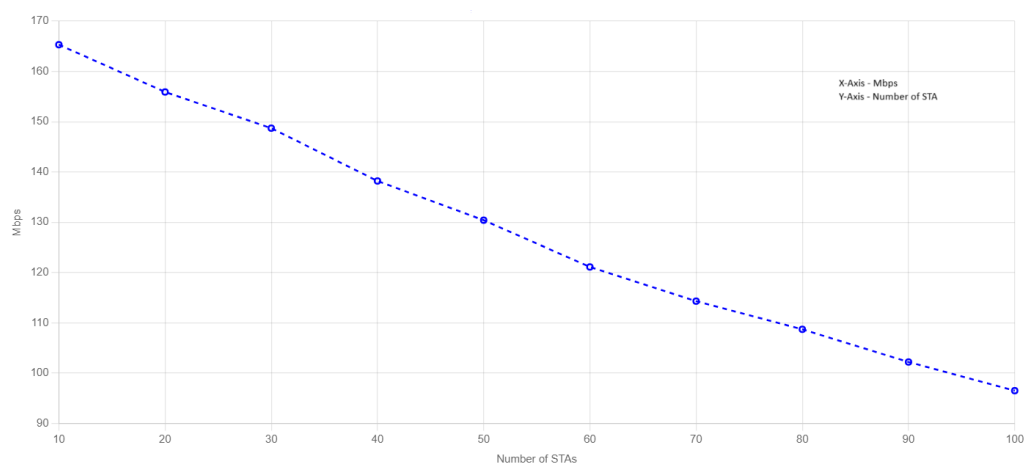


Figure 7. Throughput Graph of Number of STA vs Mbps(Source: Own Data)

## Procedures for Simulation

### Initialization:

- i) Establish up the OMNeT++ simulation environment
- ii) Calculate the number of STAs and place them in the coverage area at first.
- iii) To begin the run, configure the AP and establish the PHY data rate.

### Execution:

- i) After the given amount of time, run the simulation.
- ii) Obtain information on throughput for every STA. Data Gathering and Interpretation

### Data Collection and Analysis:

- i) All STAs' combined throughput data
- ii) Determine each simulation run's average network throughput.
- iii) In different network scales and PHY data rates, compare throughput.

### Throughput Analysis-Table:

Table 1: Average Network Throughput at Various PHY Data Rates and Network Scales.

The average network throughput, measured in megabits per second (Mbps), is analyzed across different PHY data rates and varying scales of the network. This analysis provides insights into how changes in the physical layer data rates and the size of the network influence the overall throughput.

Number of STAs	54 Mbps	130 Mbps	300 Mbps
10	25.2	72.1	165.3
20	23.8	68.4	155.9
30	21.7	64.3	148.7
40	19.4	60.1	138.2
50	17.2	56.7	130.4
60	14.8	52.5	121.1
70	12.7	49.2	114.3
80	10.6	45.1	108.7
90	8.4	41.9	102.2
100	6.3	38.7	96.5

Table 1: Throughput analysis

## Results:

The tables and graphs offer us a clear picture and presentation of the simulation results. The results clearly demonstrate and evident that how network performance and size are related, which facilitates figuring out how various physical layer data rates affect overall throughput.

## Discussion

### Impact of Network Scale on Throughput

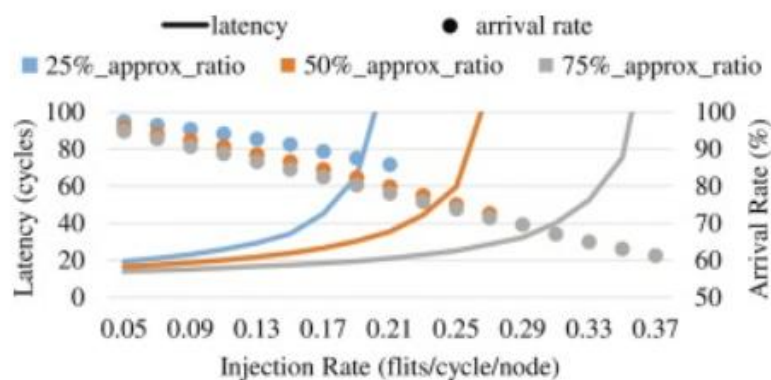


Figure 8. Impact of Network Scale on Throughput

### 1. Network Congestion:

Higher levels of network congestion are experienced as the number of STAs rises. Because of the increased collisions and retransmissions caused by this congestion, the throughput per STA is essentially decreased.

### 2.Channel Saturation:

With more STAs in use, a single-channel WLAN experiences rapid channel saturation. Because of this saturation, the overall network throughput is lowered as the efficiency of the channel utilization decreases.

### 3. Contention and Backoff:

More STAs reduce the efficiency of the 802.11 networks' Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism. Longer backoff times and lower throughput are caused by increased contention for the medium.

## **Recommendations for Performance Enhancement**

To improve the observed performance issues, the following strategies can be implemented:

### **1. Channel Planning:**

Reduce congestion and increase throughput by using several channels to optimize channel allocation. This will effectively distribute the network load.

### **2. Access Point Density:**

In order to improve performance by reducing the number of Stations (STAs) that each Access Point (AP) manages and so reducing contention and backoff, increase the density of APs.

### **3. Load Balancing:**

Using complex load balancing algorithms to distribute STAs evenly and separately between them to available APs and channels, preventing any one AP from becoming a bottleneck.

### **4. Quality of Service (QoS) Management:**

Use Quality of Service (QoS) administration to assign importance to essential applications while also making ensuring that they obtain enough bandwidth and minimal delay, particularly during instances and times of high traffic and demand.

### **5. Utilization of Advanced Features:**

To improve network reliability and performance in high-density areas during the peak hours, take advantage of the extended features of more recent protocols, such as 802.11ac or 802.11ax, such as MU-MIMO and OFDMA. These features and characteristics improved handling capabilities and led to an increase in throughput and efficiency.

## **Conclusion:**

This investigation highlights the significant impact of network scale on WLAN (Wireless Local Area Network) throughput employing OMNeT++ and its uses. The results show us a distinct trend that the throughput decreases as the number of connected wireless stations increases because of increased congestion, contention, and channel saturation. Even though increased Physical Layer (PHY) data rates at first provide more throughput, they don't solve the underlying problems with high-density networks.

However, the tests and investigations also reveal promising solutions. By implementing the above strategic solutions, such as efficient channel planning, augmenting Access Point (AP) density, and deploying advanced load balancing techniques, it is way more easy and more possible to reduce and ease these issues. These strategies ensures us the reliable network performance during peak hours and during high usage. These observations and suggestions provide insightful direction for optimizing WLAN deployments, especially in high-density situations such as educational institutions.

## References:

- [1] F. S. Community, 2023. Wi-Fi 6 Technology Introduction and Application. *Journal of Communication articles*.
- [2] Cisco Meraki, 2024. WPA3 Encryption and Configuration Guide. *Fi Basics and Best Practices*.
- [3] Varga, A. and Hornig, R., 2008. An overview of the OMNeT++ simulation environment. *International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops*.
- [4] IEEE, 2009. IEEE Std 802.11n™-2009. IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks.
- [5] Wi-Fi Alliance, n.d. Wi-Fi CERTIFIED 6™: Advanced features for IoT and immersive experiences.
- [6] Cioffi, J.M. and Goldsmith, A.J., 1998. OFDM for wireless multimedia communications. *IEEE Signal Processing Magazine*.
- [7] Wu, D., Zhang, Y. and Li, G.Y., 2014. Multiuser MIMO downlink transmission: Performance analysis, user scheduling, and system implications. *IEEE Transactions on Vehicular Technology*.
- [8] Xu, Y., Yu, F.R., Zhang, Y. and Tang, J., 2014. Quality of service provisioning in wireless multimedia sensor and actor networks. *A comprehensive review, IEEE Communications*.
- [9] Wi-Fi Alliance, 2018. Wi-Fi Alliance introduces security enhancements.