Anbar Journal of Engineering Science (AJES) **Vol. 15 , No. 1 (2024) , pp. 41 ~ 54**
P-ISSN: 1997-9428 ; E-ISSN: 2705-7440 DOI: http://doi.org/10.37649/aengs.2024.144601.1065

University of Anbar

Anbar Journal of Engineering Science
journal homepage: https://ajes.uoanbar.edu.iq/

Smart Hospital Network Enterprise Design for Medicine City Hospital via Packet Tracer

Mohammed Rajih Jassim
Department of production Engineering and metallurgy, University of Technology, Iraq, Baghdad
Email: mohammed.r.jassim@uotechnology.edu.iq; ORCID: https://orcid.org/ 0000-0002-0895-6360

PAPER INFO

Paper history
Received: 20/11/2023
Revised: 24/02/2024
Accepted: 29/03/2024

Keywords:
PAT
Subnetting
IP Addressing
Cisco
Packet Tracer

ABSTRACT

The scientific paper examined the possibility of developing an advanced healthcare management system in Iraq using Cisco Packet Tracer software. The article stated that the software above has the potential to speed up network management operations and reduce expenses incurred in maintenance and repair activities. In addition, the article explained several challenges that may arise while implementing the innovative hospital management system, including providing the required technical expertise, infrastructure provisions, and procedural measures necessary to protect the confidentiality of patient and employee information. The study confirmed that implementing an intelligent hospital management system in Iraq can improve healthcare quality, mitigate medical errors, enhance employee communication, and reduce disturbances within the hospital setting. Furthermore, this intervention is expected to enhance the efficiency of resource and inventory management and increase patients' experience and satisfaction with healthcare services. The article concludes that achieving the desired results in implementing a smart hospital management system using Cisco Packet Tracer software depends on the collaborative contributions of employees, managers, and technical professionals. This initiative is expected to enhance the hospital's ability to provide exceptional medical services and effectively meet patients' diverse needs.

1. Introduction

Iraq's healthcare system must be updated to improve patient care and boost productivity. With the aid of the Smart Hospital Network initiative, the Iraqi healthcare system can accomplish these objectives. The critical components of the Smart This proposal describes the Hospital Network Foundation and how it might be used in Iraq (more will be covered in the following parts).

The Internet of Things (IoT) is a network of millions of sensors and intelligent gadgets. With linked devices and sensors, data gathering and exchange are both feasible. Aggregated data are used for assessment by many entities, including homes, businesses, communities, governments, hospitals, and people [1]. The Internet of Things (IoT) enables inter-object communication. The number of other objects is growing swiftly, and for them to connect

* Corresponding author: Mohammed Rajih Jassim ; mohammed.r.jassim@uotechnology.edu.iq; +964-7832034308

through the Internet, each one must be able to be individually identified. The Internet of Things (IoT) is a clever and well-known concept that has offered a fresh perspective on efficiency, accuracy, and improved economic advantages for the Internet [2]made this suggestion in 1999. Intelligent buildings "utilize technology and processes to enhance operational efficiency, safeguard the health and safety of occupants, enhance employee productivity, and minimize their environmental impact. Smart hospitals are one example. Safety and health are essential in reducing patient stress caused by long wait times, streamlining activities for healthcare personnel, and providing high-quality treatment to those in need [3].

The H-IoT field, including internet-connected devices, sensors, and healthcare software, is proliferating. The goal is to enhance patient outcomes, boost efficiency, and cut costs with real-time data, predictive analytics, and remote monitoring. H-IoT applications include wearable devices, remote patient monitoring, telemedicine, and intelligent hospital systems [4]. H-IoT has the potential to revolutionize healthcare delivery with AI and machine learning for personalized and efficient care. Data confidentiality and safety must be addressed for secure and effective H-IoT use. The IoT is a promising technology in healthcare [5]. we Conducted a comprehensive review of H-IoT in healthcare. This study examines the technological advancements in H-IoT and the challenges that must be addressed. Rodrigues et al. Further research is essential to address current H-IoT challenges. Our thorough review will be valuable for researchers, tech specialists, healthcare providers, and the general public looking to enhance H-IoT [6]. Researchers have developed a strong cryptosystem for secure MRI image transmission in H-IoT environments. The study investigates the dynamics of a 2D trigonometric map with infinite solutions. This text utilizes phase portraits, bifurcation diagrams, and the Lyapunov exponent to illustrate the map's complex dynamics. The proposed cryptosystem is highly secure and suitable for H-IoT in the medical image transmission field [7].

In this article, the design and implementation of the suggested innovative hospital taken as a scale model of the Medical City Hospital (the main headquarters) and Baghdad Teaching Hospital, considered the sub-headquarters, were done using simulation software from Cisco Pact Tracer. For instructional reasons, students registered in the Cisco Networking Academy program can utilize Cisco Packet Tracer, a network software for simulation and visualization. Since Packet Tracer utilizes little hardware, runs on many different platforms, and doesn't require much, it is occasionally used as a substitute for actual hardware[8]. Some IoT and brilliant network research will be covered in the following part. We analyzed various publications that are closely relevant to the current study, which examines the design of an innovative hospital, smart home, or smart city using a packet tracer due to the absence of scientific research on creating and implementing a smart hospital.

2. Related work

In 2006, Patrik Fuhrer and Dominique Guinard [9] explain how RFID technology is used in healthcare to enhance patient safety, streamline administrative procedures, and eliminate mistakes. The article begins with an overview of RFID technology, including its core ideas and standards. It provides an example of an RFID-enhanced hospital and explains how RFID may be utilized to create a smart hospital. The article also introduces the RFIDLocator application and demonstrates how it may be set up for usage in a medical facility. The paper's primary accomplishments are outlined in the conclusion and several outstanding issues that must be resolved before the healthcare industry completely embraces RFID. The study provides examples of hospitals that have used RFID technology, including the Massachusetts General Hospital and the Saarbrücken Clinic Winterberg in Germany.

In 2017, DMHT Dasanayake et al. [10] presented "WARDBOT," a smart hospital ward management system that employs a mobile robot to manage hospital wards effectively. By utilizing automation and technology, this creative idea seeks to improve the overall administration of hospital wards. The WARDBOT system helps with various duties inside the hospital ward, resulting in better patient care, more efficient operations, and better resource use. The system offers an efficient method for managing hospital wards using mobile robotics and smart technology, possibly altering how medical facilities run.

In 2018, Istabraq M. Al-Joboury and Emad H. Al-Hemiary [11] presented a study that uses Cisco Packet Tracer to verify a suggested cloud-based architecture for people living with asthma and is

included in the literature review of this publication. In this design, a temperature sensor collects patient-provided temperature readings and transmits them wirelessly to the cloud. The study's authors put this suggested architecture into practice. According to this literature assessment, the Cisco Packet Tracer can be helpful for mimicking Internet of Things applications, such as medical monitoring systems.

In 2019, Mayaga Elsaid et al. [12] released a paper that analyzes intelligent houses. Numerous research projects have been conducted to develop and evaluate safe, smart houses for older adults. Remotely controlled home automation systems have been created using cloud computing and Internet of Things (IoT) technology to meet the requirements of those who live alone, especially older people, by offering security, comfort, and health monitoring. These technologies have been proven to be highly safe and successful in enhancing more senior citizens' daily lives in their homes through a practical analysis. For those who live alone, especially older adults, the use of IoT technologies in the design of smart systems has the potential to offer comfort and protection. It might provide a remedy for the problems people experience.

In 2020, Faris A. Almalki [13] showed a 5G implementation for smart buildings utilizing IoT. Using visual simulation tools, a virtual network is designed with Cisco Packet Tracer. This article sought to create a smart building structure with 5G technology in communication and interaction with the Internet of Things (IoT) devices to increase the building's energy efficiency, comfort, and security level. Cisco Packet-Tracer software utilizes VLAN technology to classify various networks and allocate them to IoT devices. The structure, energy efficiency, and sensor data from IoT devices were gathered. The findings revealed a noticeable improvement in comfort, safety, and energy economy through Tracer's implementation of VLAN technology.

In 2020, Banu Calis Uslu and Ertuğ Okay, Erkan Dursun [14] introduced The investigation of the variables influencing IoT-based clever hospital design as the primary emphasis of the paper's literature review. It discusses how the healthcare industry is undergoing a digital transition and how IoT technology might help improve healthcare management systems. This study presents a five-layered IoT architecture for intelligent hospitals, and each layer's technological infrastructures and efficacy are examined. It thoroughly examines innovative healthcare environments' prospects, technology, and optimization considerations. The study also emphasizes the scope and dimensions of big data analytics in real-time and intelligent computing in smart hospital architecture. The study attempts to offer a road map for managers, system developers, and academics interested in improving the design of smart hospital systems.

In 2021, S. Rava[15]li and Dr R. Lakshmi Priya [16] proposed research to develop and deploy an Internet of Things (IoT)-based innovative hospital. A collection of wireless actuators and sensors has been included in the design to enhance the hospital's functionality and increase its efficiency. The program was developed using the Raspberry Pi operating system, and a prototype for the smart hospital was created utilizing a communication and networking technologies platform using the Packet Tracer package. Critical variables like temperature, humidity, air quality, and noise were evaluated to assess the smart hospital's functioning. The outcomes demonstrated that a smart hospital might lower expenses while raising the standard of medical treatment. The article also reached some conclusions and recommendations that can help improve health care in different hospitals using IoT technologies.

In 2022, Nesreen Alsbou et al. [16], The article described the designing and implementation of a smart hospital via Internet of Things (IoT) technologies. The design uses sensors and wireless controllers to improve the hospital's performance and efficiency. Cisco Packet Tracer was used to design the initial model, while Raspberry Pi was used for implementation. The hospital's performance was evaluated in a simulated environment, measuring key indicators such as temperature, humidity, air quality, and noise. The results showed that smart hospitals can improve healthcare quality and reduce costs. The article concludes with recommendations to improve healthcare in different hospitals using IoT technologies.

In 2023, Md. Harun-Ar-Rashid et al. [17] explored utilizing the Health Level Seven (HL7) standard to construct an IoT medical picture monitoring system on a hospital database. By delivering real-time updates on patient states and medical image data, the design seeks to improve the accuracy and efficacy of medical image monitoring. The article goes into the architecture of the system and its

many parts, such as the sensors, the data-gathering module, and the HL7 interface. The system has undergone hospital testing and demonstrated increased accuracy and efficacy in monitoring medical images. Overall, the study emphasizes the necessity of uniformity in transferring medical data and the potential advantages of IoT systems in healthcare.

3. Internet Protocol Overview (IP)

An IP address may be an arrangement of numeric values isolated by periods. IP addresses are spoken to as a set of four numbers. Each number inside the set features a run from 255. Consequently, the total extent of IP tends to range from 0.0.0.0 to 255.255.255.255. IP addresses are not haphazardly created. These addresses are scientifically inferred and distributed by the Web Alloted Numbers Specialist (IANA), a department of the Web Enterprise for Relegated Names and Numbers (ICANN). ICANN, a non-profit organization built in the United States in 1998, plays a pivotal part in keeping up the security and openness of the Web for all clients. At whatever point a person registers a space on the Web, the method includes a space title enlistment center that transmits [18][19].

3.1 IP Address Classes

The private IP address is the internal address used within a local network.

The IANA organization has allocated IP addresses in a specific manner, defining ranges within each class that users are authorized to use and identifying off-limits addresses. When you take action, it involves the allocation of IP addresses within your local network. We will provide you with a specific range that must be used as the basis for distributing IP addresses. The category in which we allocate IP addresses is the Private IP range [20] [21].

The domain for which I have permission to use is:

1 Class A ranges from 10. 000 to 10255255255
2 Class B range extends from 172. 1600 to 17231255255
3 Class C ranges from 192. 16800 to 19216800.

3.2 A Public IP Address

The public IP address is the unique identifier for when you are connected to the Internet or a device outside of the local network.

This means that while working within the internal network, you use a Private IP inaccessible from the Internet. When you wish to access the internet, you connect to the router. The router contains both an internal and an external user interface. The internal interface uses the Private IP within the local network, allowing internal devices to connect to the Internet by having the router communicate with the Internet Service Provider (ISP). This company offers its customers the ability to attach to the Internet. When you are connected to the ISP, the ISP establishes a network between itself and you without our knowledge and automatically provides the external interface. The Internet service provider assigns the router an IP address through its corresponding interface, creating a network connection between the router and the ISP. This assigned IP from the ISP is known as the Public IP [22][23].

In brief, a Public IP is the unique address assigned to me when I go online, which means that all devices must use a Public IP to access the Internet. Private IPs cannot be used to connect to the Internet. Instead, every device within the local network accesses the Internet using the IP address assigned to the router by the ISP located in the country. The ISP company acquires Public IP addresses from the IANA organization and pays a significant amount for a specific range to distribute to routers. Once assigned, the IANA organization does not allocate that same range to the ISP company again, ensuring the router's public IP belongs to the ISP. It is not possible to replicate it using a different router's Public IP [24].

4. Methodology

The present topology utilized the following steps to design the hospital:

4.1 Network Design and Beatification

Below will be explained the design of our network as shown in the figure 1:

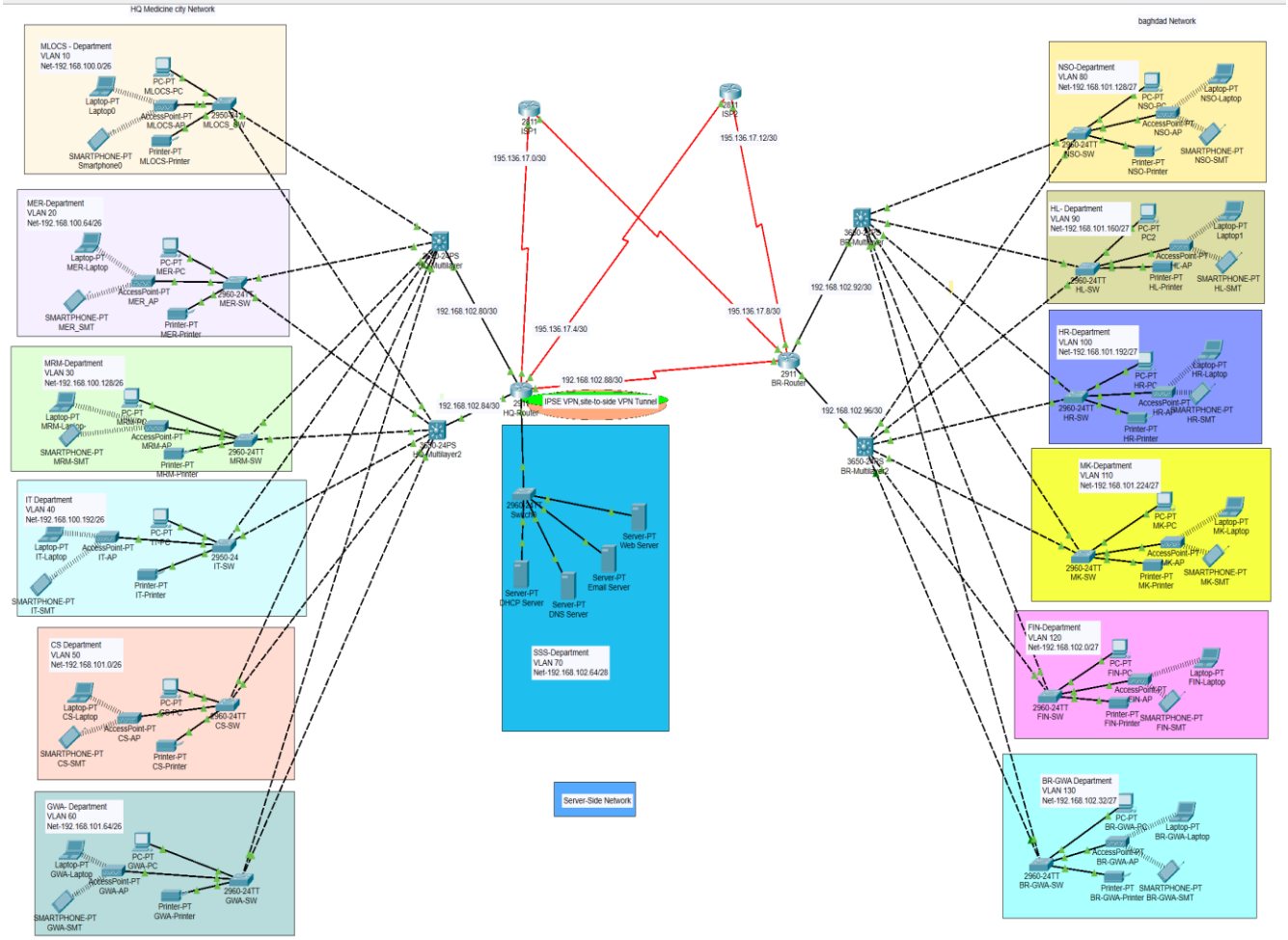

Figure 1. Proposed Topology

4.2 Basic Setting to All Devices Plus SSH on the Routers and 13 Switches

When setting up a network, devices must be configured with unique IP addresses and subnet masks for communication. The default gateway, usually a router's IP address, is necessary for devices to communicate with other networks. A DNS server is required to translate the domain name to IP address. To enable remote access and management, it is recommended that SSH be configured on routers and switches. Configuration is typically done through a console cable, CLI, or a web GUI,
With commands varying by device model and manufacturer. Referring to the device documentation is recommended for specific instructions.

4.3 VLANs Assignment Plus All Access and Trunk Ports on 12 and 13 Switches.

VLANs divide a network into separate broadcast domains for improved performance, security, and management. VLANs are configured on switches, and ports on switches are assigned to specific VLANs. The process involves creating unique VLAN IDs and names, setting VLANs to access and trunk ports, and configuring VLAN tagging on trunk ports to accept traffic of multiple VLANs toward pass-through. Access ports can only be assigned to a single VLAN, while trunk ports can carry traffic from multiple VLANs. Configuration is typically done through the switch's CLI or GUI interface, with commands varying by manufacturer and model—these results as shown in Table 1.

Table 1. Layer one in each network (port connections)

HQ Hospital			Branch Hospital		
Device Name	Port No.	VLAN No.	Device Name	Port No.	VLAN No.
MLOCS Department			NSO Department		
MLOCS-SW	Fa0/1-2	10	NSO-SW	Fa0/1-2	80
MLOCS-PC	Fa0/3	10	NSO -PC	Fa0/3	80
MLOCS-AP	Fa0/4	10	NSO- AP	Fa0/4	80
MLOCS-Printer	Fa0/5	10	NSO- Printer	Fa0/5	80
Other Devices	Fa0/6-24	10	Other Devices	Fa0/6-24	80
MER Department			HL Department		
MER-SW	Fa0/1-2	20	HL-SW	Fa0/1-2	90
MER -PC	Fa0/3	20	HL-PC	Fa0/3	90
MER -AP	Fa0/4	20	HL-AP	Fa0/4	90
MER -Printer	Fa0/5	20	HL- Printer	Fa0/5	90
Other Devices	Fa0/6-24	20	Other Devices	Fa0/6-24	90
MRM Department			HR Department		
MRM-SW	Fa0/1-2	30	HL-SW	Fa0/1-2	100
MRM-PC	Fa0/3	30	HL-PC	Fa0/3	100
MRM-AP	Fa0/4	30	HL-AP	Fa0/4	100
MRM- Printer	Fa0/5	30	HL- Printer	Fa0/5	100
Other Devices	Fa0/6-24	30	Other Devices	Fa0/6-24	100
IT Department			MK Department		
IT-SW	Fa0/1-2	40	IT-SW	Fa0/1-2	110
IT-PC	Fa0/3	40	IT-PC	Fa0/3	110
IT-AP	Fa0/4	40	IT-AP	Fa0/4	110
IT- Printer	Fa0/5	40	IT- Printer	Fa0/5	110
Other Devices	Fa0/6-24	40	Other Devices	Fa0/6-24	110
GWA Department			BR-GWA Department		
CS-SW	Fa0/1-2	50	FIN-SW	Fa0/1-2	120
CS -PC	Fa0/3	50	FIN -PC	Fa0/3	120
CS-AP	Fa0/4	50	FIN -AP	Fa0/4	120
CS- Printer	Fa0/5	50	FIN - Printer	Fa0/5	120
Other Devices	Fa0/6-24	50	Other Devices	Fa0/6-24	120
GWA Department			BR-GWA Department		
GWA-SW	Fa0/1-2	60	BR-GWA-SW	Fa0/1-2	130
GWA -PC	Fa0/3	60	BR-GWA-PC	Fa0/3	130
GWA-AP	Fa0/4	60	BR-GWA-AP	Fa0/4	130
GWA- Printer	Fa0/5	60	BR-GWA-Printer	Fa0/5	130
Other Devices	Fa0/6-24	60	Other Devices	Fa0/6-24	130

Switch port security to the finance department.

Switchport security is helpful within a hospital network to limit access to network resources for departments or individuals. This process configures ACLs on switch ports to restrict device connections. This mechanism helps prevent breaches and improve security integrity by limiting unauthorized access. To apply switch port security to a department, first, determine the specific switch ports the department uses. Customize security settings, including device limit and MAC address constraints. Testing switch port security is essential for its correct operation in academia. Switch port security in the hospital network protects sensitive data, upholding data confidentiality and integrity.

Subnetting and IP addressing.

Subnetting and IP addressing are crucial for network communication and management in our enterprise. Subnetting divides networks for optimization, security, and management. IP addressing uniquely identifies network devices for communication. To subnet and assign IP addresses in a smart hospital enterprise, follow these steps:

The present discourse aims to provide an academic analysis of the given text. To ascertain the network necessities, the number of subnets required, the number of devices per subnet, and any distinct network prerequisites must be appraised.

In academic writing, the text provided can be revised as follows: 2. Over the years, advancements have been made in numerous fields, leading to a

wide range of improved technologies and methodologies. As a result, these developments have significantly impacted various societal aspects and have brought about substantial transformations. The selection of a subnet mask is paramount as it plays a pivotal role in delineating the total count of subnets and the number of devices that can be effectively hosted within a given network. One potential way to rewrite the text in a more academic style could be as follows: The given passage presents an opportunity to express the information in a scholarly manner. The subnetting process entails partitioning a network into smaller and distinct logical subnets, which is done by the requirements identified during the initial step.

The allocation of IP addresses is performed to associate each device within the network with a respective subnet. Subsequently, it is crucial to subject the network to comprehensive testing procedures to verify seamless communication among all devices and achieve optimal network performance. By subnetting and assigning IP addresses in a smart hospital enterprise, the network can be efficiently managed and optimized to meet the needs of different departments and applications within the hospital. Base addressing: 192.168.100.0

5. HQ Hospital

The IP configuration is shown in Table 2: Branch Hospital. The IP configuration is shown in table 3: Server-Side Site. The IP configuration is shown in table 4: The IP Addressing configurations between Switches and routers are shown in table 5

Table 2. IP Addressing Between the Routers and layer-3 switches

No.	Network Address
HQR1-HQMLSW1	192.168.102.80/30
HQR1-HQMLSW2	192.168.102.84/30
HQR1-HQMLSW1	192.168.102.88/30
HQR1-HQMLSW1	192.168.102.92/30
HQR1-HQMLSW1	192.168.102.96/30

Between the routers and ISPs

Public IP addresses 192.168.136.17.0/30, 192.168.136.17.4/30, 192.168.136.17.8/30, and 192.168.136.17.12/30

6. OSPF on the Routers and 13 Switches

OSPF routers are crucial in a smart hospital network, ensuring reliable and secure communication between computers, servers, medical equipment, and IoT devices. OSPF routers create a network topology map using a link-state database containing detailed information about the network's links, such as bandwidth, delay, and reliability. In the smart hospital scenario, OSPF routers are configured with an OSPF process ID, and their interfaces are enabled for OSPF. They discover neighboring routers by exchanging OSPF Hello packets, generate Link-State Advertisements (LSAs), maintain an LSDB, calculate the shortest path using the Dijkstra algorithm, build a routing table, share information about routes, and support load balancing. This dynamic approach allows routers and switches to dynamically adapt to network changes, finding the most efficient paths for data packets and ensuring reliable and optimized communication between devices within the hospital.

Static IP address to Server Room device.

In the context of this intelligent hospital, a static IP address refers to a predetermined and unalterable numerical label designated to a particular device within the server room. In the intelligent hospital setting, a static IP address corresponds to a fixed and unchangeable numeric identifier assigned to a specific device in the server room. Within this intelligent hospital, a static IP address is a set and unmodifiable numerical tag given to a particular device in the server room. In the context of the intelligent Rephrase hospital, a static IP address represents an established and unchangeable numeric label assigned to a specific device in the server room. The acronym IP denotes Internet Protocol, comprising a codified system of regulations that govern the establishment of communication channels among interconnected devices within a network. A Dynamic Host Configuration Protocol (DHCP) server is responsible for the automated allocation of dynamic IP addresses, whereas static IP addresses are assigned manually to individual devices. These addresses confer many advantages, encompassing dependability, ease of use, protection, and the ability to discern devices. In the healthcare environment, network administrators must meticulously plan and coordinate static IP assignments. This practice is advocated to circumvent conflicts, guarantee uninterrupted communication, and proficient management of vital systems.

Table2. IoT devices sitting in the network.

Department	Network Address	Subnet Mask	Host Address Range	Broadcast Address
MLOCS	192.168.100.0	255.255.255.192/25	192.168.100.1 to 192.168.100.62	192.168.100.63
MER	192.168.100.64	255.255.255.192/25	192.168.100.64 to 192.168.100.126	192.168.100.127
MRM	192.168.100.128	255.255.255.192/25	192.168.100.129 to 192.168.100.190	192.168.100.191
IT	192.168.100.192	255.255.255.192/25	192.168.100.193 to 192.168.100.254	192.168.100.255
CS	192.168.101.0	255.255.255.192/25	192.168.100.1 to 192.168.100.62	192.168.100.63
GWA	192.168.101.64	255.255.255.192/25	192.168.100.64 to 192.168.100.126	192.168.100.127

Table 3. Branch hospital IP Addressing

Department	Network Address	Subnet Mask	Host Address Range	Broadcast Address
NSO	192.168.101.128	255.255.255.224/ 27	192.168.101.129 to 192.168.101.158	192.168.101.159
HL	192.168.101.160	255.255.255.224/ 27	192.168.101.116 to 192.168.101.190	192.168.101.191
HR	192.168.101.192	255.255.255.224/ 27	192.168.101.193 to 192.168.101.222	192.168.101.223
MK	192.168.101.224	255.255.255.224/ 27	192.168.101.225 to 192.168.101.254	192.168.101.255
FIN	192.168.102.0	255.255.255.224/ 27	192.168.102.1 to 192.168.102.30	192.168.102.31
GWA	192.168.102.32	255.255.255.224/ 27	192.168.102.33 to 192.168.102.62	192.168.102.63

Table 4. Server-Side Site IP Addressing

Department	Network Address	Subnet Mask	Host Address Range	Broadcast Address
SSS	192.168.102.64	255.255.255.240/28	192.168.102.65 to 192.168.102.78	192.168.102.79

7. DHCP Server Device Configuration

A DHCP server manages and distributes IP addresses to network devices. To configure a DHCP server, identify the device, assign a static IP address, install DHCP server software, configure the server, define an IP address pool, configure lease duration, configure additional parameters, implement security measures, and test and monitor the server's functionality. The specific steps and options for configuring a DHCP server may vary depending on the device and software used, so it's recommended to consult the manufacturer's documentation or user guides for detailed instructions. A smart hospital may ensure that every device connected to the network obtains a unique IP address and other relevant network setup parameters by carrying out these procedures.

Inter-VLAN routing on the 13 switches plus IP DHCP helper address.

Inter-VLAN routing in a smart hospital with 13 switches enables communication between different Virtual Local Area Networks (VLANs) for security, management, and optimization purposes. To implement Inter-VLAN routing, follow these steps: VLAN Configuration, VLAN Trunking, Layer 3 Switch, IP Addressing, Routing Configuration, IP DHCP Helper Address, Access Control Lists (ACLs), And Testing. The Layer 3 switch handles VLAN Interfaces, assigning IP addresses to each VLAN interface, and implementing DHCP services for devices in each VLAN. Regular monitoring and maintenance are crucial to ensure optimal and secure network operations.

7.1 Wireless network configuration.

At this stage, a username and password have been created for each department's access point, and all devices have been connected to this network. Each department now has its private network, as shown in figures 2, 3, and 4.

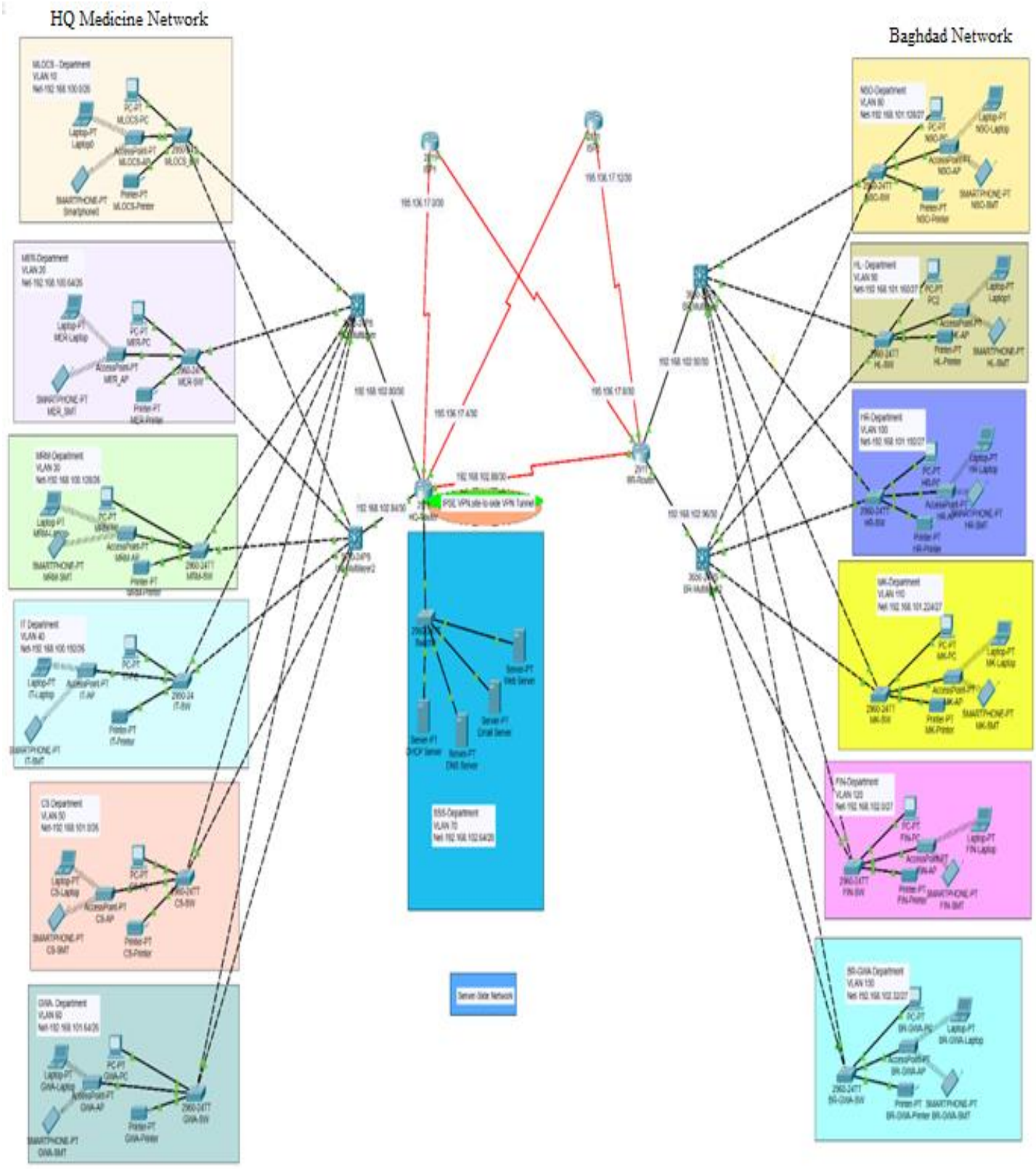

Figure 2.Wireless Network Configuration

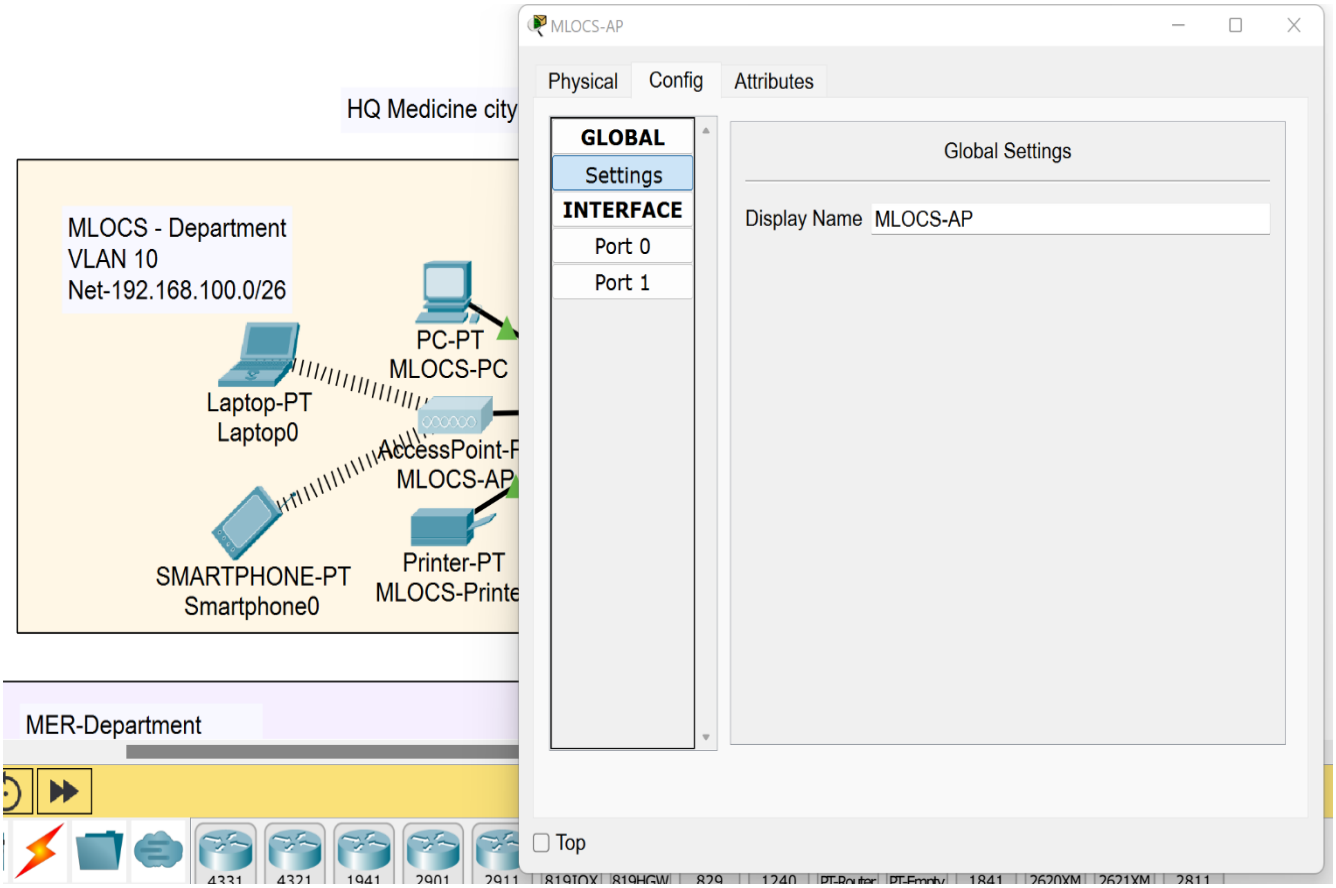

Figure 3. Copy the (Display Name) of the current Access Point

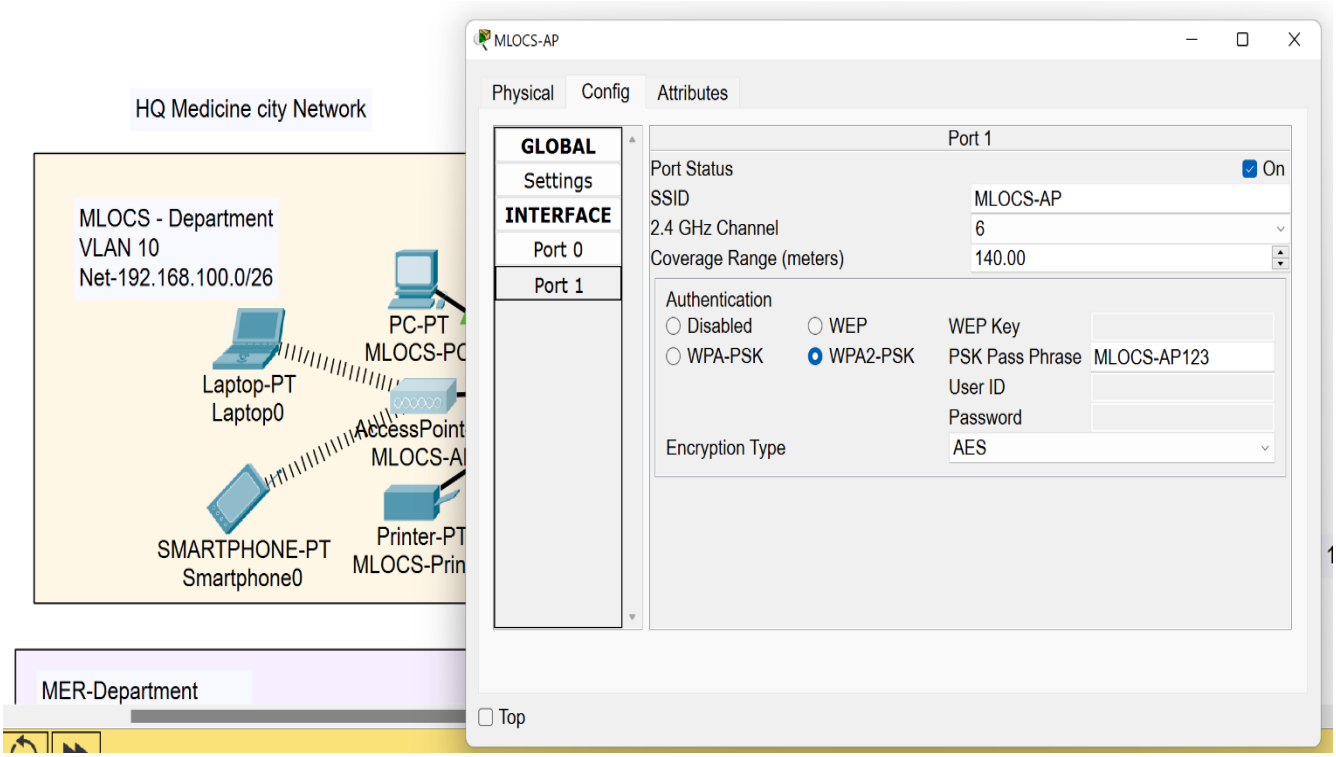

Figure 4. Port 1 sitting

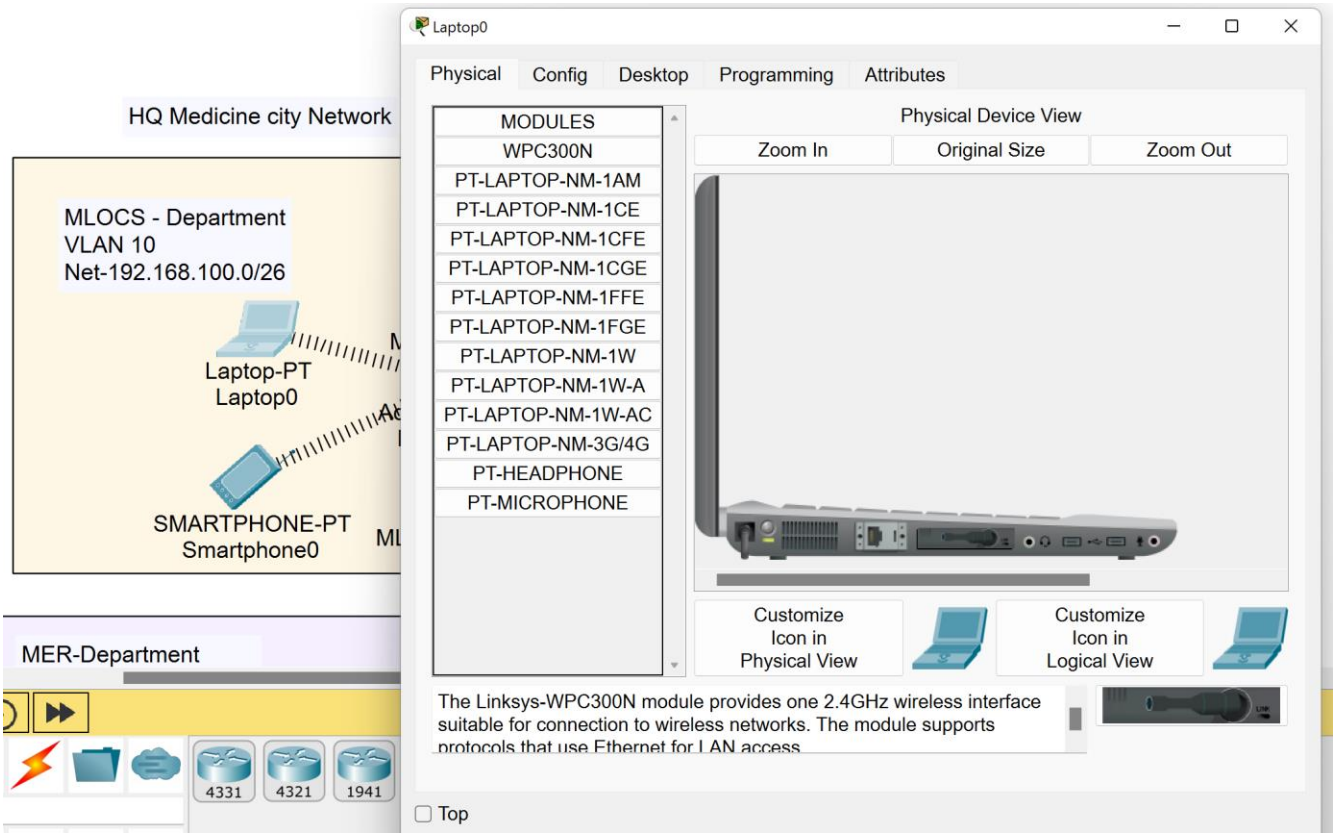

Figure 5. connect laptop with MLOCS Access point

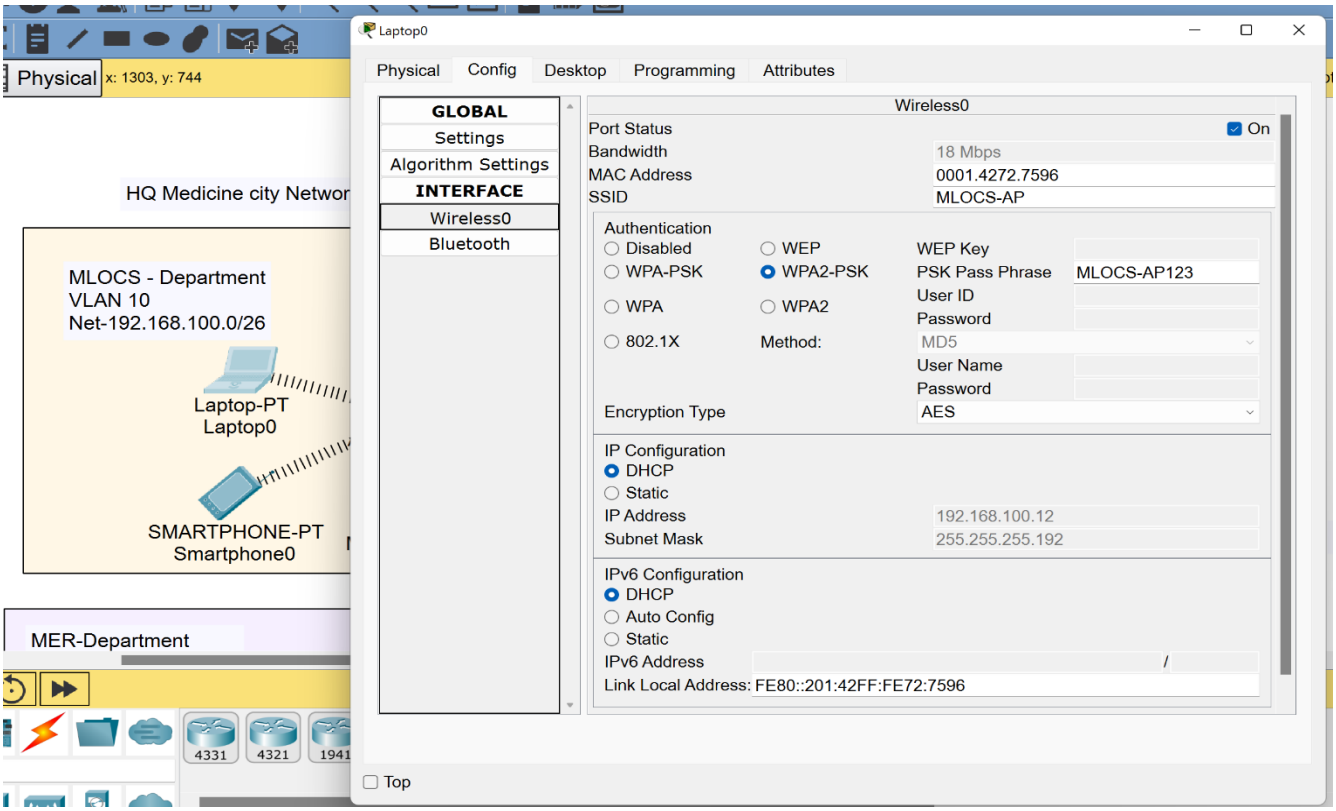

Figure 6. Configure the laptop sitting wireless to connect with the access point

After that, we must link all devices to the access point in the exact department, as shown in Figure (5). Then, the wireless network must be configured, as indicated in Figure (6). Now, we will do these configurations with smartphone devices in this department and all departments in two hospitals.
Do this configuration for all departments in HQ-hospital and branch-hospital. Note that the names should be configured with the same Access Point for each department. The next stage comes after that, Site-to-Site IPSec, VPN, which will explain the next step. Site-to-site IPSec. VPN. Site-to-site IPSec VPN is a secure and private VPN connection that enables secure communication between multiple sites or networks. An intelligent hospital environment consists of interconnected networks and systems across various locations. VPN gateway devices like satellite clinics and research centers are the entry and exit points for secure traffic between sites. IPSec encryption, a suite of protocols, ensures IP communications by providing encryption, authentication, and integrity. VPN configuration defines authentication methods, encryption algorithms, and other parameters for secure transmission.
Data encryption is encapsulated within an IPSec packet, with the sending VPN gateway encrypting and adding IPSec headers. Authentication protocols ensure that only authorized devices can establish a VPN connection using pre-shared keys, digital certificates, or a separate authentication server like RADIUS. Routing and network integration enable seamless communication between machines across different sites, allowing data to flow securely between them. This configuration is shown in Figure 7.

```
HQ-Router(config)#do sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 195.136.17.5:5    192.168.100.72:5   195.136.17.6:5     195.136.17.6:5
icmp 195.136.17.5:6    192.168.100.72:6   195.136.17.6:6     195.136.17.6:6
icmp 195.136.17.5:7    192.168.100.72:7   195.136.17.6:7     195.136.17.6:7
icmp 195.136.17.5:8    192.168.100.72:8   195.136.17.6:8     195.136.17.6:8
```

Figure 7. Nat configuration for HQ router

8. Default Static Route

In our Smart Hospital network, a default static route is a routing configuration that specifies the path or next-hop for forwarding network traffic when no specific matching route exists in the routing table. It acts as a default gateway, allowing packets to be sent to destinations outside the local network. This routing configuration simplifies network management and enables seamless connectivity for various hospital systems, such as patient monitoring devices, electronic health records, and communication systems. The configuration details may vary depending on the hospital's network infrastructure, routing equipment, and network topology. Network administrators typically configure the default static route to point to the next-hop IP address or the IP address of the hospital's internet service provider (ISP) gateway.

9. PAT + Access Control List

PAT (Patient Access Token) and ACL (Access Control Lists) manage and control access to resources and areas in an innovative hospital. PATs are unique identifiers assigned to each patient, providing essential information about their identity, medical history, and prescribed treatments. Conversely, ACLs are rules or permissions that define who can access specific resources or areas within the smart hospital. The hospital administration maintains and manages these lists, which can be customized based on patient status, staff roles, and time of day. By combining PATs and ACLs, the smart hospital ensures that only authorized individuals, such as patients, healthcare providers, and support staff, can access the appropriate resources and areas; these configurations are shown in Figure 8.

```
BR-Router(config)#access
BR-Router(config)#access-list 1 permit 192.168.101.128 0.0.0.31
BR-Router(config)#access-list 1 permit 192.168.101.160 0.0.0.31
BR-Router(config)#access-list 1 permit 192.168.101.192 0.0.0.31
BR-Router(config)#access-list 1 permit 192.168.101.224 0.0.0.31
BR-Router(config)#access-list 1 permit 192.168.102.0 0.0.0.31
BR-Router(config)#access-list 1 permit 192.168.102.32 0.0.0.31
BR-Router(config)#
BR-Router(config)#
BR-Router(config)#do wr
Building configuration...
[OK]
BR-Router(config)#
BR-Router(config)#
BR-Router(config)#sh ip nat tra
BR-Router(config)#sh ip nat tran
BR-Router(config)#sh ip nat translations
BR-Router(config)#sh ip nat translations
                 ^
% Invalid input detected at '^' marker.

BR-Router(config)#do sh ip nat translations
BR-Router(config)#
BR-Router(config)#
BR-Router(config)#
BR-Router(config)#
BR-Router(config)#
BR-Router(config)#
BR-Router(config)#do sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 195.136.17.9:2    192.168.101.168:2  195.136.17.2:2     195.136.17.2:2
icmp 195.136.17.9:4    192.168.101.168:4  195.136.17.2:4     195.136.17.2:4
```

Figure 8. NAT configuration for BR-router

10. Verify and Test Configurations

In a smart hospital setting, proper functioning and reliability are crucial. A systematic approach to verifying and testing configurations involves documentation, functional testing, integration testing, performance testing, security testing, data integrity and accuracy testing, user acceptance testing (UAT), compliance and regulatory testing,

and documentation and reporting. These checks ensure the system functions correctly, ensuring smooth data exchange and communication. UAT identifies usability issues, glitches, and functionality gaps, while compliance testing ensures compliance with regulations and certifications. By following these steps, the smart hospital system can operate optimally, ensuring effectiveness and reliability for all stakeholders.

11. Results and Discussion

The research successfully created an advanced smart hospital network using Cisco Packet Tracer. This involves establishing VLANs, assigning IP addresses, and enabling secure SSH on routers and switches. The implementation showed a strong network structure that efficiently manages various hospital operations. Performance indicators like network delay, data transfer rates, and system dependability were evaluated. The findings showed fast data transfer rates and minimal delays, crucial for monitoring patients in real time and managing data effectively in healthcare settings. Challenges emerged while implementing the new system, such as integrating outdated hospital systems and ensuring data security. However, these concerns are efficiently addressed using state-of-the-art security measures and tailored integration options. The study's findings validate Packet Tracer's capability to design hospital networks. The network's strong performance and dependability suit critical healthcare operations. In contrast to conventional hospital networks, the innovative hospital network developed in this study offers enhanced effectiveness, adaptability, and protection. Its performance indicators also show a substantial enhancement in speed and reliability compared to current systems. The study results could lead to the increased use of intelligent hospital networks, which would significantly impact future healthcare infrastructure. It emphasizes the significance of utilizing advanced networking solutions to improve the delivery of healthcare and the care of patients.

12. Conclusion and Future Works

A smart hospital network enterprise is a network architecture that connects medical equipment, patient data, and hospital operations to improve patient care and efficiency. The following characteristics are included in the smart hospital network enterprise:

Wireless Infrastructure: The competent hospital network organization will have a wireless infrastructure allowing medical equipment and personnel to connect to the network anywhere within the hospital. High-speed data transfer and low-latency communication will be possible thanks to the wireless infrastructure.

IoT Devices: The smart hospital network enterprise will include IoT (Internet of Things) devices that can monitor patient vital signs, track medical equipment, and automate hospital operations. IoT devices will be connected to the hospital's Electronic Medical Record (EMR) system to offer real-time patient data and improve patient care.

Analytics and Machine Learning: The smart hospital network enterprise will include Analytics and machine learning capabilities to evaluate patient data and uncover trends that might enhance patient care. These capabilities will also improve hospital operations while lowering expenses.

Security: The business's innovative hospital network will be built with security in mind. The network infrastructure will be secured using firewalls, intrusion detection systems, and other security measures to protect patient data and prevent unwanted access.

13. Funding

No funding support is to be declared.

14. Acknowledgements

The authors wish to acknowledge the unlimited support from the University of Technology, IRAQ, Department of Production Engineering and Metallurgy.

15. Conflicts of Interest

No conflict of interest is to be declared.

References

[1] R. R. Chaudhari, K. K. Joshi, N. Joshi, and M. Kumar, “Smart and secure home using IOT Simulations with Cisco Packet Tracer,” International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2020.

[2] S. A. Rafea and A. A. Kadhim, “Routing with Energy Threshold for WSN-IoT Based on RPL Protocol,” Iraqi Journal of Computer, Communication, Control and System Engineering, 2019,

[3] Y. AL - Saffar, S. Gitaffa, and A. H. Issa, "Design and Implement the Innovative Drugstore for Health Care Services Based on Health Mobile Applications and Advanced IoT," Engineering and Technology Journal, vol. 41, no. 2, 2022.

[4] D. V. Dimitrov, "Medical internet of things and big data in healthcare," Healthcare Informatics Research, vol. 22, no. 3. 2016.

[5] J. J. P. C. Rodrigues et al., "Enabling Technologies for the Internet of Health Things," IEEE Access, vol. 6, 2018,

[6] N. Tsafack et al., "A New Chaotic Map with Dynamic Analysis and Encryption Application in Internet of Health Things," IEEE Access, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3010794.

[7] M. Kumar et al., "Healthcare Internet of Things (H-IoT): Current Trends, Future Prospects, Applications, Challenges, and Security Issues," Electronics (Switzerland), vol. 12, no. 9. 2023.

[8] S. Bassem, S. Ismael, and J. Jalil, "Build and Implement Radiation Control using IoT in Parabolic Trough Solar Collector (PTSC)," Engineering and Technology Journal, vol. 40, no. 8, 2022, doi: 10.30684/etj.v40i8.2240.

[9] P. Fuhrer and D. Guinard, "Building a Smart Hospital using RFID technologies : Use Cases and Implementation Table of Contents," 1st European Conference on eHealth, 2006.

[10] D. Dasanayake et al., "Smart Hospital Ward Management System with mobile robot WARDBOT: An efficient management solution for a hospital ward."

[11] I. M. Al-Joboury and E. H. Hemiary, "Internet of Things Architecture Based Cloud for Healthcare," Iraqi Journal of Information & Communications Technology, vol. 1, no. 1, 2018,

[12] M. Elsaid, S. Altuwaijri, N. Aljammaz, and A. Ara, "Design and Analysis of Secure Smart Home for Elderly People," International Journal of Distributed and Parallel systemsSystems, vol. 10, no. 6, 2019.

[13] F. A. Almalki, "Implementation of 5G IoT Based Smart Buildings using VLAN Configuration via Cisco Packet Tracer," International Journal of Electronics Communication and Computer Engineering, vol. 11, no. 4, 2020.

[14] B. Ç. Uslu, E. Okay, and E. Dursun, "Analysis of factors affecting IoT-based smart hospital design," Journal of Cloud Computing, vol. 9, no. 1, 2020, doi: 10.1186/s13677-020-00215-5.

[15] S. Ravali and R. Lakshmi Priya, "Design and Implementation of Smart Hospital using IoT," in Proceedings - 5th International Conference on Computing Methodologies and Communication, ICCMC 2021, 2021.

[16] N. Alsbou, D. Price, and I. Ali, "IoT-Based Smart Hospital using Cisco Packet Tracer Analysis," in 2022 IEEE International IOT, Electronics and Mechatronics Conference, IEMTRONICS 2022, 2022.

[17] M. Harun-Ar-Rashid et al., "IoT-Based Medical Image Monitoring System Using HL7 in a Hospital Database," Healthcare (Switzerland), vol. 11, no. 1, 2023.

[18] R. J. Diaz, "An Overview of IP Addressing," 2022. https://www.researchgate.net/publication/361053333

[19] A. Jorgensen, Network Theory and Analysis. 2018. doi: 10.2307/j.ctt9qgrjc.8.

[20] D. Reynders and E. Wright, "Internet layer protocols," in Practical TCP/IP and Ethernet Networking for Industry, 2003.

[21] T. Rytilahti and T. Holz, "On Using Application-Layer Middlebox Protocols for Peeking Behind NAT Gateways," in 27th Annual Network and Distributed System Security Symposium, NDSS 2020, 2020. doi: 10.14722/ndss.2020.24389.

[22] A. J. Jara, L. Ladid, and A. Skarmeta, "The internet Internet of everything through IPv6: An analysis of challenges, solutions, and opportunities," J Wirel Mob Netw Ubiquitous Comput Dependable Appl, vol. 4, no. 3, 2013.

[23] S. R. S. P. Paul, "Proposed Methods of IP Spoofing Detection & Prevention," International Journal of Science and Research (IJSR), vol. 2, no. 8, 2013.

[24] Handbook of Intellectual Property Research. 2021. doi: 10.1093/oso/9780198826743.001.0001.