MediNet: An Optimized Networking Architecture for Secure and Efficient Healthcare Data Traffic Management

Satakshi Ghosh[1]
School of Electronics Engineering
Vellore Institute of Technology
Vellore, Tamil Nadu, India
satakshi.ghosh04@gmail.com

Tuhina Bhuniya [2]
School of Electronics Engineering
Vellore Institute of Technology
Vellore, Tamil Nadu, India
tuhinabhuniya2688@gmail.com

Deepika Rani Sona[*]
School of Electronics Engineering
Vellore Institute of Technology
Vellore, Tamil Nadu, India
deepika.rs@vit.ac.in

Abstract— **MediNet is a secure healthcare networking solution designed to transform traditional communication systems in hospitals and clinical settings that include security weaknesses, inefficient data management and increased operational demands. The literature proposes a robust hierarchical network architecture, modeled and simulated using Cisco Packet Tracer, representing a practical healthcare IT infrastructure. The network is divided into layers that ensure optimum data flow, secure interdepartmental communication, and modular scalability. The design leverages technologies such as Virtual LANs (VLANs) for traffic isolation, Access Control Lists (ACLs) for permission- based filtering, Network Address Translation (NAT) for secure internet access, Voice over IP (VoIP) for integrated communication, and Demilitarized Zones (DMZs) for securing publicly accessible resources. It also includes redundant routing paths and load balancing mechanisms to maintain high availability and reliability. Furthermore, AWS cloud simulation is incorporated to demonstrate remote data access and cloud- based backups.MediNet not only meets existing healthcare networking requirements but also gives future growth room for IoT-based patient monitoring, network automation using AI, and real-time threat detection systems. Therefore, resulting in a complete communications backbone for contemporary healthcare facilities.**

Keywords— Computer networking, communications, Cisco Packet Tracer, healthcare IT infrastructure, Internet of Things, Voice over IP

I . Introduction

The speedy evolution of technology has immensely impacted the healthcare industry, calling for new networking architectures to handle the burgeoning amount of healthcare data traffic. With healthcare providers relying more on computer systems to deliver patient care, fast and secure data transfer has become a priority. Conventional networking models in healthcare environments have historically been infested with security loopholes, lack of scalability, and ineffective data transmission, which made them more vulnerable to cyberattacks and operations downtime [1]. MediNet presents itself as a revolutionary solution that unites enhanced security measures, data segmentation for optimal processing, and VoIP transmission to counter these issues. Using technologies like firewalls, VLANs, and Access Control Lists (ACLs), MediNet successfully protects confidential medical information while providing low-latency, high-availability connectivity [2]. The enforcement of such security frameworks is critical with the expanding rate of cyberattacks on healthcare networks, which has caused notable disruptions in patient care and hospital functions [3]. Moreover, the shift away from legacy systems to a hierarchical network structure with modernization provides better scalability and interoperability [4]. The use of cloud-based resources, specifically Amazon Web Services (AWS), supports remote access and the system's ability to recover from data loss [5]. Thus, MediNet offers a complete networking architecture that not only resolves the inefficiencies of conventional healthcare networks but also prepares healthcare institutions to cope with the challenges of modern data management and security. This groundbreaking framework provides the foundation for future development in secure and effective healthcare communication, promoting collaboration among clinicians and improving patient care.

II. LITERATURE REVIEW

Over the last few years, healthcare infrastructure transformation has emerged as a high-priority task because of expanding requirements of real-time monitoring, scalability, and security. The conventional hospital network does not have the degree of flexibility and interoperability essential to facilitate contemporary healthcare services. The MediNet architecture is a new paradigm that is specifically designed to optimize healthcare data traffic with security and efficiency. This literature review aggregates current research on healthcare networking architectures, security of data, and efficiency in data transfer. Healthcare traffic data management has received much interest in the past few years, especially with the rising number of electronic health records (EHRs) and telemedicine adoption. It calls for scalable architectures that can handle this influx of data while addressing low latency and high throughput [6]. They introduce a modular approach that can scale with changing traffic levels, which is compliant with the principles behind the MediNet architecture.

The significance of security during transmission of healthcare data cannot be overemphasized. Infringements of healthcare data can lead to serious implications on patient privacy and institutional integrity [7]. A number of studies emphasize the weakness that comes with conventional networking models, especially when it comes to data integrity and authentication [8]. MediNet recommends a multilayered security model incorporating encryption and access control elements that have proven to increase data protection in healthcare environments [9]. Data transmission efficiency is also an important issue in cases where information access is time-sensitive for patient management. Dynamically adaptive routing capability of the architecture formulates that adaptive routing can have a remarkable positive impact on network performance in healthcare environments [10].

Interoperability is also a serious issue in healthcare data management because different systems tend to prevent smooth data exchange. An interoperable architecture is vital to support coordination between various healthcare providers [11]. The design of MediNet includes interoperability standards for seamless data sharing between different platforms, which aligns with the HL7 organization's recommendations [12]. Internet of Things (IoT) devices play an increasingly important role in healthcare, with wearables and remote monitoring systems producing a huge amount of data [12]. The MediNet design aims at interconnecting IoT data wirelessly to consolidate the solution for the heterogeneous problem presented by IoT devices. This consolidation follows the contention that network optimization in terms of IoT traffic is critical to improving the care of patients [13]. In addition, the financial ramifications of applying optimized networking solutions to healthcare are significant. A number of studies have also pointed towards cost reductions due to better data management and efficiency in data transmission [14]. Lastly, the regulatory framework around healthcare data transmission is changing, with more focus on adhering to standards like the Health Insurance Portability and Accountability Act (HIPAA) [15]. MediNet's design not only seeks to improve efficiency of operations but also decrease data breach and network downtime costs, thereby making a strong case for its implementation.

The objective of this paper is to introduce MediNet, a compliance-oriented network architecture engineered for secure, efficient, and interoperable healthcare data traffic management. It emphasizes the urgent necessity of such sophisticated solutions in healthcare. The System design and Methodology outlined in Section 3, with technical specifications in section 3.2 and working principles discussed in 3.4. The results and discussions are presented in Section 4, followed by conclusion and future scope in Section 5.

III. SYSTEM DESIGN AND METHODOLOGY

To achieve a top-tier, redundant, and scalable network infrastructure, a hierarchical design was implemented, with clear separation of network segments. This involved creating distinct networks for WLAN, LAN, Voice, and DMZ, each with its own IP address range. Robust security measures, such as firewalls, VLANs, and access control lists, were implemented to safeguard sensitive data. Redundant links and load balancing were employed to enhance reliability and scalability. Additionally, QoS mechanisms were configured to prioritize critical traffic. To enable internet access, NAT was used to translate private IP addresses to public IP addresses. This section further discusses the Open Shortest Path First (OSPF) configuration in algorithm 1 and the Spanning Tree Protocol (STP) Configuration in algorithm 2.

Considering the average throughput T in Eq. (1) for a given number of packets, the following equation is used:

$$T = \frac{N \times S}{D} \tag{1}$$

Here, T is the throughput in bits per second (bps), N is the number of packets sent, S is the size of each packet in bits and D being the total transmission delay in seconds.

Considering bandwidth efficiency η, the effective utilization of a link in Eq. (2) is calculated as:

$$\eta = \frac{T_{useful}}{T_{total}} \tag{2}$$

Where, T_{useful} refers to the useful throughput and T_{total} is the total throughput data.

For a DHCP address pool, the number of available dynamic IPs A is depicted in Eq. (3) as:

$$A = T - E \tag{3}$$

Where, T is the total IPs in subnet and E is excluded addresses for static devices.

The security filtering efficiency using ACL matching can be defined in Eq. (4) as:

$$M_{eff} = \frac{P_{matched}}{P_{total}} \tag{4}$$

Where, $P_{matched}$ is the number of packets matched by ACL and P_{total} is the number of packets examined.

Algorithm 1: Open Shortest Path First (OSPF) Configuration Algorithm

```
1: Let R denote a multi-interface router within an Autonomous System (AS).
    If the router is OSPF-capable, then initialize the OSPF process with:
        router ospf <process-id>
    Else, return error and exit.
2: Let I = {$i_1$, $i_2$, ..., $i_n$} be the set of active interfaces on R.
    For each interface $i_k$ in I:
        If $i_k$ belongs to a known subnet, then assign it to an appropriate OSPF area $A_j$ using:
            network <ip-address> <wildcard-mask> area <area-id>
        Else, exclude $i_k$ from OSPF participation.
3: Suppress unnecessary updates by default:
    passive-interface default
    For each interface $i_k$:
        If $i_k$ requires neighbor formation, then apply:
            no passive-interface <$i_k$>
        Else, keep it passive.
4: For every directly connected network $N_k$:
    If $N_k$ falls under the advertised subnet range, then include in OSPF using:
        network <$N_k$> area <$A_j$>
    Else, ignore.
5: If configuration is complete, then save it persistently using:
    do write memory
    Else, return to step 1.
6: Invoke Dijkstra's SPF algorithm:
    If LSDB (Link State Database) is populated, then compute the routing table (RIB).
    Else, reinitiate adjacency or wait for LSAs.
```

```
7: End — OSPF now ensures dynamic route computation and convergence.
```

Algorithm 2: Spanning Tree Protocol (STP) Configuration Algorithm

```
1: Let SW be a Layer 2 switch, and IA = {$int_1$, $int_2$, ..., $int_m$} denote access interfaces.
    For each $int_k$ in IA:
        If $int_k$ connects to an end device, then mark it as an access port.
        Else, exclude it from PortFast configuration.
2: For each valid access interface $int_k$:
    If $int_k$ is not a trunk port, then enable PortFast to accelerate convergence:
        spanning-tree portfast
    Else, skip.
3: For each interface where PortFast is enabled:
    If the interface must be protected from receiving unexpected BPDUs, then enable BPDU Guard:
        spanning-tree bpduguard enable
    Else, leave default protection in place.
4: If multiple interfaces require configuration, then use interface range mode:
        interface range <$int_k$ - $int_n$>
        spanning-tree portfast
        spanning-tree bpduguard enable
5: If configuration is valid and verified, then save it to NVRAM using:
    write memory
    Else, rollback or review for misconfigurations.
6: If loop prevention and path determination is functioning correctly via STP (802.1D or RSTP), then network is protected from broadcast storms.
    Else, review topology for redundant or misconfigured links.
7: End — STP dynamically maintains loop-free Layer 2 topology and fast edge access.
```

A. Software setup

Cisco Packet Tracer is a network simulation tool used to design, configure, troubleshoot, and visualize complex IT networks. Thereby providing a user-friendly interface to build and test network topologies, configure devices, and simulate network traffic. Therefore, the software enables to design and configure networks, creating detailed network diagrams, assigns IP addresses, and configures devices like routers, switches, and end devices. Also tests security measures by implementing security protocols like firewalls, ACLs, and VPNs to assess their effectiveness in protecting the network.

B. Technical Specifications

This section deals with the Network Components in Table I, Network Architecture of Proposed Model in section C, Working Principle in section D, Data Flow & Routing Mechanism Internet & External Access outlined in sub-section 1, Security & Access Control in sub-section 2, and Workflow in the network discussed in sub-section 3.

TABLE I. VARIOUS COMPONENTS USED TO CONSTRUCT MEDINET

Device Type	**Model / Series**	**Purpose**
Router	Cisco 2811	Connects to ISP and routes between network segments
Router (ISR Series)	ISR 4331	Handles WAN and inter-VLAN routing
Multilayer Switch	Catalyst 3650-24PS	Layer 3 switching at the core layer
Access-Layer Switch	Catalyst 2960	Layer 2 switching with port security
IP Phone	7960	Provides VoIP communication between departments
End-User Devices	Various	Used by staff and visitors for daily tasks and data access
Perimeter Firewall	ASA 5506-X	Protects against external threats
Wireless Access Point (via WLC)	WLC 2504	Delivers Wi-Fi managed centrally by the WLC

Table I lists the network components used in the construction of the MediNet architecture. It includes routers, switches, firewalls, IP phones, wireless access points, and end-user devices, each selected to support secure, efficient, and scalable data traffic management across various layers of the network.

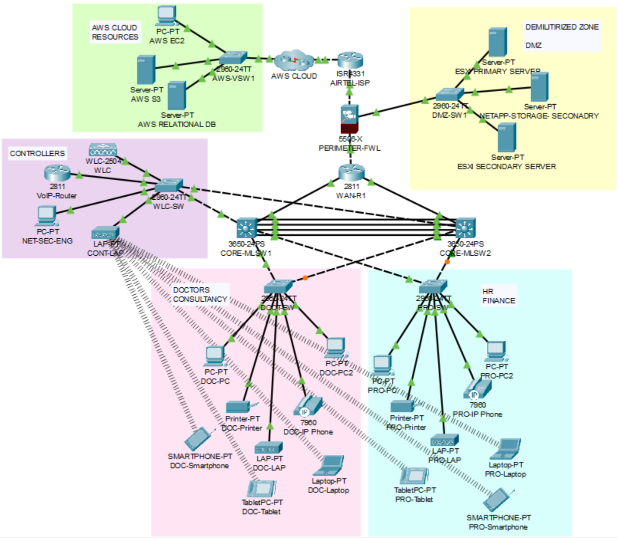


Fig 1: System Design of MediNet.

C. Network Architecture of Proposed Model

A hierarchical model of MediNet is designed consisting of Core Routers for backbone traffic routing, Distribution Layer Switches for departmental segregation, Access Layer Switches for end-user connectivity, DMZ zone for secure to external facing servers, AWS Cloud for remote data access by hospital staff, Client devices and IP Phones for VoIP-based communication between departments.

Fig. 1. Depicts the network architecture of the proposed model depicting 2 departments and 16 end-user devices. However, the same circuit can be expanded to include multiple departments and up to 100 nodes.

D. *Working Principle*

The working principle of the MediNet network is based on a structured and secure hierarchical network model that integrates cloud services, local enterprise infrastructure, and user devices.

1) Data Flow & Routing Mechanism Internet & External Access

Network traffic from sources outside the organisation passes through the Perimeter Firewall (PERIMETER FWL), which applies security policies, thus filtering the traffic and controlling who gains VPN access to the network resources. The WAN Router (2811 WANR1) routes all network traffic between external networks such as the Internet and AWS cloud and private shared resources within the organisation. Data transfer within the organisation will occur through the Core Routers namely Active(main router), Standby(back-up router), and Virtual(logical router) for high-speed packet switching between departments. The devices are logically separated into different broadcast domains so that devices in different department cannot communicate directly, but only through the Layer 3 switch. The AWS Cloud hosts virtual machines and relational databases, acting as a large-scale data centre and providing a resource for. The Demilitarized Zone separates internal organisational resources from cloud services, databases and public servers.

2) Security & Access Control

Critical resources which are accessible to the public, such as ESXi Servers and NetApp Storage are isolated from the rest of the network to prevent unauthorized access and create a demilitarized zone. Each department, namely Doctors, IT, Finance, etc. is assigned its own specific VLAN with limited access to important resources. Firewall configurations and access control lists are added to the perimeter firewall server to make sure that anyone other than the hospital staff cannot access sensitive patient data, internal hospital resources, or unauthorized network segments, thereby preventing external threats and ensuring data confidentiality and integrity[6].

3) Workflow in the network

The Fig. 2. depicts the network access control workflow for external users. Incoming traffic first passes through a perimeter firewall with ACL and NAT rules. If the packet matches the ACL, it is forwarded to the WAN router; otherwise, it is dropped. SSH access requests are verified based on source IP (192.168.1.0). Valid requests are allowed; others are denied. Devices are then checked for correct VLAN tagging, and traffic is either routed to VLAN 100, 50, or 99, or dropped/isolated if improperly tagged.

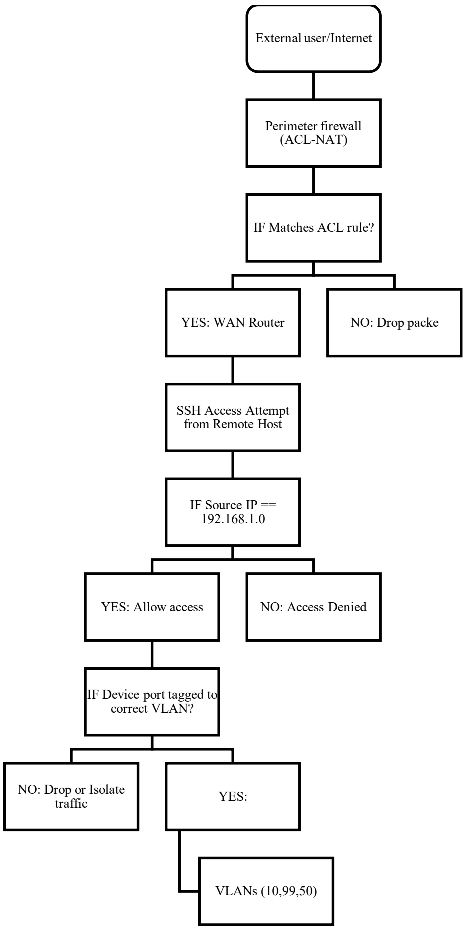

External user/Internet
Perimeter firewall (ACL-NAT)
IF Matches ACL rule?
YES: WAN Router
NO: Drop packe
SSH Access Attempt from Remote Host
IF Source IP == 192.168.1.0
YES: Allow access
NO: Access Denied
IF Device port tagged to correct VLAN?
NO: Drop or Isolate traffic
YES:
VLANs (10,99,50)

Fig 2: Overall workflow in the proposed network.

IV. RESULTS AND DISCUSSION

The components of specific models were placed in a new Cisco packet tracer file, and borders were drawn to indicate separate departments and segments of the network. The zones were segregated according to colour to easily distinguish one from the other. Connections were made using Gigabit ethernet and Fast ethernet cables across all devices except wireless devices.

A. *Basic Configuration for All Network Devices*

TABLE II. CONSOLE LOGS FOR SECURE SHELL(SSH) ACCESS

Console Logs	**Purpose**
en *conf t* *hostname CORE-SW1* *banner motd &UNAUTHORISED ACCESS& enable password cisco* *line console 0 password cisco login* *exit* *no ip domain-lookup* *service password-encryption ip domain-name medinet.com username cisco password cisco* *crypto key generate rsa general-keys modulus 1024 ip ssh version 2* *do wr*	First, in order to grant secure access to authorised personnel and staff, an encrypted remote access was set up using SSH. A hostname, domain name, username and password were provided for accessing the network. Following that, certain basic general settings were applied, which are common to all devices in the network.

Table II lists the Console logs for configuring the hostname, domain name, username and password for secure

SSH access. This configuration sets the hostname, displays a login banner, secures access with a password, disables unnecessary DNS lookups, enables password encryption, and generates cryptographic keys for SSH access. The changes were saved using do wr to ensure they remain the same in the future.

The VLAN Configuration for Wired, Wireless and Voice were configured. VLAN 10 was assigned to wired clients, VLAN 50 to wireless access points, and VLAN 99 to voice traffic (IP phones). Using this setup, the network automatically sorts the traffic types by priority.For Port configuration, the Console logs for configuring the switch ports as trunk or access ports. Ports fa0/1-3 were set as trunks for VLAN traffic between switches. Ports fa0/3-20 were configured as access ports for wired PCs (VLAN 10) and IP phones (voice VLAN 99). Ports fa0/21-24 were assigned for wireless access points (VLAN 50).

B. *Access Control Rules (ACLs) for Specific Traffic*

TABLE III. CONSOLE LOGS FOR CONFIGURING ACLS TO FIREWALL SERVER AND AIRTEL ROUTER

Console Logs	**Purpose**
tcp any any eq 80 *udp any any eq 57* *udp any any eq 58* *udp any any eq 53* *tcp any any eq 53*	In order to control traffic and allow only necessary services like HTTP, DNS, and NTP, specific access control lists were created. These specify what type of data traffic can be routed between specific source and destination IPs, and the destination port number.

Table III depicts the Console logs for configuring access control lists to the firewall server and Airtel router. These rules allow essential services such as browsing online websites and resources, synchronizing the time across all the network devices, and resolving domain names. In a hospital these services are very important as they allow doctors and nurses to access online information, put accurate time stamps on medical reports and block traffic from unauthorised sources, thus preventing malware or ransomware attacks. The console logs assigns static IP addresses to the servers in the Demilitarized Zone do not change over time and provide constant stable access.

C. *Firewall Configuration with Security Zones*

TABLE IV. CONSOLE LOGS FOR CONFIGURING FIREWALL SECURITY

Console Logs	**Purpose**
interface gig0/0 nameif Outside security-level 0 ip address 203.0.113.1 255.255.255.0 interface gig0/1 nameif Inside security-level 100 ip address 192.168.1.1 255.255.255.0 interface gig0/2 nameif DMZ security-level 50 ip address 192.168.100.1 255.255.255.0	Cisco ASA (adaptive security appliance) is a firewall platform which allows us to protect corporate networks and data centres. This is important for the hospital network, as the ASA helps to assign different security levels to interfaces, thus separating the trusted areas such as the internal network from untrusted areas such as the Internet. A lower security level indicates less trust which's security levels to differentiate between trusted and untrusted zones.

Table IV outlines the Console logs for configuring firewall security rules at different levels using Cisco ASA. The firewall distinguishes between internal, external, and DMZ traffic based on trust levels, controlling access accordingly. Firewall inspection policy allows it to intelligently inspect the traffic and allow traffic only from trusted sources, while blocking malicious attacks. The console logs for configuring a standard access control permits the traffic from only one IP address while denying the rest. This improves the security of the network greatly, by tightly restricting SSH access and thus protecting all the sensitive patient information.

4.6 Wireless Configuration & IP Phones (Telephony Service)

TABLE V. CONSOLE LOGS FOR CONFIGURING DEDICATED VLANS

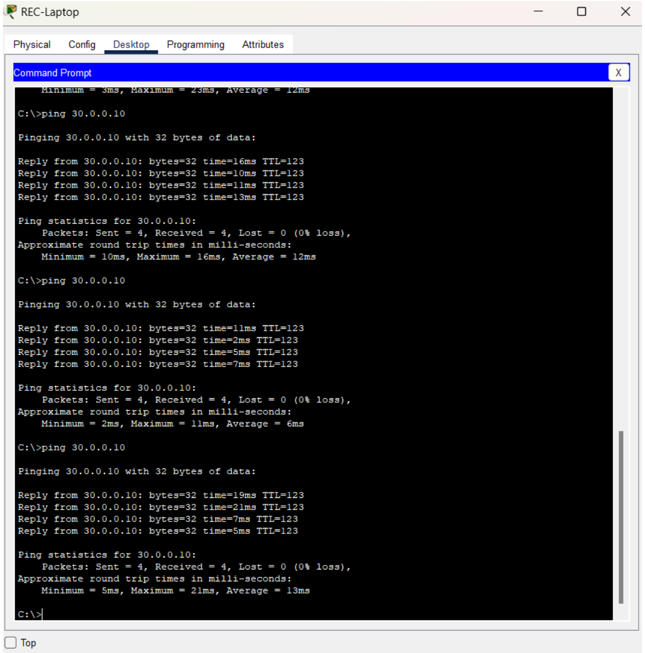
Console Logs	**Purpose**
telephony-service max-dn 10 max-ephones 20 ip source-address 192.168.50.1 port 2000 auto assign 1 to 20	Dedicated VLANs were configured, which support wireless devices, IP phones, and other wireless traffic. The telephony-service command was used to make the VoIP connection quick and automatic whenever a call is made, and a maximum of 20 IP phones is allowed on the network. Directory(phone) numbers were automatically assigned to each one using the auto assign command.

Table V lists the Console logs for configuring dedicated VLANs for telephony service between IP phones placed in different departments. This ensures fast and secure deployment of phones across all departments, and very little manual configuration is required.

D. *Verification & Testing*

Once the configurations were completed, extensive testing was carried out. These included ping tests between devices, between the controllers and end devices, and to the AWS services which confirmed IP connectivity, VoIP calls between departments verified voice traffic routing, and DHCP and DNS testing ensured successful IP assignment and name resolution. These tests proved that the network met all the initially set goals and requirements.

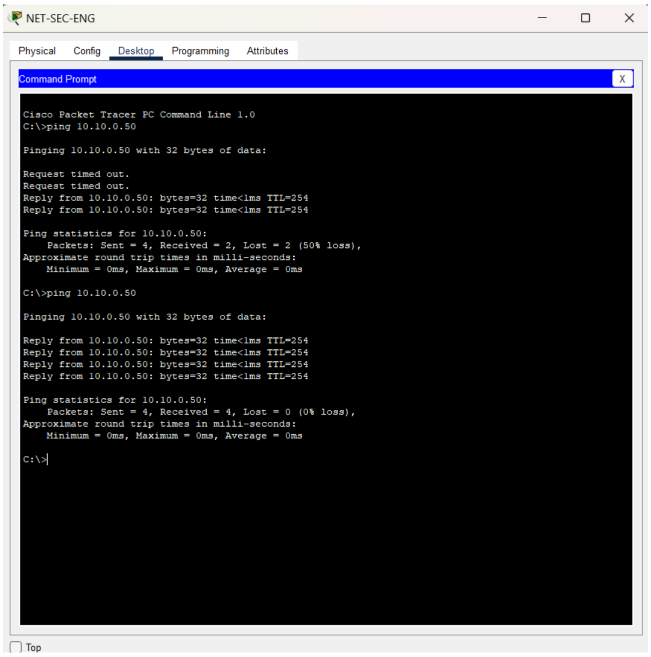
Fig. 3. depicts the Ping tests that were conducted continuously and the delay was noted in each case. Throughput was also calculated. In the above diagram, a laptop in reception area is pinging an AWS EC2 resource.



```
    Minimum = 3ms, Maximum = 23ms, Average = 12ms

C:\>ping 30.0.0.10

Pinging 30.0.0.10 with 32 bytes of data:

Reply from 30.0.0.10: bytes=32 time=16ms TTL=123
Reply from 30.0.0.10: bytes=32 time=10ms TTL=123
Reply from 30.0.0.10: bytes=32 time=11ms TTL=123
Reply from 30.0.0.10: bytes=32 time=13ms TTL=123

Ping statistics for 30.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 16ms, Average = 12ms

C:\>ping 30.0.0.10

Pinging 30.0.0.10 with 32 bytes of data:

Reply from 30.0.0.10: bytes=32 time=11ms TTL=123
Reply from 30.0.0.10: bytes=32 time=2ms TTL=123
Reply from 30.0.0.10: bytes=32 time=5ms TTL=123
Reply from 30.0.0.10: bytes=32 time=7ms TTL=123

Ping statistics for 30.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 11ms, Average = 6ms

C:\>ping 30.0.0.10

Pinging 30.0.0.10 with 32 bytes of data:

Reply from 30.0.0.10: bytes=32 time=19ms TTL=123
Reply from 30.0.0.10: bytes=32 time=21ms TTL=123
Reply from 30.0.0.10: bytes=32 time=7ms TTL=123
Reply from 30.0.0.10: bytes=32 time=5ms TTL=123

Ping statistics for 30.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 21ms, Average = 13ms

C:\>
```

Fig. 3: Ping tests between admin PC and reception

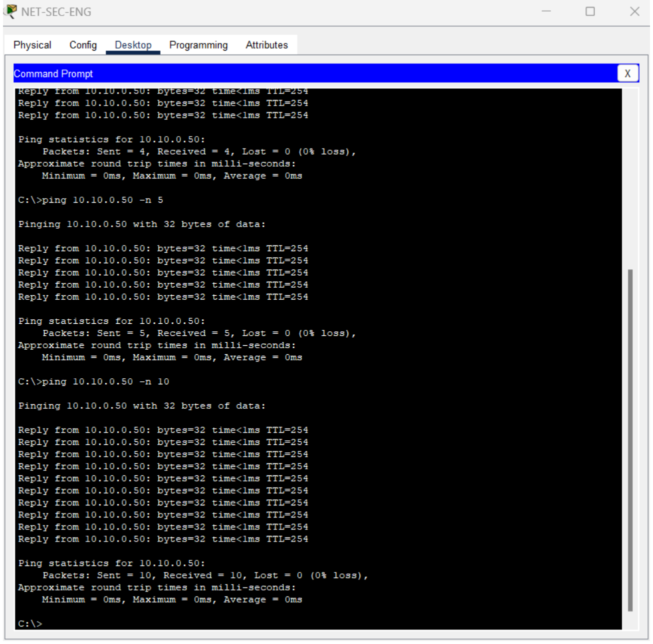
Whereas Fig. 4 outlines the Wireless LAN controller is pinged from the network security engineer's PC to ensure stable and secure connection between the two, before signing into the WLC.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.0.50

Pinging 10.10.0.50 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254

Ping statistics for 10.10.0.50:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.10.0.50

Pinging 10.10.0.50 with 32 bytes of data:

Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254

Ping statistics for 10.10.0.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fig. 4: Ping tests between admin PC and WLC

Fig. 5. depicts the Ping tests which were conducted, increasing the number of packets sent from 5 to 25, in intervals of 5.



```
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254

Ping statistics for 10.10.0.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.10.0.50 -n 5

Pinging 10.10.0.50 with 32 bytes of data:

Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254

Ping statistics for 10.10.0.50:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.10.0.50 -n 10

Pinging 10.10.0.50 with 32 bytes of data:

Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254
Reply from 10.10.0.50: bytes=32 time<1ms TTL=254

Ping statistics for 10.10.0.50:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fig. 5: Increasing number of packets

Fig. 6. illustrates a successful voice call established between the Reception and IT Support IP phones, indicating proper VoIP configuration.

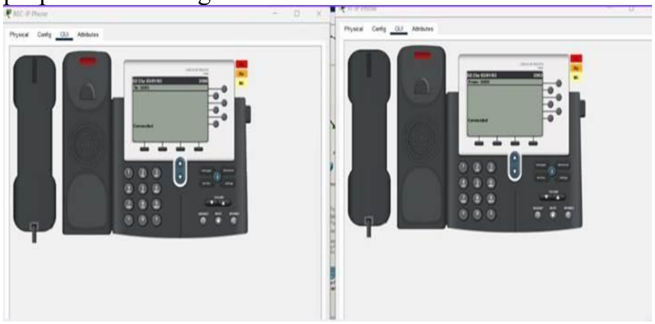


Fig. 6: Successful network and VoIP operations

Fig. 7. outlines the Throughput graph. As a result of the ping tests that were conducted, wherein the packets sent was specified starting from 5 to 25 with intervals of 5.

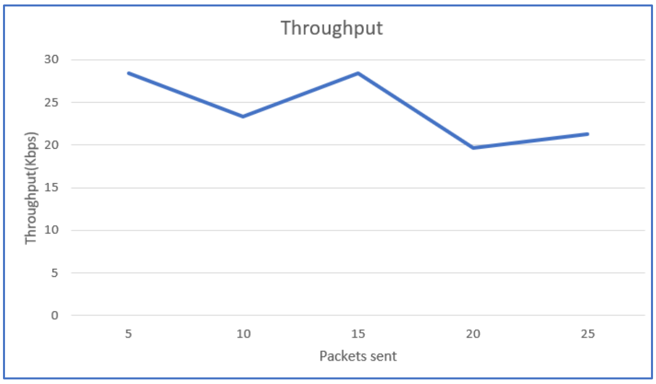


Fig. 7: Throughput graph

Fig. 8 depicts the Delay graph as a result of the ping tests that were conducted, wherein the packets sent was specified starting from 5 to 25 with intervals of 5.

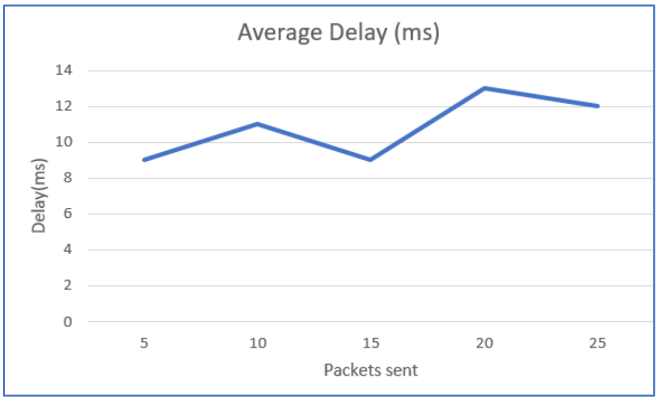
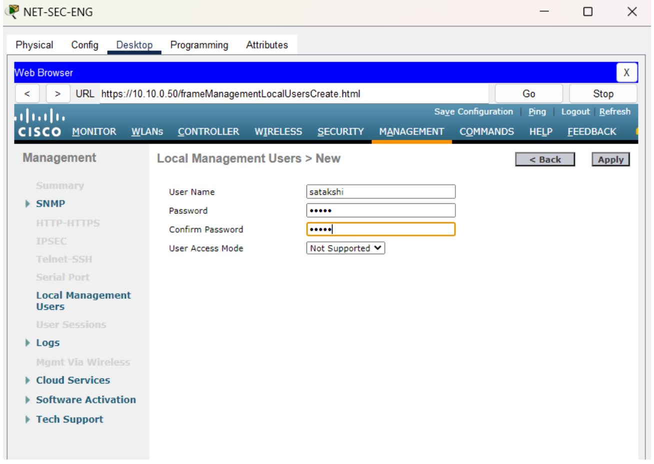


Fig. 8: Delay graph

Fig. 9. shows the management interface of the WLC where a new username and password are set to access the WLC.



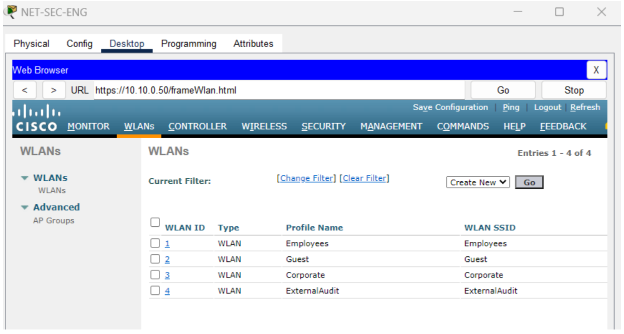
URL https://10.10.0.50/frameManagementLocalUsersCreate.html

Local Management Users > New

User Name: satakshi
Password: •••••
Confirm Password: •••••
User Access Mode: Not Supported

Fig. 9: Creating new user in WLC

In Fig. 10, few Wireless LANs have been created in the past while testing the network, which can be viewed in the above image. In order to configure another WLAN, Create New is pressed.



URL https://10.10.0.50/frameWlan.html

WLANs

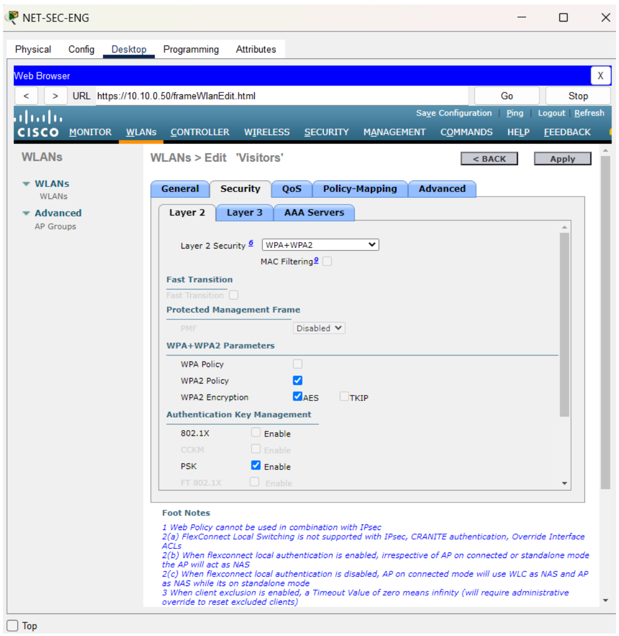
Entries 1 - 4 of 4

Current Filter:

WLAN ID	Type	Profile Name	WLAN SSID
1	WLAN	Employees	Employees
2	WLAN	Guest	Guest
3	WLAN	Corporate	Corporate
4	WLAN	ExternalAudit	ExternalAudit

Fig. 10: Existing Wireless LANs

Fig. 11. depicts creating a new WLAN named as Visitors. The Security is configured as WPA+WPA2. PSK is enabled and password is set as visitors123. Any device is any department of the hospital can now access this WLAN provided the password is known.



URL https://10.10.0.50/frameWlanEdit.html

WLANs > Edit 'Visitors'

Layer 2 Security[6] WPA+WPA2
MAC Filtering[9] □

Fast Transition
Fast Transition □

Protected Management Frame
PMF Disabled

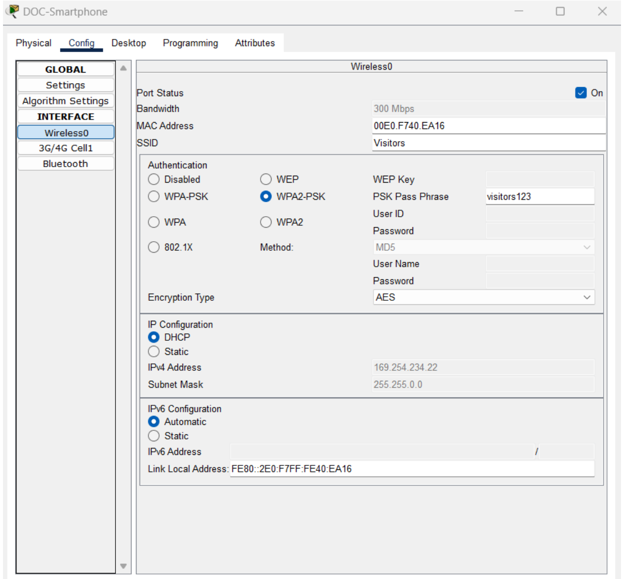
WPA+WPA2 Parameters
WPA Policy □
WPA2 Policy ☑
WPA2 Encryption ☑AES □TKIP

Authentication Key Management
802.1X □ Enable
CCKM □ Enable
PSK ☑ Enable
FT 802.1X □ Enable

Foot Notes
1 Web Policy cannot be used in combination with IPsec
2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)

Fig. 11: Creating new WLAN

Fig. 12. shows connection of a smartphone in the Doctor's department to wireless network 'Visitors' by providing authentication and pass phrase.



Wireless0

Port Status ☑ On
Bandwidth 300 Mbps
MAC Address 00E0.F740.EA16
SSID Visitors

Authentication
○ Disabled ○ WEP WEP Key
○ WPA-PSK ● WPA2-PSK PSK Pass Phrase visitors123
User ID
○ WPA ○ WPA2 Password
○ 802.1X Method: MD5
User Name
Password
Encryption Type AES

IP Configuration
● DHCP
○ Static
IPv4 Address 169.254.234.22
Subnet Mask 255.255.0.0

IPv6 Configuration
● Automatic
○ Static
IPv6 Address /
Link Local Address: FE80::2E0:F7FF:FE40:EA16

Fig. 12: Connecting a device to the new wireless network

E. *Performance Analysis*

The main function of the hospital network which needed to be tested was the fast and secure transfer of data between various departments and also layers. The sensitive patient data is protected using encryption. Entering the incorrect username or password prompts the console to display an error message. From the ping tests conducted between devices, it is observed that the internal routing protocols are effective, as the data transfer occurs with a minimal delay in the range of, indicating low latency. This can also be attributed to the wired LANs, wireless devices and voice calls having their own separate network space. The segregation of the devices using VLAN proves to be useful as well, as network congestion is prevented as is seen by successful pinging of end devices from the network security engineer's PC. Due to the presence of demilitarized zone and firewall ACL rules, the network remained free from outside attacks. The voice communication between the Reception and IT departments is also tested using the IP phones. VoIP communication was given the most priority, and placed in its own dedicated VLAN using Quality of Service settings, meaning voice calls always had bandwidth available to them. As a result, calls were instant, with no delays or audio issues. This is very important in an environment such as a hospital where urgent care must be provided to patients in life or death situations.

F. Challenges Faced and Solutions Implemented

Network implementation posed some of the following challenges: facilitating wireless communication between departments and controller devices, and integrating with AWS resources seamlessly. Setting up NAT rules to accommodate internet access while maintaining internal security was a tricky process, as was accommodating ACLs that threatened to block necessary internal traffic. These problems were addressed by logically segregating departmental modules to ease testing and troubleshooting. Cisco Packet Tracer simulation tools were employed to pre-test ACLs and observe traffic behaviour via a simulated Cisco ASA firewall configured with logging. While restrictive to simulation, this environment provides a robust proof of concept for large-scale, real-world deployment across heterogeneous environments.

V. CONCLUSION

The proposed MediNet architecture demonstrated a secure, efficient, and scalable healthcare network using hierarchical topology, network segmentation, and Cisco Packet Tracer simulations. Key limitations of traditional healthcare IT systems including poor security, inefficiency, and limited data storage were addressed through logical isolation of departments, firewall-based access control, OSPF and STP protocols, and cloud integration via AWS for remote access and cost-effective storage. In the future, the network can be further enhanced by integrating AI for automated monitoring and configuration, reducing manual errors and staffing costs. The SDN can simplify device management and optimize traffic dynamically. Real-time alerts for unusual activity and cyberattacks can be enabled via advanced security programs. Additionally, incorporating IoT devices and expanding cloud capabilities will provide real-time patient monitoring, increase data availability, and ensure greater flexibility and resilience in healthcare operations.

REFERENCES

[1] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," Technology and Health Care, vol. 25, no. 1, pp. 1–10, Feb. 2017.

[2] M. V. Kumar, S. S. Poovannan, V. Soundharya, K. Sureka, and M. Thirisankari, "Secure Healthcare Network Using VLAN, OSPF, IPsec VPN and ACL," 2025 Eleventh International Conference on Bio Signals, Images, and Instrumentation (ICBSII), pp. 1–6, Mar. 2025.

[3] Aditya Rai, "&lt;b&gt;Case Studies on disproportionate Impact of Cyberattacks in the Healthcare Sector&lt;/b&gt;," Journal of High School Research, vol. 1, no. 1, Dec. 2024.

[4] V. G. Yogeshappa, "Designing Cloud-Native Data Platforms for Scalable Healthcare Analytics," International Journal of Research Publication and Reviews, vol. 6, no. 3, pp. 3784–3791, Mar. 2025.

[5] G. Ganachari, "Impact of FHIR Data Format in Healthcare Interoperability," International Journal of Science and Research (IJSR), vol. 10, no. 12, pp. 1528–1531, Dec. 2021.

[6] P. Neelakrishnan, "Enhancing Healthcare Security Through Autonomous Data Protection for IoT Systems in Hospital Environments," International Journal of Computer Trends and Technology, vol. 72, no. 5, pp. 40–50, May 2024.

[7] A. H. Seh et al., "Healthcare Data Breaches: Insights and Implications," Healthcare, vol. 8, no. 2, p. 133, May 2020.

[8] A. Estepa, R. Estepa, G. Madinabeitia and J. Vozmediano, "Designing Cost-Effective Reliable Networks From a Risk Analysis Perspective: A Case Study for a Hospital Campus," in IEEE Access, vol. 7, pp. 120411-120423, 2019.

[9] T. W. York and D. MacAlister, "Healthcare Security Risks and Vulnerabilities," Hospital and Healthcare Security, pp. 49–77, 2015.

[10] "HEALTHCARE IS INTEROPERABILITY - Challenges and Solutions," Proceedings of the International Conference on Health Informatics, pp. 559–562, 2011.

[11] S. Chattopadhyay, "Iot In Healthcare: Challenges and Opportunities for Improved Patient Outcomes," INFORMATION TECHNOLOGY IN INDUSTRY, vol. 7, no. 3, pp. 60–67, Dec. 2019.

[12] F. Sallabi, F. Naeem, M. Awad, and K. Shuaib, "Managing IoT-Based Smart Healthcare Systems Traffic with Software Defined Networks," 2018 International Symposium on Networks, Computers and Communications (ISNCC), pp. 1–6, Jun. 2018.

[13] Sona, D.R. and Bagadi, K., Design of an Optimized Social Arithmetic Mean Based Relay Selection Scheme for D2D Cooperative Communication, pp.2278-3075, Volume-8 Issue-7 May, 2019.

[14] J. M. Hellerstein, "Addressing human bottlenecks in big data," 2014 IEEE International Conference on Big Data (Big Data), pp. 4–4, Oct. 2014.

[15] N. Raju and P. Kondle, "Enhancing Healthcare IT Cybersecurity Resilience: Integrating CMMC Controls with HIPAA Compliance," SSRN Electronic Journal, 2024.