TECHNOLOGIES PROJECT

Integrated Network Infrastructure for New Leaf Hospital

Submitted To:

Prof. Abid Bashir

Submitted By:

Manreet Kaur – 301300560

Arjun Singh – 301304682

Yashkumar Patel – 301305830

Kishankumar Patel – 301306242

April 2024

DECLARATION

We hereby declare that the project report titled "**Integrated Network Infrastructure for New Leaf Hospital"** submitted for the **Final Technologist project** is our original work and the project report is submitted in the fulfillment of the requirements for the completion of the course **"Technologist Project**". The results embodied in this report have not been submitted to any other Course or Institute for the award of any degree or diploma.

Manreet Kaur

Arjun Singh

Yash Kumar Patel

Kishan Kumar Patel

ABSTRACT

This abstract outline a pioneering networking endeavor for New Leaf Hospital, a newly established healthcare group with ambitions to revolutionize the Canadian healthcare landscape. TrustUs Solutions Inc., a leading IT consulting firm, is tasked with designing and implementing the hospital's inaugural network infrastructure across its five geographically dispersed sites.

The project holds paramount importance as it lays the foundation for seamless communication, robust data security, and efficient operations within the nascent hospital group. With a focus on scalability, redundancy, and compliance with healthcare data regulations, the network aims to support the hospital's growth aspirations while ensuring uninterrupted delivery of medical services.

Through a systematic approach encompassing assessment, design, implementation, and ongoing support, the project endeavors to address the unique challenges faced by a new hospital establishment. By leveraging cutting-edge technology and industry best practices, TrustUs Solutions Inc. aims to deliver a network infrastructure that not only meets the immediate needs of New Leaf Hospital but also provides a solid framework for future innovation and expansion.

In summary, this abstract underscore the pioneering nature of the networking project for New Leaf Hospital, highlighting its significance in establishing a secure, scalable, and efficient network infrastructure essential for the hospital's journey towards becoming a beacon of excellence in Canadian healthcare.

Table of Content

List of Table

List of Figures

1.Introduction

1.1 Background

The establishment of a robust network infrastructure is paramount for New Leaf Hospital, a newly introduced healthcare group poised to redefine healthcare standards across Canada. In the contemporary healthcare landscape, seamless connectivity, secure data transmission, and efficient operational processes are imperative for delivering high-quality patient care. However, as a new entrant in the industry, New Leaf Hospital faces the challenge of creating a network from scratch that not only meets current needs but also anticipates future growth and technological advancements.

1.2 Objective

The primary objective of this networking project is to design and implement a comprehensive network infrastructure that seamlessly integrates all five hospital sites, facilitates communication and collaboration among staff, ensures the confidentiality and integrity of patient data, and enhances operational efficiency. By addressing these objectives, TrustUs Solutions Inc., the chosen IT firm specializing in networking solutions, aims to provide New Leaf Hospital with a solid foundation to establish itself as a leader in healthcare quality and innovation.

Pertinent background information underscores the critical importance of this project. In today's digital age, healthcare organizations are increasingly reliant on technology to streamline processes, enhance patient care, and comply with regulatory requirements. Furthermore, the proliferation of electronic health records (EHRs) and the interconnected nature of modern

healthcare systems necessitate robust network infrastructures to support data exchange and collaboration among healthcare providers.

1.3 Executive Summary:

The networking project for New Leaf Hospital represents a pioneering endeavor aimed at establishing a secure, scalable, and efficient network infrastructure to support its operations. This project encompasses a comprehensive approach that integrates expertise from various domains, including PC Hardware, Operating Systems, Networking Fundamentals, Data Communications, Routing and Switching, and Network Security.

Drawing upon industry best practices and cutting-edge technology, TrustUs Solutions Inc. will design and implement a network infrastructure tailored to the specific needs of New Leaf Hospital. This includes assessing existing infrastructure, designing a scalable architecture, selecting appropriate network equipment, implementing robust security measures, and providing ongoing maintenance and support.

The success of this project is crucial for New Leaf Hospital's mission to provide top-notch medical care and establish itself as a national leader in healthcare quality. By investing in a robust network infrastructure, New Leaf Hospital aims to enhance communication, collaboration, and operational efficiency, ultimately improving patient outcomes and satisfaction.

About Us

TrustUs Solutions

TrustUs Solutions is a leading provider of comprehensive IT services and solutions, dedicated to delivering outstanding value and fostering business success for our clients. With a team of highly skilled and seasoned professionals, we utilize state-of-the-art technologies and industry best practices to craft customized solutions tailored to meet the unique needs of each organization we serve.

Our Key Expertise:

1. Network Management and Infrastructure Design: We excel in designing, implementing, and managing scalable network infrastructures for seamless connectivity, maximum availability, and optimal performance.

2. Cybersecurity and Risk Management: We offer comprehensive cybersecurity services, including risk assessments, vulnerability management, threat intelligence, and incident response, to protect your critical assets and data.

3. Cloud Services and Digital Transformation: We assist in leveraging cloud computing for digital transformation, providing end-to-end cloud solutions from strategy and migration to management and optimization.

4. IT Consulting and Project Management: Our IT consulting services offer strategic guidance and expert advice to navigate the technology landscape, ensuring operational efficiency and competitive advantage.

5. Managed Services and Support: We provide full-service management and support to maintain peak efficiency of your IT infrastructure, with active monitoring, issue resolution, and ongoing support.

At TrustUs Solutions, we pride ourselves on our dedication to excellence, integrity, and client satisfaction. Our collaborative approach, coupled with our technical prowess and industry acumen, enables us to forge enduring partnerships with our clients. Trust us to be your dependable IT partner, delivering innovative solutions that drive business growth and success.

Reach out to us today to discover how TrustUs Solutions can empower your organization with cutting-edge IT solutions and services.

2. Planning Stage

2.1 Proposal

From: New Leaf Hospital IT Team

Team Members: Yashkumar Patel, Kishankumar Patel, Arjun Singh, Manreet Kaur

Date of Submission: April 2024

Discipline: Computer Systems Technology – Networking

Title: Implementing Core Network Infrastructure for New Leaf Hospital's Multi-Campus (Five Campus) Environment

2.2 Introduction:

New Leaf Hospital, a burgeoning healthcare provider, seeks to establish a robust and integrated network infrastructure to connect its multiple sites efficiently. TrustUs Solutions Inc., a leading IT consultancy specializing in networking solutions, proposes to design and implement a comprehensive network solution tailored to meet the hospital's unique requirements. This proposal outlines our approach, methodology, and deliverables to address New Leaf Hospital's networking needs effectively.

2.3 Background:

New Leaf Hospital, a newly established healthcare group, envisions providing top-notch medical care across multiple locations. However, to achieve seamless collaboration and data exchange, a unified network infrastructure is imperative. TrustUs Solutions Inc. brings experience

and expertise in designing and deploying network solutions tailored to the healthcare sector's stringent requirements.

2.4 Project Objectives:

i. **Core Network Services:**
   a. Deploy Active Directory domain controllers at the main campus for centralized user/device authentication and management.
   b. Implement central DHCP and DNS services at the main campus for IP management and name resolution across all campuses.

ii. **Network Security:**
   a. Implement perimeter firewalls at each campus location for traffic filtering and security.
   b. Secure the network through proper access controls, firewalling, and threat prevention measures.

iii. **LAN/WAN Infrastructure:**
   a. Set up layer-2 LAN switching at each site to provide local area connectivity.
   b. Configure inter-site routing and WAN links to enable communication between campuses.
   c. Utilize VLANs to logically segment different service traffic like facilities, VoIP, patient/staff devices.

iv. **Wireless Connectivity:**
   a. Deploy wireless access points to provide comprehensive WiFi coverage across all campuses.

b. Ensure seamless roaming capabilities for mobile clients between buildings/campuses.

v. **Unified Communications:**

a. Implement a VoIP phone system with centralized PBX/call control.

b. Enable inter-campus voice/video communications over the data network.

vi. **Server Systems:**

a. Deploy web servers for hosting hospital websites and applications.

vii. **Network Management:**

a. Implement network monitoring tools to track performance and availability.

b. Integrate antivirus/anti-malware protection to secure endpoints and servers.

2.5 Project Requirements

- Set up various hardware and software at each site.
- Implement Active Directory domain controllers at the main campus for centralized authentication and management of users and devices.
- Implement DHCP and DNS services for IP address management and name resolution. The core servers will be at the main campus.
- Deploy firewalls at each location for perimeter security and traffic filtering.
- Set up layer-2 switches to provide LAN connectivity within each campus location.
- Set up routers to provide VLAN routing inter-site connectivity and internet access.
- Provide wireless access points for Wi-Fi connectivity across the campuses.
- Set up a Web server for web hosting.
- Implement VoIP phones and PBX for the phone/voicemail system.

- Use VLANs to segment services such as facilities systems, VoIP phones, and patient/staff computers and devices.
- Provide basic network monitoring and antivirus protection.

2.6 Project Scope:

The scope of this project encompasses the comprehensive design, deployment, testing, and commissioning of the complete unified network infrastructure required to seamlessly interconnect and operationally support New Leaf Hospital across its multi-campus locations. In-scope components include the core and distribution network layers for LAN/WAN connectivity, data center server/storage infrastructure, high-performance wireless LAN, Internet links with perimeter security, VPN remote access solution, robust security controls like firewalls/IPS/IDS/NAC, unified communications platform (VoIP/video/collaboration), centralized network management/monitoring systems, core services like directory/DHCP/DNS, documented IT policies/procedures/runbooks, and knowledge transfer to the hospital's IT staff. Out-of-scope are end-user devices, digital signage, physical cabling, environmental monitoring, surveillance systems, application development, and disaster recovery planning. Key assumptions are suitable facilities, adequate supporting infrastructure like power/cooling, a frozen design by April 2024, no major construction, and vendor solution compatibility throughout the project's duration. The overall scope focuses on delivering a secure, high-performance, fully redundant multi-gigabit network fabric with seamlessly integrated voice/data/wireless to enable hospital-wide connectivity across the campuses.

2.1.1 Project Deliverables

Team has agreed with the management and sponsors to have the following deliverables which include the project, management-based deliverables. In case of any changes or updates clients need to fill the change request form and update request form accordingly.

Project based deliverables –

- Design documentation outlining the architecture and layout of the network.
- Configuration files for routers, switches, firewalls, and other network devices.
- Physical installation of network hardware components, such as routers, switches, cables, and access points.
- Software configurations.
- Implementation of security measures such as firewalls, intrusion detection systems, and virtual private networks (VPNs).
- Security policies and procedures for user authentication, access control, and data encryption.
- Testing and verification of service monitoring tools and systems for performance monitoring, fault detection, and troubleshooting.
- Deployment of network services such as DHCP, DNS and NTP.

Project management-based deliverables –

- Completing project plan
- Documentation on monitoring dashboards, alerts, and reports.
- Comprehensive documentation including network diagrams, configurations, and user manuals.

- Training materials and sessions for network administrators and end-users.
- Progress reports in specified timelines.
- Cost estimation and expenditure.
- Time schedule.
- Handover documentation outlining system operation, maintenance procedures, and support contacts.
- Final report.

2.1.2 Project Procedure and Implementation Plan

The procedures and implementation plan for the networking project for New Leaf Hospital involves a systematic approach to designing, deploying, and maintaining the network infrastructure. This plan outlines the steps and tasks involved in each phase of the project, ensuring a structured and efficient implementation process.

1. **Site Preparation:**
   i. Conduct site visits to assess the physical environment and infrastructure at each hospital location.
   ii. Identify requirements for power, cooling, cabling, and physical space for network equipment.
   iii. Coordinate with facility management to ensure readiness for equipment installation and deployment.
2. **Equipment Procurement:**
   i. Develop a procurement plan based on the network architecture design and equipment specifications.

ii. Obtain quotes from vendors for network devices, software licenses, and other necessary equipment.

iii. Review proposals and select vendors based on criteria such as price, quality, and compatibility with project requirements.

iv. Place orders for equipment and ensure timely delivery to each hospital site.

3. Configuration and Installation:

i. Configure network devices according to the design specifications, including routers, switches, firewalls, and servers.

ii. Install network equipment in designated locations, ensuring proper mounting, connectivity, and cable management.

iii. Test connections and verify the functionality of network devices to ensure they are operational and properly configured.

4. Security Implementation:

i. Implement security measures such as firewalls, intrusion detection/prevention systems, and access controls to protect the network from unauthorized access and cyber threats.

ii. Configure encryption protocols, VPNs, and secure authentication mechanisms to safeguard sensitive patient data.

iii. Conduct security audits and vulnerability assessments to identify and address potential risks and vulnerabilities.

5. Testing and Verification:

i. Develop test plans and procedures to verify the performance, stability, and security of the network infrastructure.

ii. Conduct network stress tests, traffic analysis, and penetration testing to identify and address any issues or vulnerabilities.

iii. Verify compliance with industry standards and regulatory requirements through rigorous testing and validation.

6. Training and Knowledge Transfer:

i. Provide training sessions and workshops for hospital IT staff to familiarize them with the new network infrastructure and security protocols.

ii. Deliver user manuals, tutorials, and instructional materials to support staff proficiency in network configuration, monitoring, and troubleshooting.

iii. Encourage hands-on learning and practical experience to enhance staff confidence and competence in managing the network environment.

7. Ongoing Support and Maintenance:

i. Establish service level agreements (SLAs) for ongoing maintenance and support services, including response times, escalation procedures, and performance metrics.

ii. Monitor network performance and conduct regular maintenance activities to ensure optimal operation and reliability.

iii. Provide timely assistance and troubleshooting support to address any issues or concerns that arise during day-to-day operations.

Throughout the implementation process, close coordination and communication among project team members, hospital stakeholders, and external vendors are essential to ensure the successful deployment and operation of the network infrastructure. Regular progress updates, status reports, and meetings should be conducted to track project milestones, address any challenges, and ensure alignment with project objectives and timelines.

2.7 Gantt Chart

Figure 1
Timeline of Project

2.8 Allocated Budget

New Leaf Hospital has approved a budget of $150,000 for the network infrastructure upgrade project across 5 sites. These funds will go towards paying for the labor of the IT team, hardware, and software required to implement the upgrade.

In addition to this approved budget, New Leaf Hospital has also set aside a reserve sum equal to 20% of the total estimate ($30,000), bringing the total project cost budget up to $180,000.

2.8.1 List of Hardware

Table 1
Hardware's Use

Device/Hardware	Price	Quantity	Total Cost
Servers (HPE ProLiant DL360 Gen10)	$4,500	6	$27,000
Routers (Cisco 2900 Router)	$2,000	8	$16,000
Switches (Cisco Catalyst 2960-48TT-L)	$1,000	15	$15,000
Layer 3 Switches (Cisco Catalyst 3650-48TS-L)	$1,500	2	$3,000
Access Points (Aruba AP-335)	$500	10	$5,000

Device/Hardware	Price	Quantity	Total Cost
VoIP Phones (Yealink SIP-T33G)	$75	50	$3,750
Security Cameras (Reolink 4K PoE)	$500	2 (16-channel systems)	$1,000
RFID Access Control (HID ProxPoint Plus 6005)	$500	2	$1,000
Workstations (Dell OptiPlex 3070)	$300	30	$9,000
Cabling (varies)	$2,000	1 (total for all five sites)	$2,000
Total			$82,750

2.8.2 List of Software and Services

Table 2
Software's and Services

Software/Service	Price	Quantity	Total
Windows Server 2019 (16-Core License Pack)	$1,250	4	$5,000
Microsoft 365 Business Premium	$10	300 users	$3,000 (for 1 year)
Total			$8,000

2.8.3 List of Labor Costs

Table 3
Labor Costs

Labor	Price
Analysis/Consultancy Fee	$10,000
Deployment at 5 hospital sites	$20,000
Total	$30,000

2.8.4 Project Total Cost

Table 4
Total Project Cost

Cost	Price
Hardware	$82,750
Software and Services	$8,000
Labor	$30,000
Total	$120,750
Buffer (for unexpected costs) approx. 20%	$20,000
Estimated Total + Buffer	$140,750

The estimated total cost for the New Leaf Hospital project across 5 sites (with buffer), should it proceed according to schedule, is $140,750 which is in the hospital's allocated budget of $180,000. Additional funds or cost adjustments may be necessary to accommodate the project requirements across all 5 sites.

2.9 Risk analysis and Limitations.

1. Interconnectivity Challenges:

i. **Risk:** Limited availability of reliable internet connections in certain geographic areas may hinder seamless interconnectivity between New Leaf Hospital sites.

ii. **Mitigation:** Explore alternative connectivity options such as dedicated leased lines, satellite connections, or cellular backup solutions to mitigate the risk of communication disruptions.

2. Data Security Concerns:

i. **Risk**: Vulnerabilities in third-party software or hardware components used in the network infrastructure may expose New Leaf Hospital to cybersecurity threats, including malware or ransomware attacks.

ii. **Mitigation:** Regularly update firmware and software patches, implement intrusion detection systems, and conduct regular security audits to proactively identify and mitigate potential security risks.

3. Operational Efficiency:

i. **Risk:** Resistance to change among hospital staff members may impede the adoption of new network-based technologies and processes, leading to suboptimal utilization of resources and inefficiencies.

ii. **Mitigation:** Provide comprehensive training and support to staff members during the transition to the new network infrastructure. Engage stakeholders early in the planning process to address concerns and promote buy-in.

4. Scalability Challenges:

i. **Risk:** Inadequate scalability of network equipment and infrastructure may limit New Leaf Hospital's ability to accommodate future growth and expansion, resulting in performance degradation and increased operational costs.

ii. **Mitigation:** Select network hardware and architectures that offer scalability options such as modular expansion, virtualization, and cloud integration. Regularly assess network capacity and plan for scalability upgrades as needed.

5. Redundancy and Reliability:

i. **Risk:** Single points of failure in the network infrastructure, such as hardware failures or network congestion, may lead to service disruptions and downtime, impacting patient care and operational continuity.

ii. **Mitigation:** Implement redundant network paths, devices, and power supplies to minimize the risk of downtime. Conduct regular network health checks and failover tests to ensure high availability and reliability.

Limitations:

i. **Budgetary Constraints:** Limited budget may restrict the implementation of advanced redundancy measures or the procurement of high-end network equipment, potentially compromising the level of resilience and performance achievable within the project scope.

ii. **Resource Availability:** Limited availability of skilled IT personnel or external consultants may impact the speed and efficiency of project implementation, potentially leading to delays or suboptimal outcomes.

iii. **Regulatory Compliance:** Adherence to regulatory requirements, such as HIPAA or GDPR, may impose constraints on the design and implementation of certain network security measures, necessitating careful consideration and alignment with legal and compliance frameworks.

By identifying potential risks and limitations upfront, TrustUs Solutions Inc. aims to develop effective mitigation strategies and manage expectations to ensure the successful deployment of the network infrastructure for New Leaf Hospital.

3. Technical Section – Network Design, Implementation and Testing

3.1 Detailed Design, Addressing & Number Planning

Subnetting

Main Sites

Table 5
Subnetting of main sites

Site	IP address	Subnet Mask
Toronto (HQ_Site 1) LAN	192.168.0.0	255.255.240.0
WLAN	10.10.1.0	255.255.255.0
Calgary (BR1_Site 2)	192.168.1.0	255.255.254.0
	10.10.1.0	255.255.255.0
Vancouver (BR2_Site 3)	192.168.2.0	255.255.254.0
	10.10.1.0	255.255.255.0
Brampton (BR3_Site 4)	192.168.4.0	255.255.254.0
	10.10.1.0	255.255.255.0

WAN

Table 6
WAN subnetting

Connection	IP address	Subnet Mask
Toronto to DMZ	10.20.10.10	255.255.255.192
Toronto to Calgary	192.200.100.8	255.255.255.252
Toronro to Vancouver	192.200.100.20	255.255.255.252
Toronto to Brampton	192.200.100.4	255.255.255.252

Toronto VLANs

Table 7
Toronto VLANs

Name	VLAN	IP Address	Subnet Mask
LAN_DEVICES	10	192.168.0.0	255.255.240.0
WLAN	50	10.10.0.0	255.255.0.0
VOIP	99	172.16.0.0	255.255.240.0

Calgary VLANs

Table 8
Calgary VLANs

Name	VLAN	IP Address	Subnet Mask
LAN_DEVICES	10	192.168.1.0	255.255.255.0
WLAN	50	10.10.1.0	255.255.255.0
VOIP	99	172.16.1.0	255.255.255.0

Vancouver VLANs

Table 9
Vancouver VLANs

Name	VLAN	IP Address	Subnet Mask
LAN_DEVICES	10	192.168.2.0	255.255.255.0
WLAN	50	10.10.2.0	255.255.255.0
VOIP	99	172.16.2.0	255.255.255.0

Brampton VLANs

Table 10
Vancouver VLANs

Name	VLAN	IP Address	Subnet Mask
LAN_DEVICES	10	192.168.4.0	255.255.255.0
WLAN	50	10.10.4.0	255.255.255.0
VOIP	99	172.16.4.0	255.255.255.0

Device Addressing on Toronto Site

Table 11
Device Addressing (Toronto Site)

Device	Interface	IP Address	Subnet Mask
WAN_R1	Serial0/1/0	192.200.100.2	255.255.255.252
WAN_R1	fa0/0	10.30.10.2	255.255.255.252
WAN_R1	Fa0/1	10.30.10.6	255.255.255.252
WAN_R1	Fa1/0	10.30.10.10	255.255.255.252
WAN_R1	Fa1/0	10.30.20.1	255.255.255.252
CORE_SW1	G1/0/1	10.30.10.5	255.255.255.252
CORE_SW1	Vlan 10	192.168.0.3	255.255.255.0
CORE_SW1	G1/0/1	10.10.0.3	255.255.255.0
CORE_SW2	G1/0/1	10.30.10.9	255.255.255.252
CORE_SW2	Vlan 10	192.168.0.2	255.255.255.0
CORE_SW2	G1/0/1	10.10.0.2	255.255.255.0
PC1	F0/3	192.168.0.102	255.255.240.0
PC2	F0/6	192.168.0.103	255.255.240.0
PRINTER	F0/4	192.168.0.104	255.255.240.0
IP_PHONE	F0/21	172.16.0.5	255.255.240.0

Device Addressing on Calgary Site

Table 12
Device Addressing (Calgary Site)

Device	Interface	IP Address	Subnet Mask
CALGERY_ROUT	Serial0/1/0	192.200.100.22	255.255.255.252
CALGERY_ROUT	Serial0/3/0	192.200.100.18	255.255.255.252
CALGERY_ROUT	Serial0/3/1	192.200.100.14	255.255.255.252
CALGERY_ROUT	fa0/0	10.30.10.29	255.255.255.252
CALGERY_ROUT	Fa0/1	10.30.10.33	255.255.255.252
CORE_SW1	G1/0/1	10.30.10.30	255.255.255.252
CORE_SW1	Vlan 30	192.168.3.3	255.255.255.0
CORE_SW1	Vlan 70	10.10.3.3	255.255.255.0
CORE_SW2	G1/0/1	10.30.10.34	255.255.255.0
CORE_SW2	Vlan 30	192.168.3.2	255.255.255.0
CORE_SW2	VLAN 70	10.10.3.2	255.255.255.0
PC1	F0/3	192.168.4.14	255.255.255.0
PC2	F0/6	192.168.4.15	255.255.255.0
PRINTER	F0/4	192.168.4.16	255.255.255.0
IP_PHONE	F0/21	172.16.4.5	255.255.255.0

DHCP Scopes

Table 13
DHCP Scopes

POOL NAME	DEFAULT GATEWAY	DNS SERVER	START IP ADDRESS	SUBNET
WLANPOOL_HQ	10.10.0.1	10.20.10.10	10.10.0.10	255.255.240.0
LANPOOL_HQ	192.168.0.1	10.20.10.10	192.168.0.101	255.255.240.0
WLANPOOL_BR 2	10.10.4.1	10.20.10.10	10.10.4.10	255.255.255.0
LANPOOL_BR2	192.168.4.1	10.20.10.10	192.168.4.10	255.255.255.0
WLANPOOL_BR 3	10.10.3.1	10.20.10.10	10.10.3.10	255.255.255.0
LANPOOL_BR3	192.168.3.1	10.20.10.10	192.168.3.10	255.255.255.0
WLANPOOL_BR 4	10.10.4.1	10.20.10.10	10.10.4.10	255.255.255.0
LANPOOL_BR4	192.168.4.1	10.20.10.10	192.168.4.10	255.255.255.0

3.2 Hardware's & Software's

3.2.1 Server: HPE ProLiant DL360 Gen10 Server

1. Performance: Equipped with an Intel Xeon Silver 4208 processor boasting 8 cores operating at 2.1GHz and an 11MB L3 cache, paired with 64GB of DDR4-2666 ECC RDIMM memory, the server delivers robust computing power suitable for handling the demanding workloads prevalent in hospital environments.

2. Scalability: With support for up to 8 LFF (3.5-inch) or 16 SFF (2.5-inch) hot-swap drive bays, the DL360 Gen10 provides ample storage expansion options to accommodate the hospital's growing data requirements over time.

3. Redundancy and High Availability: Features such as redundant power supplies and RAID support through the HPE Smart Array S100i SR Gen10 Controller ensure data

protection and high availability, critical for maintaining uninterrupted service in crucial hospital applications.

4. Manageability: HPE's Integrated Lights-Out (iLO) management technology enables remote monitoring, configuration, and troubleshooting, reducing reliance on on-site IT staff and improving operational efficiency.

5. Virtualization Support: Certified for various virtualization platforms including VMware ESXi and Microsoft Hyper-V, the DL360 Gen10 allows for workload consolidation, optimizing resource utilization and simplifying management.

6. Energy Efficiency: Incorporating energy-efficient components and features like HPE Adaptive Cooling, the server helps reduce power consumption and operating costs, aligning with the hospital's sustainability goals.

7. Reliability: Renowned for their robust design and reliable performance, HPE ProLiant servers ensure minimal downtime and business continuity for critical hospital operations.

By opting for the HPE ProLiant DL360 Gen10 Server, the New Leaf Hospital project benefits from its high performance, scalability, redundancy, manageability, virtualization support, energy efficiency, and reliability, making it the ideal choice for supporting demanding applications and ensuring uninterrupted service delivery.

Figure 2
HPE ProLiant DL360 Gen10 Server

3.2.1.1 Active Directory Domain Service

Active Directory Domain Services (AD DS) will be used to manage and authenticate users, computers, and other devices within the New Leaf Hospital network. This service will facilitate centralized management, security, and access control, ensuring that all devices on the network are securely connected and managed.

3.2.1.2 DHCP Server

A DHCP server will be deployed to automatically assign IP addresses to devices on the network. This will streamline the network setup process, reduce the administrative burden, and ensure that all devices have a valid IP address configuration.

3.2.1.3 DNS Service

The DNS service will be used to resolve domain names to IP addresses within the New Leaf Hospital network. This will enable users to access network resources using domain names instead of IP addresses, improving usability and network management.

3.2.1.4 Web Server

An Internet Information Services (IIS) web server will be set up to host the New Leaf Hospital's internal and external websites. This server will support HTTPS, HTTP, FTP, and SMTP, providing a secure and efficient platform for web services.

3.2.2 Other Device Specifications

3.2.2.1 Firewall: Palo Alto Networks PA-820 Next-Generation Firewall

The Palo Alto Networks PA-820 is a high-performance Next-Generation Firewall suitable for mid-sized enterprise networks like the New Leaf Hospital.

Hardware Specifications:

Form Factor:	1U Rack-Mountable Appliance
Processor:	Quad-core Xeon
Memory:	16GB RAM
Storage:	200GB SSD
Network Interfaces:	8x Gigabit Ethernet (including 4x bypass ports), 4x 10Gigabit Ethernet SFP+

Performance and Capacity:

Firewall Throughput: 9.2 Gbps

Threat Prevention Throughput: 6.8 Gbps

IPSec VPN Throughput: 6.4 Gbps

Concurrent Sessions: 4 million

New Sessions per Second: 120,000

Security Features:

Next-Generation Firewall capabilities with application visibility and control

Intrusion Prevention System (IPS)

Advanced Threat Prevention with malware and exploit detection

URL Filtering and Content-ID

SSL/TLS Decryption and Inspection

User-ID and Role-Based Access Control

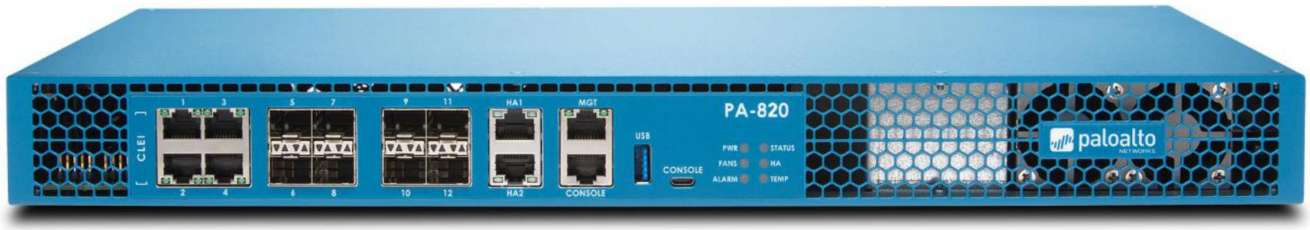
Management and High Availability:

Centralized management with Panorama

Active/Passive High Availability (HA) support

Redundant power supplies and fans

Figure 3
Palo Alto Networks PA-820 Next-Generation Firewall



3.2.2.2 Smart App LCD UPS Series - OR700LCDRM1U

The OR700LCDRM1U is an uninterruptible power supply (UPS) unit from CyberPower Systems, designed to provide backup power and protection for critical network devices and servers in case of power outages or fluctuations.

Key Features:

Form Factor:	1U Rackmount/Tower Convertible
Output Power Capacity:	700VA/490W.
Input Voltage:	120V
Output Voltage:	120V
Runtime:	Up to 12 minutes at full load (490W)
Battery:	12V/7Ah x 2 Sealed Lead-Acid batteries
LCD Display:	Provides UPS status, runtime, load, and battery information.
Communication Ports:	USB and Serial (DB9)
Management Software:	PowerPanel® Business Edition Software (Windows/Linux/Unix)
Surge Protection:	480 Joules
Outlets:	6 NEMA 5-15R outlets (4 battery backup & surge protected, 2 surge only)

Automatic Voltage Regulation (AVR)

Cold Start Function (Allows the UPS to be powered on without AC input)

This UPS is part of CyberPower's Smart App LCD series, which offers advanced features and LCD monitoring for network and server applications. The OR700LCDRM1U is designed to fit in a 1U

rackmount or can be converted to a tower form factor, making it suitable for various installation environments.

Figure 4
UPS Series - OR700LCDRM1U

3.2.2.3 Switches: Catalyst 2960 Series

Manufacturer:	Cisco
Model:	Catalyst 2960 Series (Specific models include 2960-X, 2960-24TT, 2960-24T, 2960-24P, 2960-48TT, 2960-48T, 2960-48P, etc.)
Type:	Managed Switch
Port Configuration:	Varies by model, but typically includes a mix of 10/100/1000Base-T (Gigabit Ethernet) and 10/100Base-TX (Fast Ethernet) ports.

Switching Capacity:	Varies by model, but generally offers high switching capacity to support the needs of small to medium-sized networks.
Layer 2/3 Features:	Supports VLANs, STP, RSTP, and VTP for network segmentation and management.
Security Features:	Includes features such as Access Control Lists (ACLs), 802.1X authentication, and IP Source Guard for enhanced network security.
Quality of Service (QoS):	Supports QoS to prioritize critical network traffic.
Power over Ethernet (PoE):	Some models support PoE, allowing for the powering of devices like IP phones and wireless access points over the same network cables.
Management:	Offers web-based management and the Cisco Catalyst Command-Line Interface (CLI) for configuration and management.

Figure 5
Catalyst 2960 Series

3.2.2.4 Router – 2900

Manufacturer:	Cisco
Model:	2900
Type:	Integrated Services Router
WAN Ports:	2 x Gigabit Ethernet
LAN Ports:	4 x 10/100 Ethernet
Memory:	512 MB DRAM, 64 MB Flash
Security Features:	Firewall, VPN, IPS, Content Filtering
Voice Support:	Yes (with appropriate module)
Additional Features:	
Routing Protocols:	OSPF, EIGRP, BGP, RIP
Quality of Service (QoS):	Supports QoS for voice, video, and data traffic.
Network Services:	DHCP, DNS, NAT, IPsec VPN

Redundancy:	Virtual PortChannel (vPC), In-Service Software Upgrade (ISSU)

Figure 6
Router – 2900

3.2.2.5 VOIP Phones: SIP-T33G

Manufacturer:	Yealink
Model:	SIP-T33G
Type:	IP Phone
Display:	2.8" 192 x 64-pixel graphical LCD
Voice Codecs:	G.722, G.711 (A/μ), G.723, G.729AB, G.726, iLBC
Network Protocols:	SIP v1 (RFC2543), v2 (RFC3261)
PoE Support:	Yes

Figure 7
SIP-T33G

3.2.2.6 Security Camera: Reolink 4K 16-Channel PoE Security

Manufacturer:	Reolink
Model:	Reolink 4K 16-Channel PoE Security
Type:	Network Video Recorder (NVR) System
Video Resolution:	4K (8MP)
Number of Channels:	16
Power over Ethernet (PoE):	Yes
Storage:	Supports up to 8TB HDD (not included)

Figure 8
Reolink 4K 16-Channel PoE Security

3.2.2.7 RFID Controller: HID Global's ProxPoint Plus 6005

Model:	HID Global's ProxPoint Plus 6005
Manufacturer:	HID Global
Model:	ProxPoint Plus 6005
Type:	Access Control System
Reader Type:	Proximity Card
Communication:	Wiegand Interface
Capacity:	Up to 2000 users, 2500 events

Figure 9
HID Global's ProxPoint Plus 6005

3.2.2.8 Dell OptiPlex 3000 Series

Specification:	Dell OptiPlex 3000 Series
Processor:	Intel Core i5 or i7 processors
Memory:	Up to 16GB DDR4 2666MHz
Storage:	1TB 7.2K RPM SATA HDD or 256GB PCIe NVMe SSD
Graphics:	Integrated Intel UHD Graphics 630
Keyboard/Pointing Devices:	Dell USB Keyboard and Mouse
Networking Communications:	Gigabit Ethernet
Audio/Multimedia:	Integrated audio with microphone and headphone jacks
Ports:	USB 3.1 Gen 1 ports, DisplayPort 1.2, HDMI 1.4, RJ-45 Ethernet port
Expansion Slots:	Up to 4 PCIe 3.0 slots
Power Supply:	Hot-plug power supply
Management:	Dell Remote Access Manager (DRAC)
Form Factor:	2U Rack Mountable
Operating System:	Windows 10 Pro, Windows 11, Linux distributions
Warranty:	Standard warranty options, extended coverage available

Figure 10
Dell OptiPlex 3000 Series

3.2.2.9 Cables

LC UPC to LC UPC Duplex OS2 Single Mode PVC (OFNR) 2.0mm Tight-Buffered Fiber Optic Patch Cable

Type:	Fiber Optic Cable
Connector:	LC UPC (Lucent Connector, Ultra-Polished Connector)
Length:	3 feet
Fiber Grade:	G.657.A1 (Compatible with G.652.D)
Fiber Mode:	OS2 9/125µm
Wavelength:	1310/1550nm
Insertion Loss:	≤0.3dB
Return Loss:	≥50dB
Min. Bend Radius (Fiber Core):	10mm

Attenuation at 1310 nm: 0.36 dB/km

Attenuation at 1550 nm: 0.22 dB/km

Fiber Count: Duplex

Cable Diameter: 2.0mm

Cable Jacket: PVC (Riser/OFNR)

Polarity: A (Tx) to B (Rx)

Operating Temperature: -20~70°C

Commonly used for high-speed data communications and telecommunication applications.

Figure 11
LC UPC to LC UPC Duplex OS2 Single Mode PVC (OFNR)

Cat6 1000ft Twisted Pair 23AWG Solid UTP Network Ethernet Router Cable, 550Mhz, PVC RJ45 Wire Bulk Pull Box, Blue

Cable Type: Category 6 Ethernet Cable

Length: Varies based on your project requirements

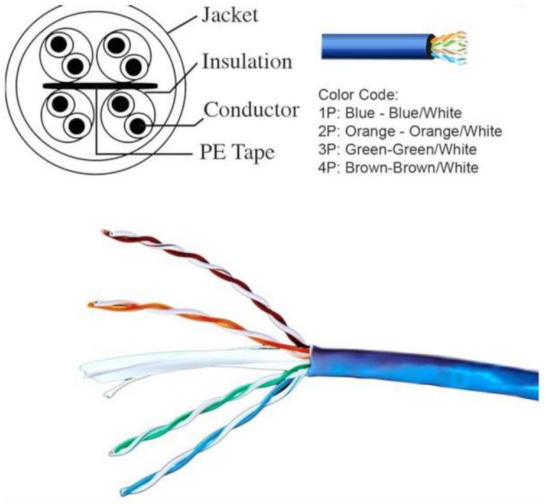
Connector Type: RJ-45

Data Transfer Rate: Up to 1 Gbps

Maximum Distance: Up to 100 meters

PoE Compatibility: Yes

Figure 12
Category 6 Ethernet Cable



3FT Length Router Cable CAB-SS-2626X DTE/DCE Smart Serial Cable for Cisco Router

Brand: EDIMS

Cable Type: Network Router Cable

Compatible Devices: Router

Color: Blue

Connector Gender: Male-to-Male

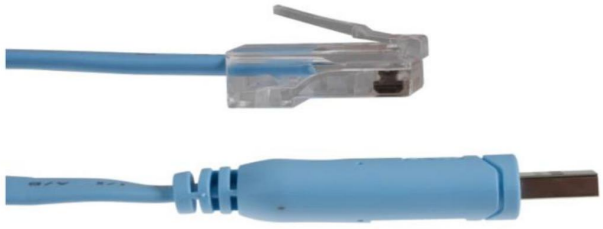
Figure 13
Serial Cable

Cisco Compatible Console Cable, 6ft, RS232, CAB-CONSOLE-USB-RJ45

Features:

Type:	Console
Length:	6'
Color:	Light Blue
Connector:	USB A to RJ45
Compatibility:	100% Compatible USB 2.0 (1.1 compatible)
Brand:	CablesAndKits

Figure 14
Console Cable



3.3 Network Diagrams & Figures

Figure 15
Toronto (Main Site) Topology

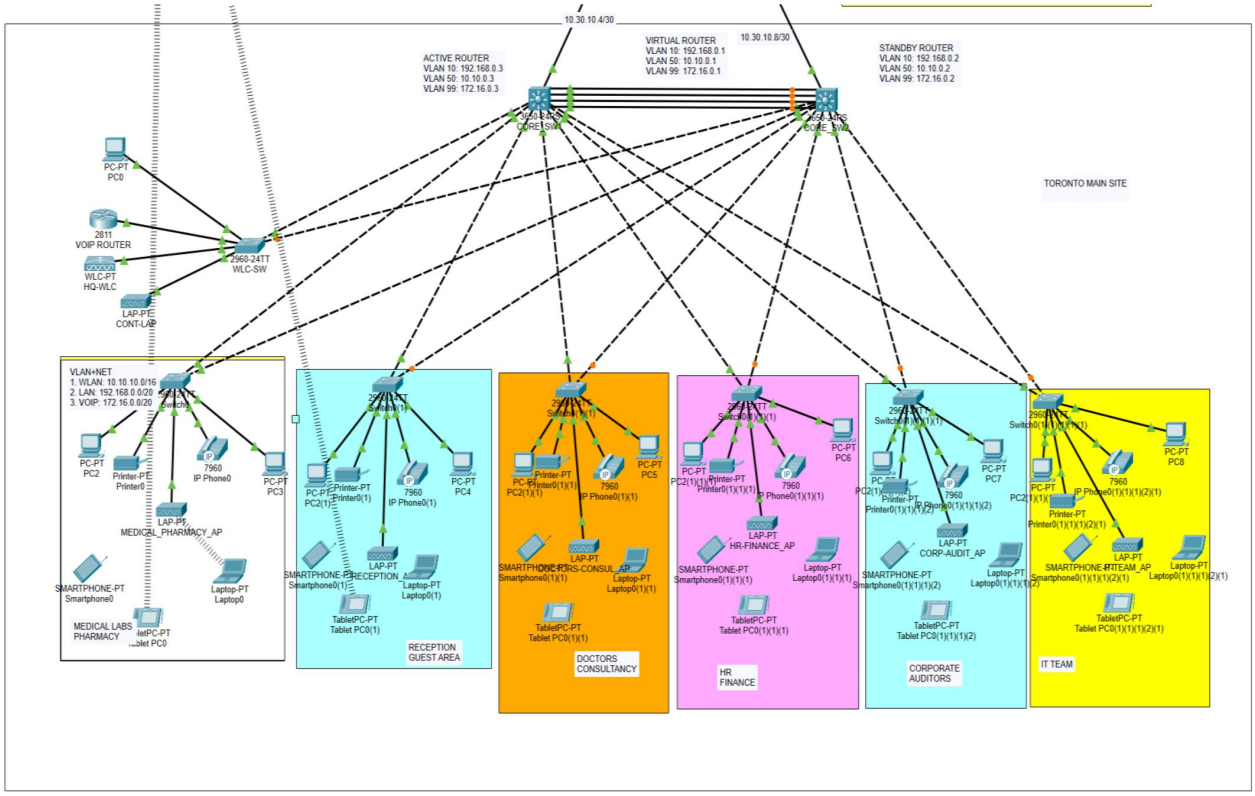


Figure 16
Vancouver Site Topology

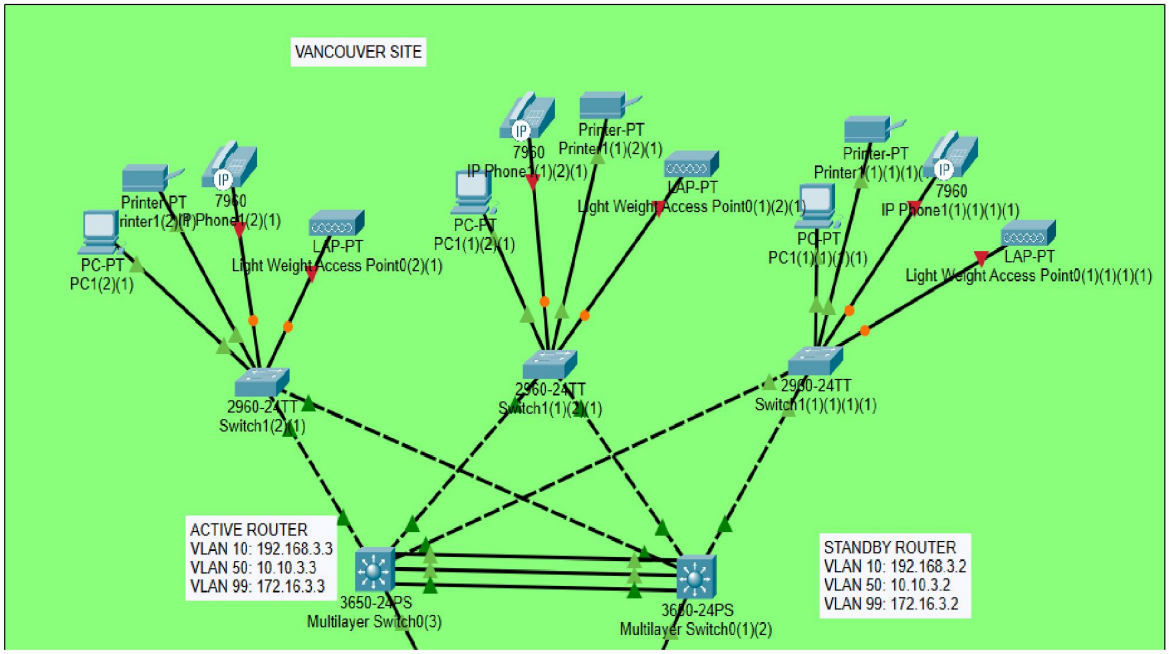


Figure 17
Calgary Site Topology

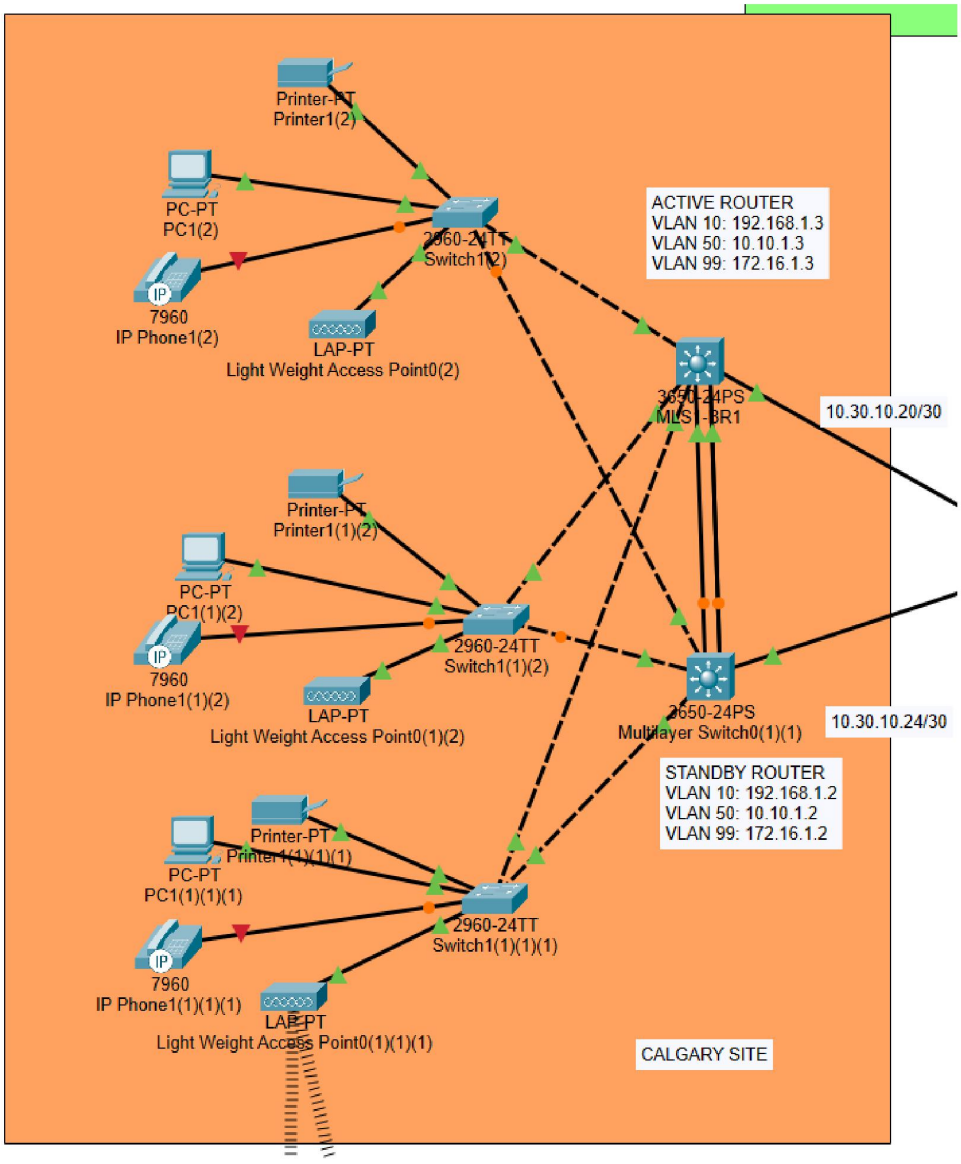


Figure 18
Brampton Site Topology

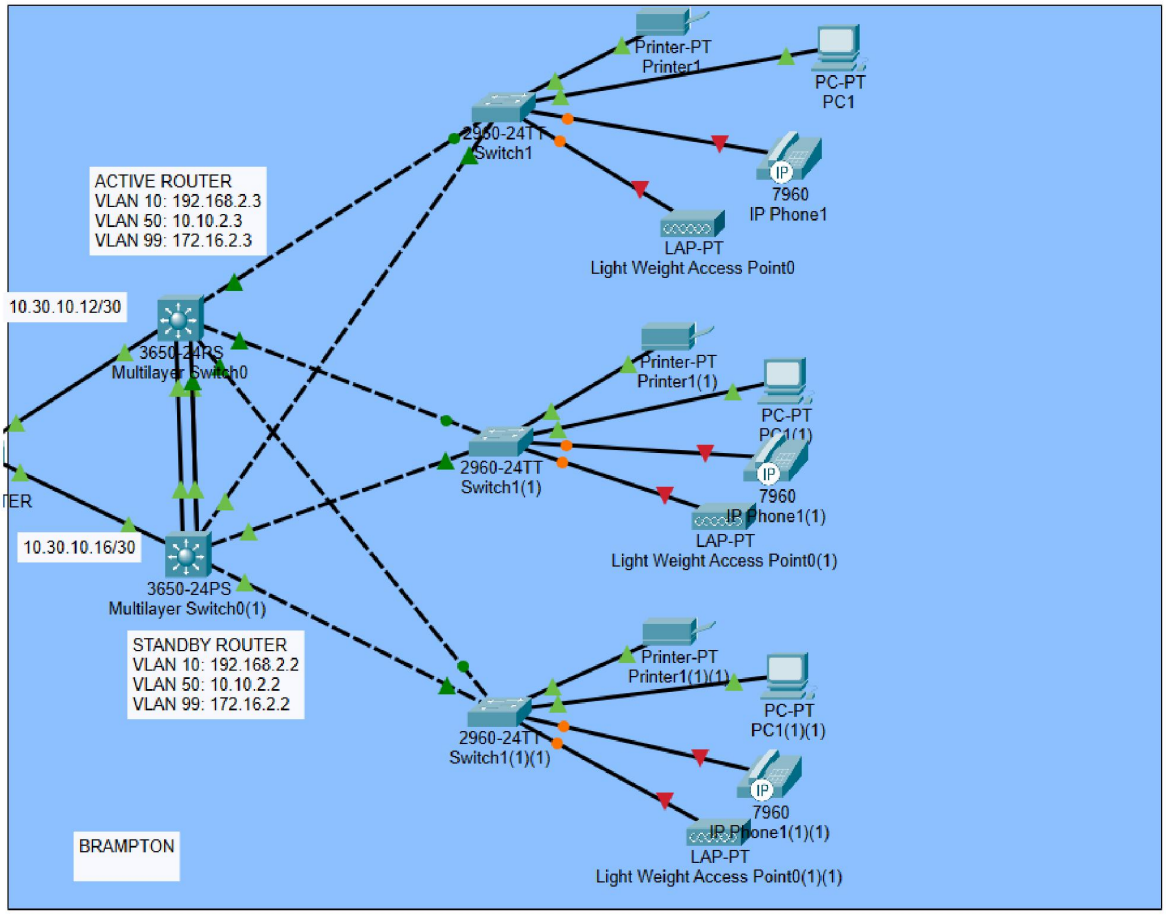


Figure 19
Demilitarized Zone (DMZ) Topology

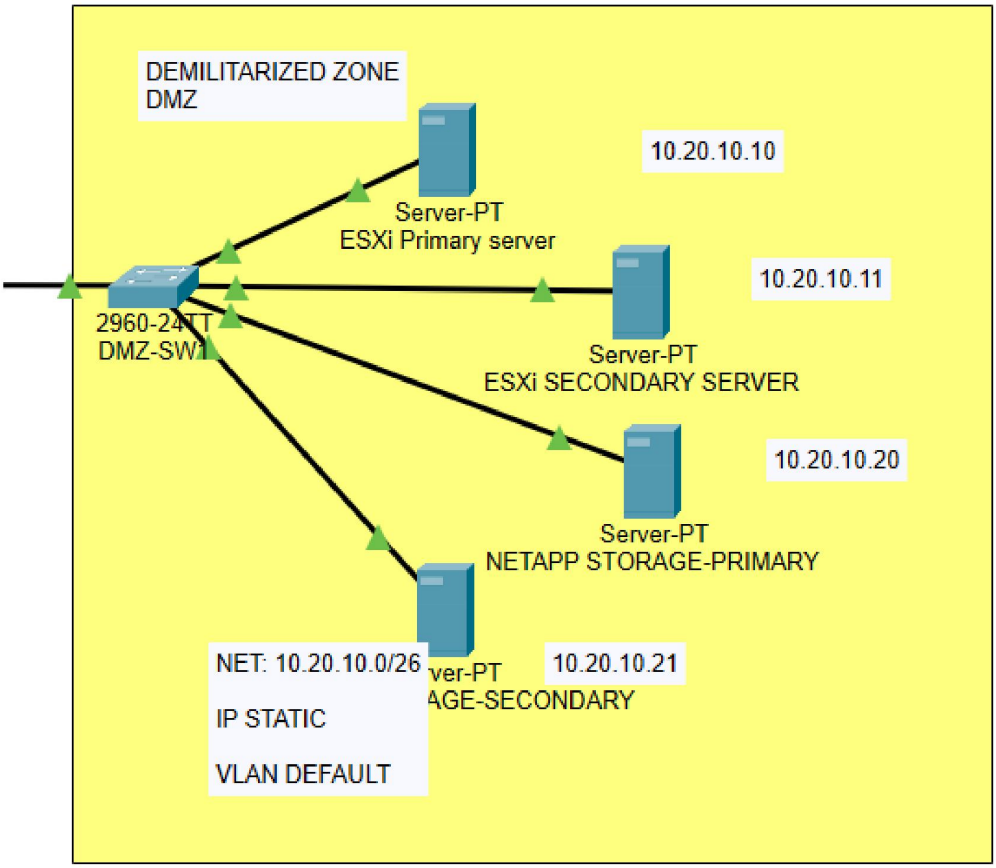
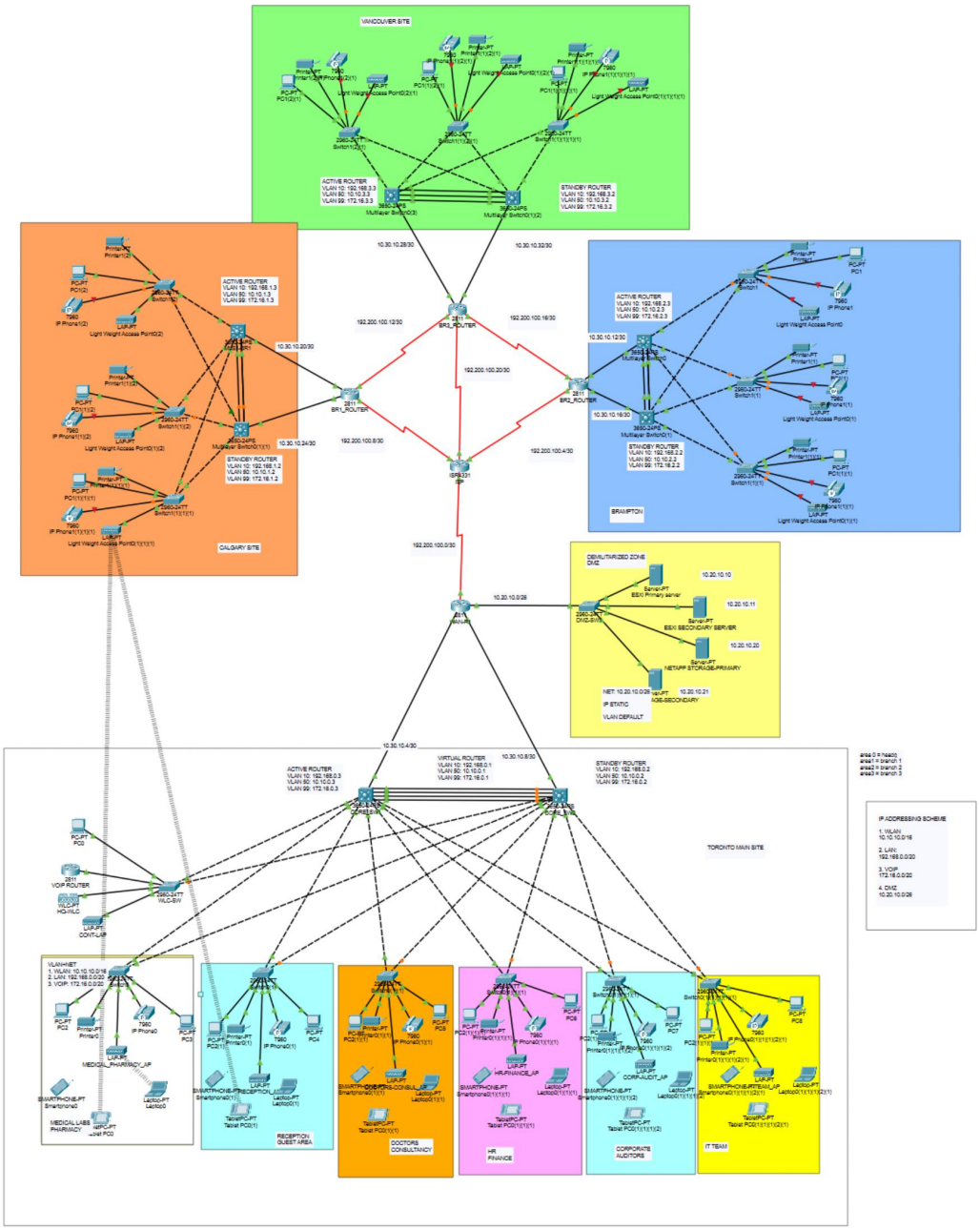


Figure 20

2Whole Network Topology



3.4 VOIP Implementation

Deployment Scope:

VoIP phones have been installed in every room throughout all levels of the hospital. Additionally, phones have been deployed at each hospital site, and these sites are interconnected to facilitate communication between them.

Configuration:

Every VoIP phone is set up with the appropriate configurations, which include SIP accounts, extension numbers, and network parameters. Quality of Service (QoS) settings are applied to prioritize voice traffic, ensuring clear communication. Security measures, such as secure SIP authentication, are implemented to safeguard against unauthorized access and eavesdropping.

Inter-Site Communication:

The VoIP phone system enables seamless communication between users at different hospital sites. Connectivity between sites is established through SIP trunks and other VoIP gateway devices. A standardized numbering plan simplifies dialing between sites.

Integration with Hospital Communication Systems:

The VoIP phones are seamlessly integrated into the hospital's communication infrastructure, which includes nurse call systems and emergency alerts. This integration facilitates efficient communication among staff members and enables timely responses to patient needs.

3.5 Wireless Technologies Implementation

We have incorporated wireless devices connectivity to enhance communication efficiency. This includes integrating smartphone connectivity, tablets, and laptops into the hospital network infrastructure.

To facilitate seamless wireless communication, we have strategically deployed wireless access points (APs) on every floor and in every room of the hospital. This ensures comprehensive coverage and enables users to connect their devices to the network from anywhere within the hospital premises.

By implementing wireless technologies, we aim to provide staff members and patients with greater flexibility and mobility in accessing critical information and communication services. This enhances productivity, collaboration, and overall user experience within the hospital environment.

3.6 IT Network Security Features

Advanced Firewall Deployment

The project features the deployment of the Palo Alto Networks PA-820 Next-Generation Firewall (NGFW) at New Leaf Hospital. This NGFW goes beyond the capabilities of traditional firewalls by offering:

- Detailed application monitoring and management
- Intrusion Prevention System (IPS)
- Sophisticated Threat Prevention, including malware and exploit detection.
- Web content filtering and Content-ID
- SSL/TLS Decryption and Inspection

- User-ID and Role-Based Access Control

The PA-820 NGFW enables precise control over network traffic, allowing the hospital to implement security policies based on applications, users, and content. It also includes advanced threat prevention capabilities to detect and block complex cyber threats, ensuring the protection of medical data and compliance with regulations like HIPAA.

Enhanced Network Security Through Segmentation

The network design includes segmentation strategies using VLANs and routing protocols to logically separate different network zones, such as:

- User Networks (e.g., staff, guests)
- Server Networks (e.g., database servers, application servers)
- DMZ (Demilitarized Zone) for public-facing services
- Management Network for administrative purposes

Access between these zones is tightly controlled and limited according to established security policies and the principle of least privilege. The PA-820 NGFW's User-ID and Role-Based Access Control features allow for detailed control over network access based on user roles and identities.

Endpoint Protection

Beyond network-level security, the project includes the deployment of endpoint security solutions on workstations and servers. This involves installing antivirus/antimalware software, host-based firewalls, and other endpoint protection measures to protect against threats targeting individual systems.

Centralized Security Monitoring

The project may also implement a Security Information and Event Management (SIEM) solution to centralize security monitoring and incident response. A SIEM aggregates and analyzes security logs and events from various sources, such as firewalls, intrusion detection systems, and endpoints, facilitating real-time threat detection and correlation.

Secure Remote Access Solutions

Given the increasing need for remote work and telehealth services, the project may incorporate secure remote access solutions, like Virtual Private Networks (VPNs) or secure gateways, to allow authorized personnel and healthcare providers to securely access the hospital's network and resources from remote locations.

Continuous Security Management

Finally, the project should include arrangements for continuous security monitoring, threat intelligence, vulnerability assessments, and regular software updates and patches to keep the hospital's network and systems secure and updated with the latest security measures.

So, with these IT network security features, the New Leaf Hospital will establish a strong and comprehensive security framework, protecting medical data, ensuring regulatory compliance, and safeguarding critical operations from cyber threats.

3.7 Other Advanced Technologies

The New Leaf Hospital project integrates a range of Internet of Things (IoT) devices to improve operational efficiency, security, and patient care. These devices are networked, facilitating remote monitoring, data gathering, and automated procedures.

RFID Access Control Systems

A notable technology in the project is the use of RFID-based access control systems. The HID Global's ProxPoint Plus 6005 RFID Controller is employed to oversee and monitor access to restricted areas within the hospital.

This RFID system employs proximity cards or key fobs given to authorized staff, ensuring that only those with permission can enter sensitive areas like medical records rooms, server rooms, or specific patient wards. RFID readers are strategically positioned at entry points, and the ProxPoint Plus 6005 Controller handles access permissions and records all entry and exit activities, offering an audit trail for heightened security and compliance.

IoT Security Cameras

The project also features the deployment of the Reolink 4K 16-Channel PoE Security Camera System. These high-tech IoT cameras utilize Power over Ethernet (PoE) technology, enabling streamlined cabling and power supply throughout the hospital.

The 4K ultra-high-definition cameras deliver high-quality video, facilitating effective surveillance of key areas, such as entrances, lobbies, and patient wards. These cameras come with features like motion detection, night vision, and remote access, enabling hospital security teams to swiftly monitor and respond to any incidents.

3.8 Network Testing and Troubleshooting

Ensuring the reliability and functionality of the network infrastructure is a critical step before it goes live. For New Leaf Hospital, comprehensive testing was conducted on all hardware and software components installed across the five geographically dispersed sites. This included

verifying the connectivity between routers, switches, and workstations, as well as testing the servers to ensure their services were operational.

Server Testing:

The servers were thoroughly tested to validate their services, which included:

- **Website Accessibility:** Confirming that users could access the hospital's website.
- **Domain Joining:** Verifying that users could automatically join the server domain upon connecting to the network, with dynamic IP address assignment facilitated by the DHCP server and DNS services.
- **VoIP Services:** Testing the Voice over Internet Protocol (VoIP) functionality to ensure reliable voice communication within the hospital.
- **IP Camera Integration:** Validating the integration of IP cameras for surveillance and security purposes, ensuring smooth operation and video feed accessibility.

Troubleshooting and Correction:

All test results were meticulously documented, and any services not functioning as expected were promptly addressed. For instance, if workstations in a specific department were not automatically receiving IP addresses, troubleshooting involved verifying the computers' domain status. If they were not correctly added to the domain, the issue was resolved by integrating the computers into the hospital's network domain.

Scalability and Futureproofing:

The network design for New Leaf Hospital is inherently scalable, ensuring that the quality of services remains unimpaired even as the number of users increases. This scalability is a key

feature of the design, allowing the hospital to expand its operations without compromising network performance or security.

Documentation and Future Reference:

All test results and troubleshooting outcomes were compiled into comprehensive documentation. This documentation serves as a valuable resource for future reference, aiding hospital operators in maintaining the network's efficiency and reliability. It also provides a historical record of the network's performance and any issues encountered, facilitating proactive troubleshooting and preventive maintenance.

4 Analysis of Results

4.1 Network Performance and Capacity

The integration of high-performance networking equipment, including Cisco routers, switches, and the Palo Alto Networks Next-Generation Firewall, has markedly improved the network's performance and capacity. With enhanced bandwidth and throughput, the hospital's network can now effortlessly support demanding applications, such as Electronic Medical Records (EMR) systems, telemedicine services, and large file transfers (e.g., medical imaging).

4.2 Scalability and Flexibility

The adoption of server virtualization and cloud services has allowed the hospital to achieve greater scalability and flexibility in its IT infrastructure. As the hospital's requirements evolve, additional virtual servers and resources can be rapidly deployed, ensuring that the network can adjust to future needs without significant infrastructure modifications.

4.3 Improved Security and Compliance

The integration of advanced security features, like the Palo Alto Networks NGFW, network segmentation, and role-based access control, has substantially enhanced the hospital's security framework. Sensitive medical data and vital systems are now better safeguarded against cyber threats, ensuring adherence to regulations such as HIPAA.

4.4 Operational Efficiency and Patient Care

The integration of IoT devices, including security cameras, environmental sensors, and RFID access control systems, has streamlined hospital operations and enhanced patient care. Real-time monitoring and automation have optimized resource allocation, boosted staff efficiency, and created a safer and more comfortable setting for patients.

4.5 Reliability and Uptime

The deployment of redundant servers, failover mechanisms, and high-availability configurations has significantly boosted the reliability and uptime of critical systems and applications. This ensures that essential services, such as the EMR system and patient care applications, always remain accessible and operational.

5. Conclusion

The New Leaf Hospital's network infrastructure upgrade project has successfully laid a solid and forward-looking IT framework across all five hospital sites. Our team's comprehensive approach has introduced innovative technologies and industry standards to facilitate efficient and secure healthcare operations.

By leveraging top-tier networking equipment from Cisco and Palo Alto Networks, virtualization technologies, cloud services, and advanced security protocols, the hospital now enjoys superior network performance, effortless scalability, and strong cybersecurity safeguards. The incorporation of IoT devices, including security cameras, environmental sensors, and automated building systems, has further streamlined operations, optimized resource allocation, and enhanced patient care quality.

Despite the significant initial investment in this new project, the long-term benefits, such as energy efficiency savings, increased staff efficiency, and better patient results, make the investment worthwhile. Additionally, the hospital's IT infrastructure is now prepared for future technological advancements and changing healthcare industry needs.

Looking forward, the hospital might explore further improvements, like a comprehensive disaster recovery strategy, remote patient monitoring technologies, and data analytics to gain deeper insights into operational performance and patient care results.

In summary, this project has successfully created a modern and secure IT infrastructure for New Leaf Hospital, allowing for the provision of top-quality healthcare services, ensuring adherence to regulations, and maintaining a competitive position in the rapidly changing healthcare sector across all its sites.

6. Installing and Setting Up Servers and Services

Figure 21
Creating New Virtual Machine

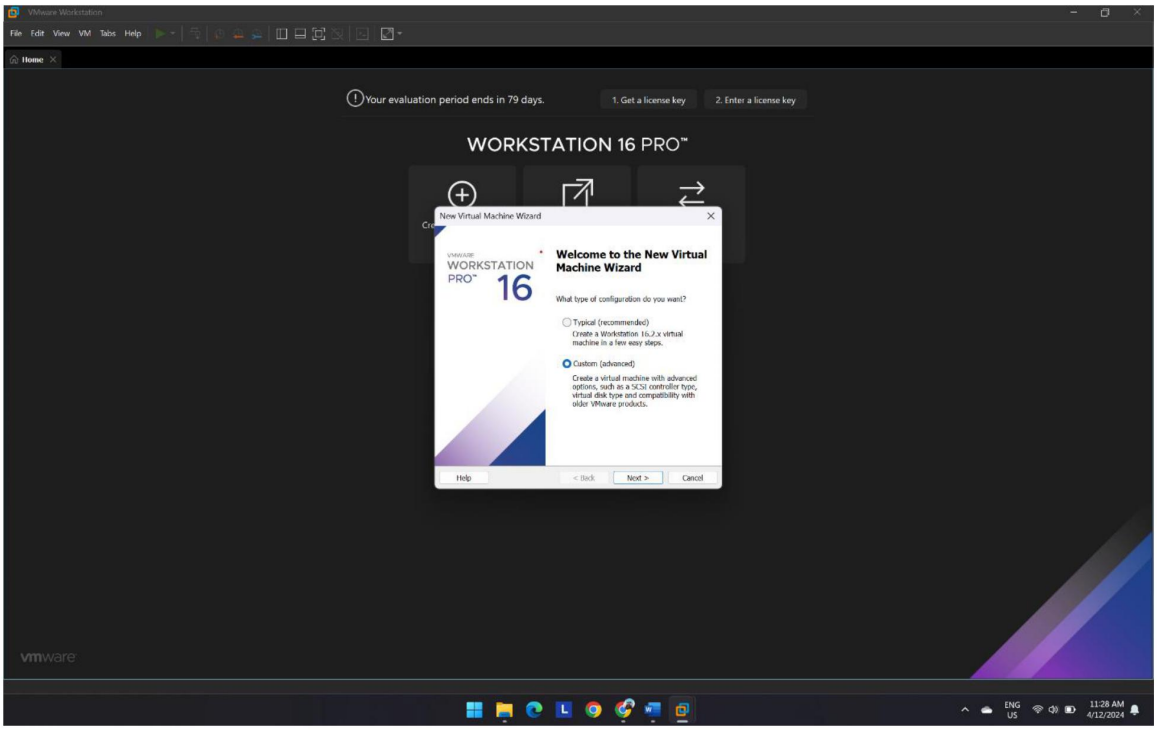


Figure 22
Selecting VM Hardware Capabilities

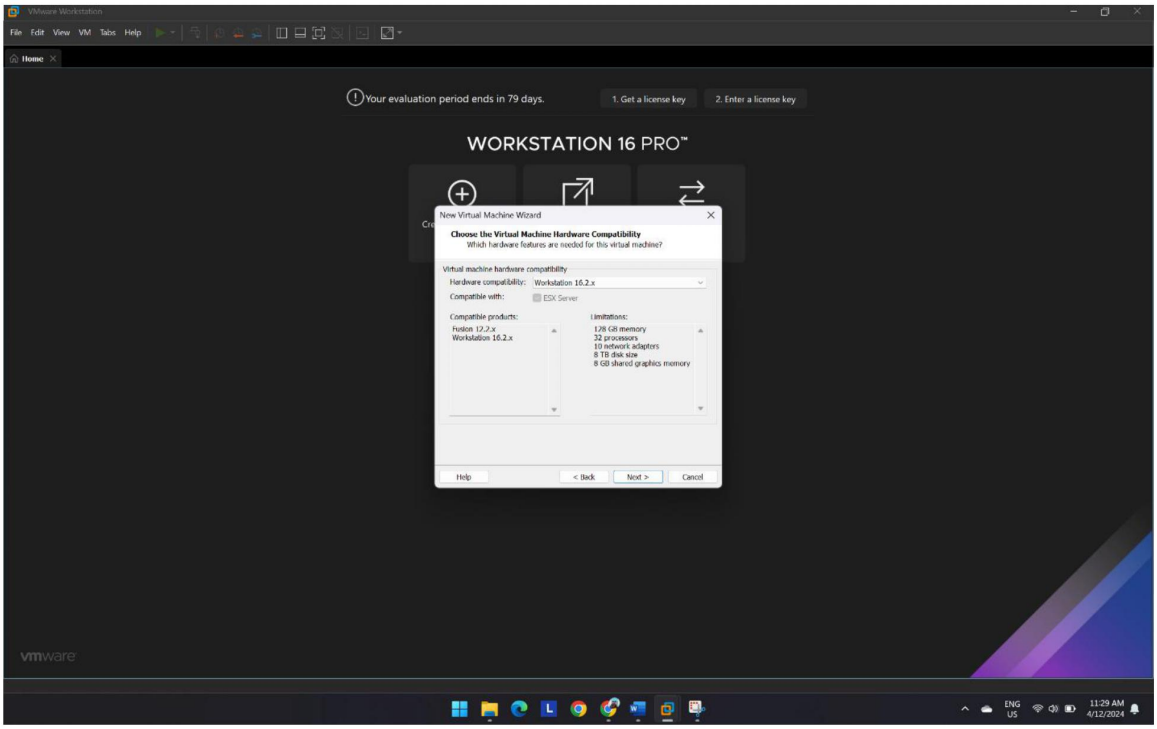


Figure 23
Select> I will install the operating system later

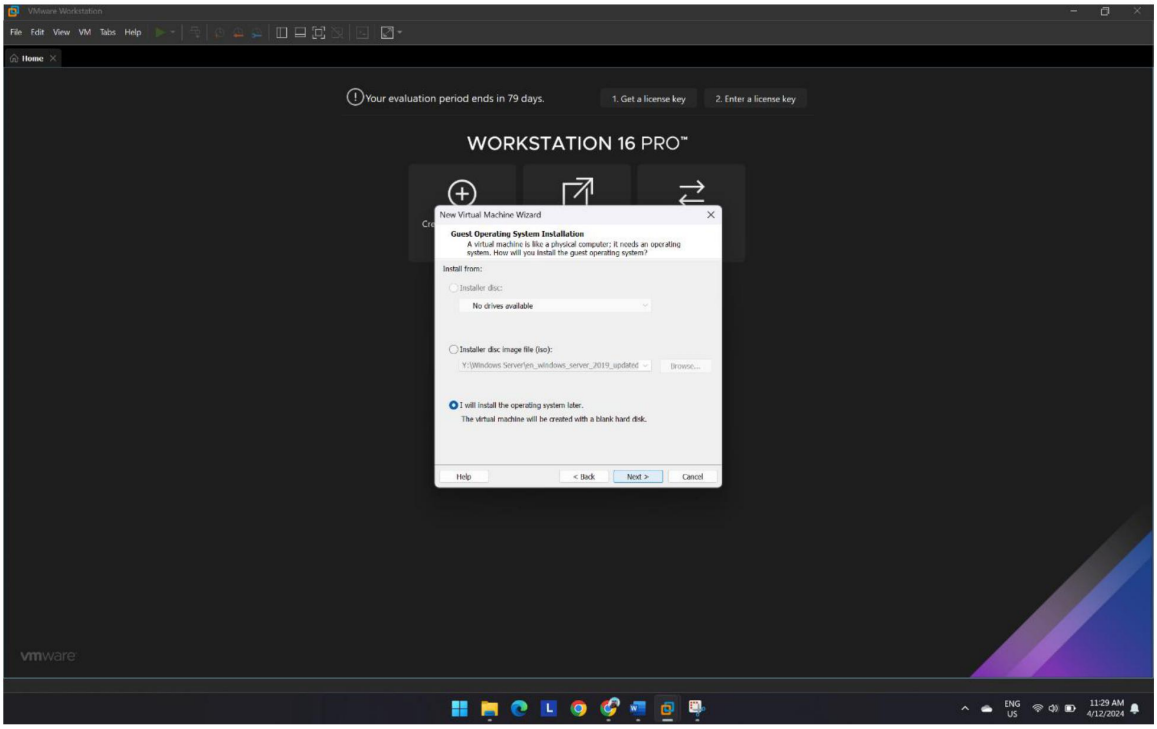


Figure 24
Name the Virtual Machine

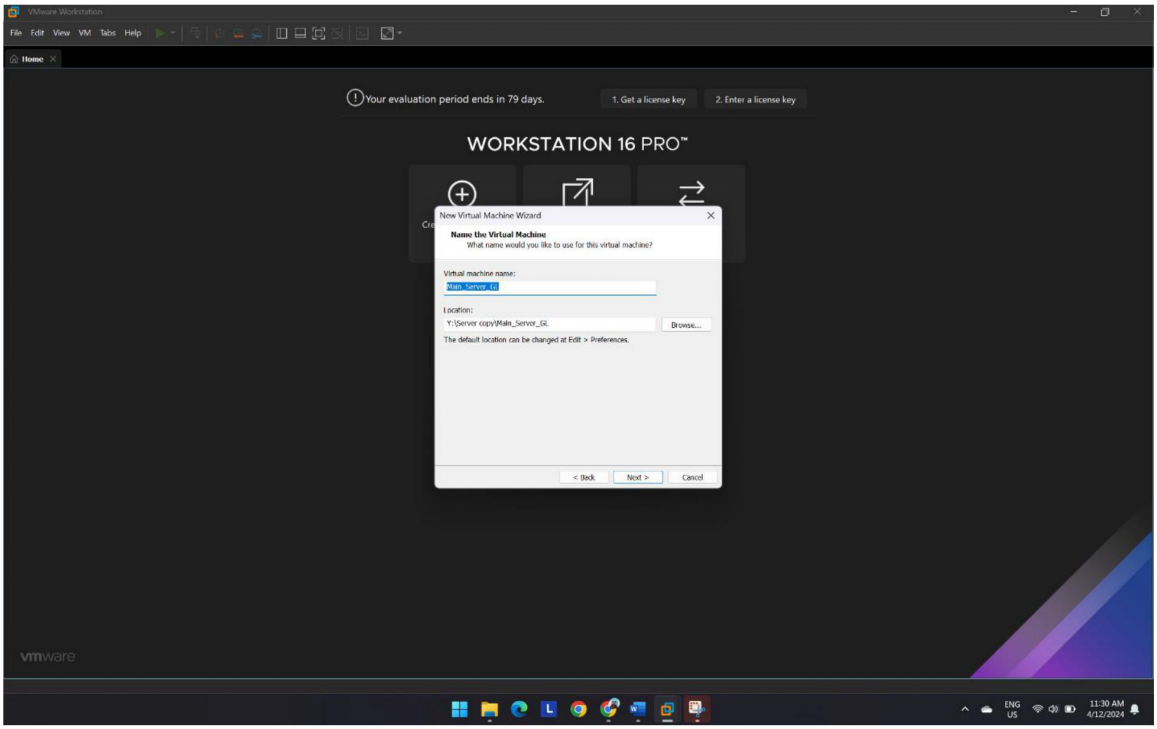


Figure 25
Select the Firmware Type

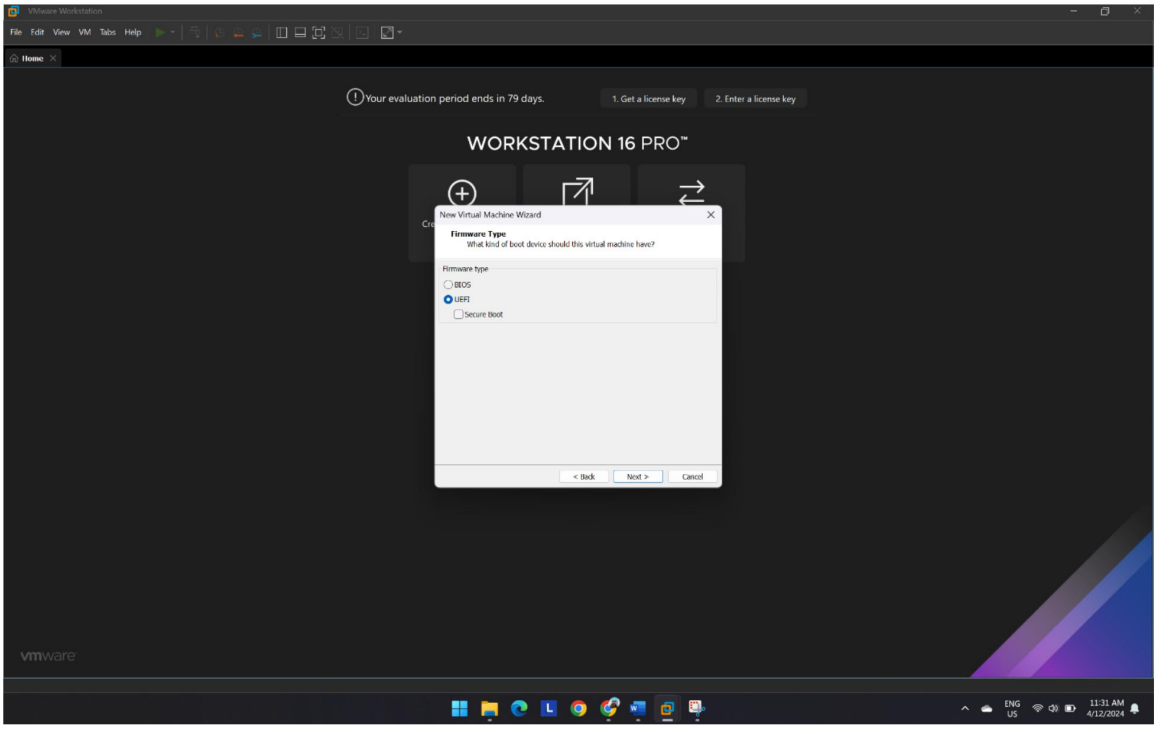


Figure 26
Configure Processor

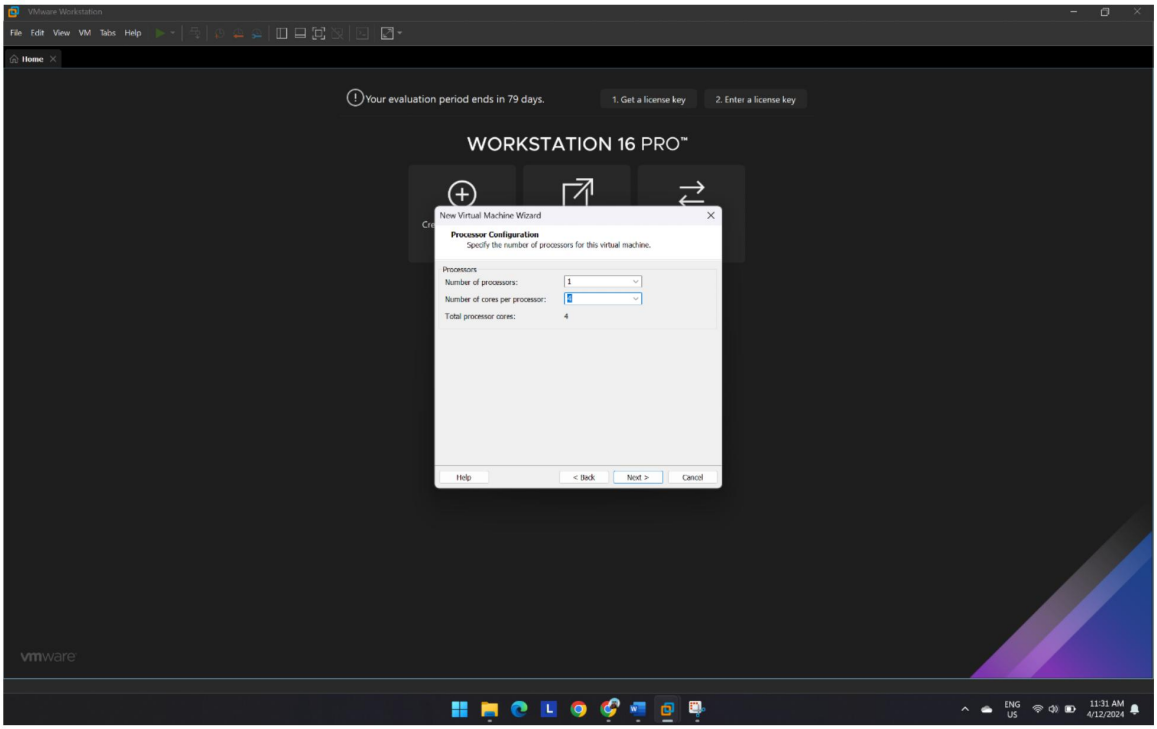


Figure 27
Memory of Virtual Machine

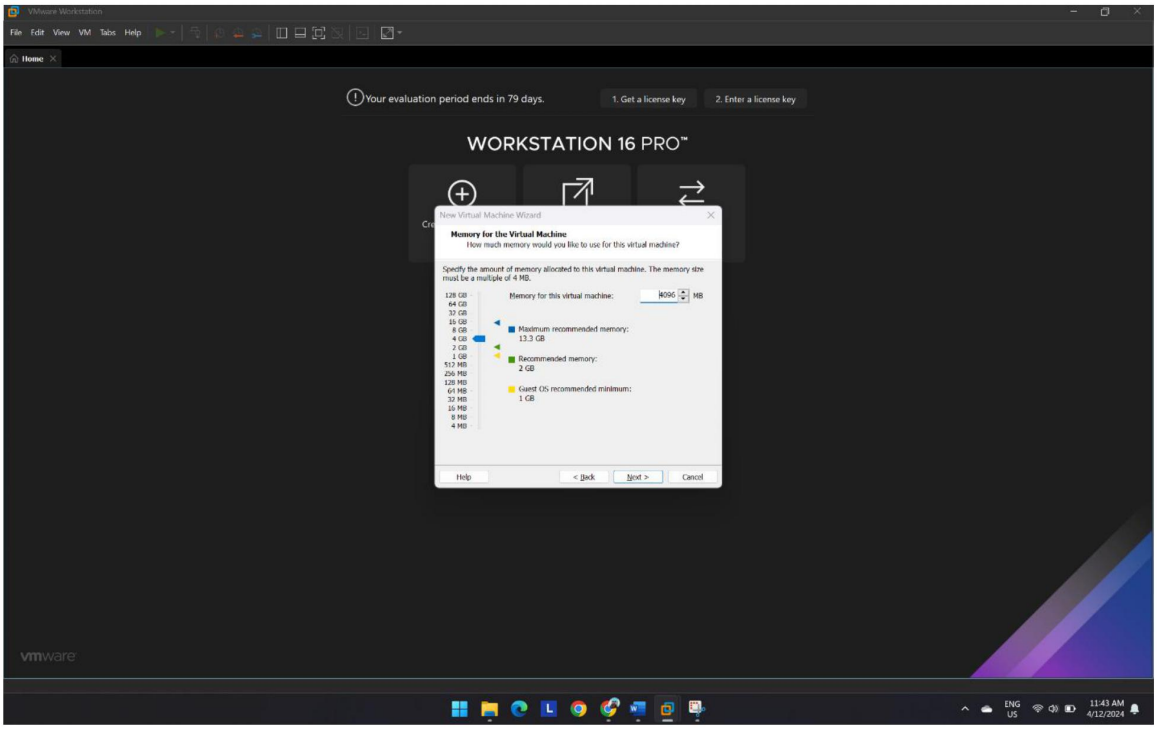


Figure 28
Select Network Type

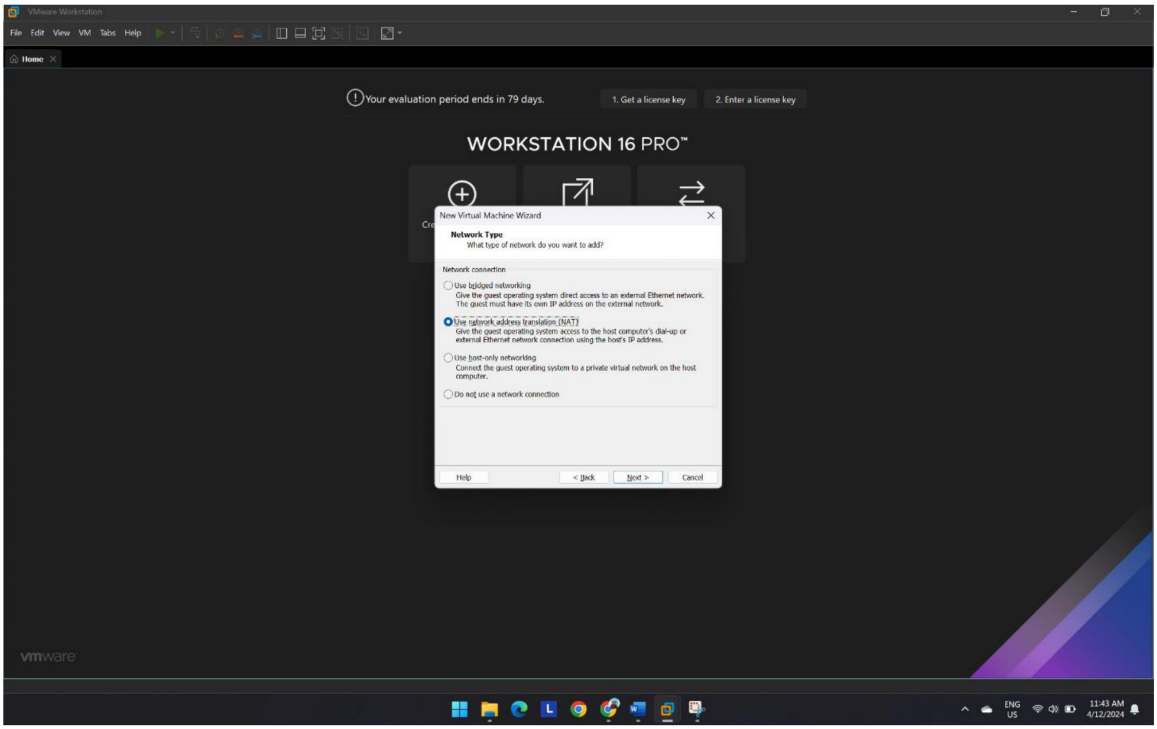


Figure 29
Select I/O Controller Types

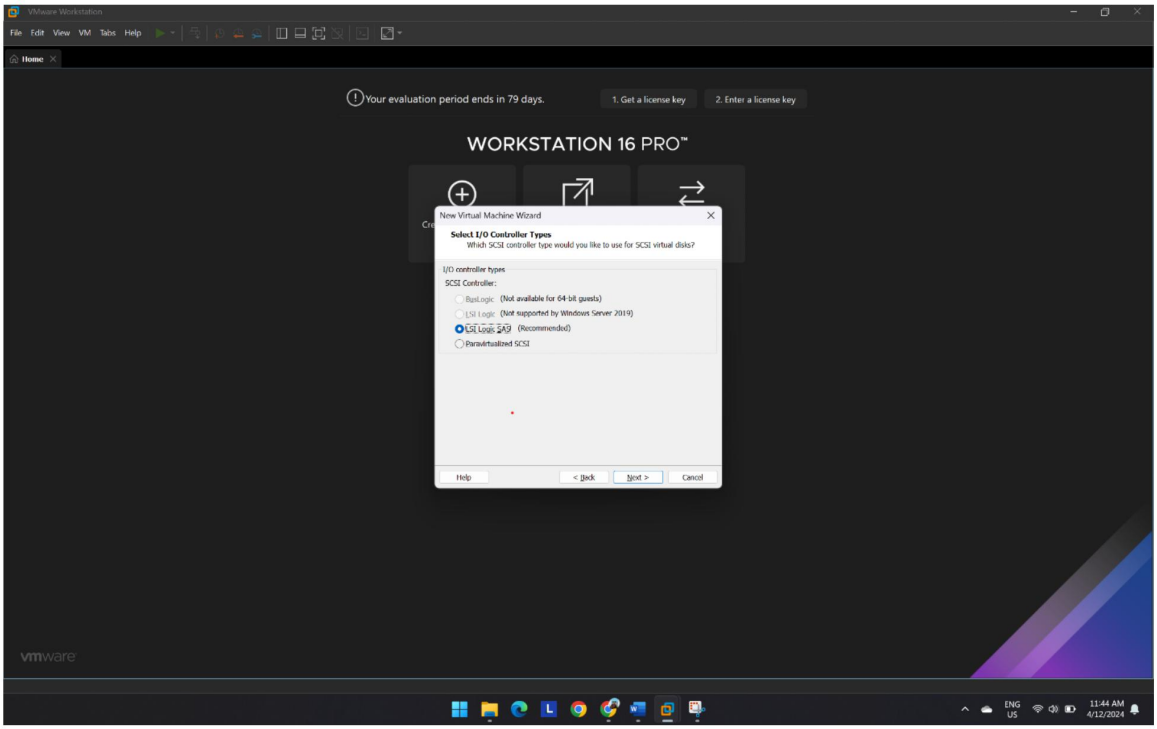


Figure 30
Select a Disk Type

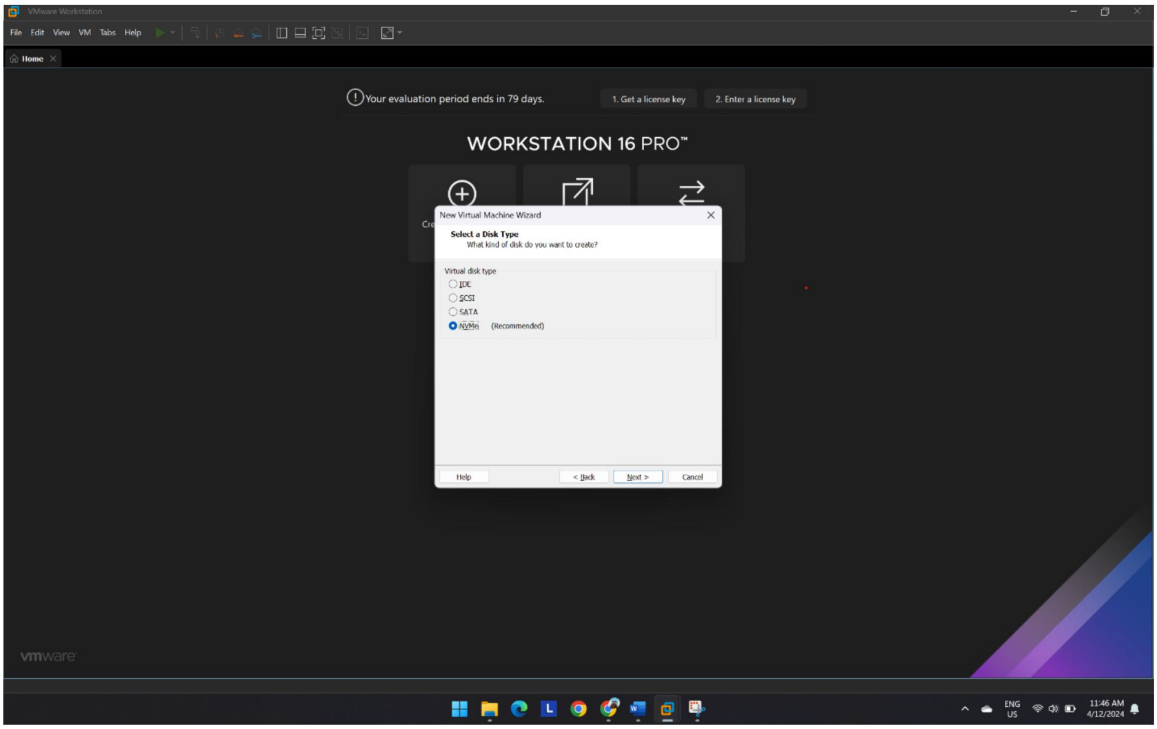


Figure 31
Click > Select a new Virtual disk > Next

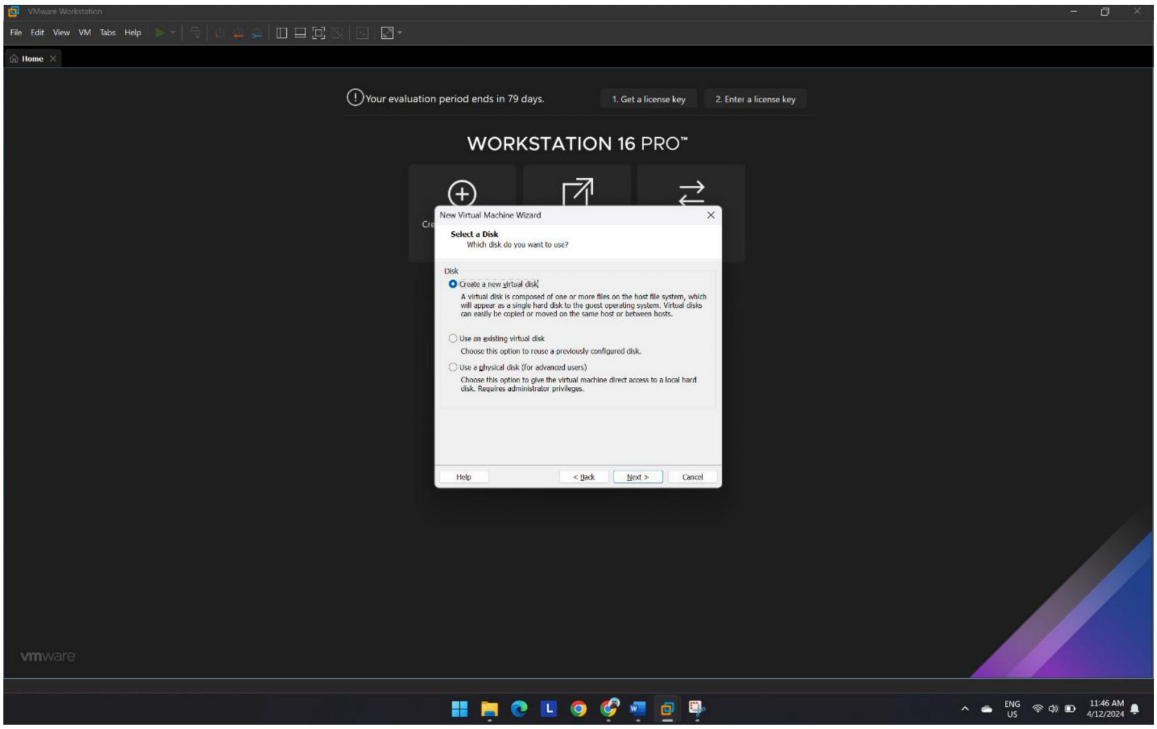


Figure 32
Specify Disk Capability

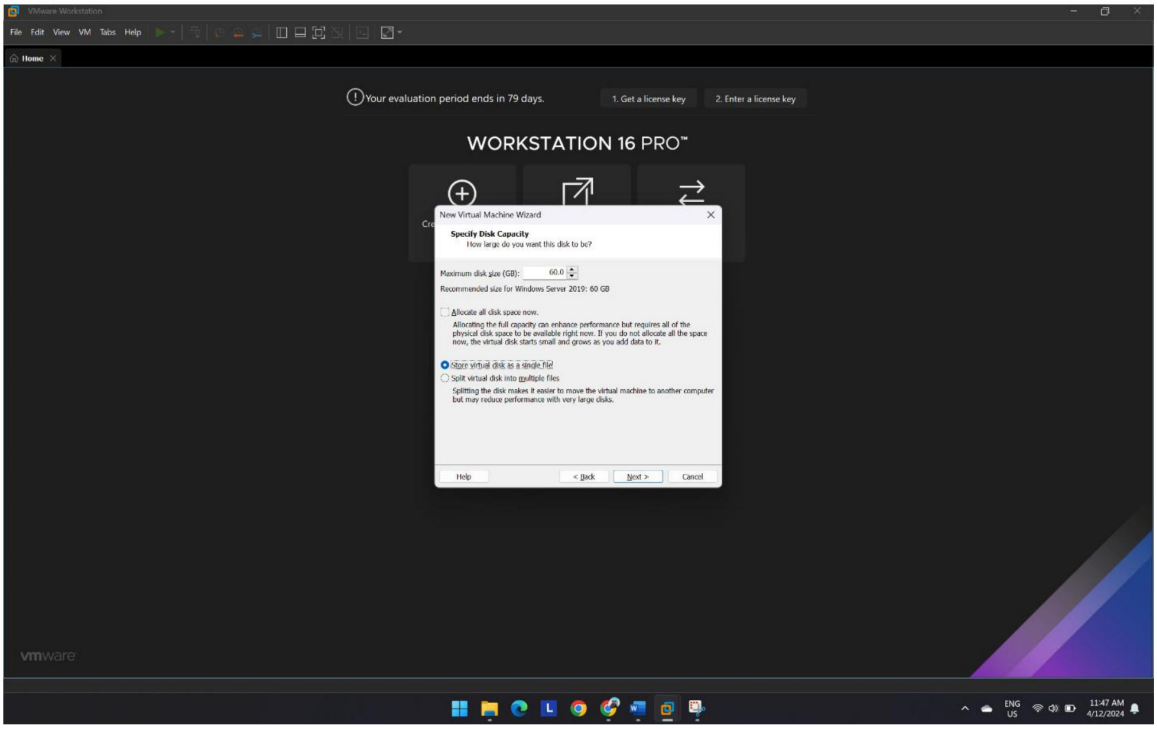


Figure 33
Specify the Disk File

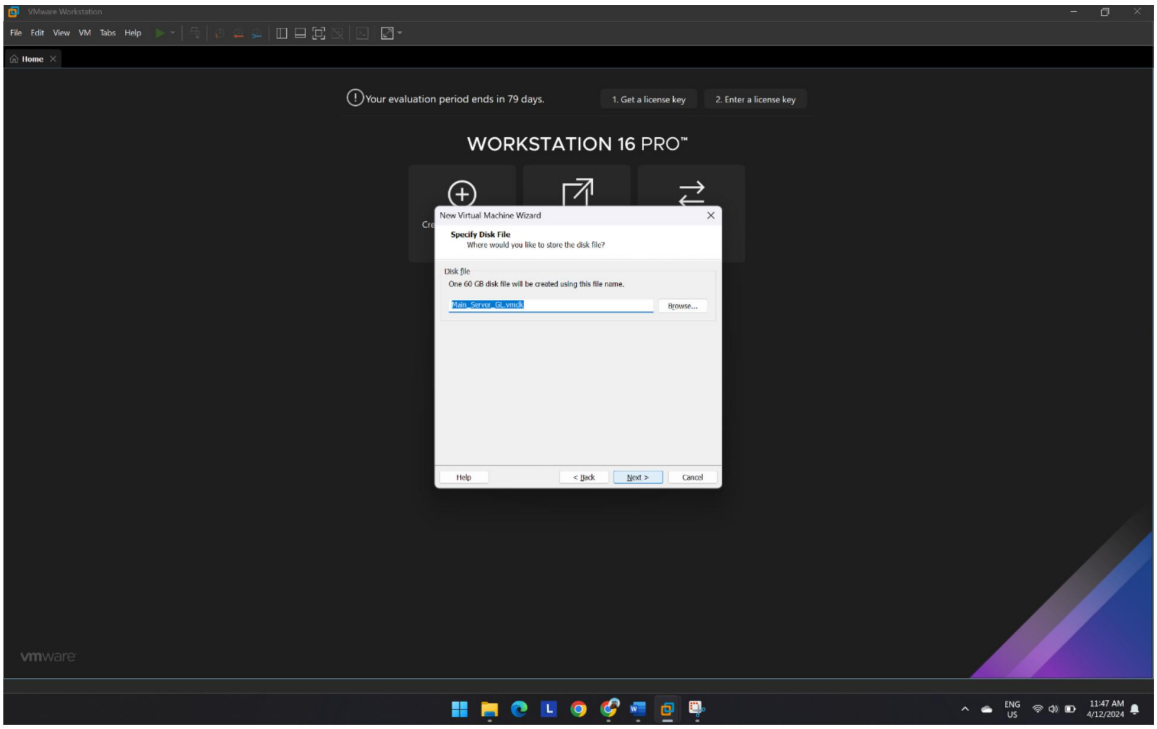


Figure 34
Add one more Network Adapter

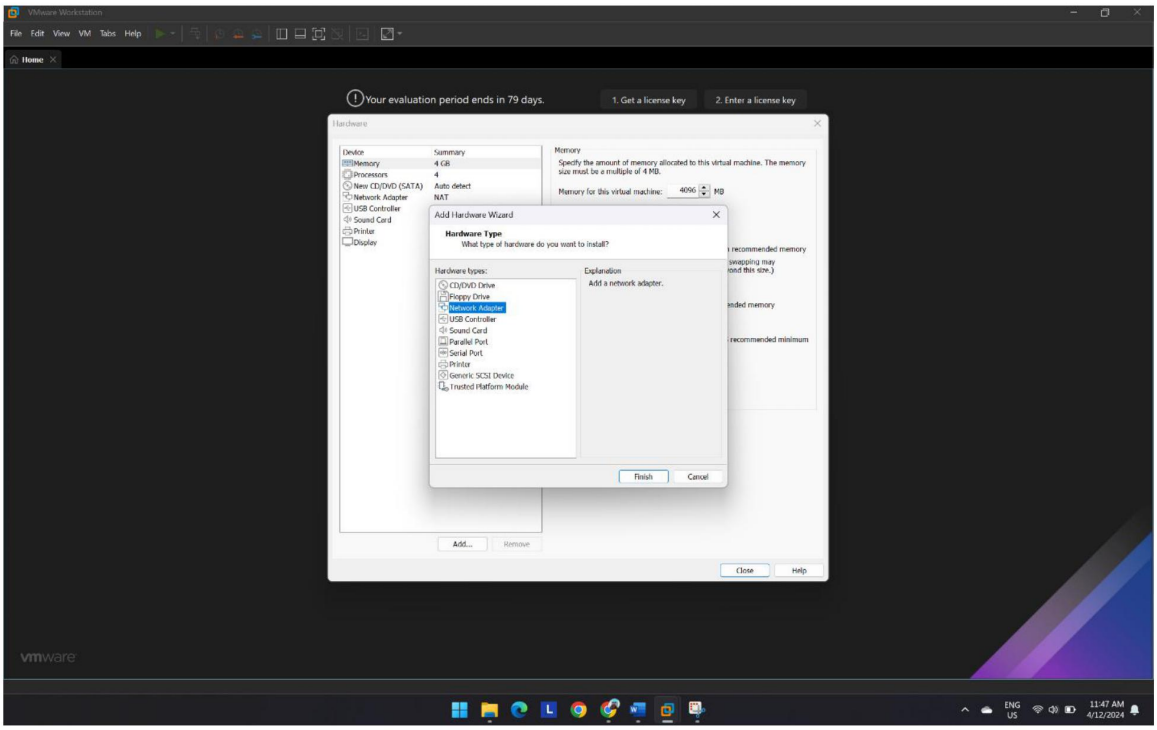


Figure 35
Select ISO image of Operating System.

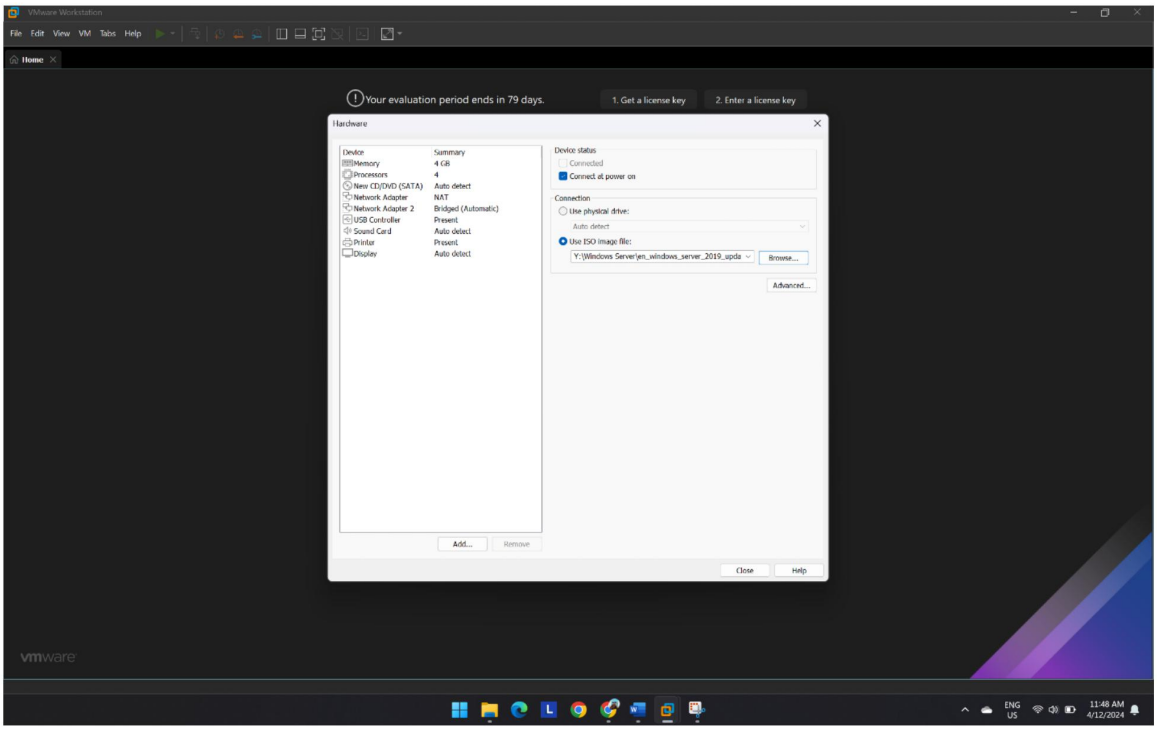


Figure 36
Finish the setup

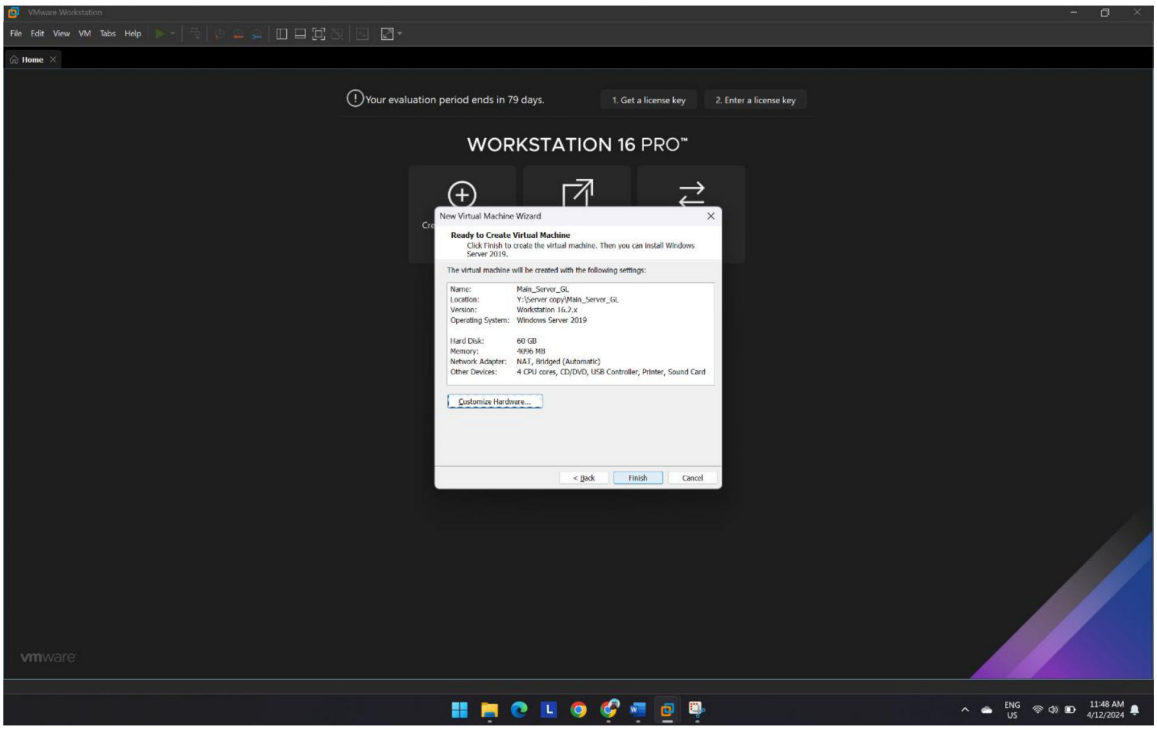


Figure 37
Run the Virtual Machine and Install Operating System

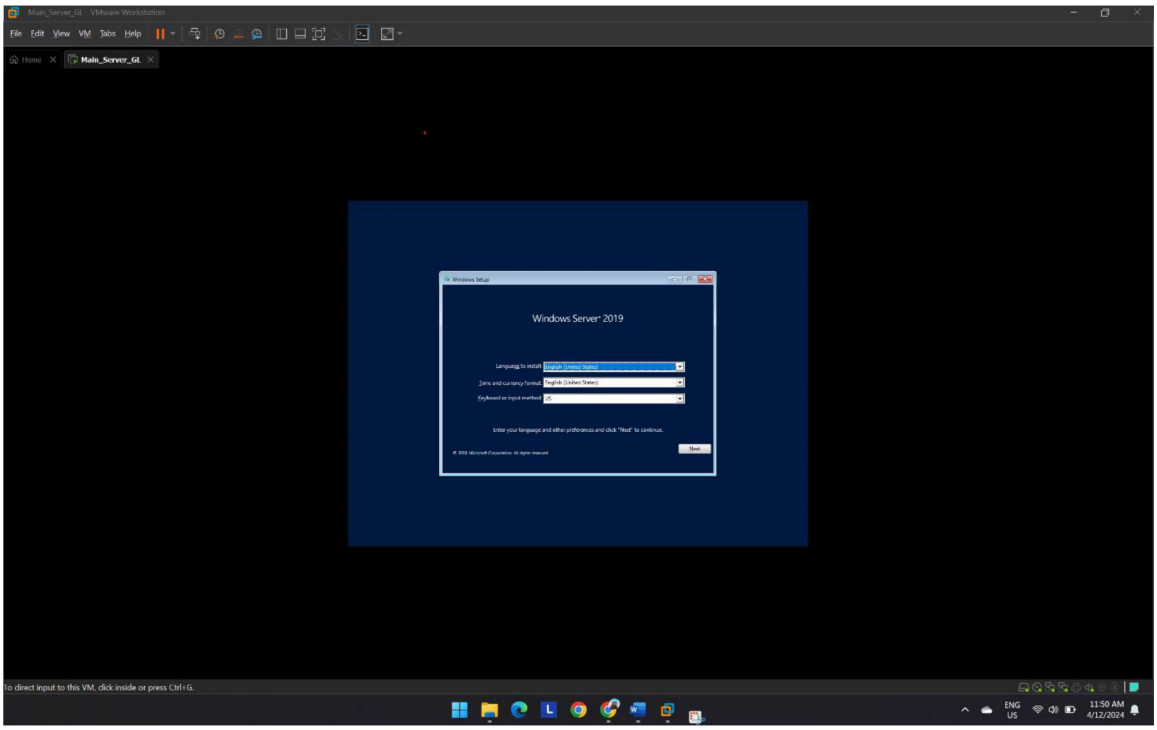


Figure 38
Click the type of Operating System (Windows server 2019 Datacenter – Desktop Version)

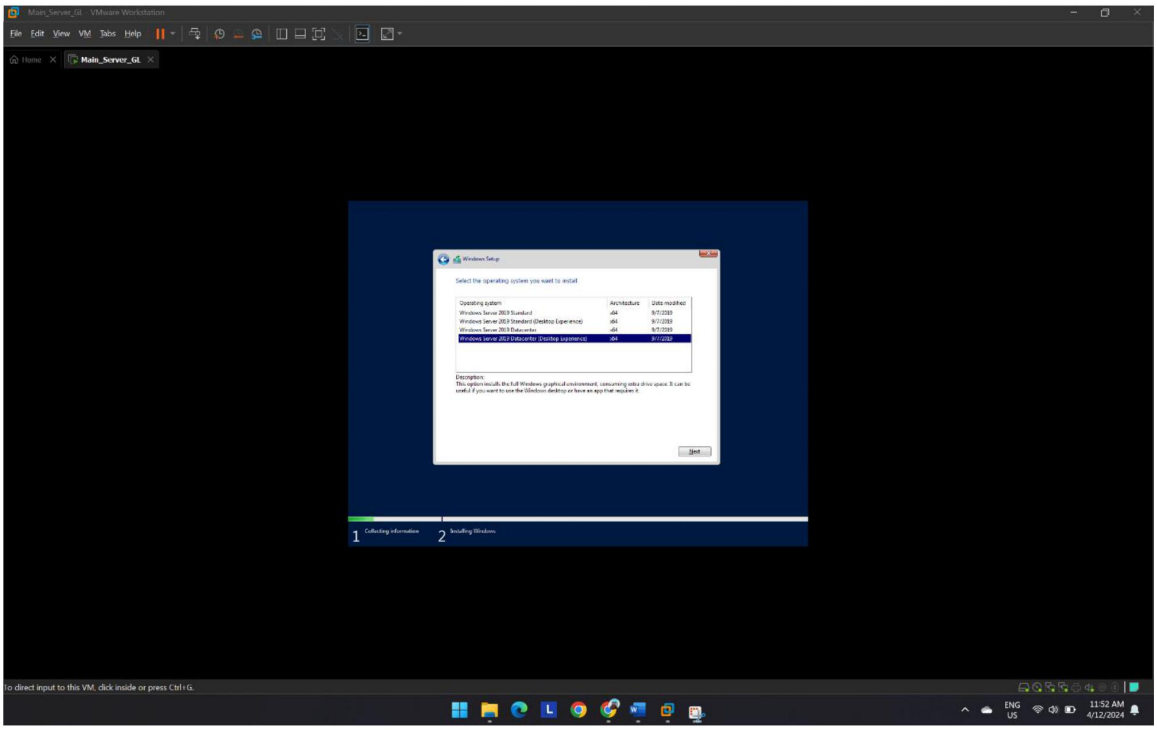


Figure 39
Click Custom Install Windows

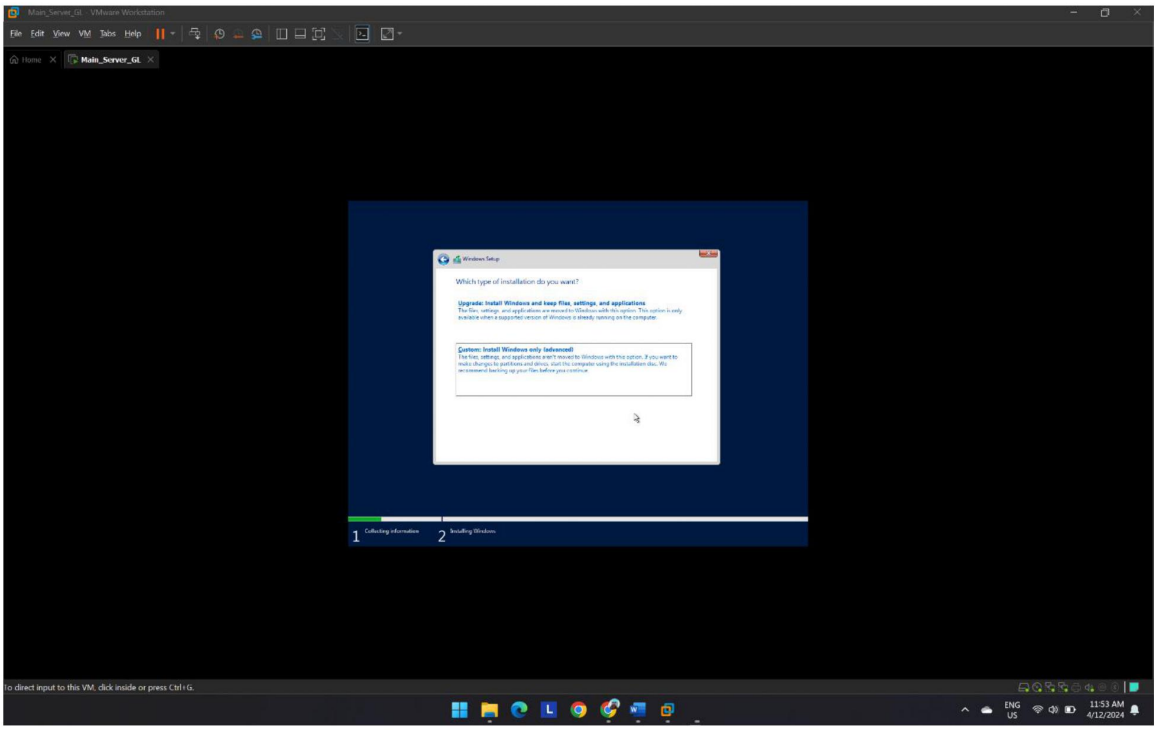


Figure 40
Click > Next

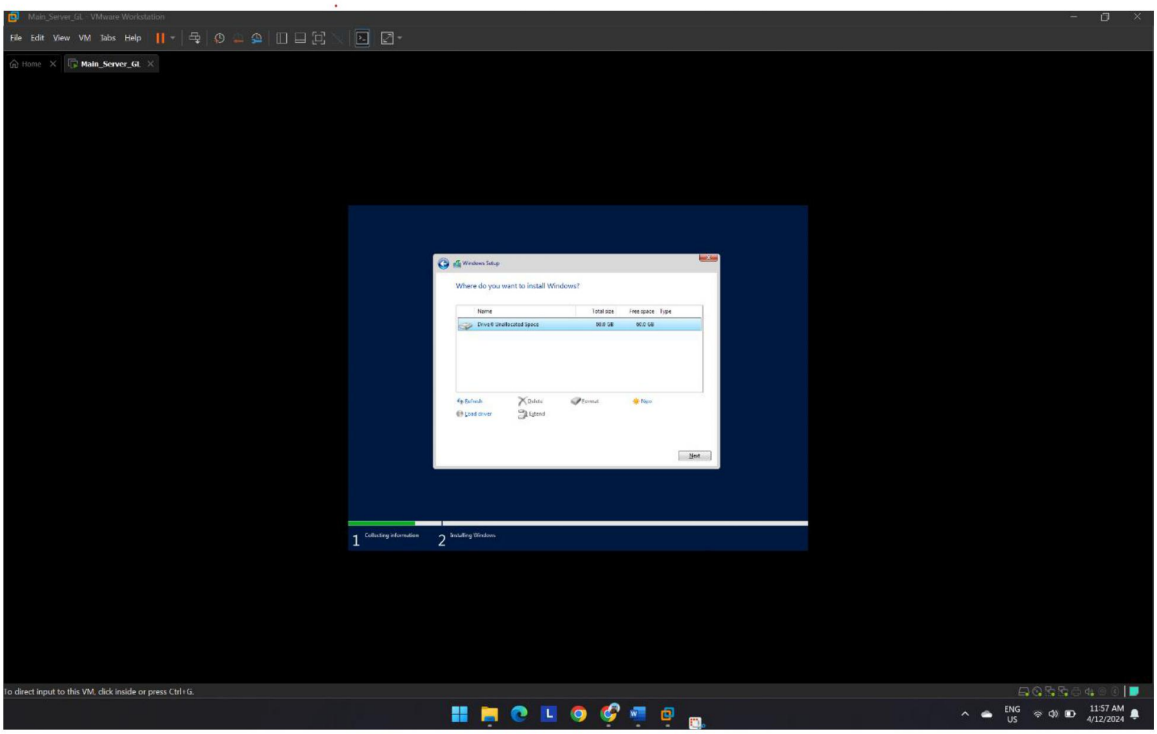


Figure 41
Wait for Installation to be completed.

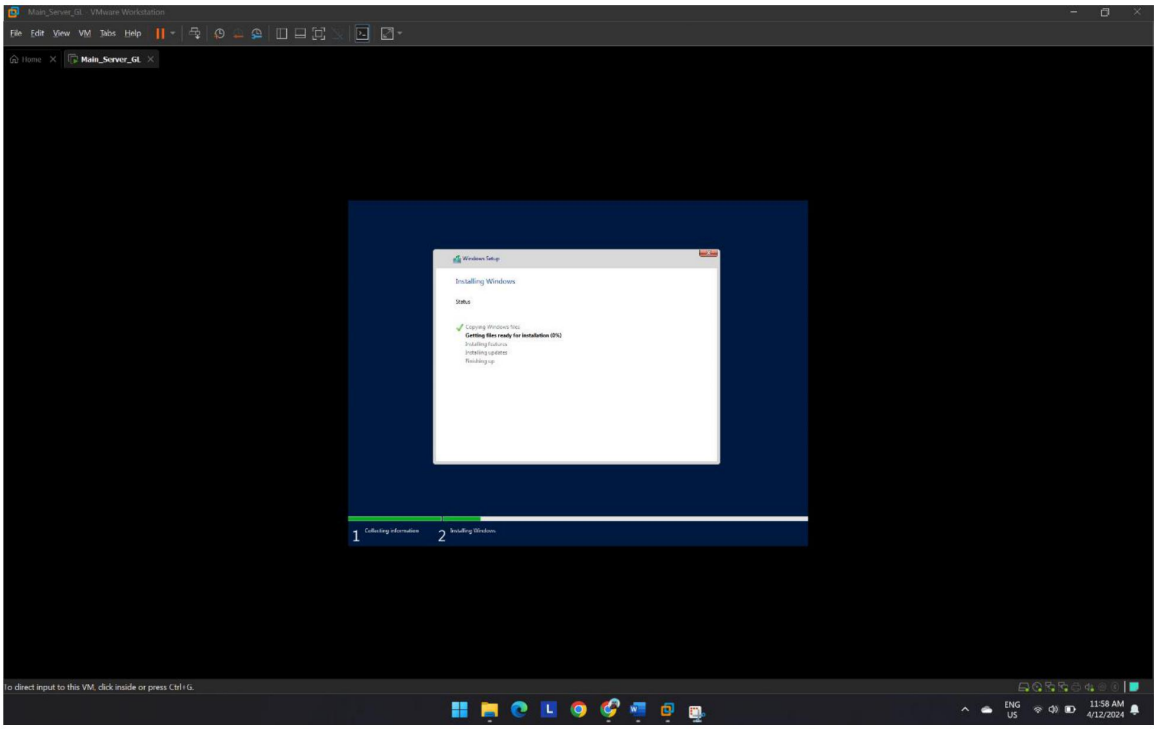


Figure 42
Create new password for Administrator account

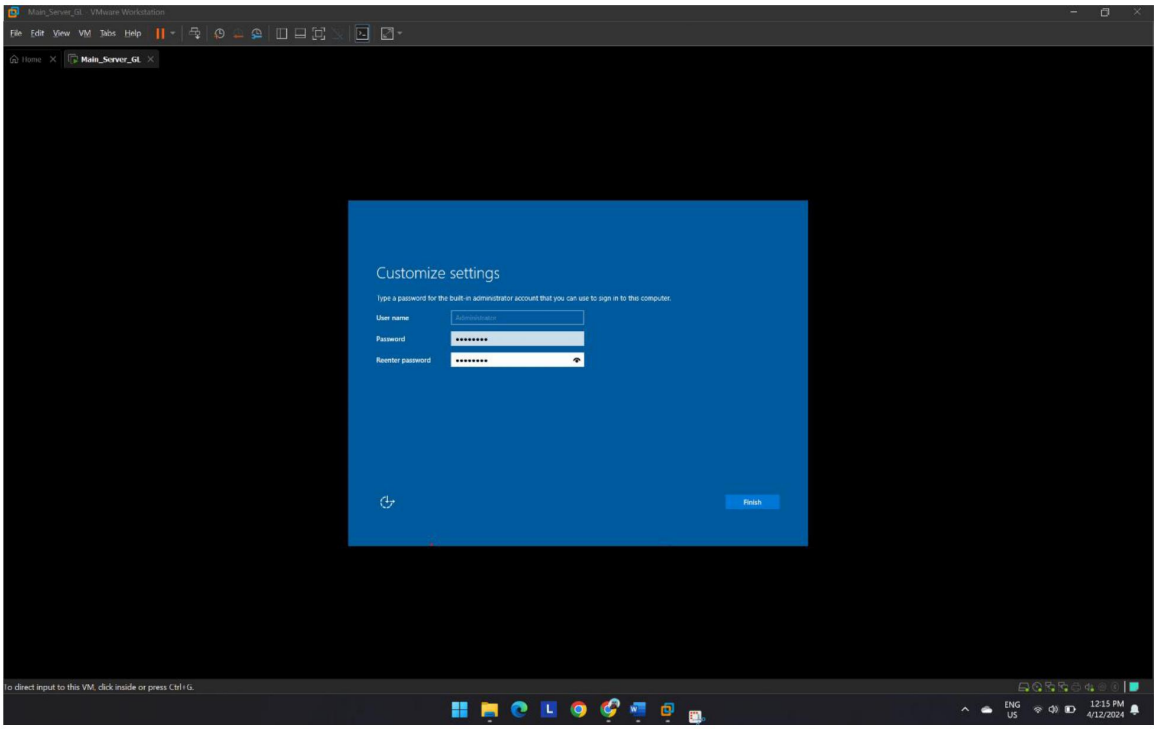


Figure 43
Click > Manage > Add Role and Features

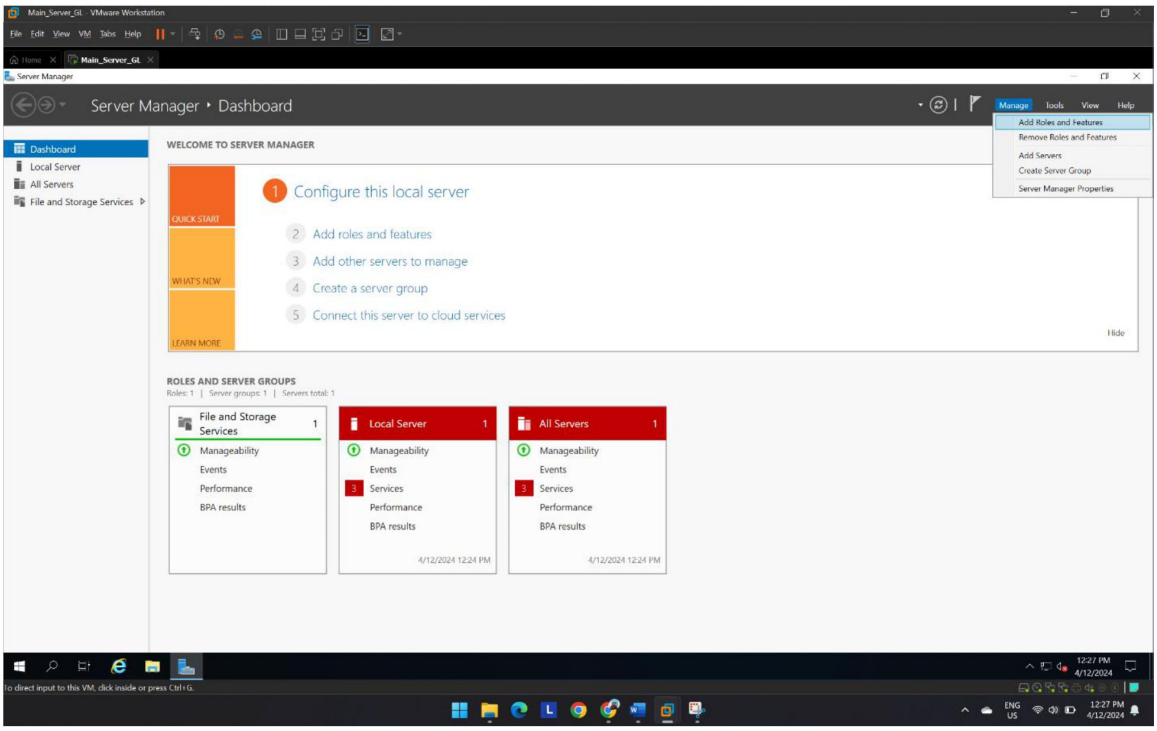


Figure 44
Click > Next

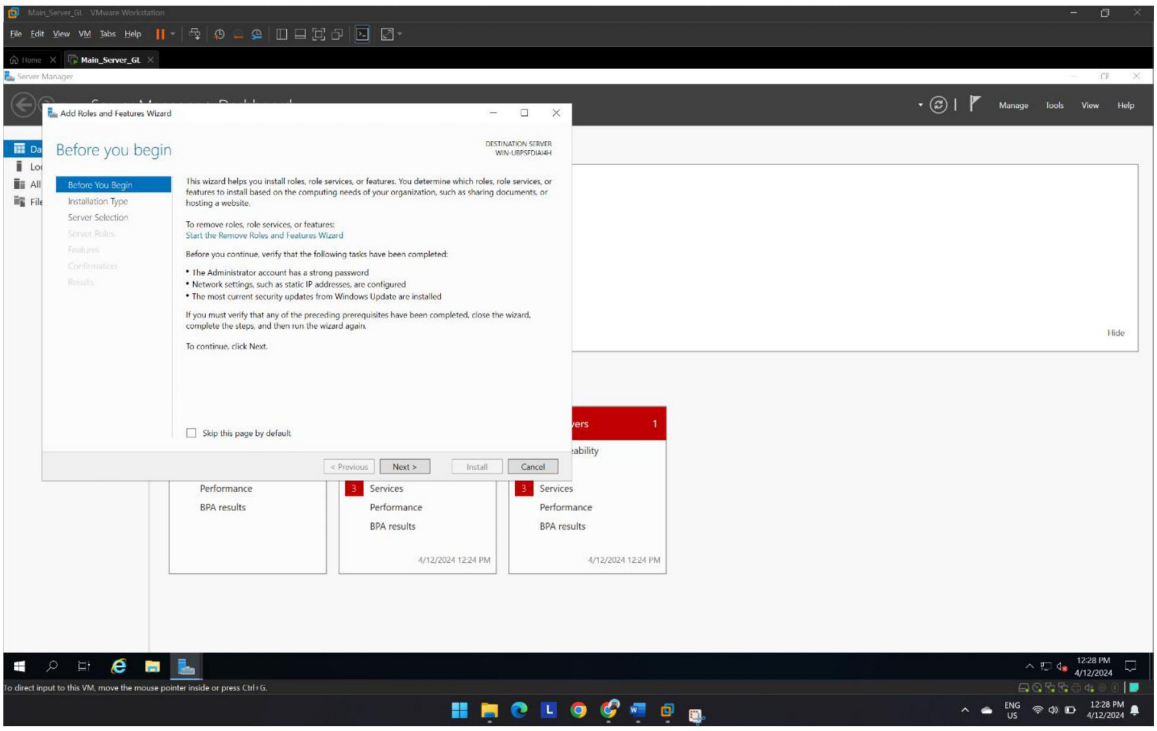


Figure 45
Click > Next

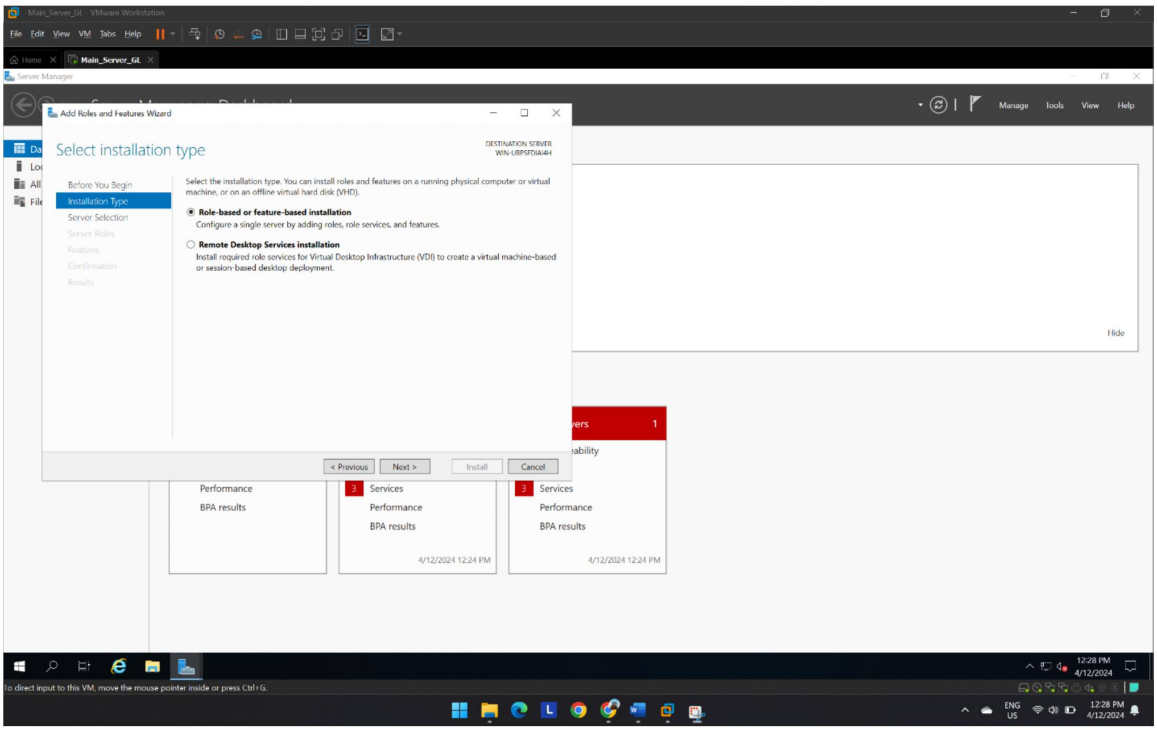
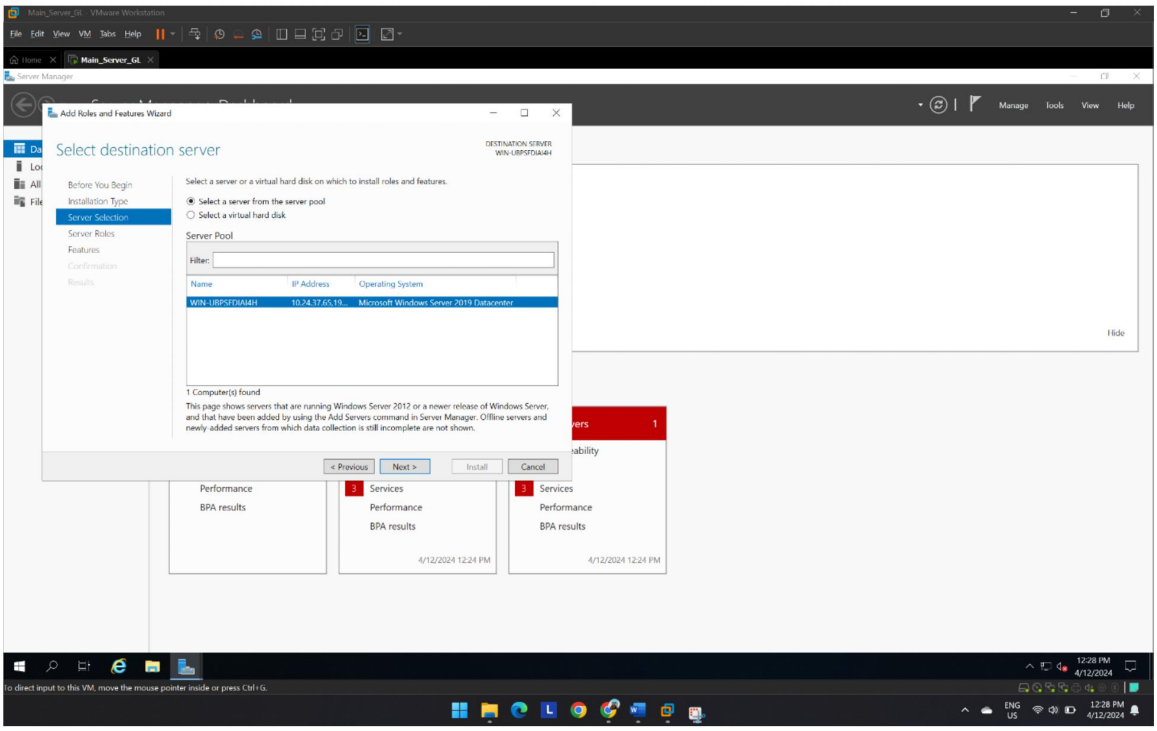


Figure 46
Click > Next.



6.1 Setting up Active Directory Server

Figure 47
Check Active Directory Domain Services and Add Feature

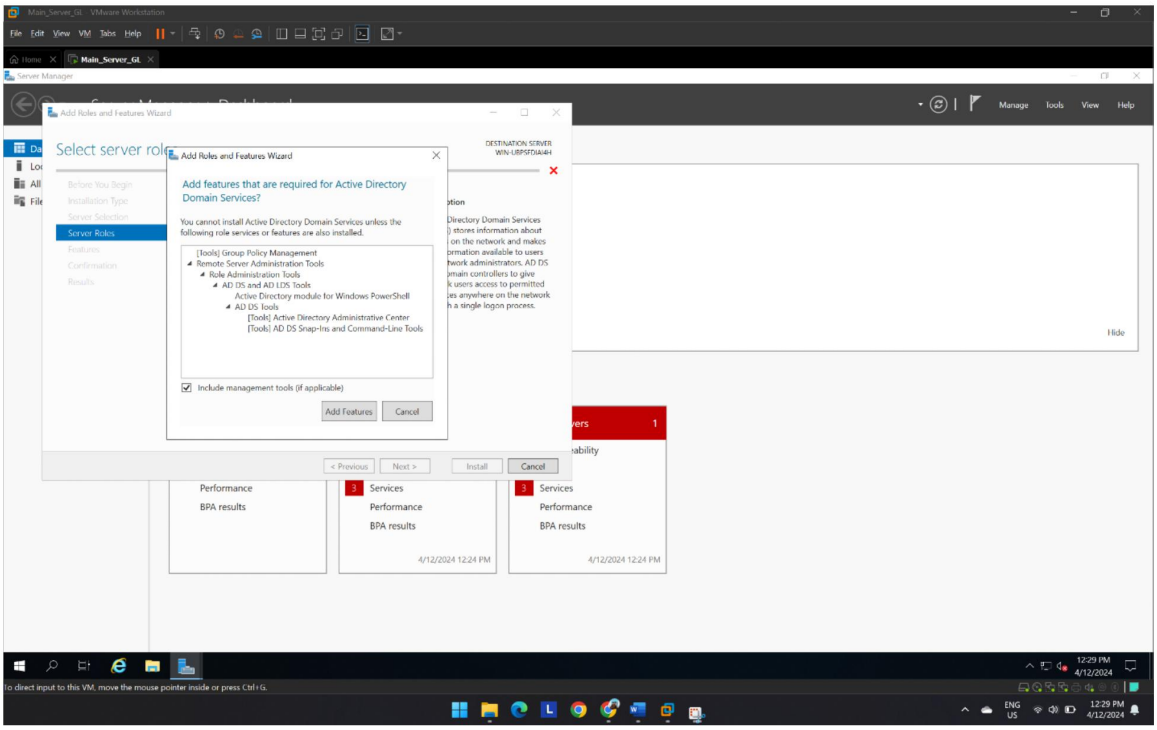


Figure 48
Click > Next

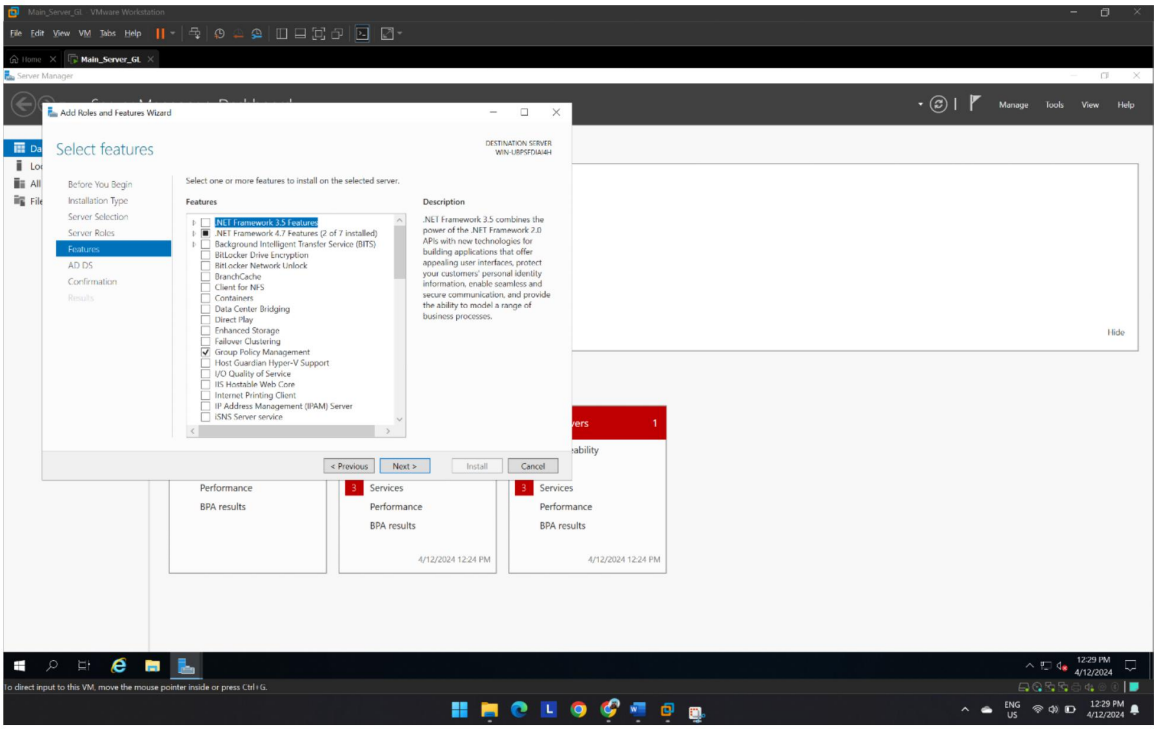


Figure 49
Click > Next

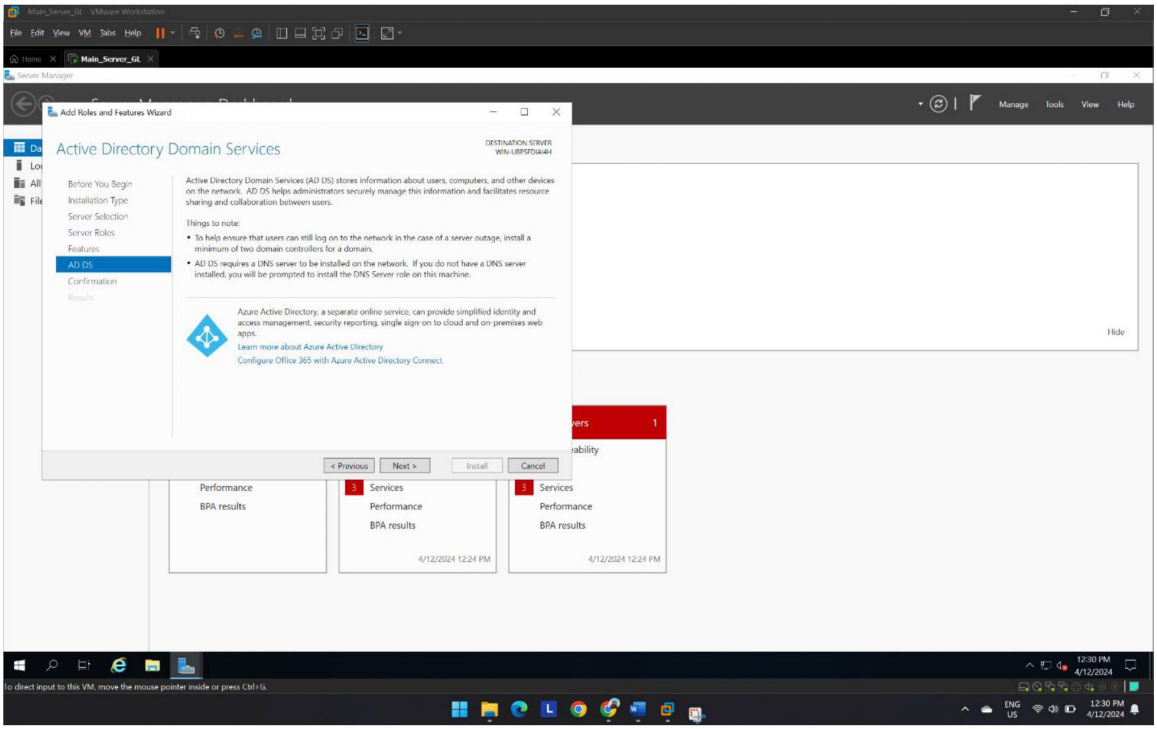


Figure 50
Click > Install

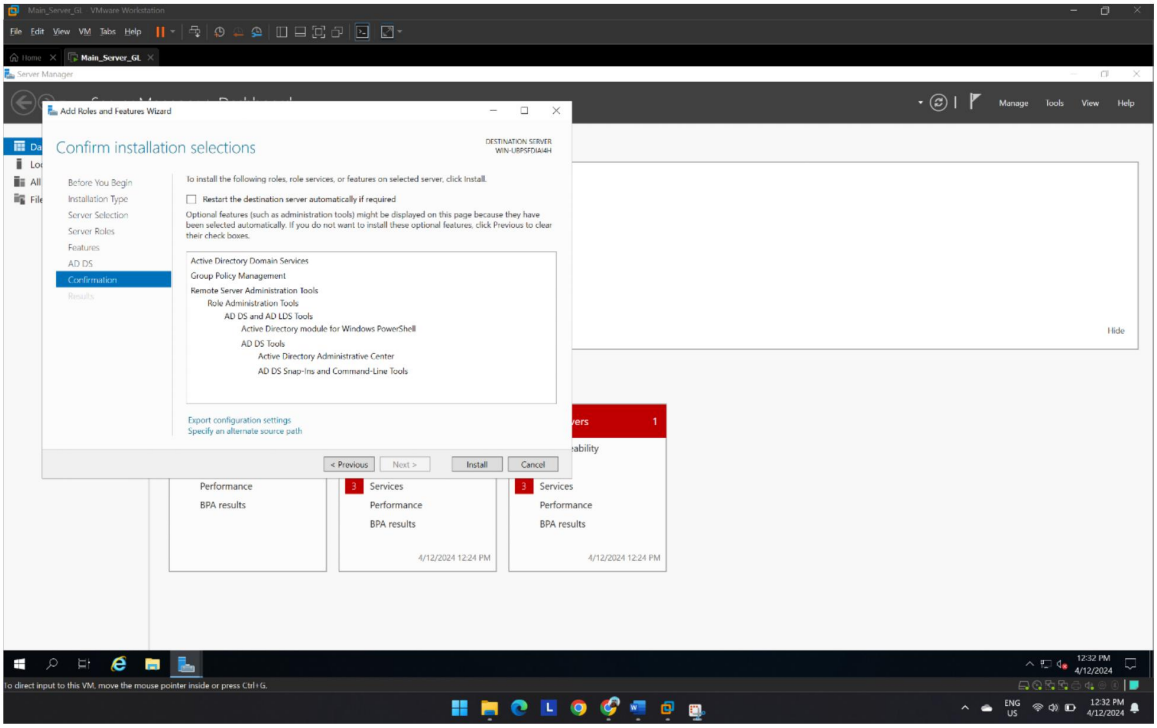


Figure 51
Once Installation is completed close the window**.**

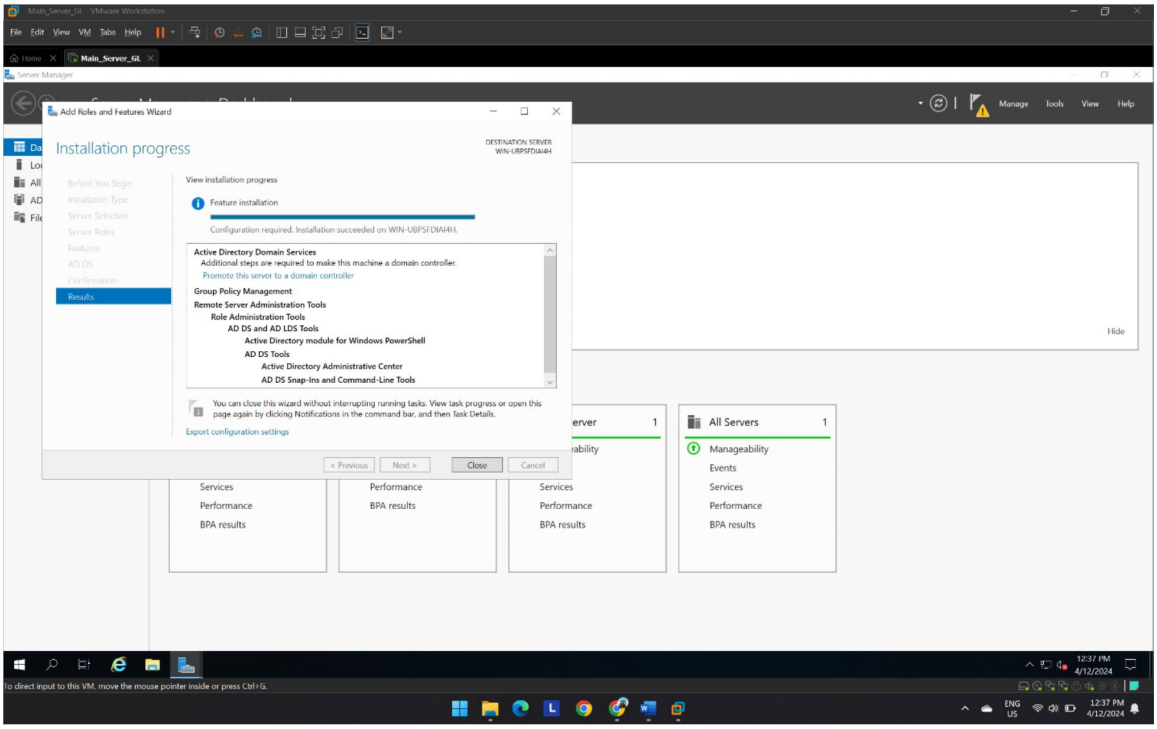


Figure 52
Setup a new forest (nlh.com)

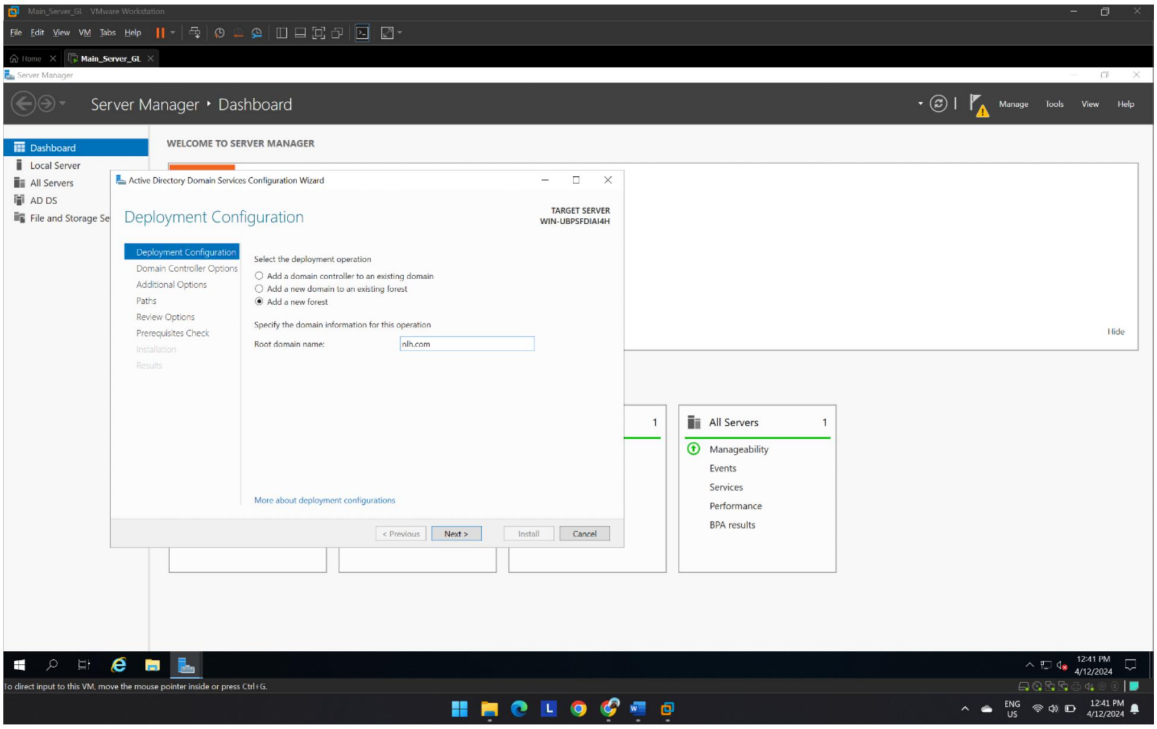


Figure 53
Add Password.

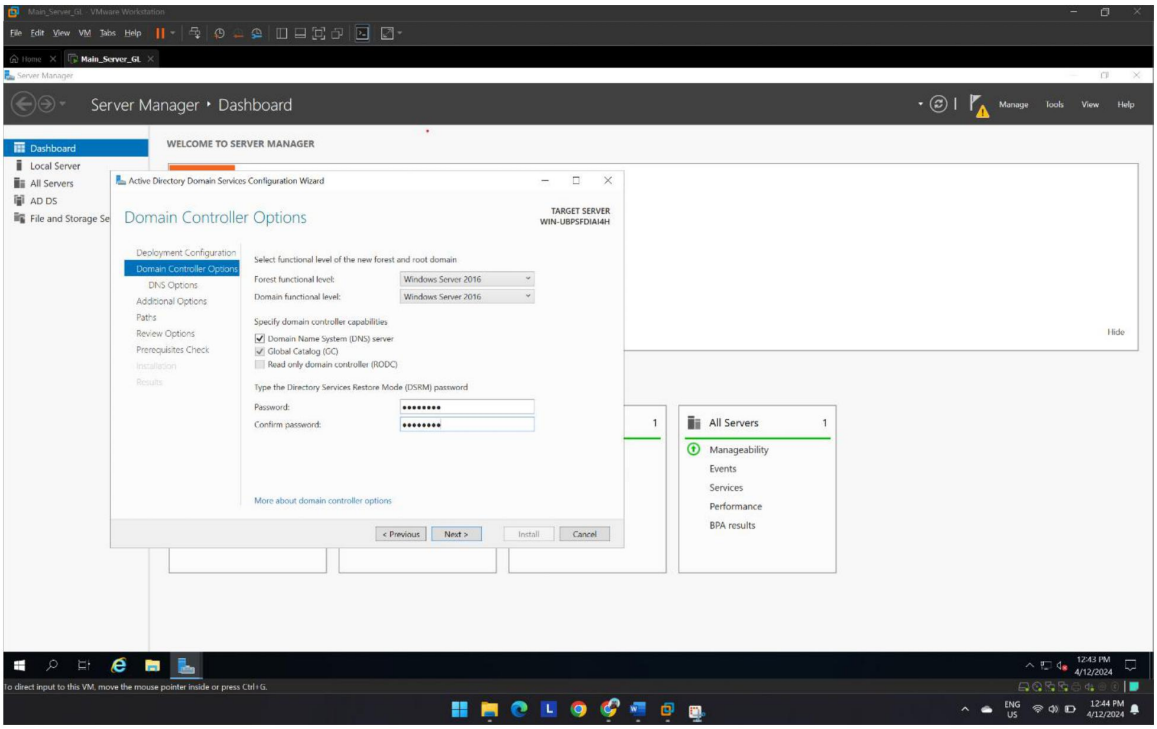


Figure 54
Click > Next

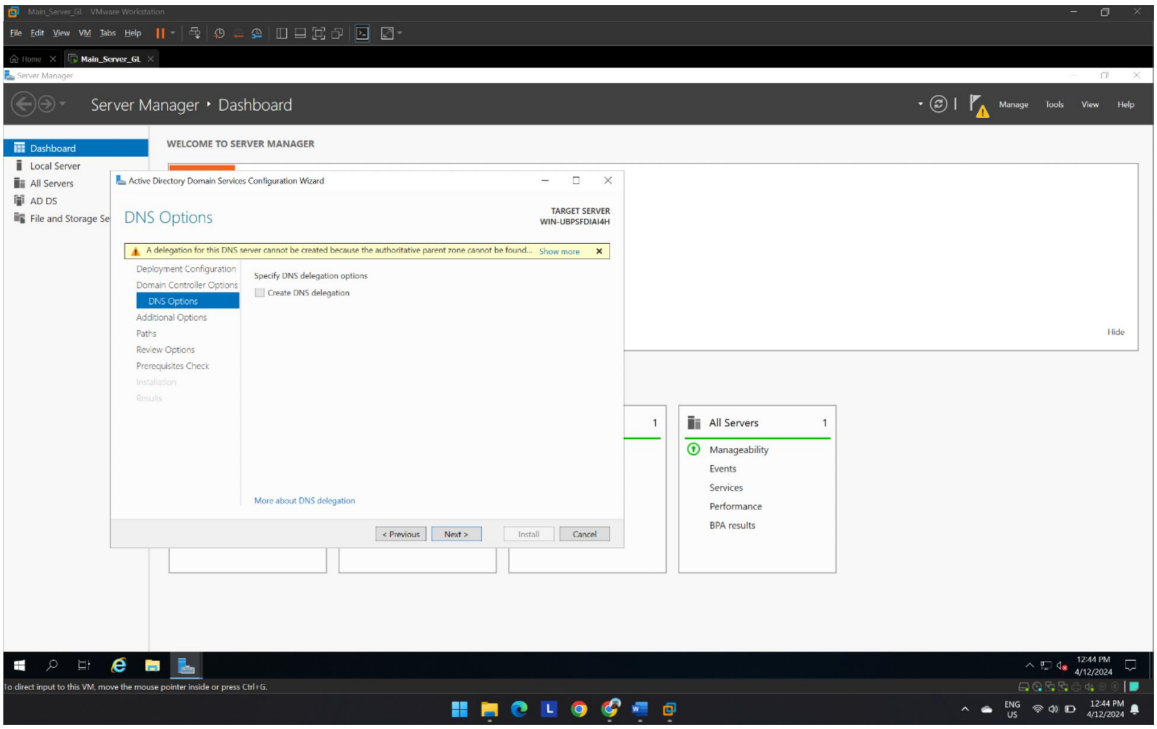


Figure 55
Click > Next

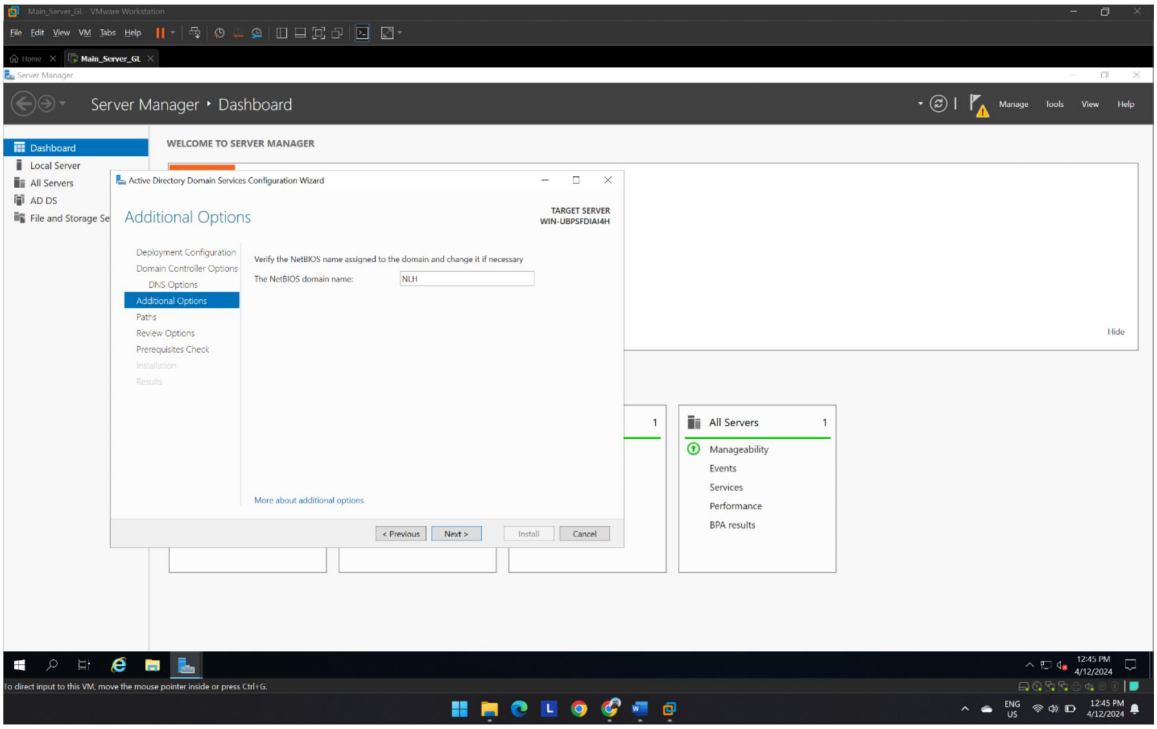


Figure 56
Click > Next

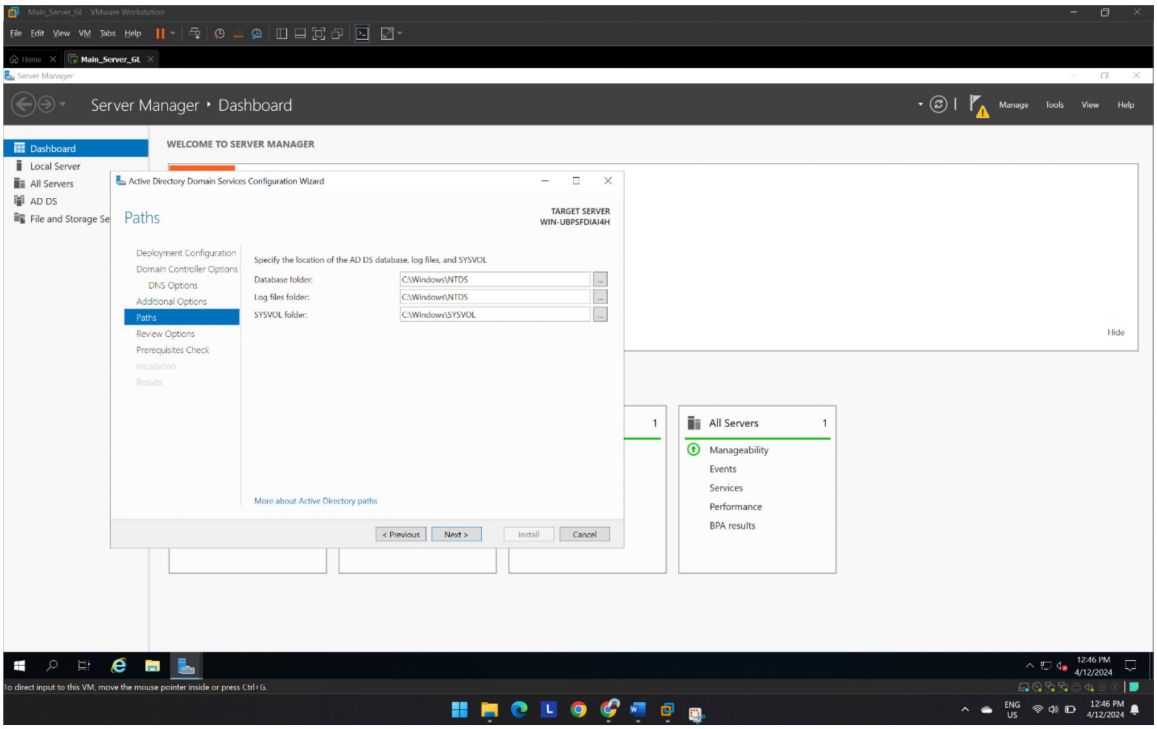


Figure 57
Click > Next

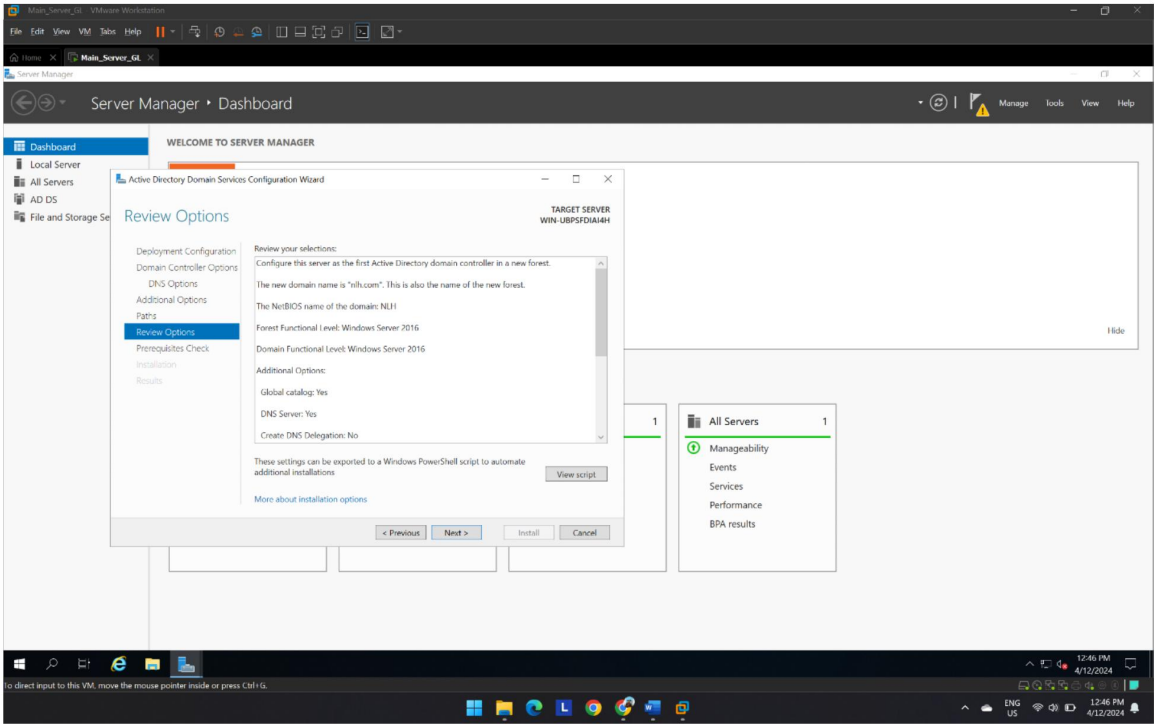


Figure 58
Once prerequisite are checked click install

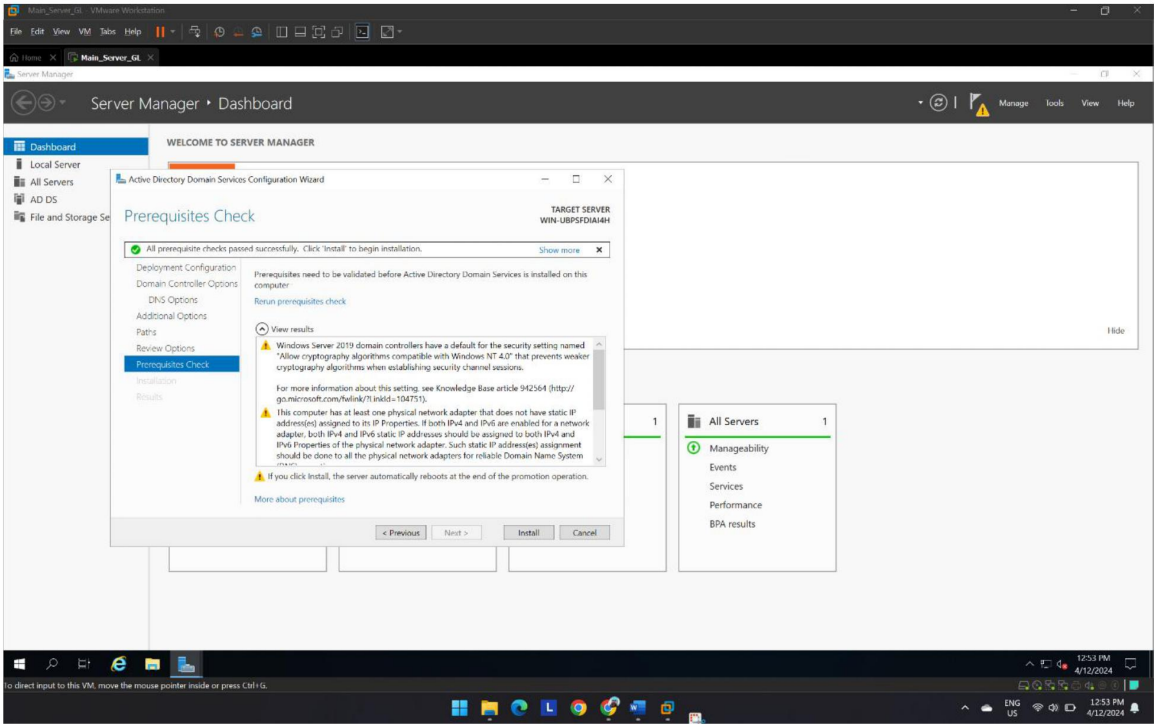
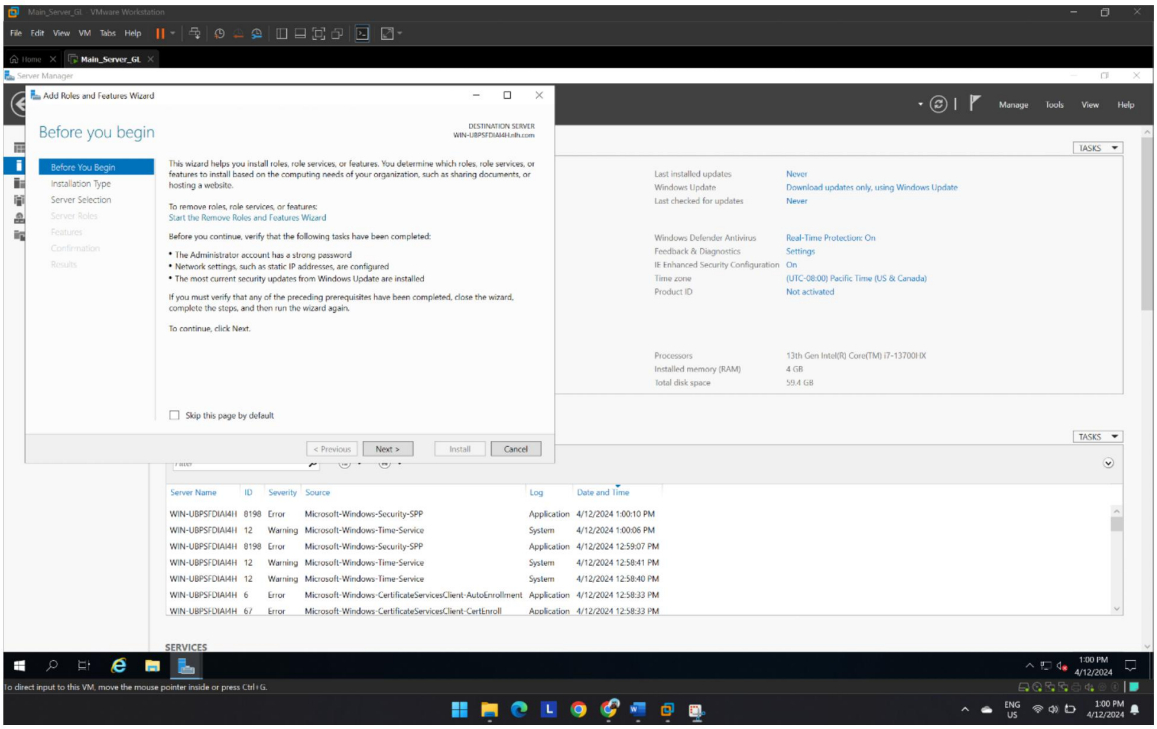


Figure 59


Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
To remove roles, role services, or features:
Start the Remove Roles and Features Wizard
Before you continue, verify that the following tasks have been completed:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The most current security updates from Windows Update are installed
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel
Manage
Tools
View
Help
TASKS
Last installed updates
Never
Windows Update
Download updates only, using Windows Update
Last checked for updates
Never
Windows Defender Antivirus
Real-Time Protection: On
Feedback & Diagnostics
Settings
IE Enhanced Security Configuration
On
Time zone
(UTC-08:00) Pacific Time (US & Canada)
Product ID
Not activated
Processors
13th Gen Intel(R) Core(TM) i7-13700H
Installed memory (RAM)
4 GB
Total disk space
59.4 GB
Server Name
ID
Severity
Source
Log
Date and Time
WIN-UBPSFDIAI4H 8198 Error Microsoft-Windows-Security-SPP Application 4/12/2024 1:00:10 PM
WIN-UBPSFDIAI4H 12 Warning Microsoft-Windows-Time-Service System 4/12/2024 1:00:06 PM
WIN-UBPSFDIAI4H 8198 Error Microsoft-Windows-Security-SPP Application 4/12/2024 12:59:07 PM
WIN-UBPSFDIAI4H 12 Warning Microsoft-Windows-Time-Service System 4/12/2024 12:58:41 PM
WIN-UBPSFDIAI4H 12 Warning Microsoft-Windows-Time-Service System 4/12/2024 12:58:40 PM
WIN-UBPSFDIAI4H 6 Error Microsoft-Windows-CertificateServicesClient-AutoEnrollment Application 4/12/2024 12:58:33 PM
WIN-UBPSFDIAI4H 67 Error Microsoft-Windows-CertificateServicesClient-CertEnroll Application 4/12/2024 12:58:33 PM
SERVICES
1:00 PM
4/12/2024

6.2 Setting up DHCP Server

Figure 60
Add DHCP Server

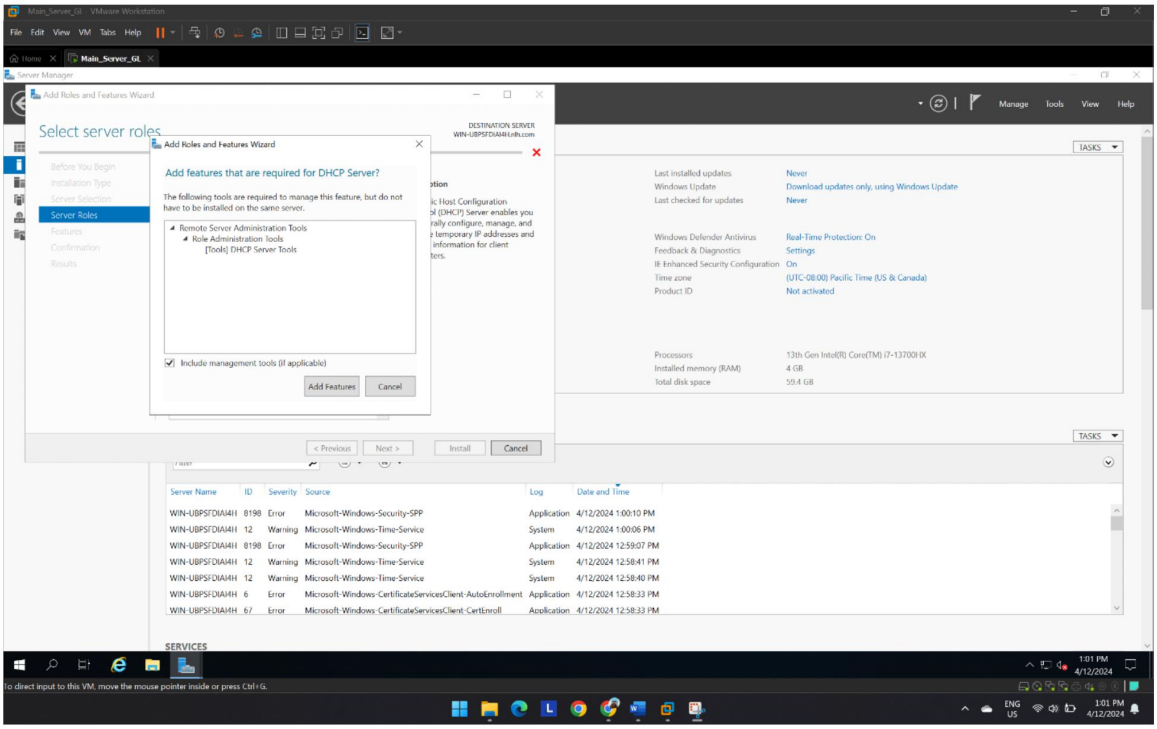


Figure 61
Add IIS service

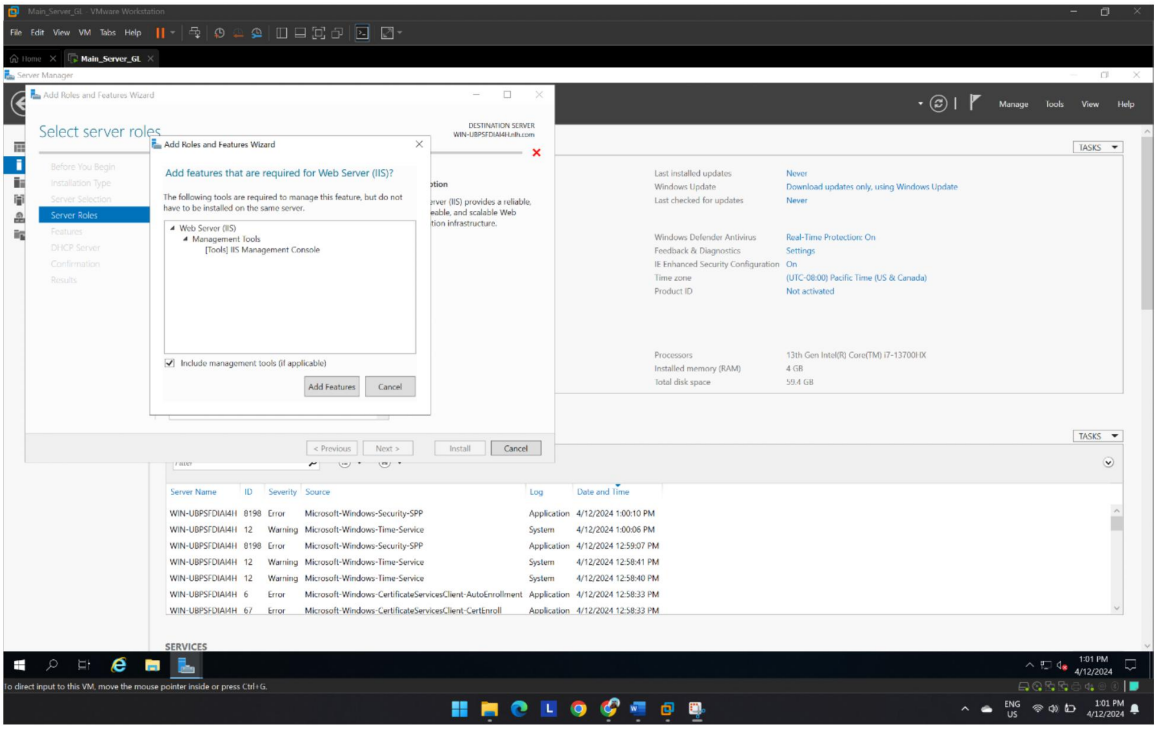


Figure 62
Click > Next

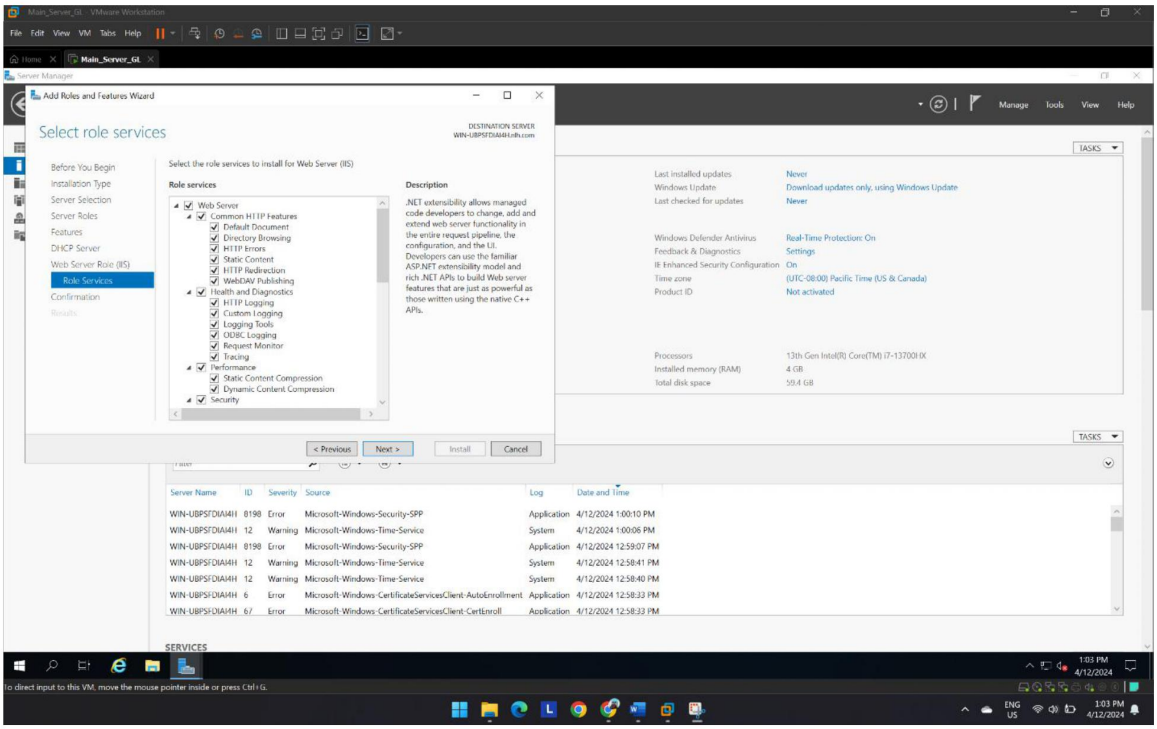


Figure 63
Close the window once DHCP and IIS are installed

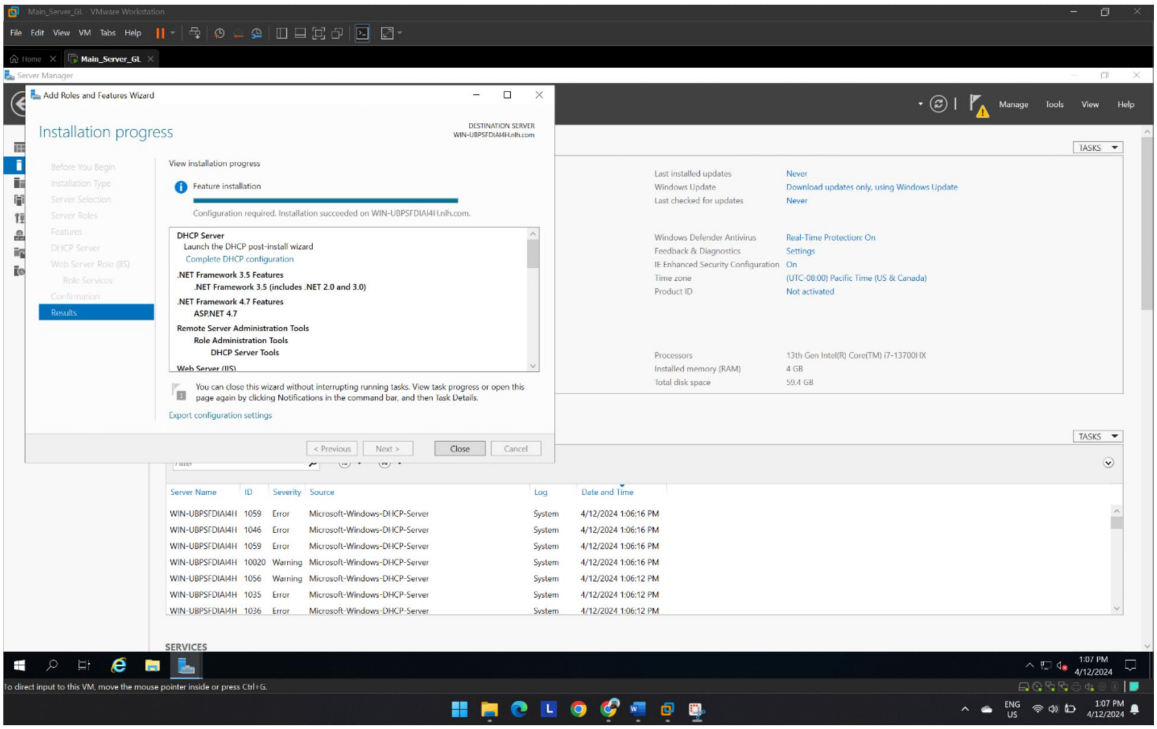


Figure 64
Configure the DHCP server

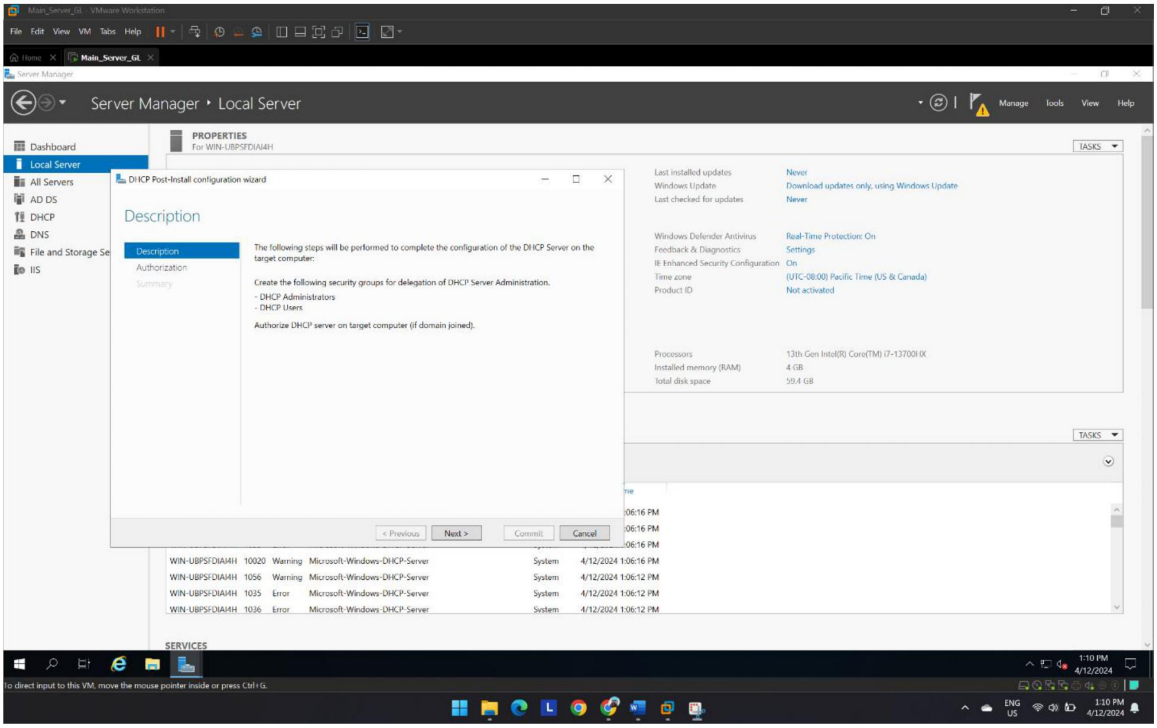


Figure 65
Authorize DHCP server for NLH domain

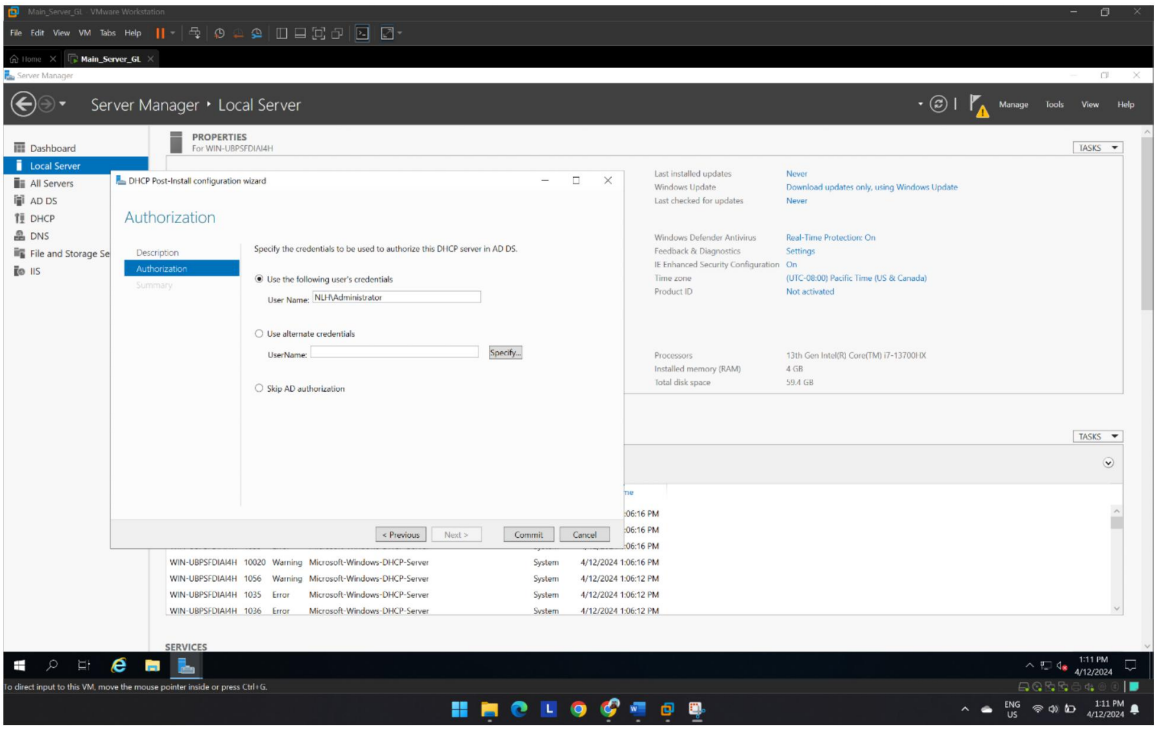


Figure 66
Close the Window

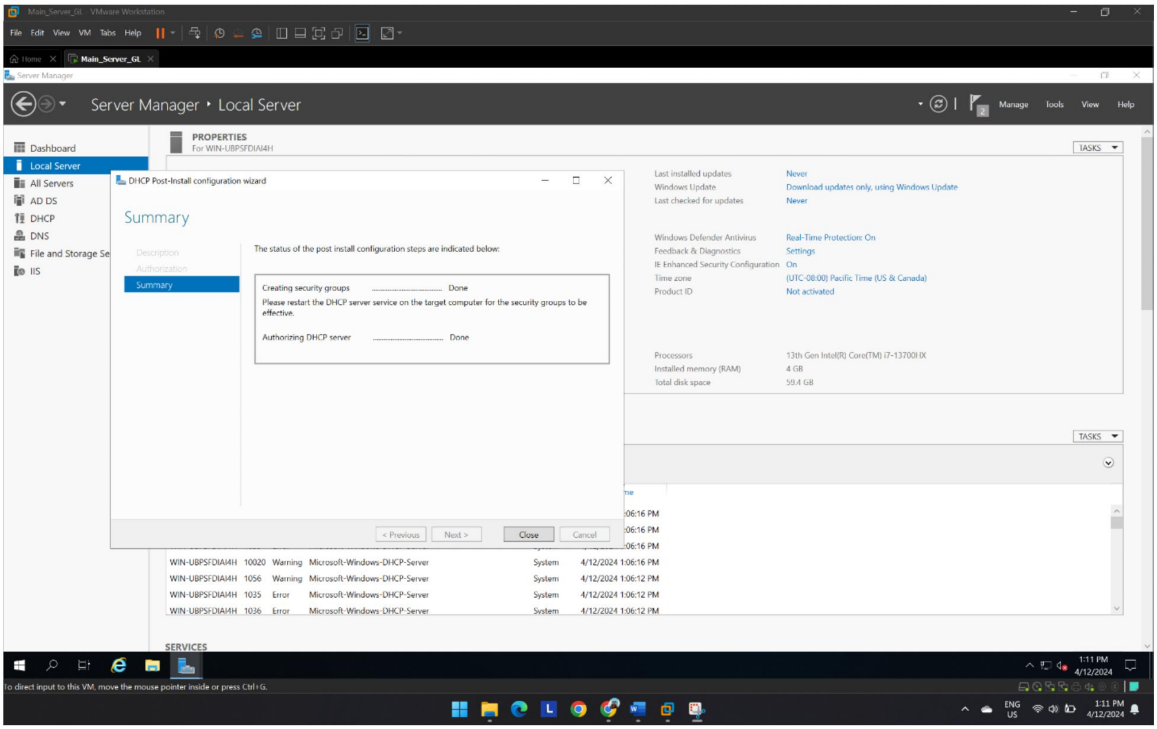


Figure 67
Open DHCP tool and add new scope for IPV4

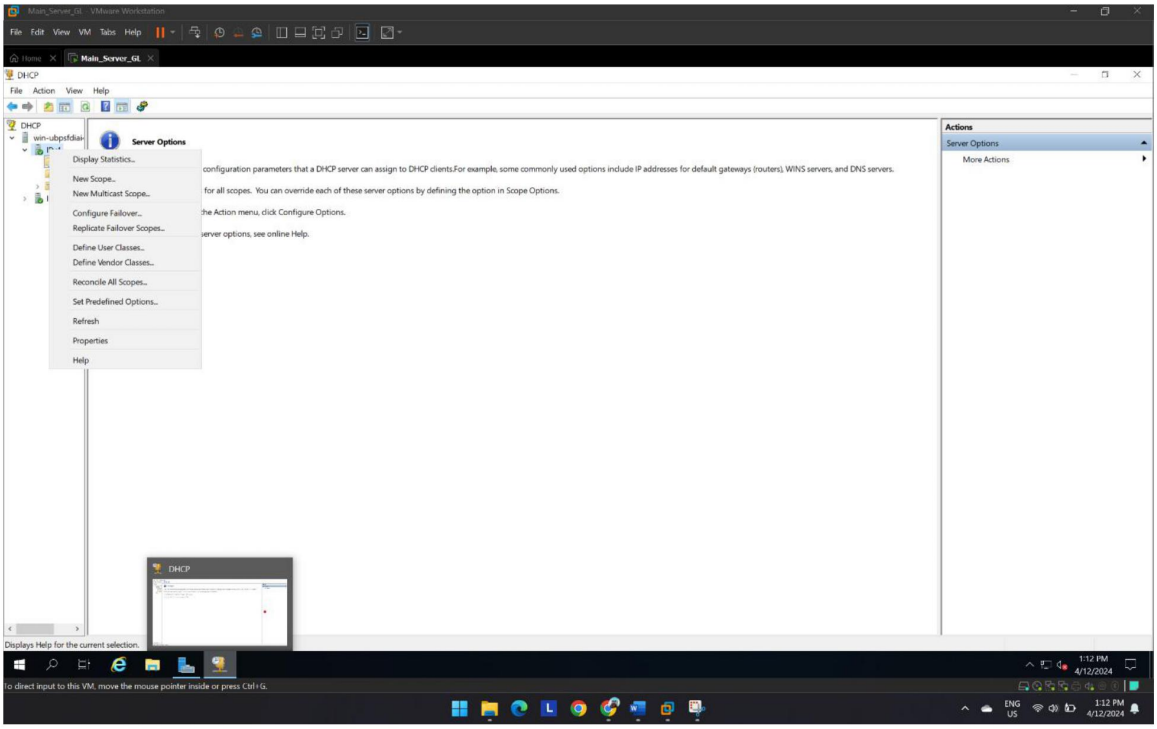


Figure 68
Name the New Scope “VLAN 10”

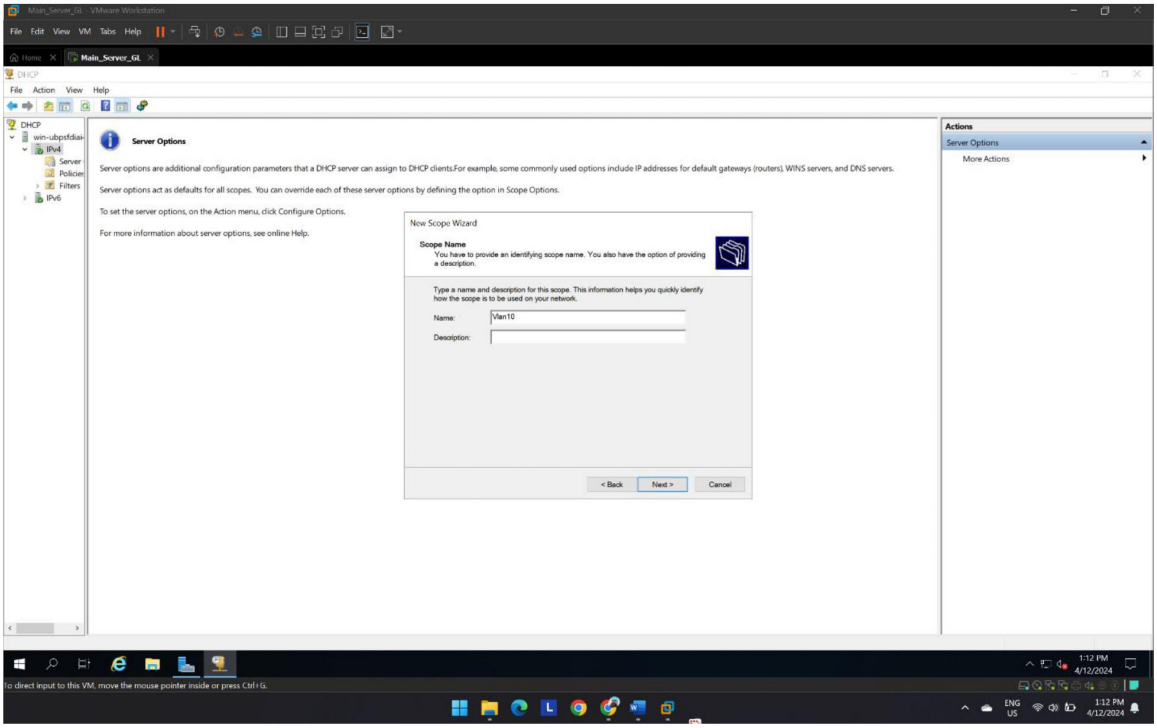


Figure 69
Add IP address Range to the Scope

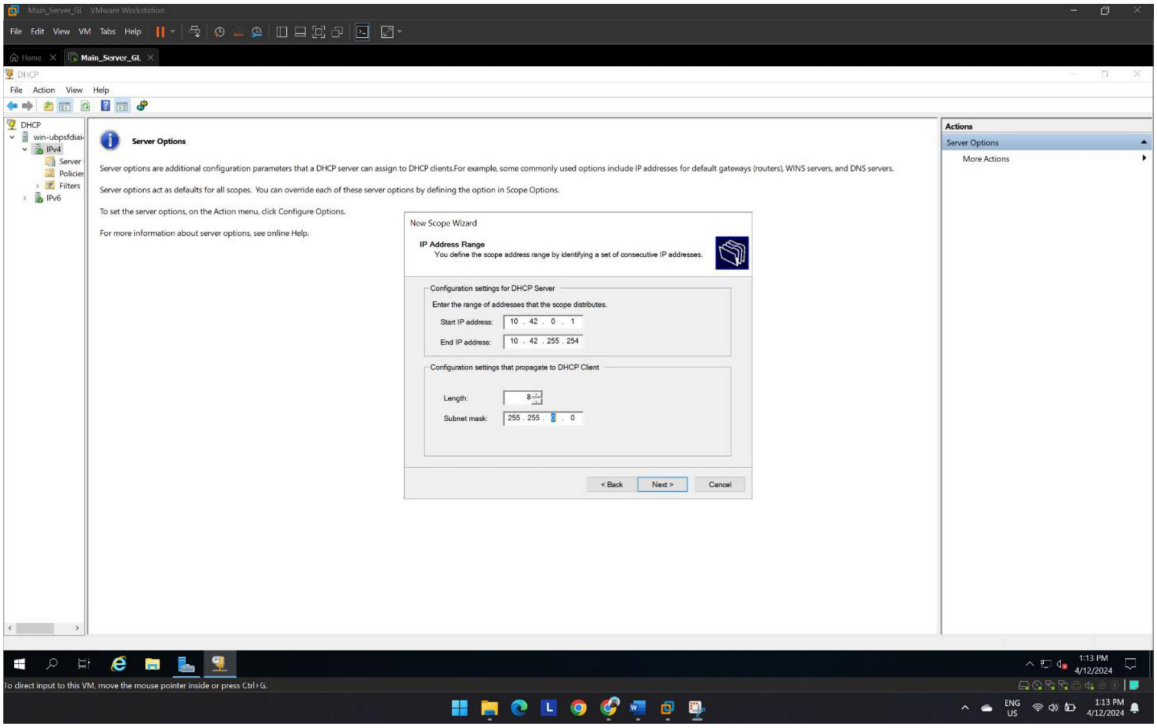


Figure 70
Exclude IP address range form the scope

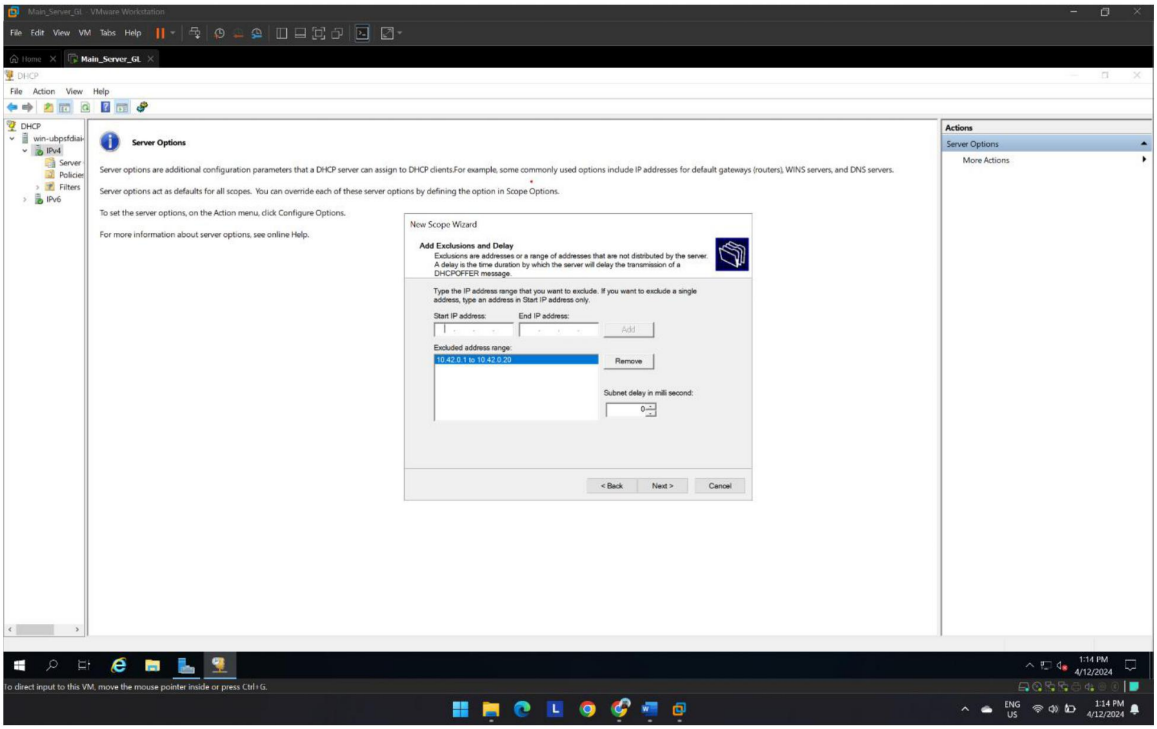


Figure 71
Add IP address for default Router for the scope

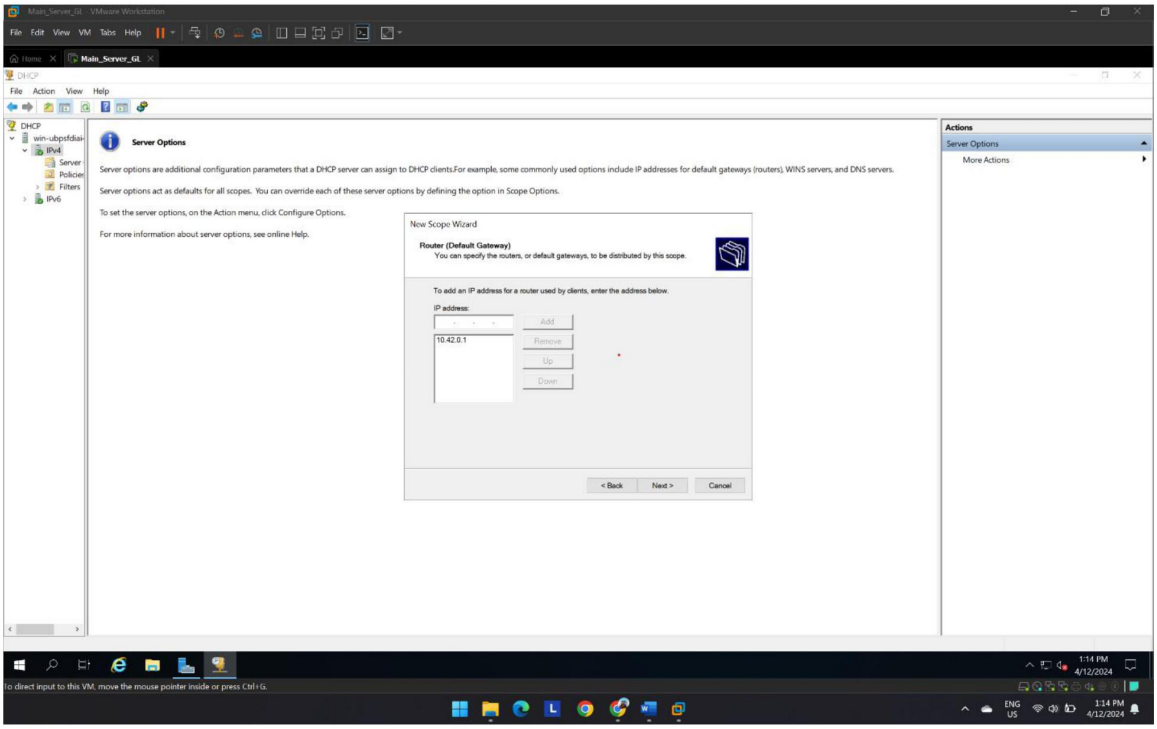


Figure 72
Add IP address for DNS Server to the scope

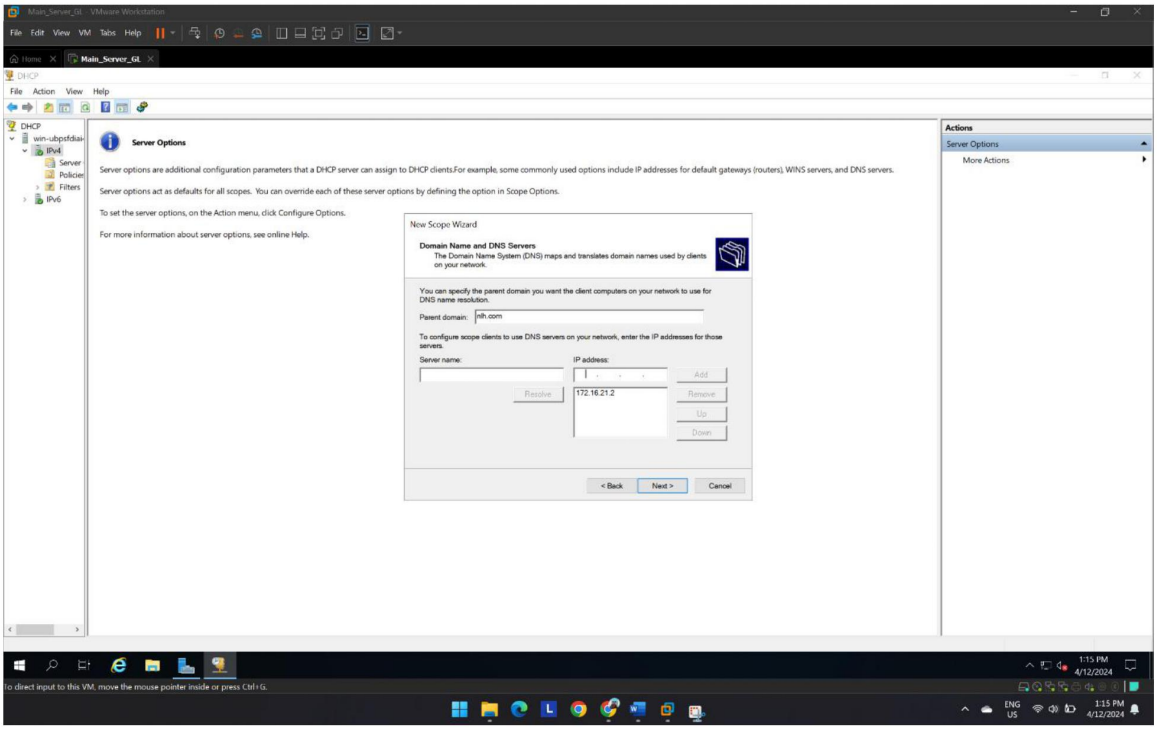


Figure 73
New Scope

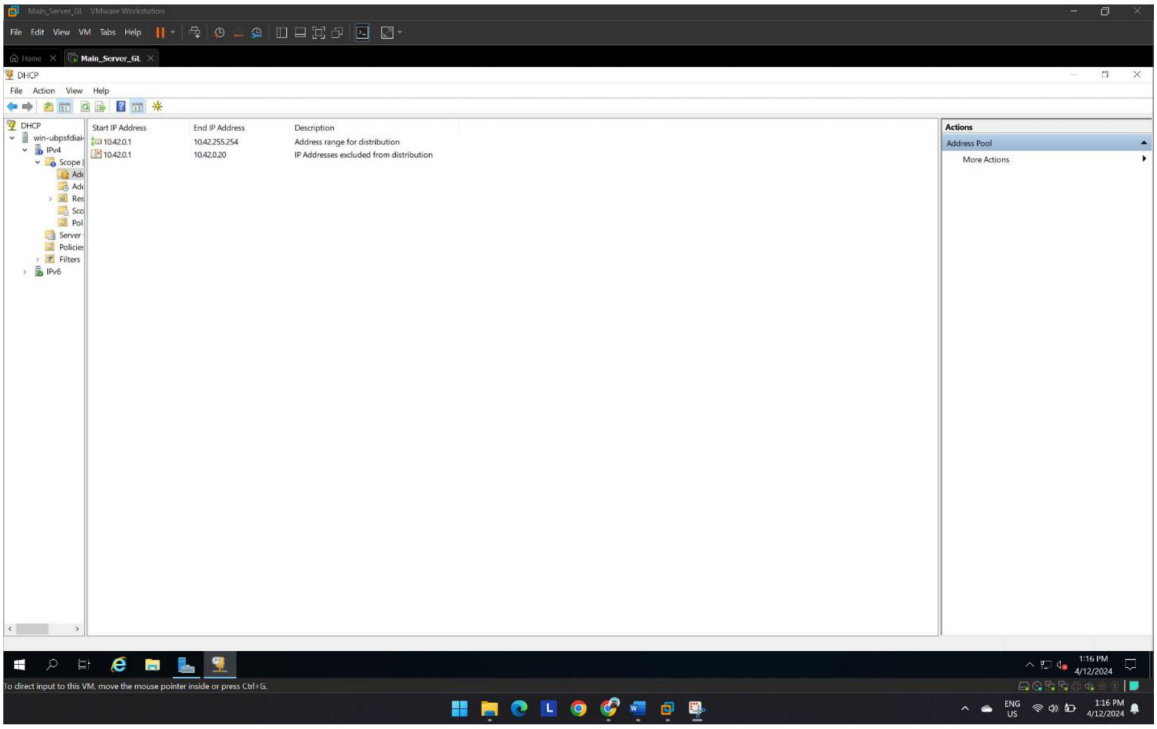


Figure 74
New Host to the DNS server

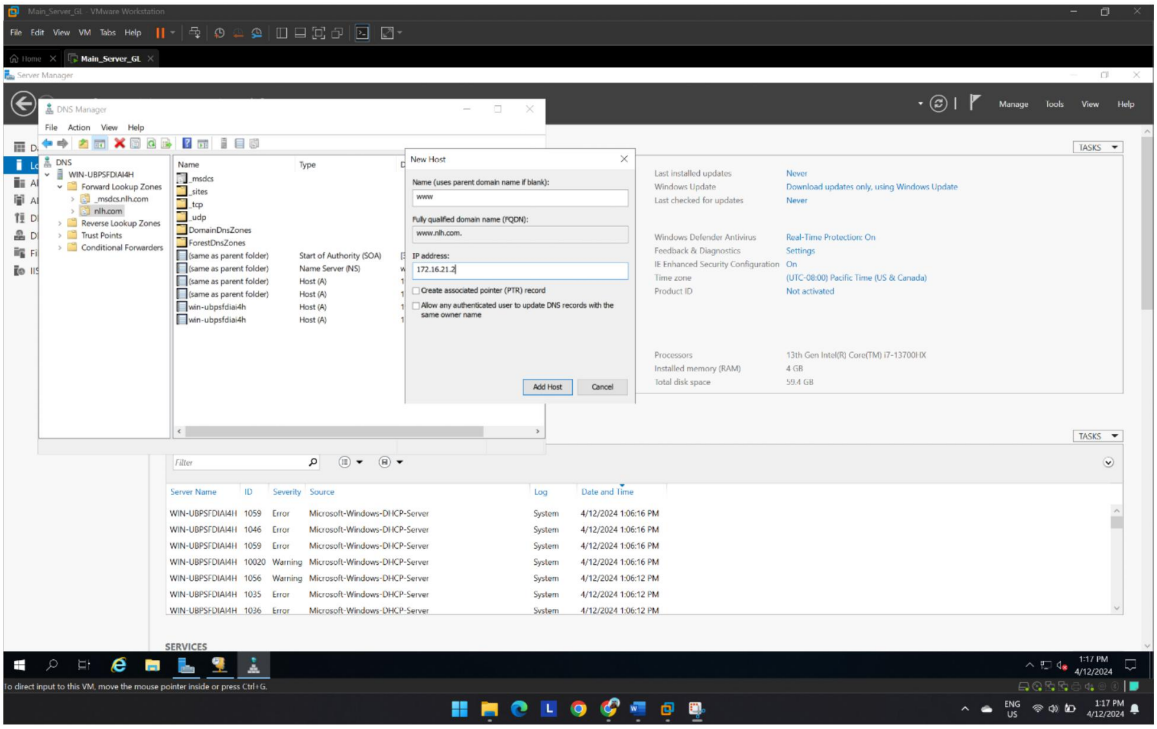
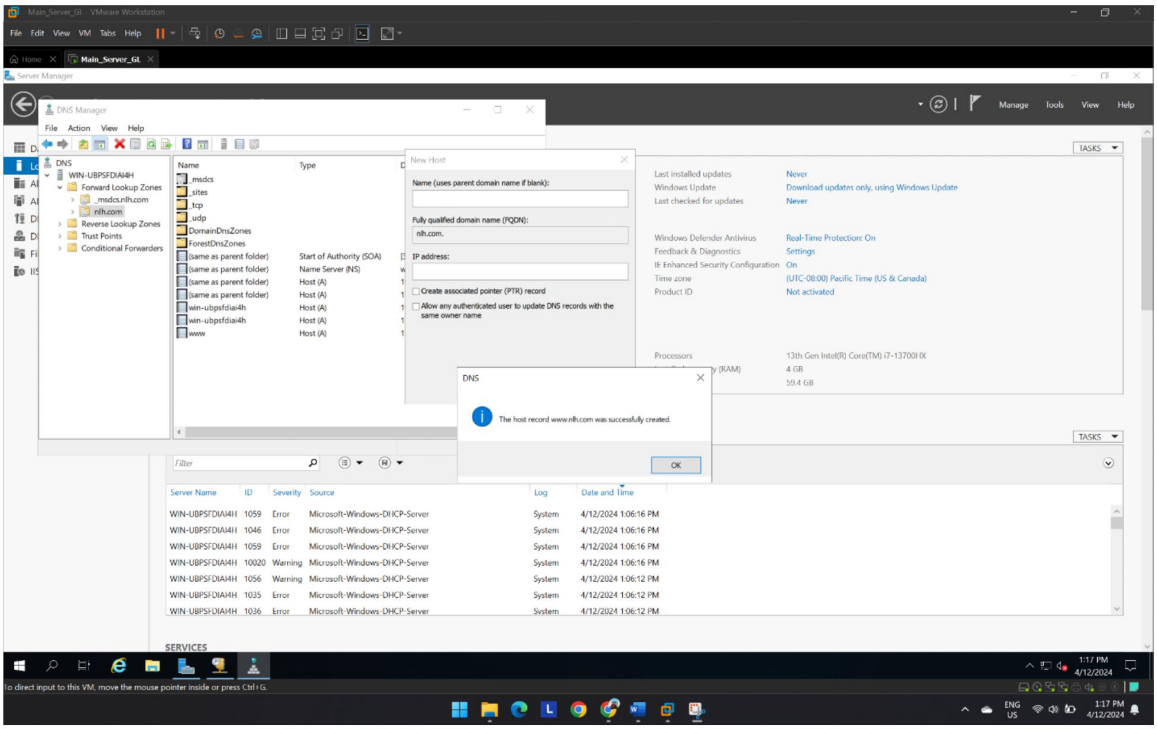
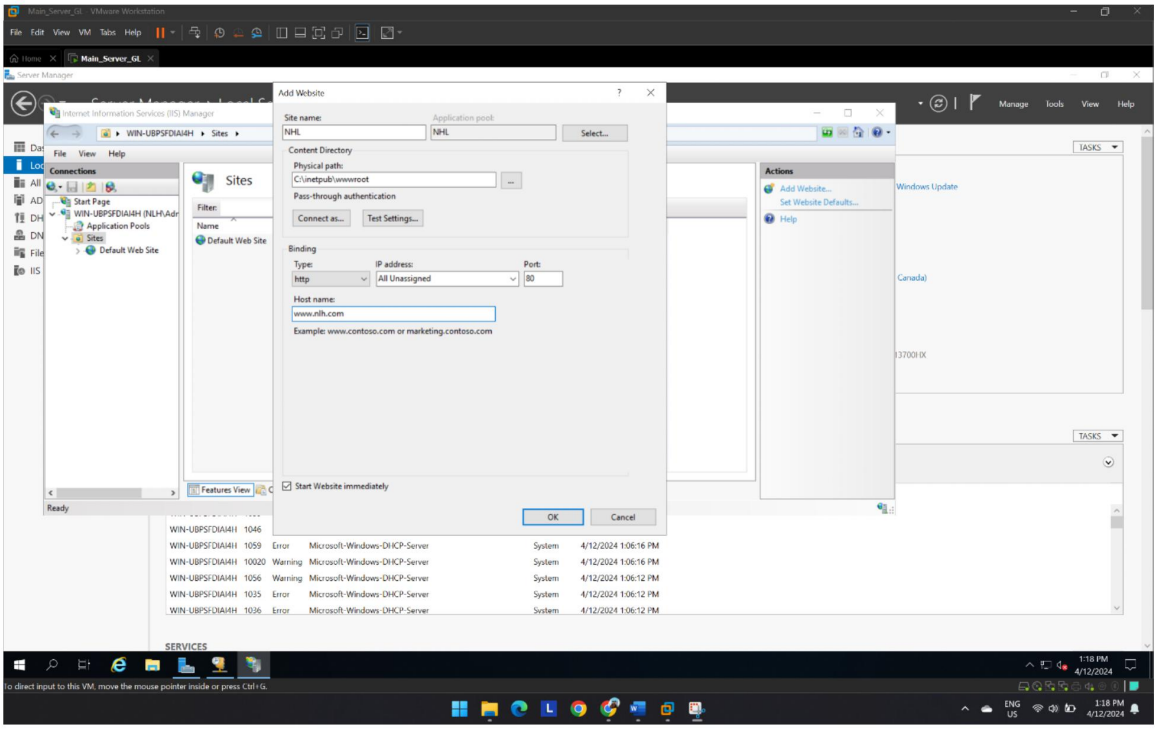


Figure 75
New host “www” added



6.3Adding website to IIS Service

Figure 76
Add website to IIS service using host “www”



6.4 Adding FTP Service

Figure 77
Add new host for FTP to DNS server

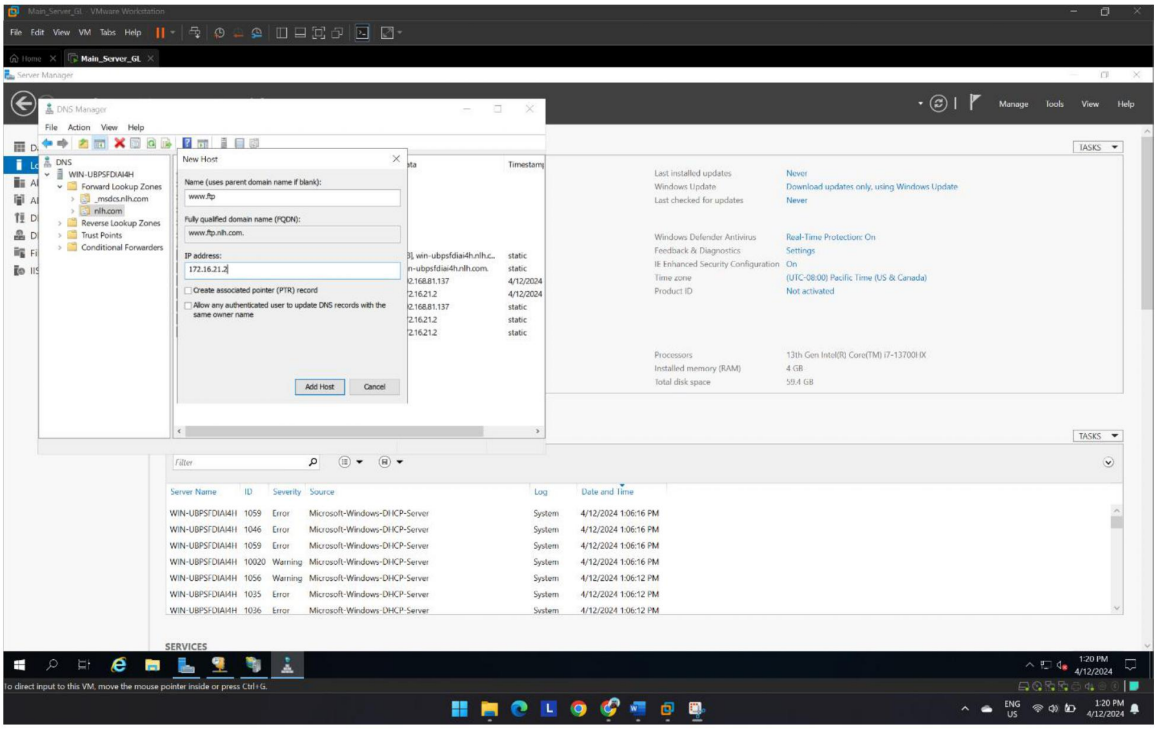


Figure 78
Add FTP role to server.

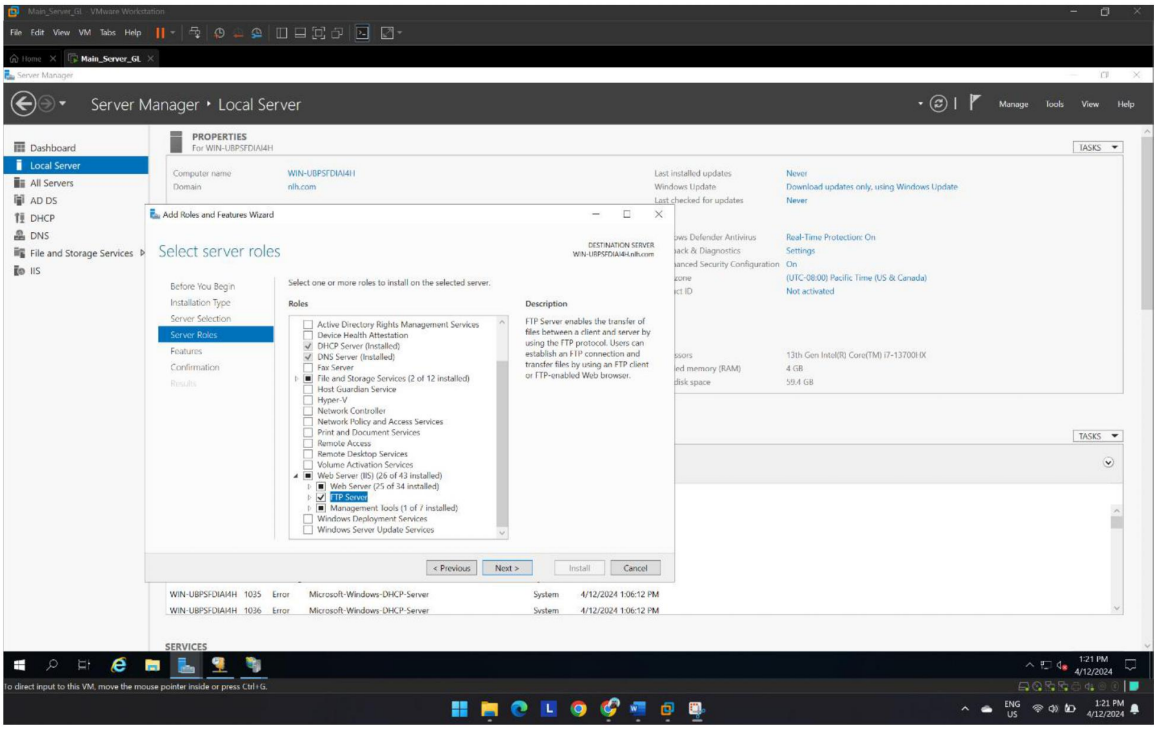


Figure 79
Close window once FTP server is installed

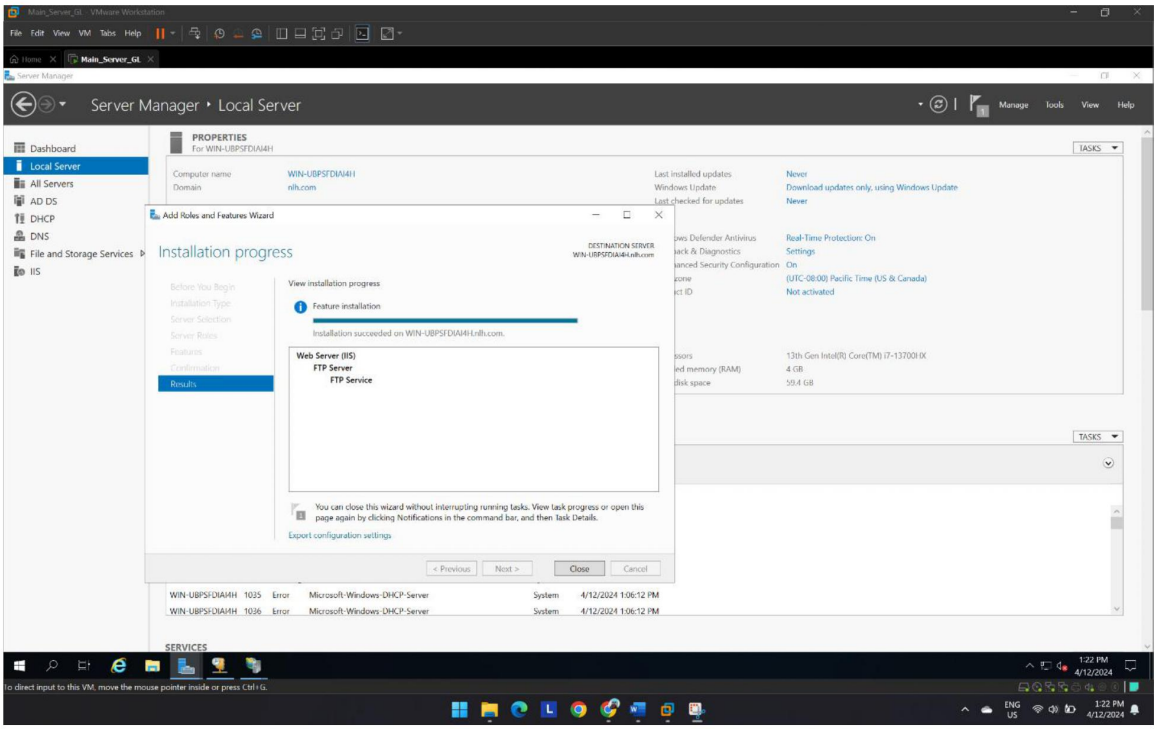


Figure 80
Add FTP site to IIS service

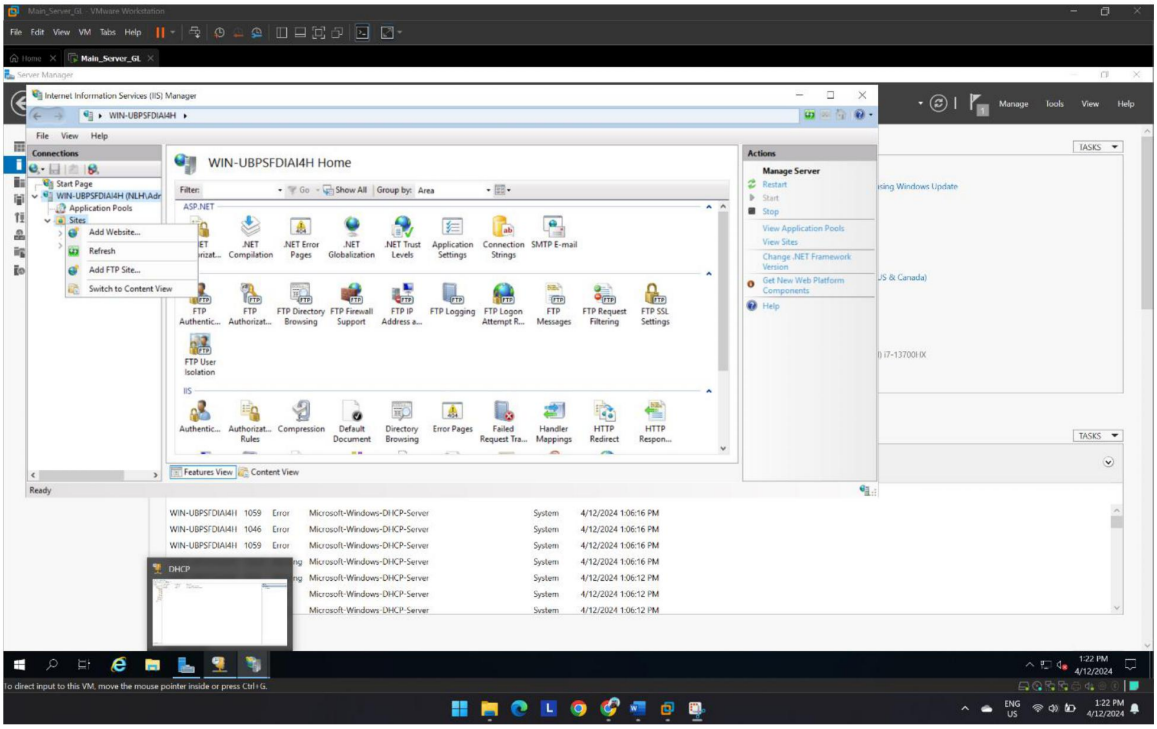


Figure 81
Set the Binding setting to FTP site

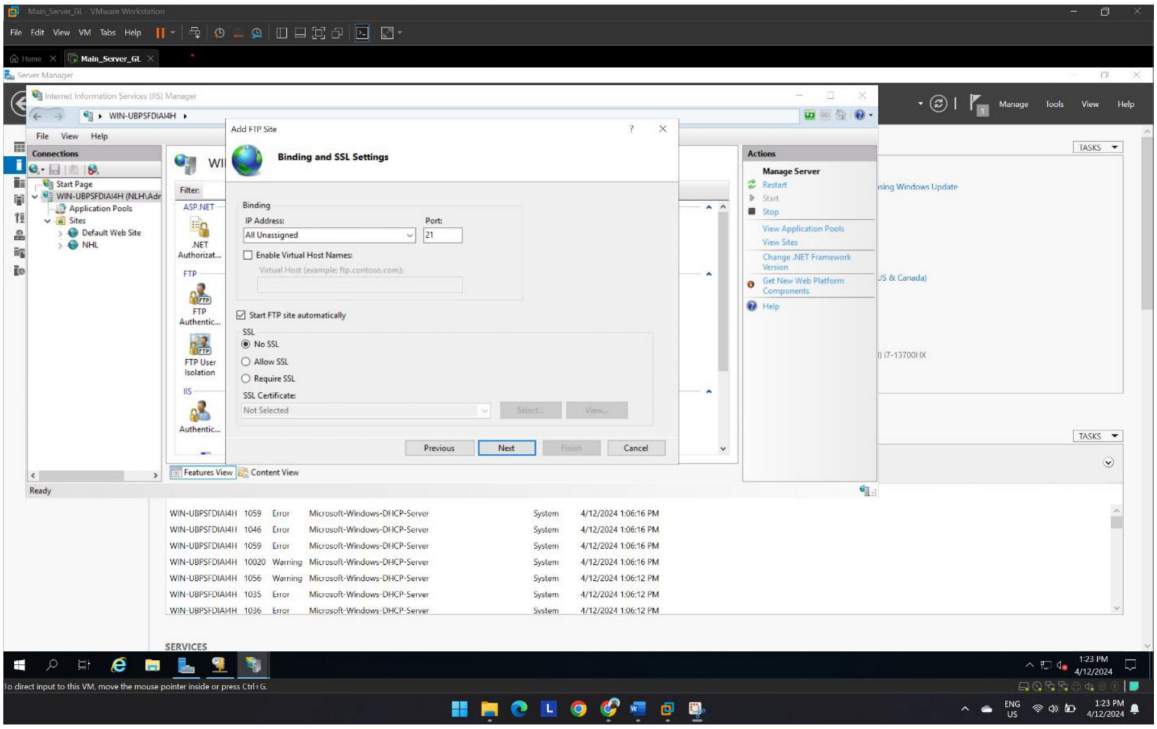


Figure 82
Set Authentication and Authorization

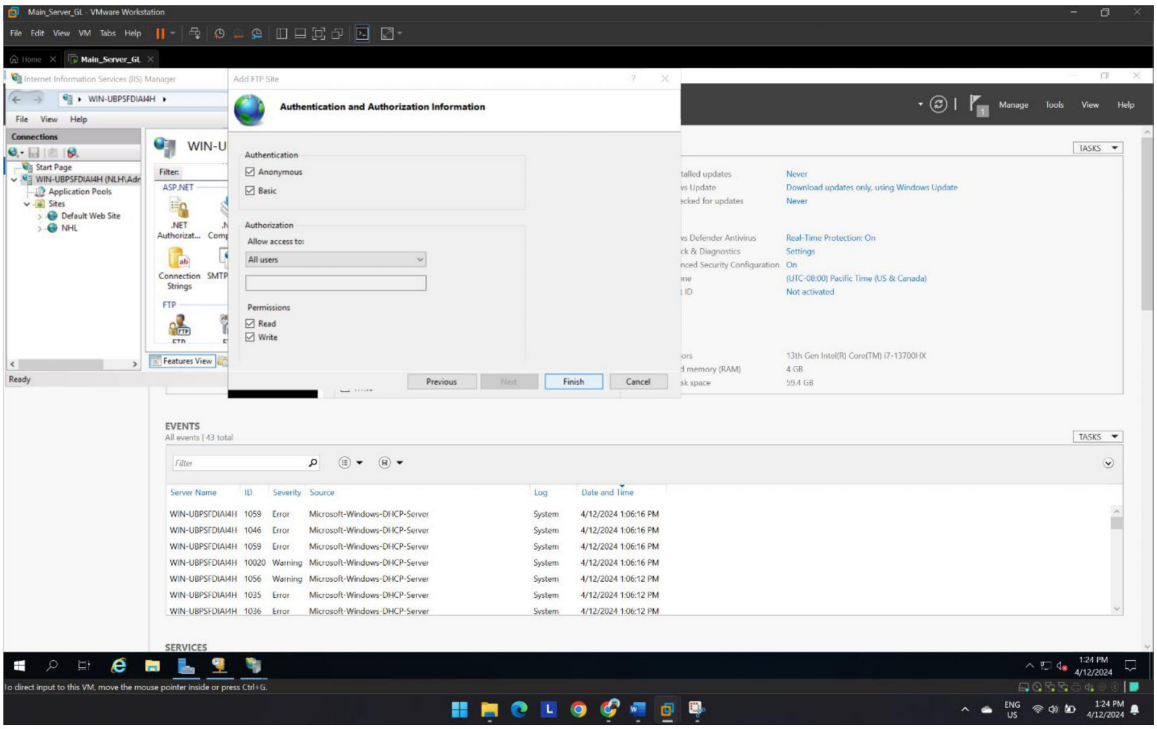
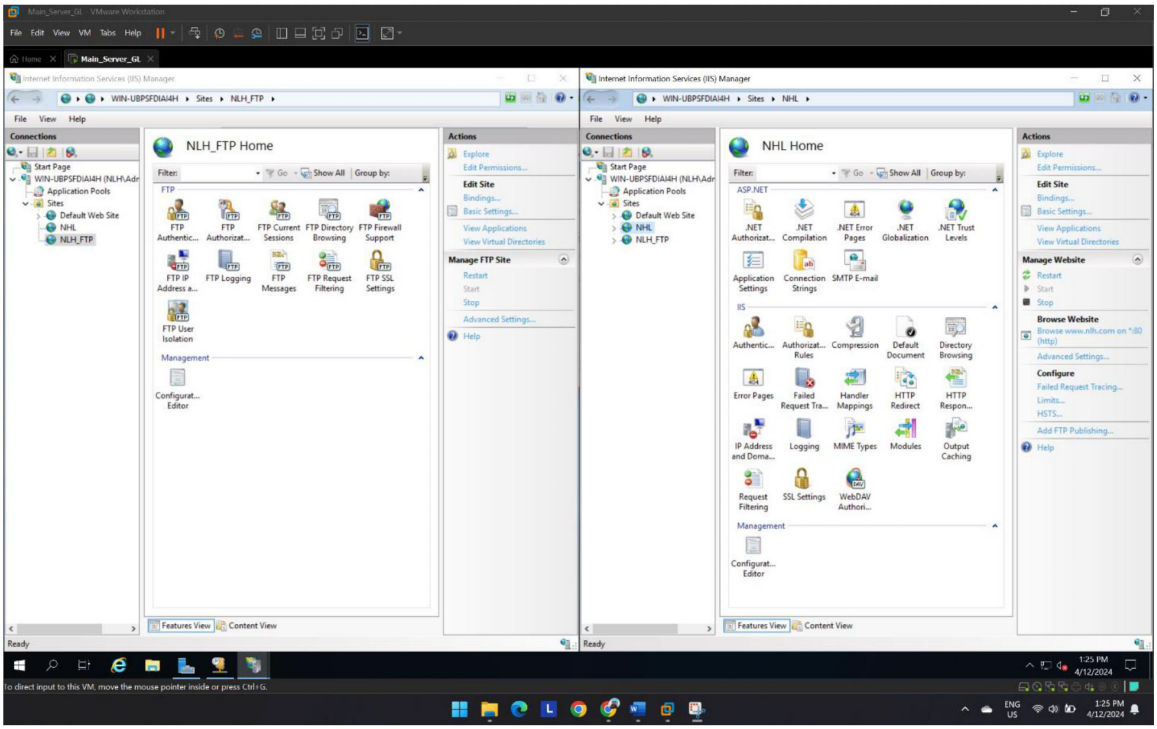


Figure 83
Window showing FTP and HTTP sites on IIS service



6.5 Installing IOT Camera

Figure 84
Access YAWCAM website

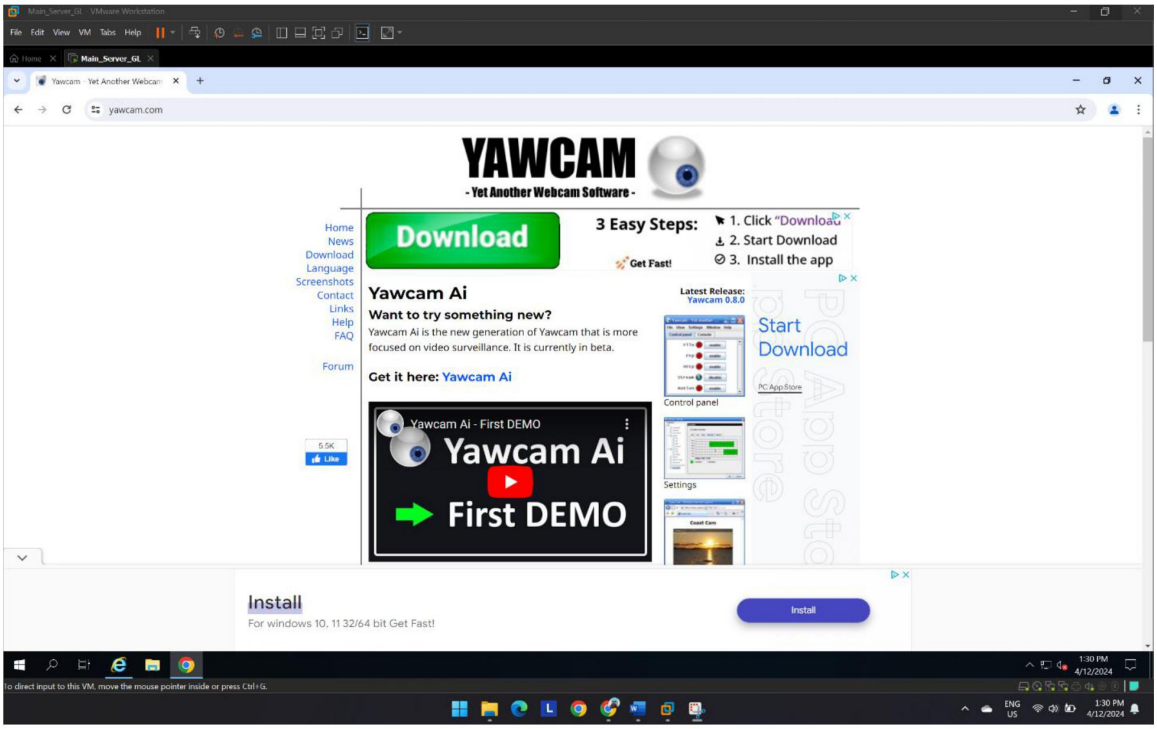


Figure 85
Download YAWCAM

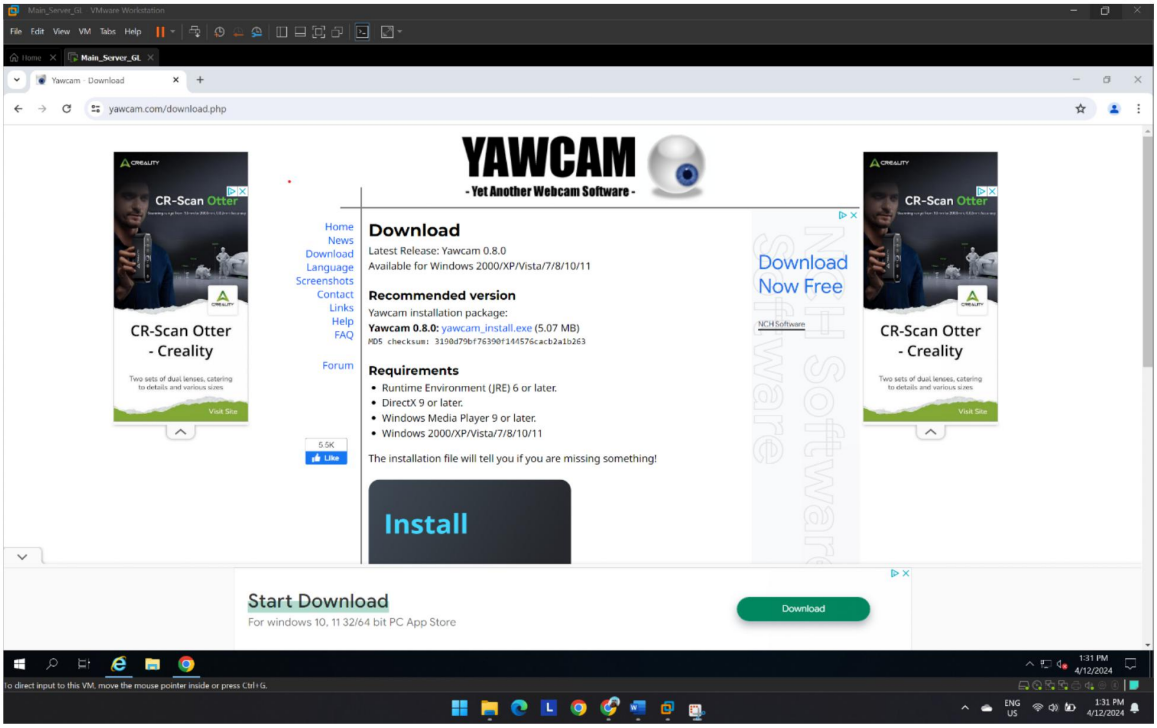
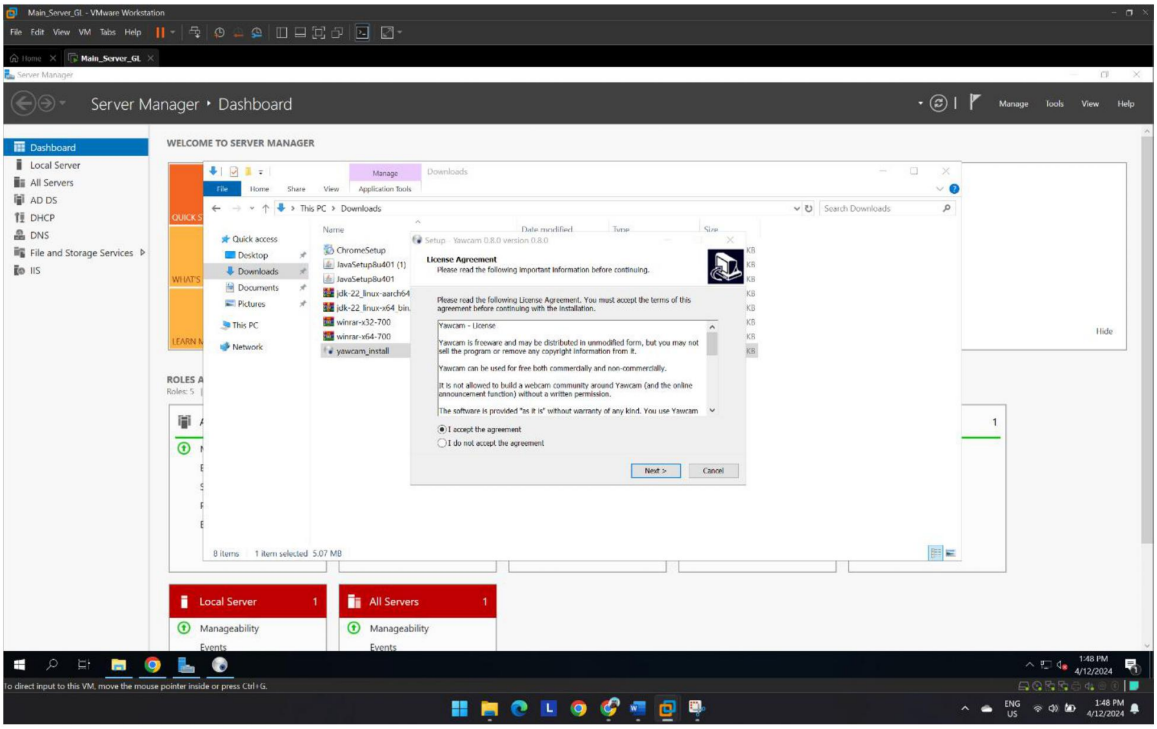
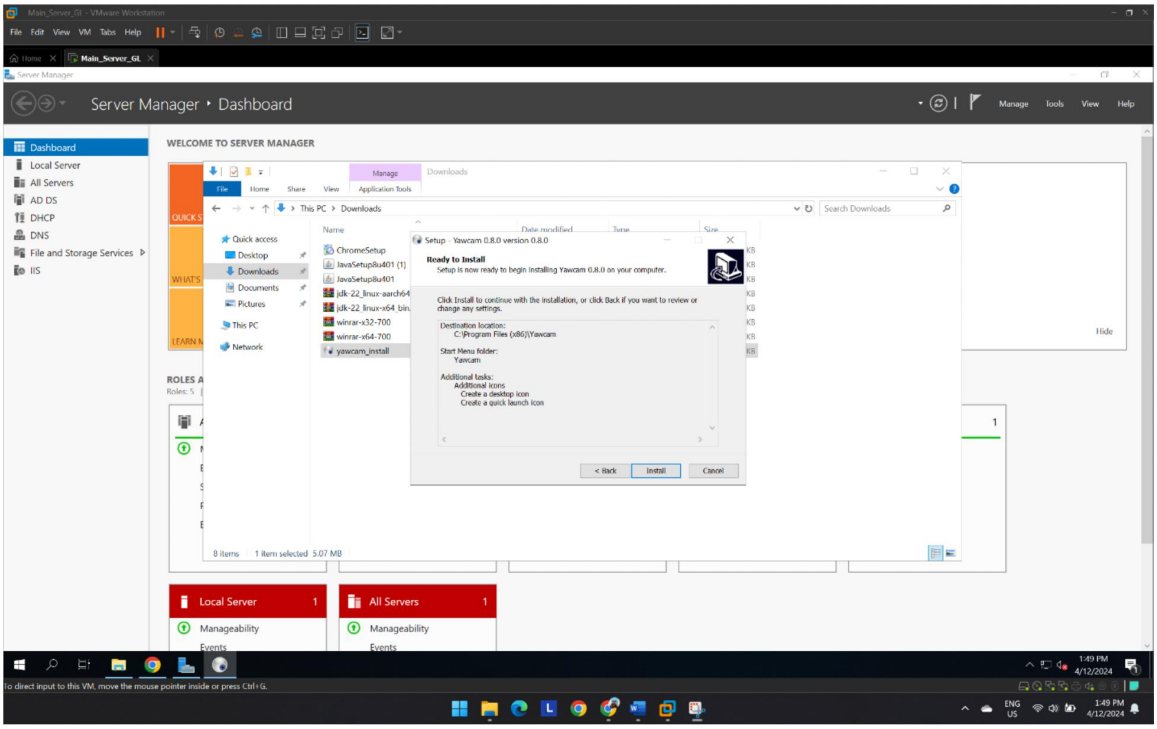
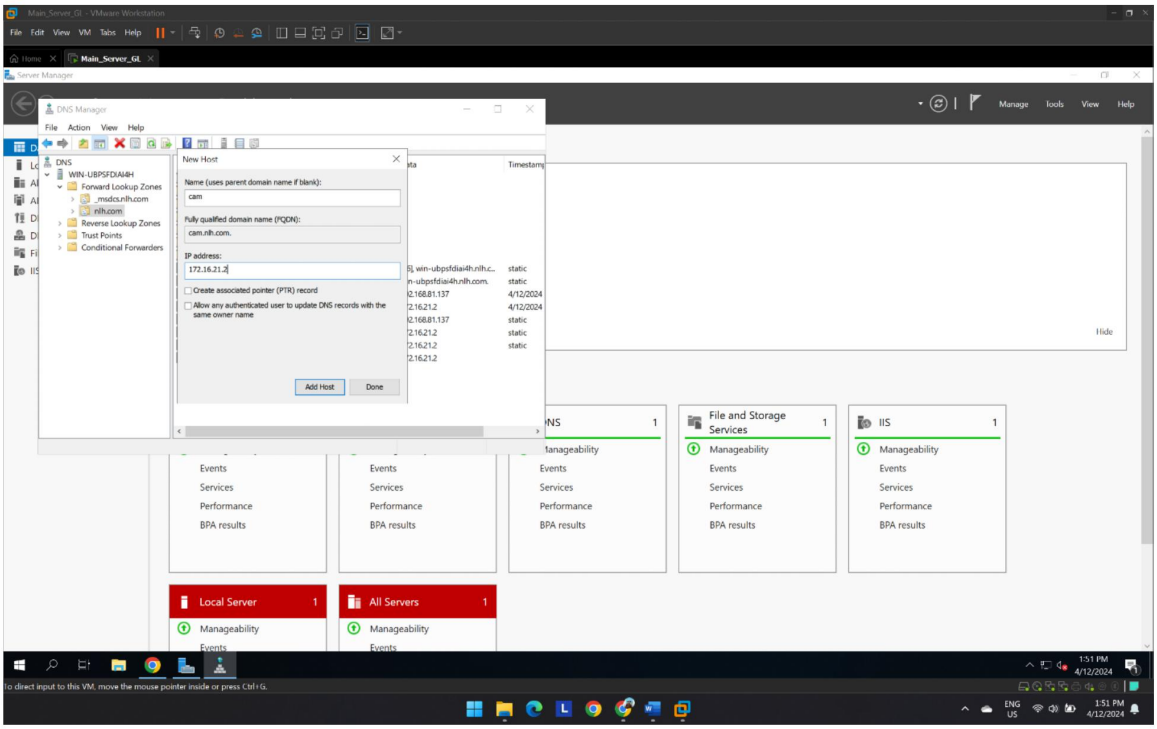


Figure 86
Install YAWCAM and add Host for IOT CAM on DNS server




Server Manager • Dashboard
WELCOME TO SERVER MANAGER
Dashboard
Local Server
All Servers
AD DS
DHCP
DNS
File and Storage Services
IIS
Setup - Yawcam 0.8.0 version 0.8.0
Ready to Install
Setup is now ready to begin installing Yawcam 0.8.0 on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
< Back
Install
Cancel
Local Server
All Servers
Manageability
Events


DNS Manager
New Host
Name (uses parent domain name if blank):
cam
Fully qualified domain name (FQDN):
cam.nlh.com.
IP address:
172.16.21.2
Create associated pointer (PTR) record
Add Host
Done
File and Storage Services
IIS
Local Server
All Servers
Manageability
Events
Services
Performance
BPA results

6.6 Ubuntu Setup for VOIP

Ubuntu Setup

Figure 87
Ubuntu Installation

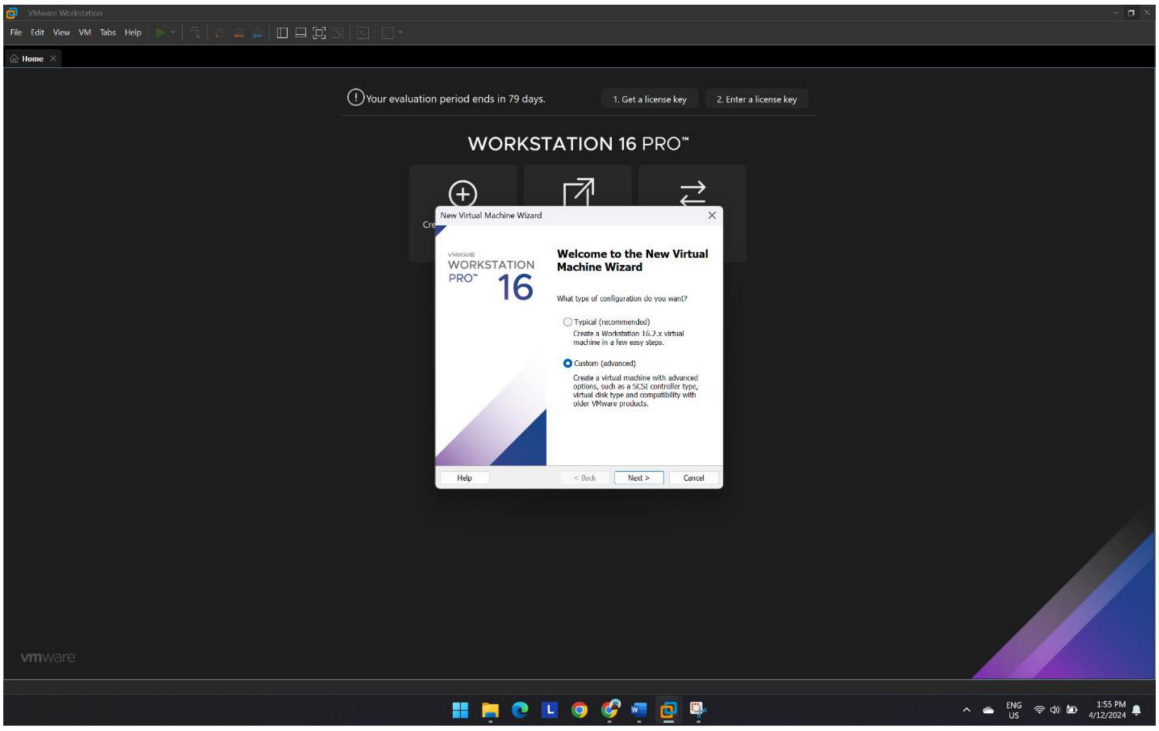


Figure 88
Ubuntu Hardware Capability

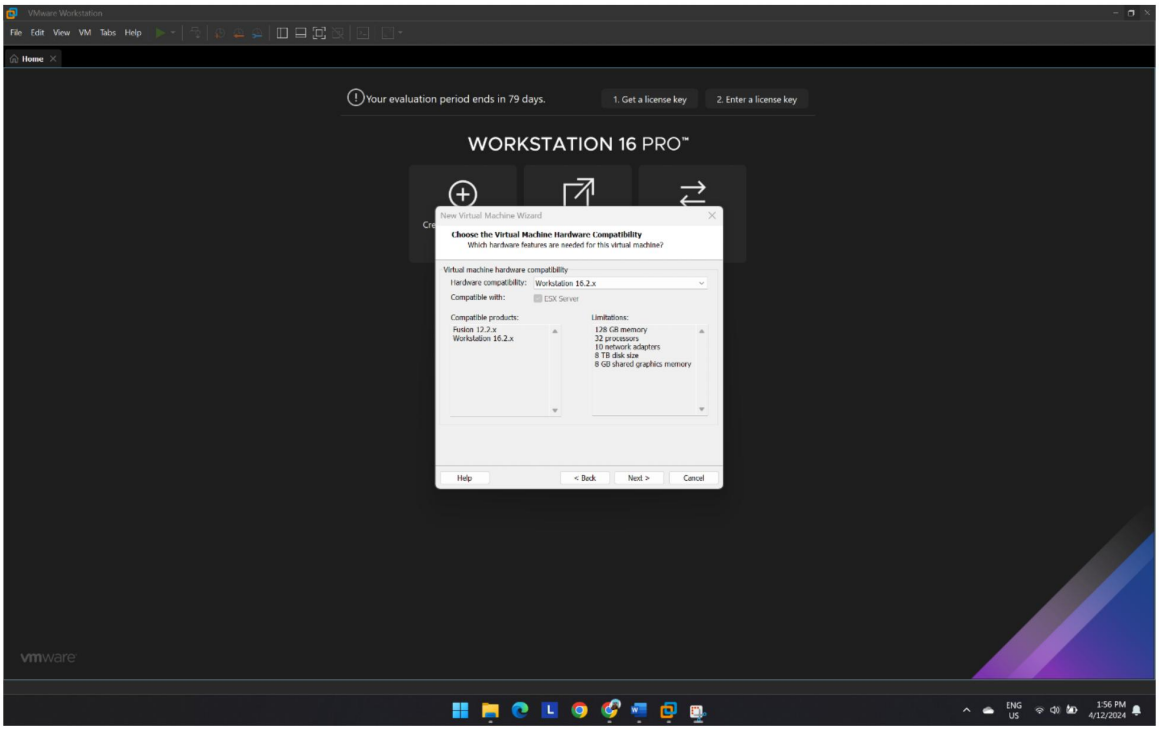


Figure 89
Guest OS Installation

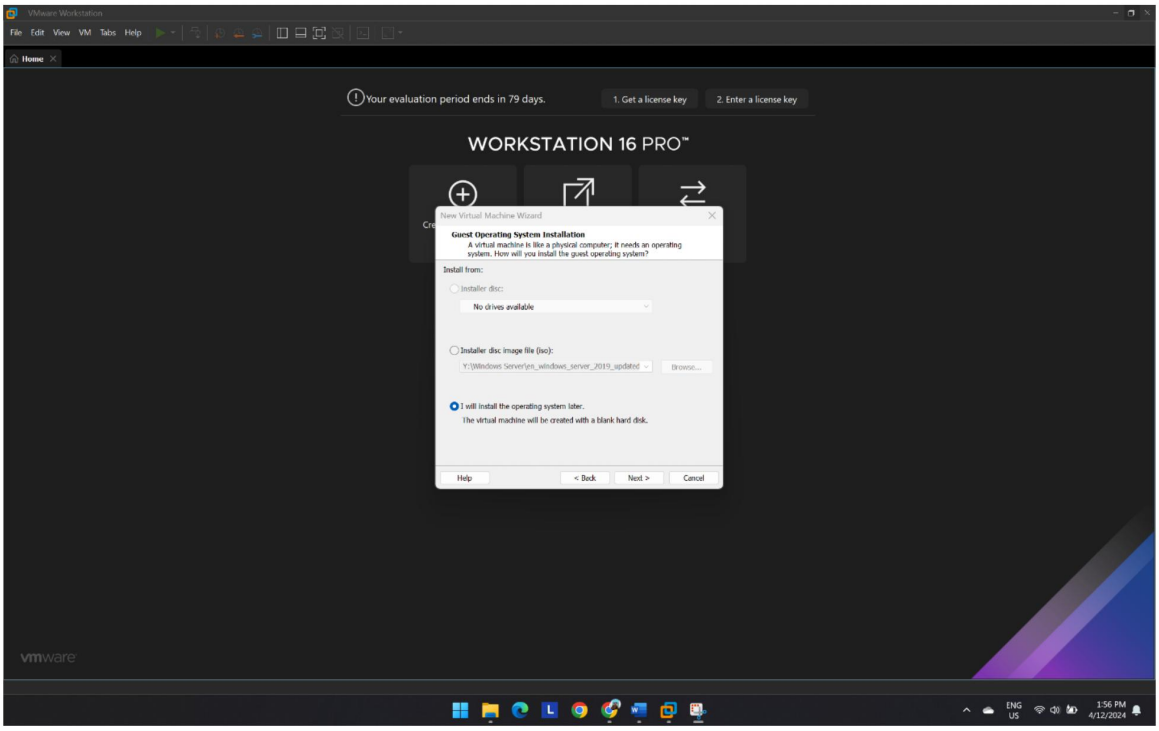


Figure 90
Linux OS

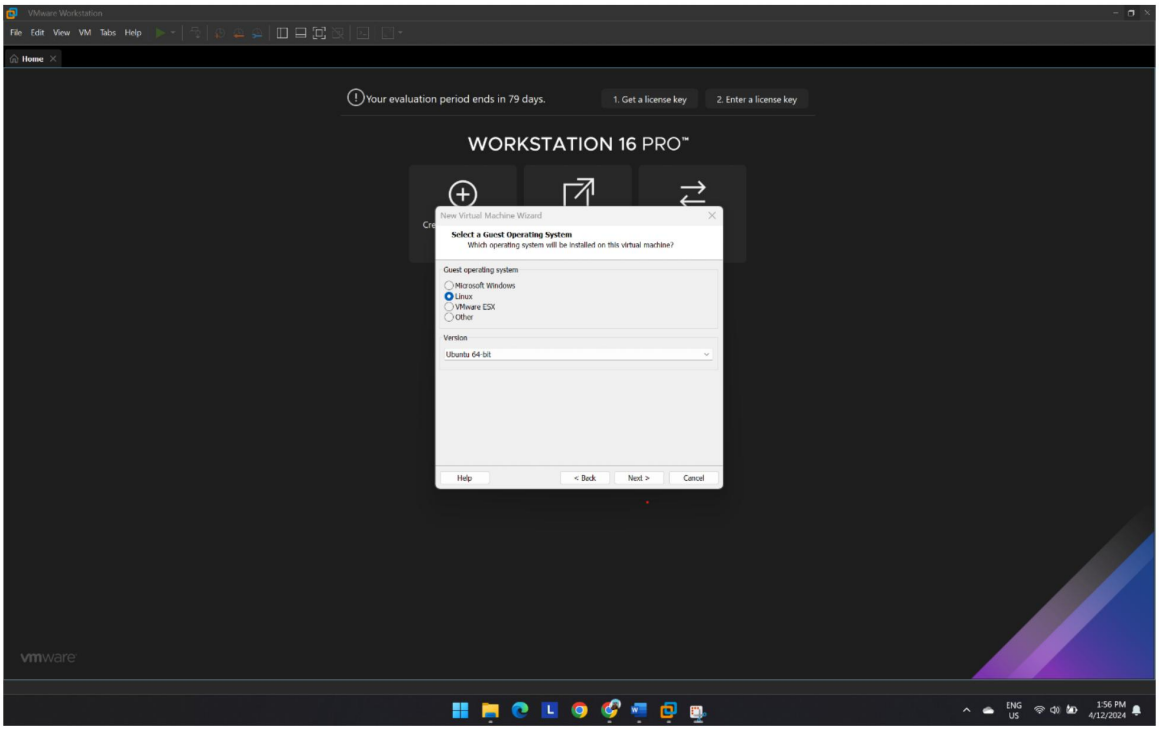


Figure 91
Ubuntu Server (VM Name)

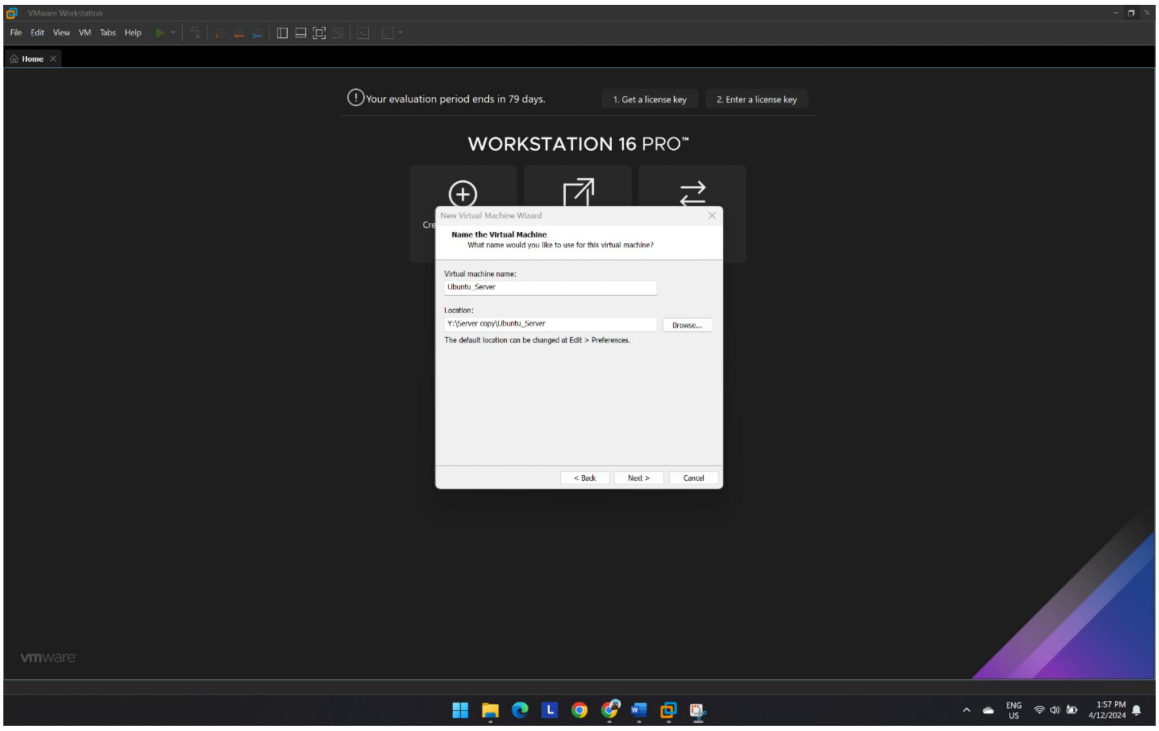


Figure 92
Disk Capacity

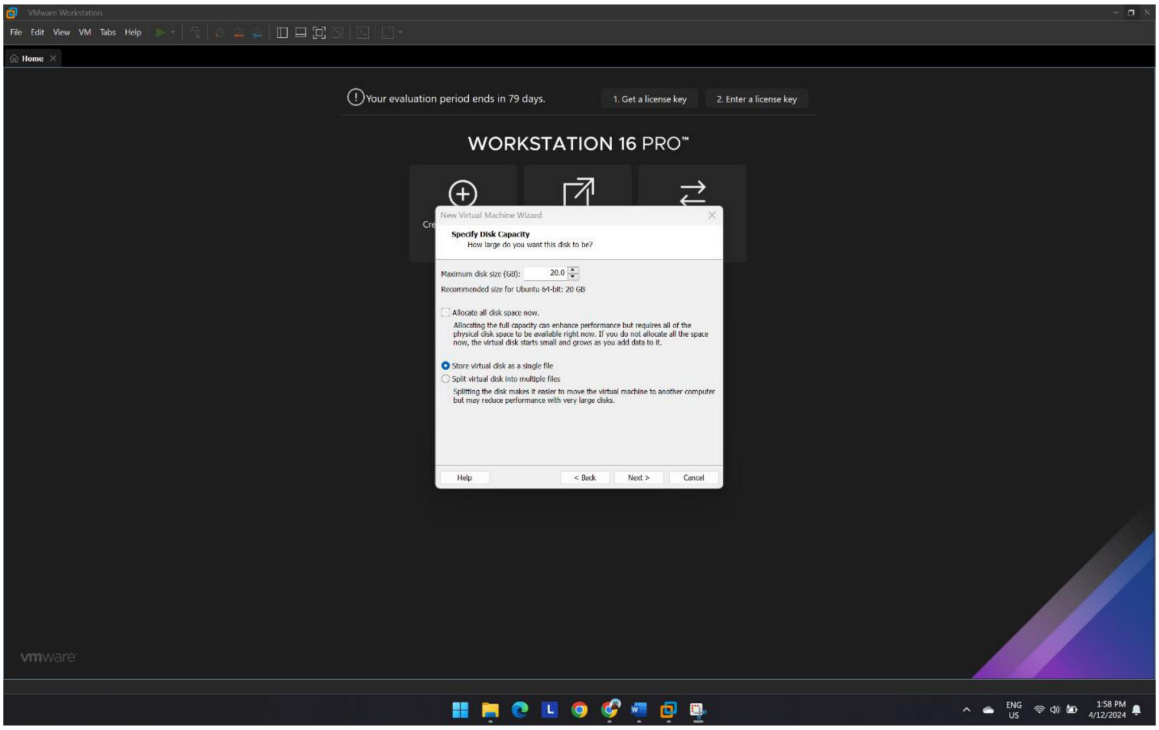


Figure 93
ISO File Ubuntu Server

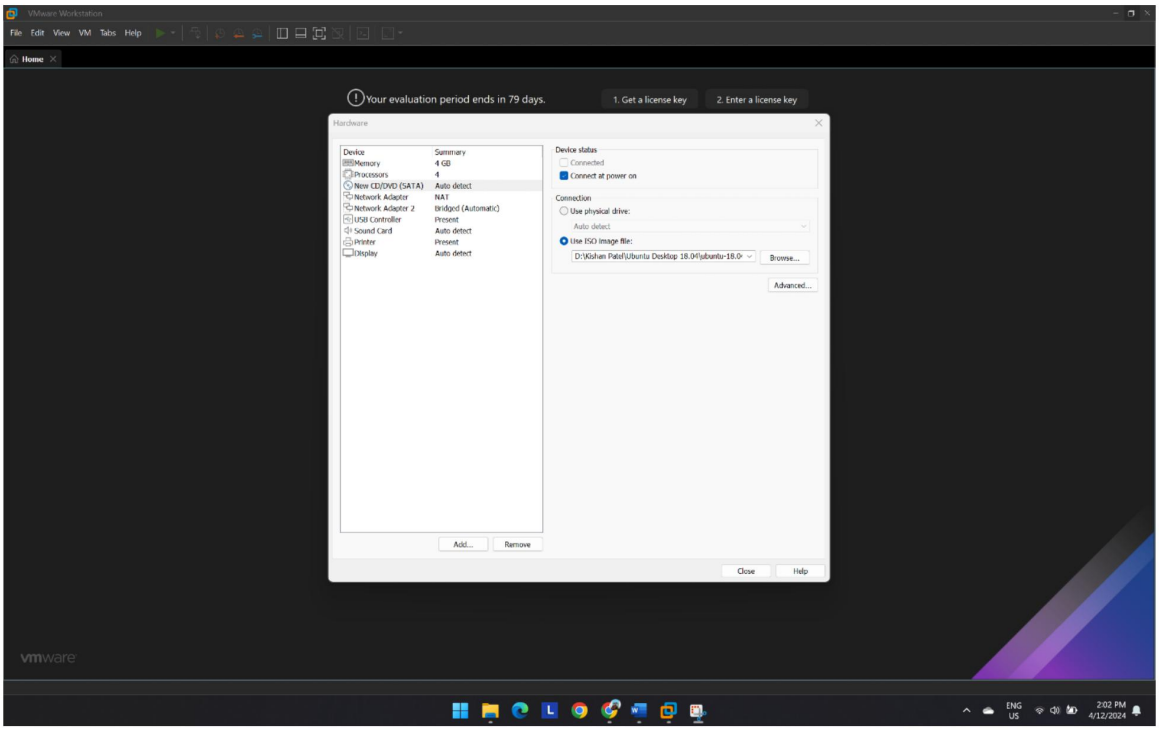


Figure 94
Ubuntu Server Installation

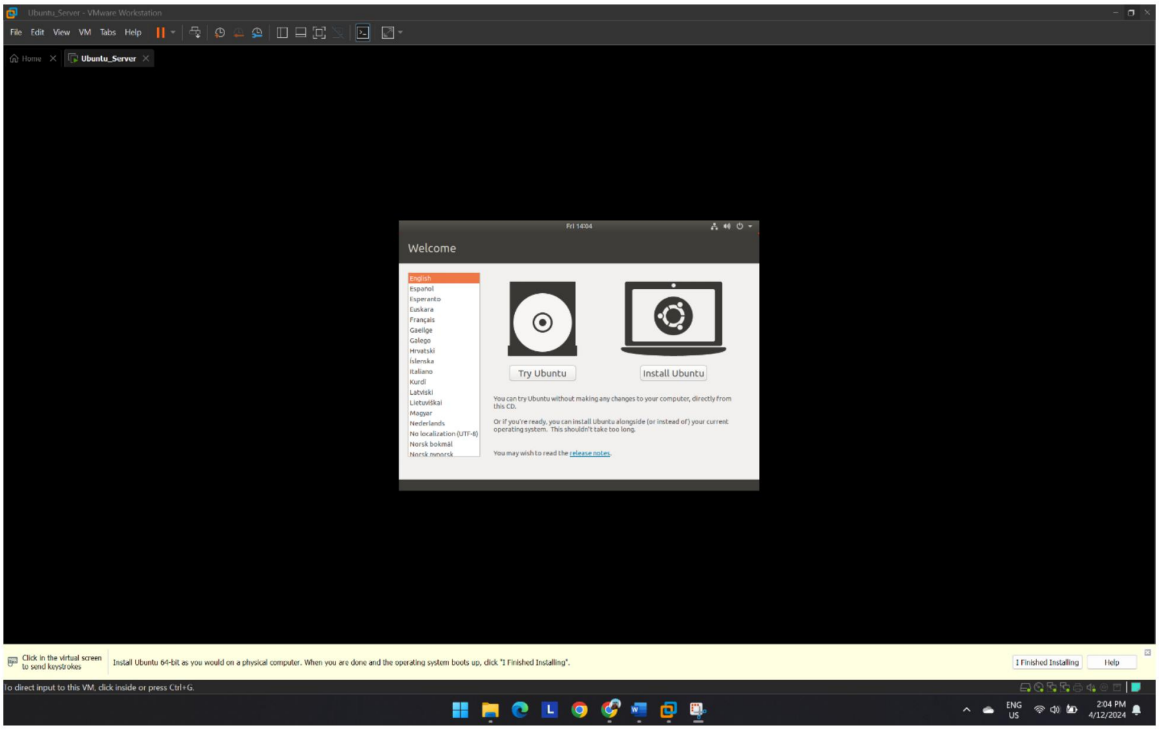


Figure 95
Ubuntu Keyboard Layout

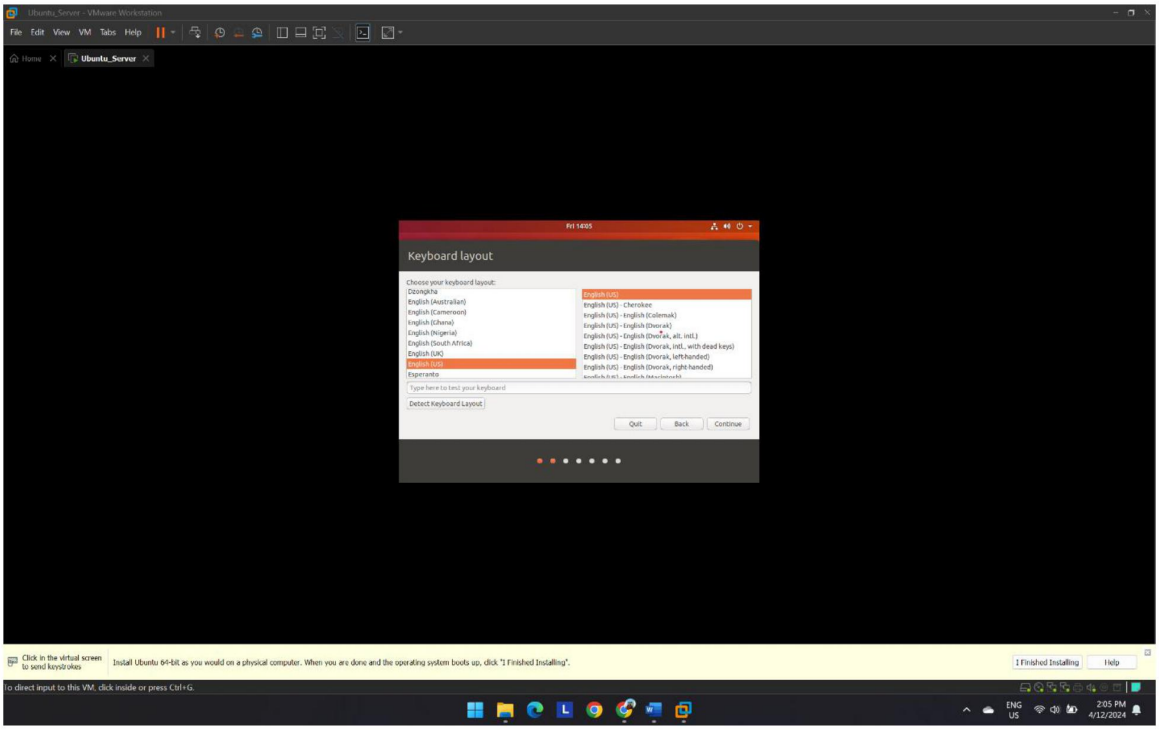


Figure 96
Updates and Other Software

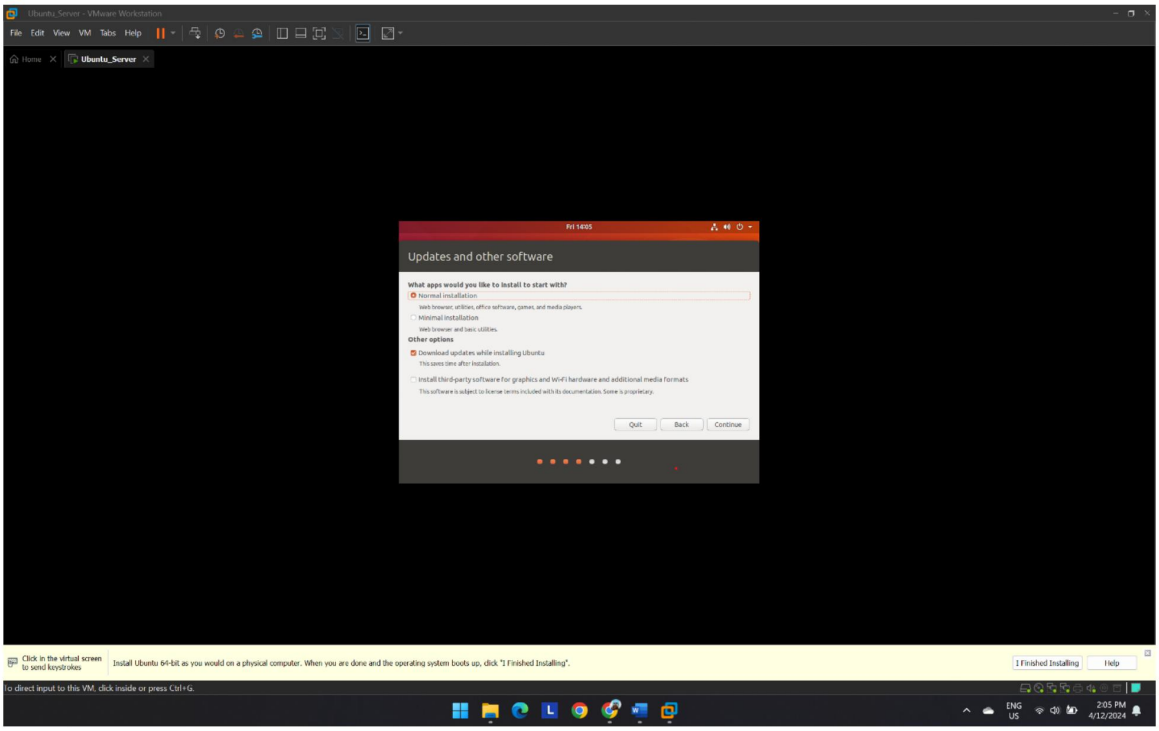


Figure 97
Installation Type

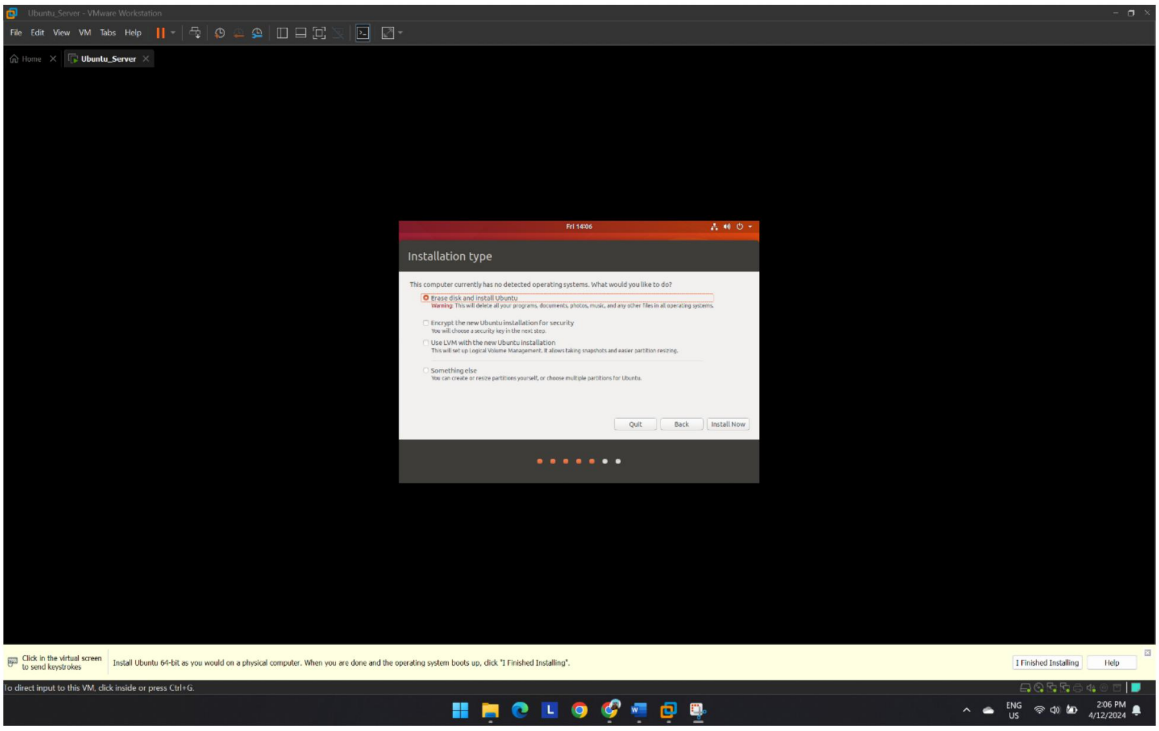


Figure 98
Disk Selection for Changes

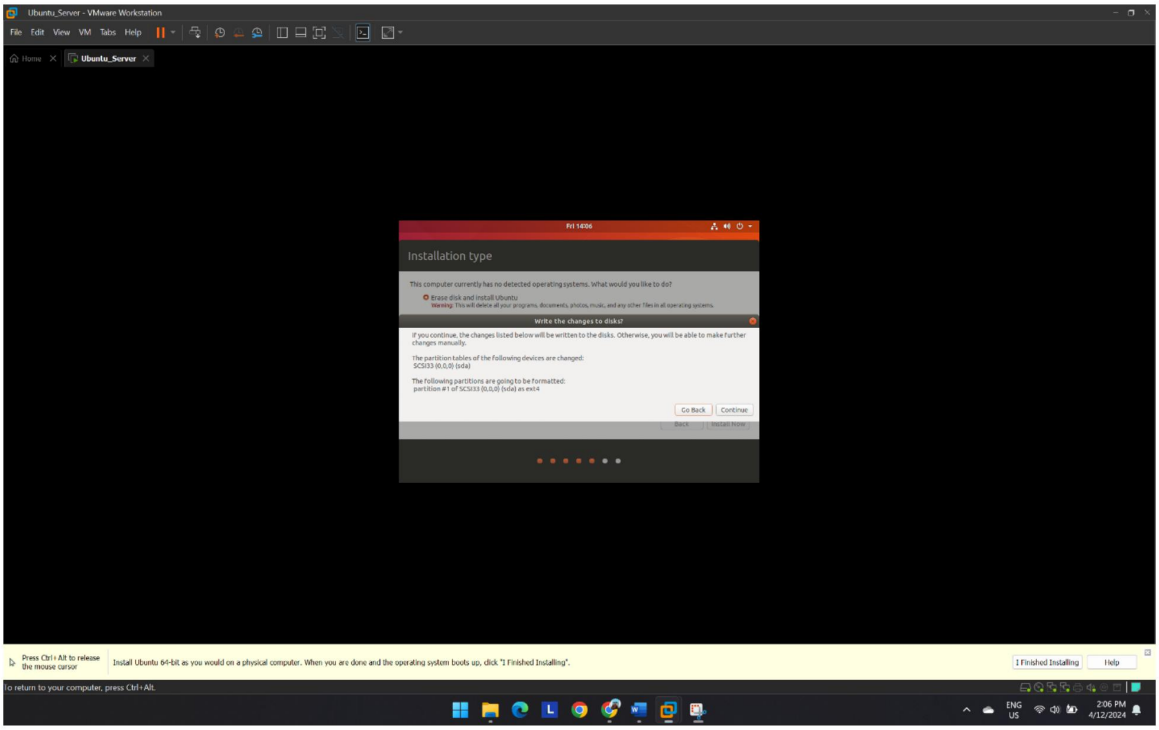


Figure 99
Location Selection

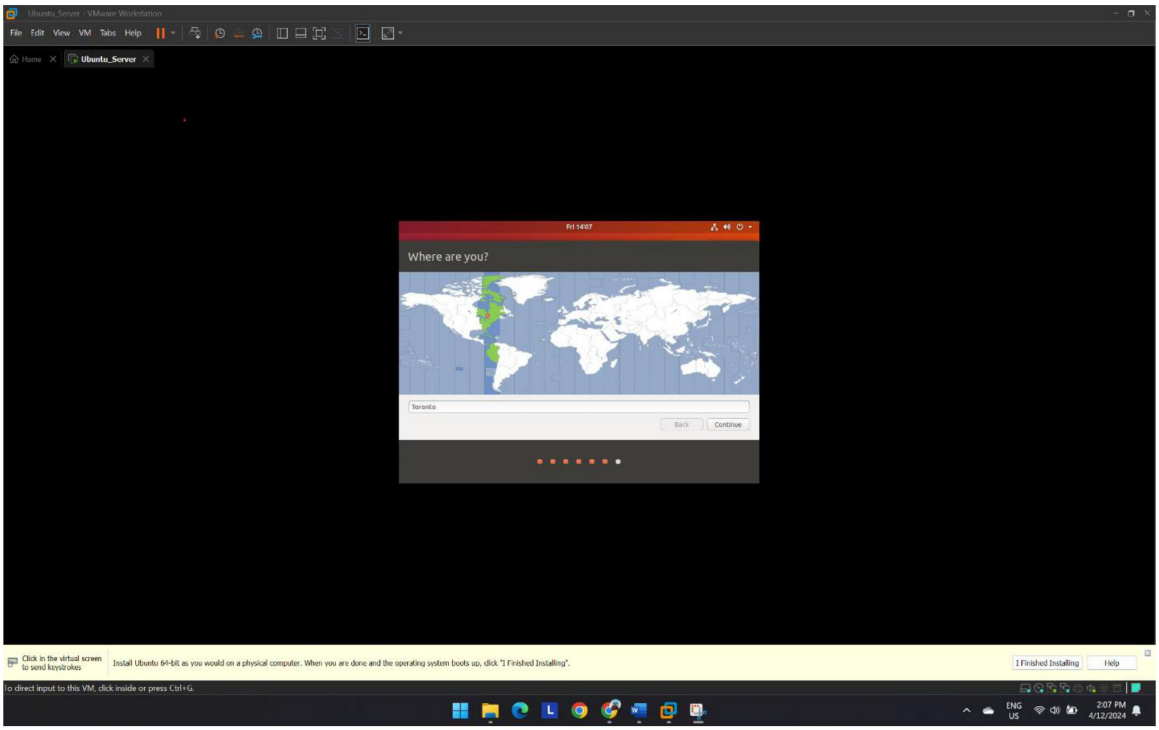


Figure 100
Authentication for User

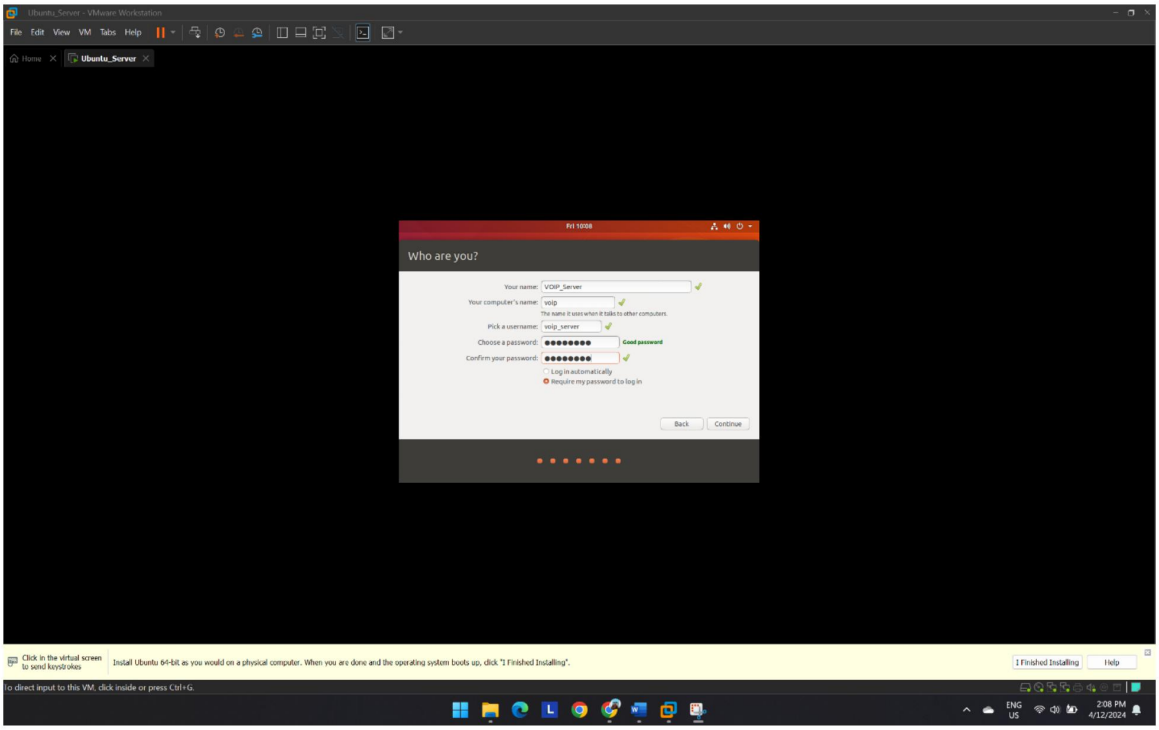


Figure 101
Ubuntu Server Hardware Specification

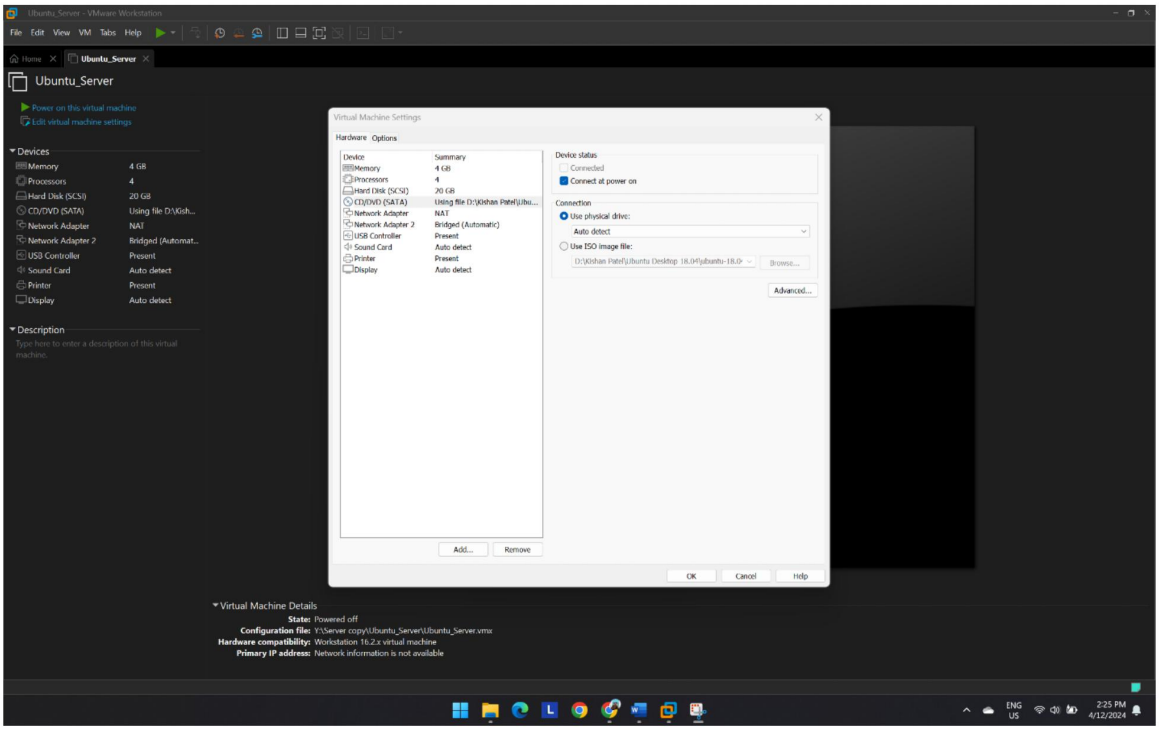


Figure 102
Help Improve Ubuntu

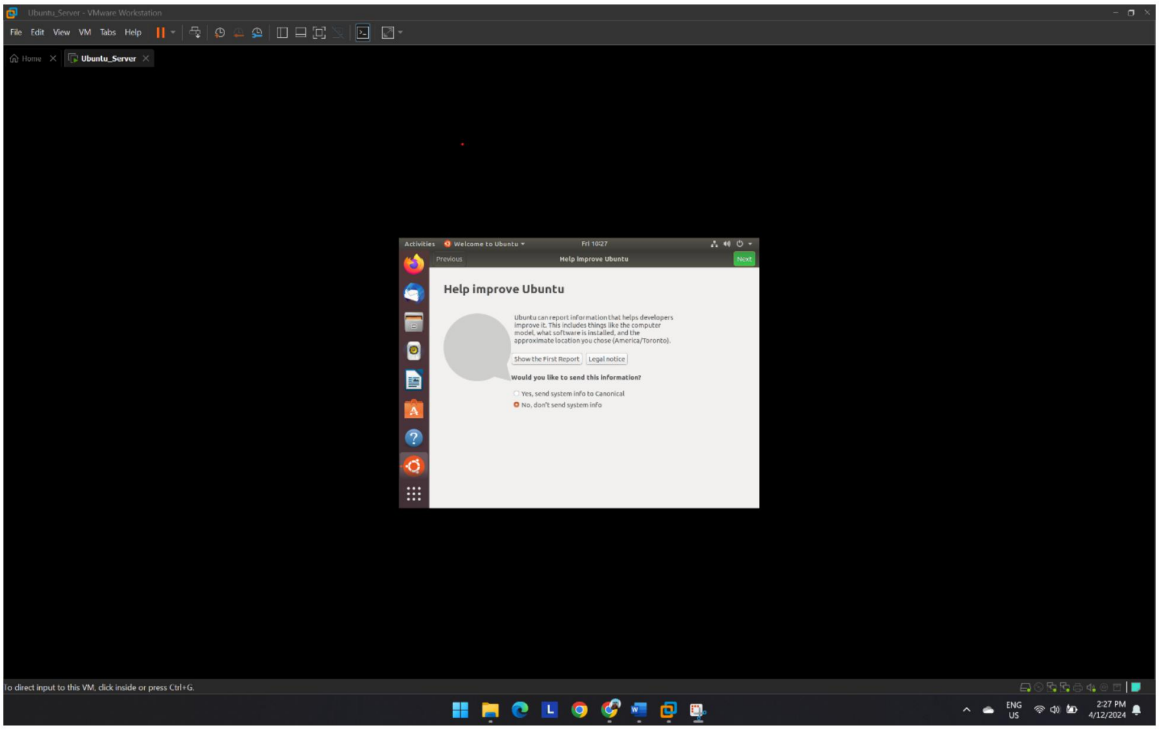


Figure 103
Update and Upgrade the Ubuntu Server

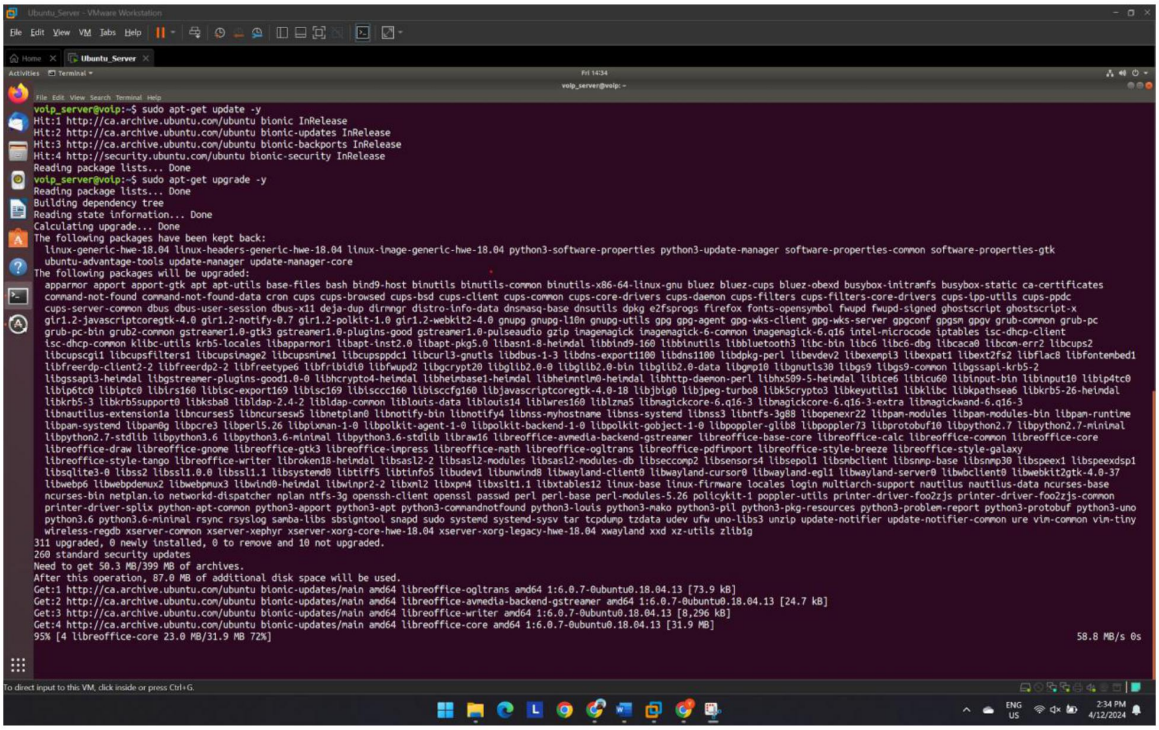


Figure 104
Install Asterisk server

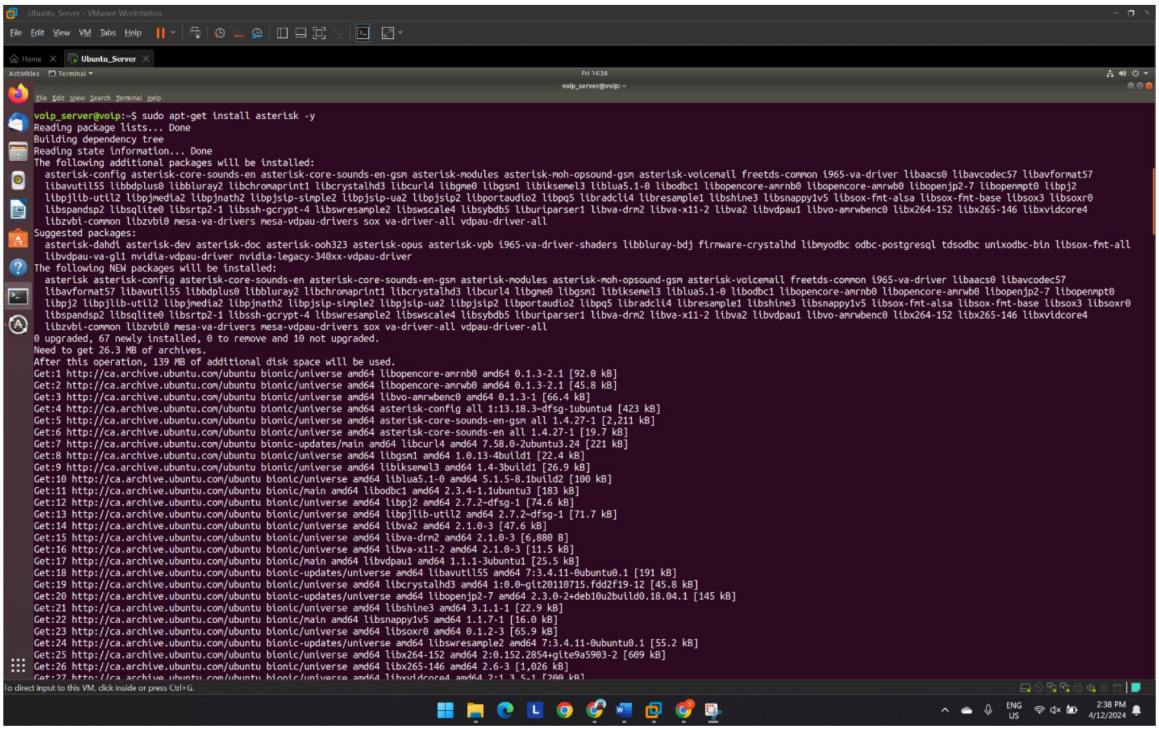


Figure 105
Default SIP Configuration for VOIP

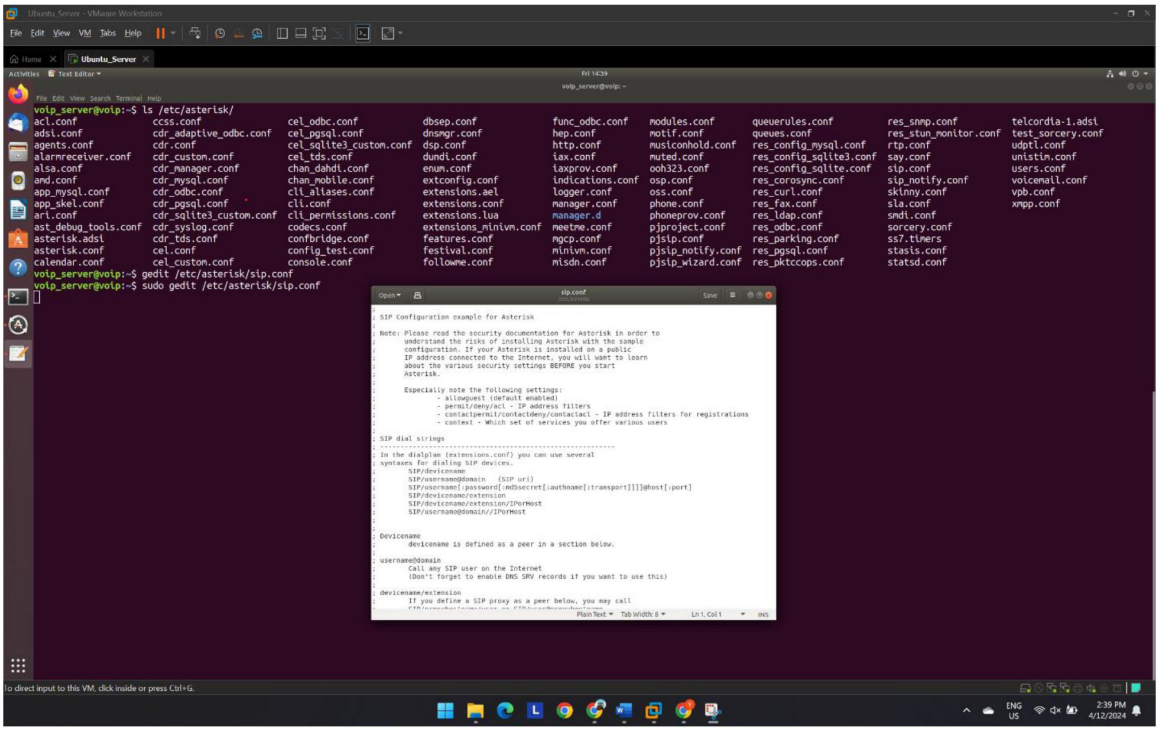


Figure 106
SIP Configuration

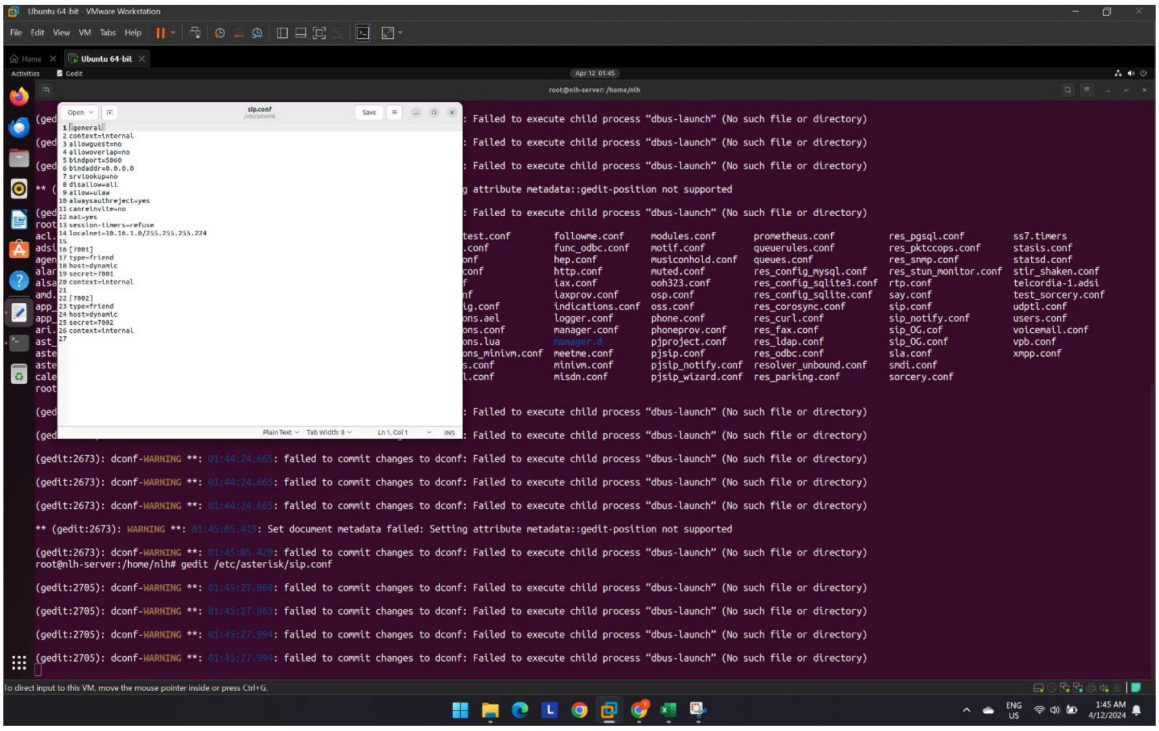


Figure 107
Default Extensions for VOIP

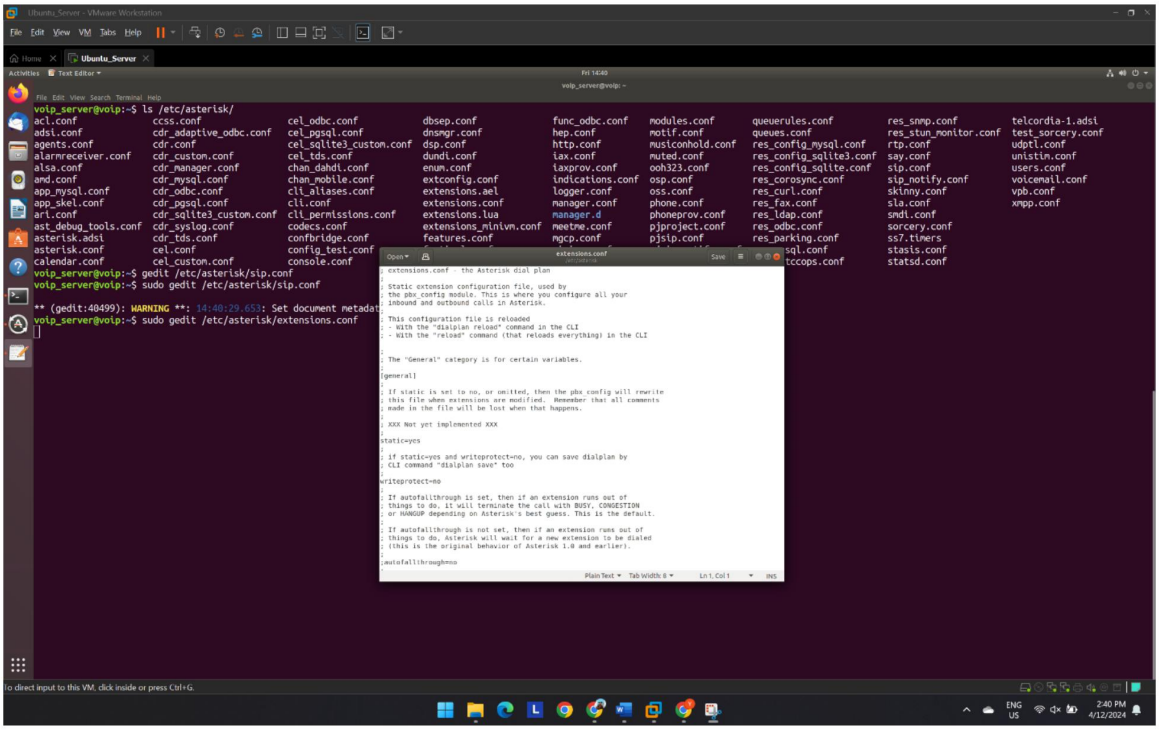
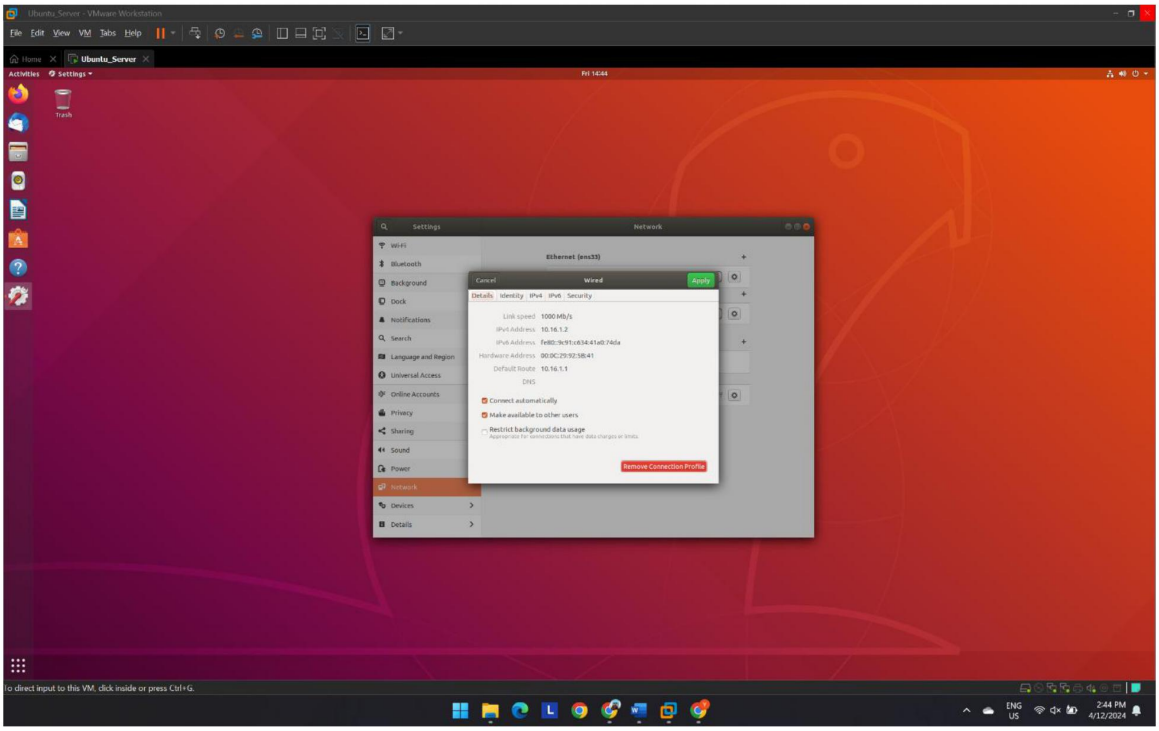


Figure 108
VOIP Virtual Machine IP address



7. DEVICE CONFIGURATIONS

7.1 WAN_R1

```
WAN_ROUTER#SHOW RUN
Building configuration...

Current configuration : 1195 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname WAN_ROUTER
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
!
```

```
interface GigabitEthernet0/0/0
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/1/0
ip address 192.200.100.9 255.255.255.252
clock rate 2000000
!
interface Serial0/1/1
ip address 192.200.100.5 255.255.255.252
clock rate 2000000
!
interface Serial0/2/0
ip address 192.200.100.21 255.255.255.252
clock rate 2000000
!
interface Serial0/2/1
ip address 192.200.100.1 255.255.255.252
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router ospf 25
router-id 2.1.2.1
log-adjacency-changes
network 192.200.100.4 0.0.0.3 area 0
network 192.200.100.8 0.0.0.3 area 0
network 192.200.100.20 0.0.0.3 area 0
network 192.200.100.0 0.0.0.3 area 0
!
ip classless
```

```
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```

7.2TORONTO

TORONTO_R1

```
WAN-R1#SHOW RUN
Building configuration...

Current configuration : 1333 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname WAN-R1
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
```

```
!
!
!
username cisco password 7 0822455D0A16
!
!
license udi pid CISCO2811/K9 sn FTX1017JCJE-
!
!
!
!
!
!
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
ip address 10.30.10.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.30.10.6 255.255.255.252
duplex auto
speed auto
!
interface Serial0/1/0
ip address 192.200.100.2 255.255.255.252
!
interface Serial0/1/1
no ip address
clock rate 2000000
!
interface FastEthernet1/0
```

```
ip address 10.30.10.10 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 10.20.10.1 255.255.255.192
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
router ospf 25
router-id 1.4.1.4
log-adjacency-changes
network 192.200.100.0 0.0.0.3 area 0
network 10.30.10.0 0.0.0.3 area 1
network 10.30.10.4 0.0.0.3 area 1
network 10.30.10.8 0.0.0.3 area 1
network 10.20.10.0 0.0.0.63 area 1
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```

TORONTO_CORE_SW_1

```
ORE-SW1#SHOW RUN
Building configuration...

Current configuration : 2498 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname CORE-SW1
!
!
!
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username cisco password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
!
spanning-tree mode pvst
!
```

```
!
!
!
!
!
interface Port-channel1
switchport mode trunk
!
interface GigabitEthernet1/0/1
no switchport
ip address 10.30.10.5 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet1/0/2
switchport mode trunk
!
interface GigabitEthernet1/0/3
switchport mode trunk
!
interface GigabitEthernet1/0/4
switchport mode trunk
!
interface GigabitEthernet1/0/5
switchport mode trunk
!
interface GigabitEthernet1/0/6
switchport mode trunk
!
interface GigabitEthernet1/0/7
switchport mode trunk
!
interface GigabitEthernet1/0/8
switchport mode trunk
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
```

```
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/22
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/23
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/24
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
mac-address 0050.0fbb.8e01
ip address 192.168.0.3 255.255.255.0
ip helper-address 10.20.10.10
standby 10 ip 192.168.0.1
```

```
!
interface Vlan50
mac-address 0050.0fbb.8e02
ip address 10.10.0.3 255.255.255.0
ip helper-address 10.20.10.10
standby 50 ip 10.10.0.1
!
router ospf 25
router-id 1.2.1.2
log-adjacency-changes
network 10.30.10.4 0.0.0.3 area 1
network 10.10.0.0 0.0.255.255 area 1
network 192.168.0.0 0.0.15.255 area 1
network 172.16.0.0 0.0.15.255 area 1
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
!
end
```

TORONTO_CORE_SW2

```
CORE-SW2#SHOW RUN
Building configuration...

Current configuration : 2498 bytes
!
```

```
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname CORE-SW2
!
!
!
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username cisco password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface Port-channel1
switchport mode trunk
!
```

```
interface GigabitEthernet1/0/1
no switchport
ip address 10.30.10.9 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet1/0/2
switchport mode trunk
!
interface GigabitEthernet1/0/3
switchport mode trunk
!
interface GigabitEthernet1/0/4
switchport mode trunk
!
interface GigabitEthernet1/0/5
switchport mode trunk
!
interface GigabitEthernet1/0/6
switchport mode trunk
!
interface GigabitEthernet1/0/7
switchport mode trunk
!
interface GigabitEthernet1/0/8
switchport mode trunk
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
```

```
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/22
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/23
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/24
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
mac-address 0090.21e6.7101
ip address 192.168.0.2 255.255.255.0
ip helper-address 10.20.10.10
standby 10 ip 192.168.0.1
!
interface Vlan50
mac-address 0090.21e6.7102
ip address 10.10.0.2 255.255.255.0
ip helper-address 10.20.10.10
standby 50 ip 10.10.0.1
!
router ospf 25
```

```
router-id 1.3.1.3
log-adjacency-changes
network 10.30.10.8 0.0.0.3 area 1
network 10.10.0.0 0.0.255.255 area 1
network 192.168.0.0 0.0.15.255 area 1
network 172.16.0.0 0.0.15.255 area 1
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
!
End
```

7.3 MEDICAL_PHARMACY

```
MEDICAL_PHARMACY#SHOW RUN
Building configuration...

Current configuration : 4122 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname MEDICAL_PHARMACY
!
!
```

```
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
username cisco privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/4
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/5
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/6
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
```

```
interface FastEthernet0/7
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/8
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/9
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/10
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/11
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/12
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/13
switchport access vlan 10
switchport mode access
switchport voice vlan 99
```

```
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/14
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/15
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/16
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/17
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/18
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/19
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/20
```

```
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/21
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/22
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/23
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/24
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
line con 0
!
line vty 0 4
login
```

```
line vty 5 15
login
!
!
!
!
end


MEDICAL_PHARMACY#
```

7.4 RECEPTION

```
RECEPTION>EN
RECEPTION#SHOW RUN
Building configuration...

Current configuration : 4115 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname RECEPTION
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
username cisco privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
```

```
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/4
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/5
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/6
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/7
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/8
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/9
switchport access vlan 10
```

```
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/10
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/11
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/12
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/13
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/14
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/15
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
```

```
!
interface FastEthernet0/16
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/17
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/18
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/19
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/20
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/21
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/22
switchport access vlan 50
switchport mode access
spanning-tree portfast
```

```
spanning-tree bpduguard enable
!
interface FastEthernet0/23
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/24
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
end


RECEPTION#
```

7.5 DOCTORS-CONSUL

```
DOCTORS-CONSUL#SHOW RUN
Building configuration...
```

```
Current configuration : 4120 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname DOCTORS-CONSUL
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
username cisco privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/4
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/5
switchport access vlan 10
switchport mode access
```

```
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/6
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/7
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/8
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/9
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/10
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/11
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
```

```
interface FastEthernet0/12
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/13
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/14
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/15
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/16
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/17
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/18
switchport access vlan 10
switchport mode access
switchport voice vlan 99
```

```
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/19
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/20
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/21
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/22
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/23
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/24
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
```

```
no ip address
shutdown
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
end


DOCTORS-CONSUL#
```

7.6 HR-FINANCE

```
HR-FINANCE#show run
Building configuration...

Current configuration : 4116 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname HR-FINANCE
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
username cisco privilege 1 password 7 0822455D0A16
!
!
```

```
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/4
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/5
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/6
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/7
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/8
```

```
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/9
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/10
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/11
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/12
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/13
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/14
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
```

```
spanning-tree bpduguard enable
!
interface FastEthernet0/15
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/16
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/17
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/18
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/19
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/20
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/21
switchport access vlan 50
```

```
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/22
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/23
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/24
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
end
```

HR-FINANCE#

7.7 CORP-AUDIT

```
CORP-AUDIT#show run
Building configuration...

Current configuration : 4116 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname CORP-AUDIT
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
username cisco privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/4
switchport access vlan 10
switchport mode access
```

```
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/5
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/6
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/7
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/8
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/9
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/10
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
```

```
interface FastEthernet0/11
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/12
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/13
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/14
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/15
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/16
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/17
switchport access vlan 10
switchport mode access
switchport voice vlan 99
```

```
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/18
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/19
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/20
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/21
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/22
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/23
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/24
switchport access vlan 50
switchport mode access
spanning-tree portfast
```

```
spanning-tree bpduguard enable
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
End
```

7.8 IT-TEAM

```
IT-TEAM# show run
Building configuration...

Current configuration : 4113 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname IT-TEAM
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
```

```
!
username cisco privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/4
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/5
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/6
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/7
switchport access vlan 10
switchport mode access
switchport voice vlan 99
```

```
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/8
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/9
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/10
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/11
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/12
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/13
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/14
```

```
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/15
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/16
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/17
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/18
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/19
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/20
switchport access vlan 10
switchport mode access
switchport voice vlan 99
spanning-tree portfast
```

```
spanning-tree bpduguard enable
!
interface FastEthernet0/21
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/22
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/23
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/24
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
```

```
!
!
end

IT-TEAM#
```

7.9 VANCOUVER

```
BR1_ROUTER#show run
Building configuration...

Current configuration : 1508 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname BR1_ROUTER
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2811/K9 sn FTX1017QVLE-
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
```

```
!
!
interface FastEthernet0/0
ip address 10.30.10.25 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
no ip address
!
interface FastEthernet0/0.60
encapsulation dot1Q 60
no ip address
!
interface FastEthernet0/1
ip address 10.30.10.21 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1.20
no ip address
!
interface FastEthernet0/1.60
no ip address
!
interface Serial0/1/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/1/1
no ip address
clock rate 2000000
shutdown
!
interface Serial0/3/0
ip address 192.200.100.10 255.255.255.252
!
interface Serial0/3/1
ip address 192.200.100.13 255.255.255.252
clock rate 2000000
!
interface FastEthernet1/0
no ip address
duplex auto
```

```
speed auto
shutdown
!
interface FastEthernet1/1
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 25
log-adjacency-changes
network 10.30.10.20 0.0.0.3 area 2
network 10.30.10.24 0.0.0.3 area 2
network 192.200.100.12 0.0.0.3 area 0
network 192.200.100.8 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end


BR1_ROUTER#
```

```
MLS1-BR1#SHOW RUN
Building configuration...

Current configuration : 2385 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname MLS1-BR1
!
!
!
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username cisco password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
!
spanning-tree mode pvst
!
!
!
!
```

```
!
!
interface Port-channel1
switchport mode trunk
!
interface GigabitEthernet1/0/1
no switchport
ip address 10.30.10.22 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet1/0/2
switchport mode trunk
!
interface GigabitEthernet1/0/3
switchport mode trunk
!
interface GigabitEthernet1/0/4
switchport mode trunk
!
interface GigabitEthernet1/0/5
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/6
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/7
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
```

```
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
no ip address
shutdown
!
interface Vlan20
mac-address 0060.3ee2.8d01
ip address 192.168.1.3 255.255.255.0
ip helper-address 10.20.10.10
standby 20 ip 192.168.1.1
!
interface Vlan60
mac-address 0060.3ee2.8d02
ip address 10.10.1.3 255.255.255.0
ip helper-address 10.20.10.10
standby 60 ip 10.10.1.1
!
router ospf 25
log-adjacency-changes
```

```
passive-interface Vlan20
passive-interface Vlan60
network 10.30.10.20 0.0.0.3 area 2
network 192.168.1.0 0.0.0.255 area 2
network 10.10.1.0 0.0.0.255 area 2
network 172.16.1.0 0.0.0.255 area 2
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
!
end
```

MLS2-BR1

```
MLS2-BR1#show run
Building configuration...

Current configuration : 2385 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname MLS2-BR1
!
```

```
!
!
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username cisco password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface Port-channel1
switchport mode trunk
!
interface GigabitEthernet1/0/1
no switchport
ip address 10.30.10.26 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet1/0/2
```

```
switchport mode trunk
!
interface GigabitEthernet1/0/3
switchport mode trunk
!
interface GigabitEthernet1/0/4
switchport mode trunk
!
interface GigabitEthernet1/0/5
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/6
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/7
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
```

```
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
no ip address
shutdown
!
interface Vlan20
mac-address 0090.0c94.d401
ip address 192.168.1.2 255.255.255.0
ip helper-address 10.20.10.10
standby 20 ip 192.168.1.1
!
interface Vlan60
mac-address 0090.0c94.d402
ip address 10.10.1.2 255.255.255.0
ip helper-address 10.20.10.10
standby 60 ip 10.10.1.1
!
router ospf 25
log-adjacency-changes
passive-interface Vlan20
passive-interface Vlan60
network 10.30.10.24 0.0.0.3 area 2
network 192.168.1.0 0.0.0.255 area 2
network 10.10.1.0 0.0.0.255 area 2
network 172.16.1.0 0.0.0.255 area 2
!
ip classless
!
ip flow-export version 9
!
!
```

```
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
!
end


MLS2-BR1#
```

7.10 CALGARY

```
Building configuration...

Current configuration : 2385 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname MLS1-BR3
!
!
!
!
!
!
!
no ip cef
ip routing
!
```

```
no ipv6 cef
!
!
!
username cisco password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface Port-channel1
switchport mode trunk
!
interface GigabitEthernet1/0/1
no switchport
ip address 10.30.10.30 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet1/0/2
switchport mode trunk
!
interface GigabitEthernet1/0/3
switchport mode trunk
!
interface GigabitEthernet1/0/4
switchport mode trunk
!
interface GigabitEthernet1/0/5
```

```
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/6
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/7
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
```

```
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
no ip address
shutdown
!
interface Vlan30
mac-address 000c.cf4d.7b01
ip address 192.168.3.3 255.255.255.0
ip helper-address 10.20.10.10
standby 30 ip 192.168.3.1
!
interface Vlan70
mac-address 000c.cf4d.7b02
ip address 10.10.3.3 255.255.255.0
ip helper-address 10.20.10.10
standby 70 ip 10.10.3.1
!
router ospf 25
log-adjacency-changes
passive-interface Vlan30
passive-interface Vlan70
network 10.30.10.28 0.0.0.3 area 4
network 192.168.3.0 0.0.0.255 area 4
network 10.10.3.0 0.0.0.255 area 4
network 172.16.3.0 0.0.0.255 area 4
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
!
line con 0
!
line aux 0
```

```
!
line vty 0 4
login
!
!
!
!
end


MLS1-BR3#


MLS2-BR3#show run
Building configuration...

Current configuration : 2385 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname MLS2-BR3
!
!
!
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username cisco password 7 0822455D0A16
!
!
!
!
!
!
!
```

```
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface Port-channel1
switchport mode trunk
!
interface GigabitEthernet1/0/1
no switchport
ip address 10.30.10.34 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet1/0/2
switchport mode trunk
!
interface GigabitEthernet1/0/3
switchport mode trunk
!
interface GigabitEthernet1/0/4
switchport mode trunk
!
interface GigabitEthernet1/0/5
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/6
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/7
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/8
```

```
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
no ip address
shutdown
!
interface Vlan30
```

```
mac-address 00e0.8f1c.6401
ip address 192.168.3.2 255.255.255.0
ip helper-address 10.20.10.10
standby 30 ip 192.168.3.1
!
interface Vlan70
mac-address 00e0.8f1c.6402
ip address 10.10.3.2 255.255.255.0
ip helper-address 10.20.10.10
standby 70 ip 10.10.3.1
!
router ospf 25
log-adjacency-changes
passive-interface Vlan30
passive-interface Vlan70
network 10.30.10.32 0.0.0.3 area 4
network 192.168.3.0 0.0.0.255 area 4
network 10.10.3.0 0.0.0.255 area 4
network 172.16.3.0 0.0.0.255 area 4
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
!
end


MLS2-BR3#
```

```
FIRST-FLOOR#show run
Building configuration...

Current configuration : 4117 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname FIRST-FLOOR
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
username cisco privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/4
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
```

```
interface FastEthernet0/5
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/6
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/7
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/8
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/9
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/10
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/11
switchport access vlan 30
switchport mode access
switchport voice vlan 99
```

```
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/12
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/13
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/14
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/15
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/16
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/17
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/18
```

```
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/19
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/20
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/21
switchport access vlan 70
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/22
switchport access vlan 70
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/23
switchport access vlan 70
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/24
switchport access vlan 70
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface GigabitEthernet0/1
!
```

```
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
end


FIRST-FLOOR#


2nd-FLOOR#show run
Building configuration...

Current configuration : 4115 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname 2nd-FLOOR
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
username cisco privilege 1 password 7 0822455D0A16
!
```

```
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/4
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/5
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/6
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/7
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
```

```
interface FastEthernet0/8
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/9
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/10
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/11
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/12
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/13
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/14
switchport access vlan 30
switchport mode access
switchport voice vlan 99
```

```
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/15
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/16
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/17
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/18
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/19
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/20
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/21
```

```
switchport access vlan 70
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/22
switchport access vlan 70
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/23
switchport access vlan 70
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/24
switchport access vlan 70
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
End
```

```
3rd-FLOOR#show run
Building configuration...

Current configuration : 4115 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname 3rd-FLOOR
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
username cisco privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/4
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/5
```

```
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/6
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/7
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/8
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/9
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/10
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/11
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
```

```
spanning-tree bpduguard enable
!
interface FastEthernet0/12
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/13
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/14
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/15
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/16
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/17
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/18
switchport access vlan 30
```

```
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/19
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/20
switchport access vlan 30
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/21
switchport access vlan 70
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/22
switchport access vlan 70
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/23
switchport access vlan 70
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/24
switchport access vlan 70
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
```

```
!
interface Vlan1
no ip address
shutdown
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
end


3rd-FLOOR#
```

7.11 BRAMPTON

```
MLS1-BR2#SHOW RUN
Building configuration...

Current configuration : 2333 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname MLS1-BR2
!
!
!
!
!
!
!
```

```
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username cisco password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface Port-channel1
switchport mode trunk
!
interface GigabitEthernet1/0/1
no switchport
ip address 10.30.10.14 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet1/0/2
switchport mode trunk
!
interface GigabitEthernet1/0/3
switchport mode trunk
!
interface GigabitEthernet1/0/4
```

```
switchport mode trunk
!
interface GigabitEthernet1/0/5
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/6
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/7
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
```

```
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
no ip address
shutdown
!
interface Vlan40
mac-address 0060.5c77.b001
ip address 192.168.4.3 255.255.255.0
ip helper-address 10.20.10.10
standby 40 ip 192.168.4.1
!
interface Vlan80
mac-address 0060.5c77.b002
ip address 10.10.4.3 255.255.255.0
ip helper-address 10.20.10.10
standby 80 ip 10.10.4.1
!
router ospf 25
log-adjacency-changes
network 10.30.10.12 0.0.0.3 area 3
network 192.168.4.0 0.0.0.255 area 3
network 10.10.4.0 0.0.0.255 area 3
network 172.16.4.0 0.0.0.255 area 3
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
!
line con 0
!
```

```
line aux 0
!
line vty 0 4
login
!
!
!
!
end
```

MLS1-BR2#

MLS2-BR2#SHOW RUN
Building configuration...

```
Current configuration : 2333 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname MLS2-BR2
!
!
!
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username cisco password 7 0822455D0A16
!
!
!
!
!
!
```

```
!
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface Port-channel1
switchport mode trunk
!
interface GigabitEthernet1/0/1
no switchport
ip address 10.30.10.18 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet1/0/2
switchport mode trunk
!
interface GigabitEthernet1/0/3
switchport mode trunk
!
interface GigabitEthernet1/0/4
switchport mode trunk
!
interface GigabitEthernet1/0/5
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/6
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/7
switchport mode trunk
channel-group 1 mode active
!
```

```
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
no ip address
shutdown
!
```

```
interface Vlan40
mac-address 0003.e461.9e01
ip address 192.168.4.2 255.255.255.0
ip helper-address 10.20.10.10
standby 40 ip 192.168.4.1
!
interface Vlan80
mac-address 0003.e461.9e02
ip address 10.10.4.2 255.255.255.0
ip helper-address 10.20.10.10
standby 80 ip 10.10.4.1
!
router ospf 25
log-adjacency-changes
network 10.30.10.16 0.0.0.3 area 3
network 192.168.4.0 0.0.0.255 area 3
network 10.10.4.0 0.0.0.255 area 3
network 172.16.4.0 0.0.0.255 area 3
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
!
end


MLS2-BR2#
```

```
FIRST-FLOOR#show run
Building configuration...

Current configuration : 4117 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname FIRST-FLOOR
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
username cisco privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/4
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/5
```

```
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/6
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/7
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/8
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/9
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/10
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/11
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
```

```
spanning-tree bpduguard enable
!
interface FastEthernet0/12
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/13
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/14
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/15
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/16
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/17
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/18
switchport access vlan 40
```

```
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/19
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/20
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/21
switchport access vlan 80
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/22
switchport access vlan 80
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/23
switchport access vlan 80
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/24
switchport access vlan 80
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
```

```
!
interface Vlan1
no ip address
shutdown
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
end


FIRST-FLOOR#


2nd-FLOOR#show run
Building configuration...

Current configuration : 4115 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname 2nd-FLOOR
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
username cisco privilege 1 password 7 0822455D0A16
!
!
```

```
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/4
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/5
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/6
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/7
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/8
```

```
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/9
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/10
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/11
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/12
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/13
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/14
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
```

```
spanning-tree bpduguard enable
!
interface FastEthernet0/15
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/16
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/17
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/18
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/19
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/20
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/21
switchport access vlan 80
```

```
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/22
switchport access vlan 80
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/23
switchport access vlan 80
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/24
switchport access vlan 80
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
end
```

2nd-FLOOR#

3rd-FLOOR#show run
Building configuration...

Current configuration : 4115 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname 3rd-FLOOR
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name nlh.com
!
username cisco privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/4
switchport access vlan 40
switchport mode access
switchport voice vlan 99

```
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/5
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/6
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/7
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/8
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/9
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/10
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/11
```

```
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/12
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/13
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/14
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/15
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/16
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/17
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
```

```
spanning-tree bpduguard enable
!
interface FastEthernet0/18
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/19
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/20
switchport access vlan 40
switchport mode access
switchport voice vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/21
switchport access vlan 80
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/22
switchport access vlan 80
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/23
switchport access vlan 80
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/24
switchport access vlan 80
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
```

```
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
banner motd ^C UNAUTHORISED ACCESS IS PUNISHABLE11111^C
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
end


3rd-FLOOR#
```

Practical Implementation:

Figure 109
Physical Implementation Network Diagram

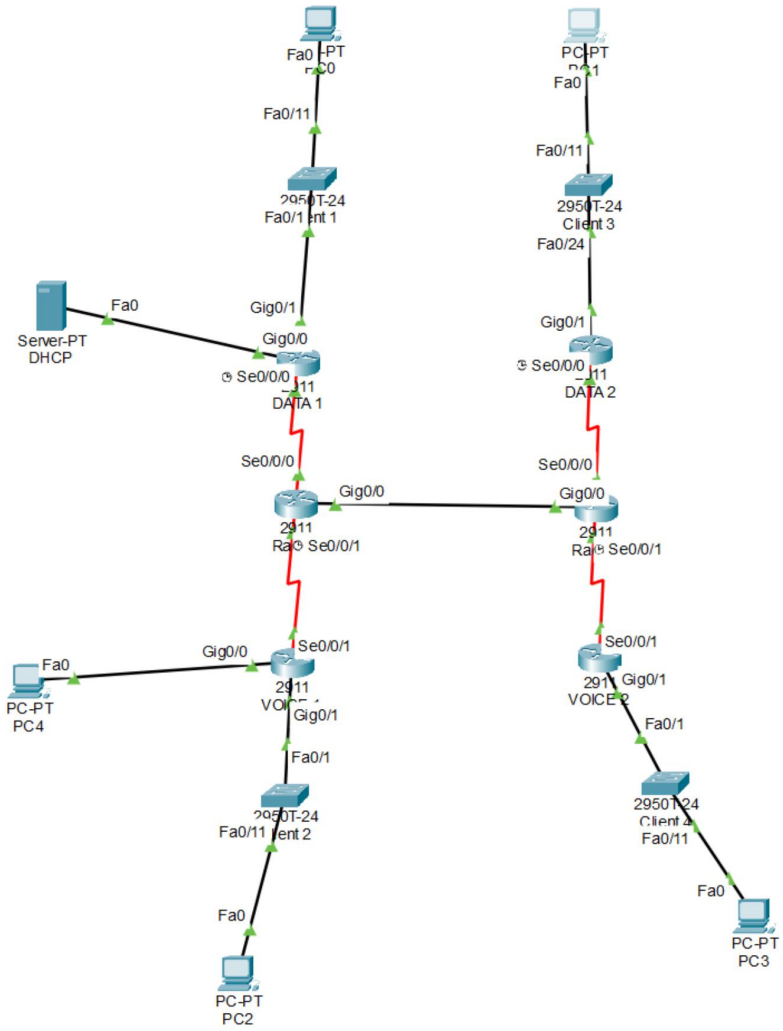


Figure 110
Routers and Switches Connection

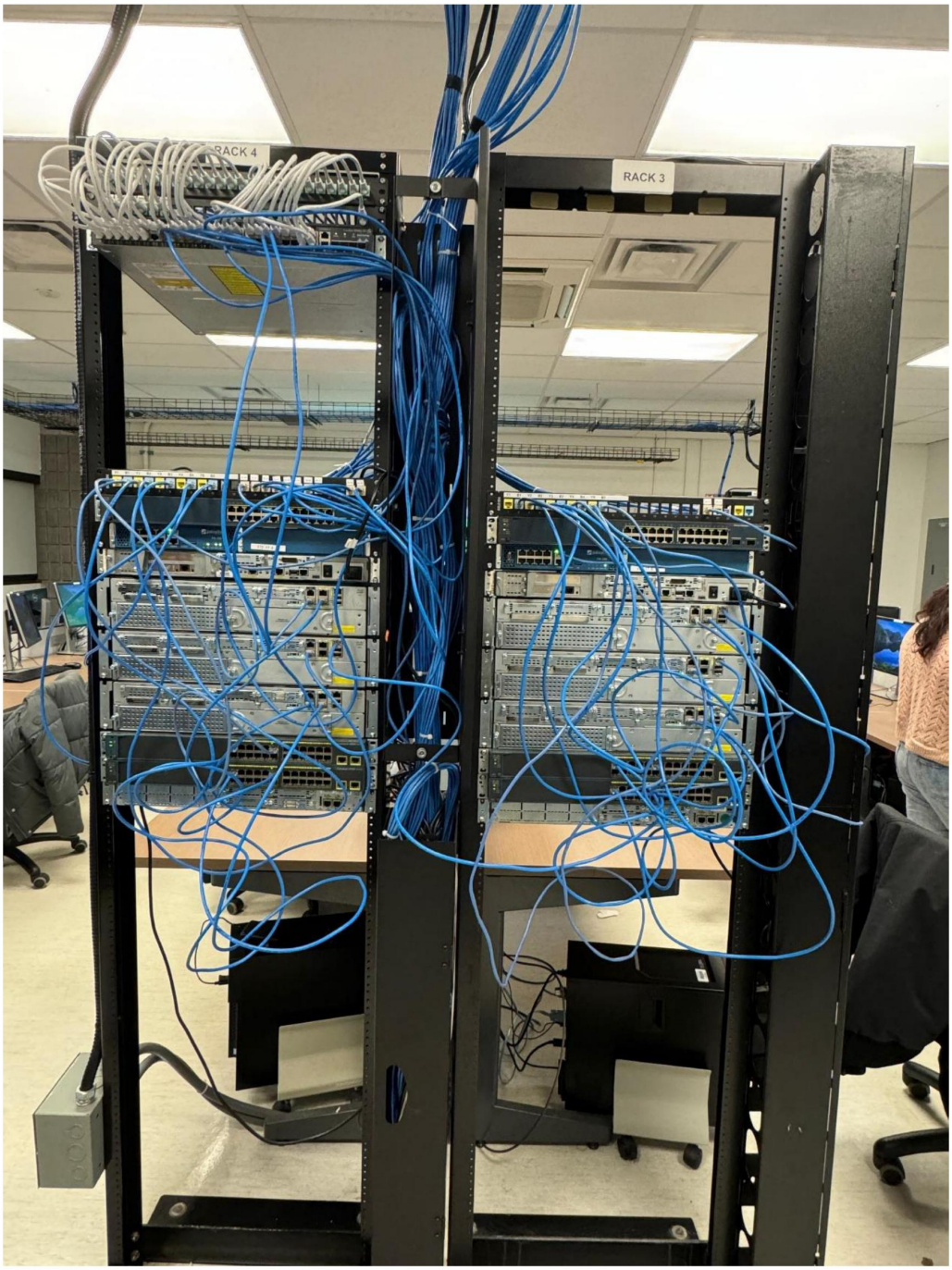


Figure 111
DHCP Pools

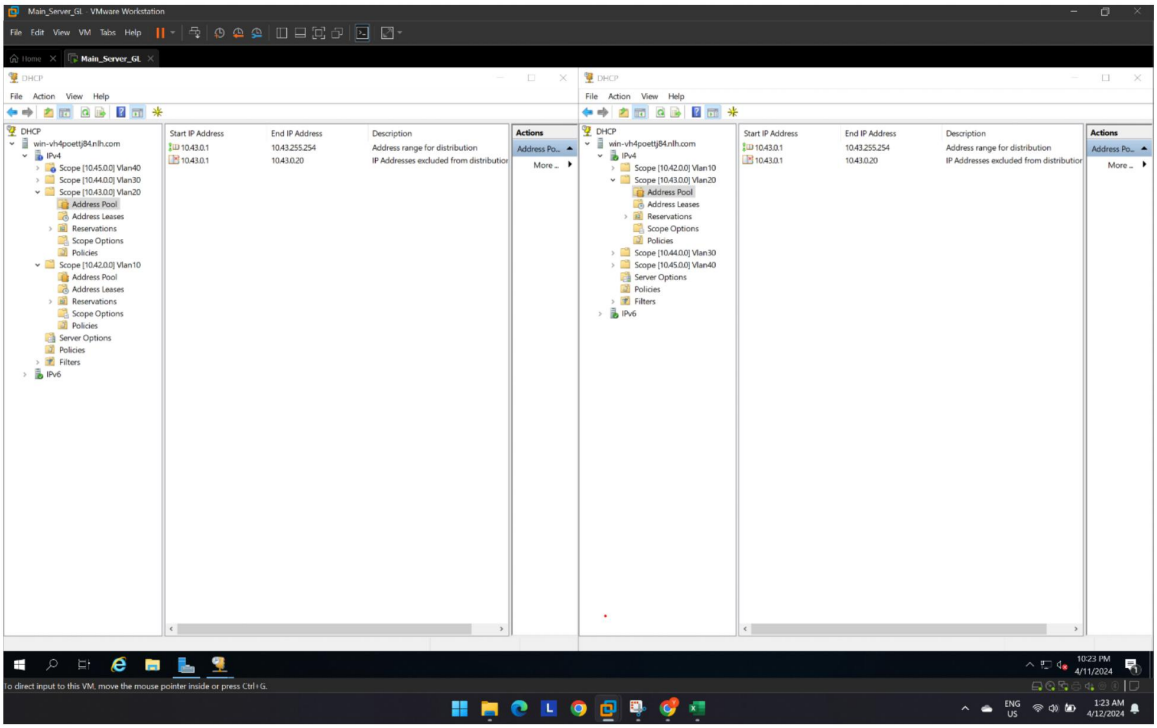


Figure 112
Client 1 IP Address From DHCP POOL

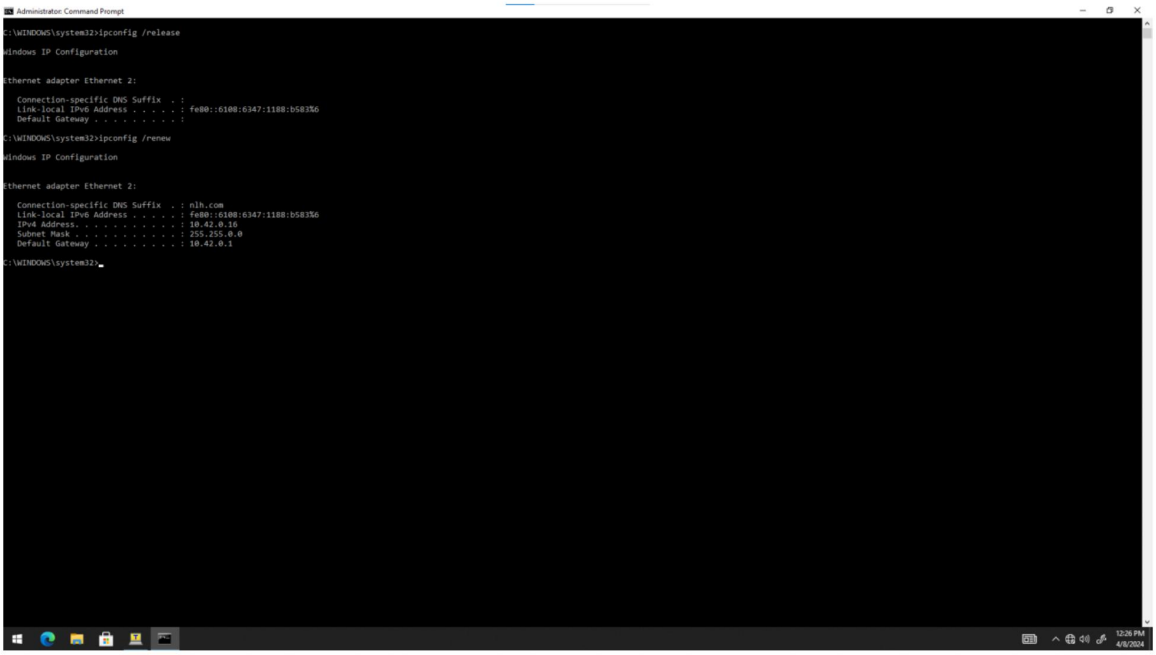


Figure 113
Client 2 IP Address from DHCP

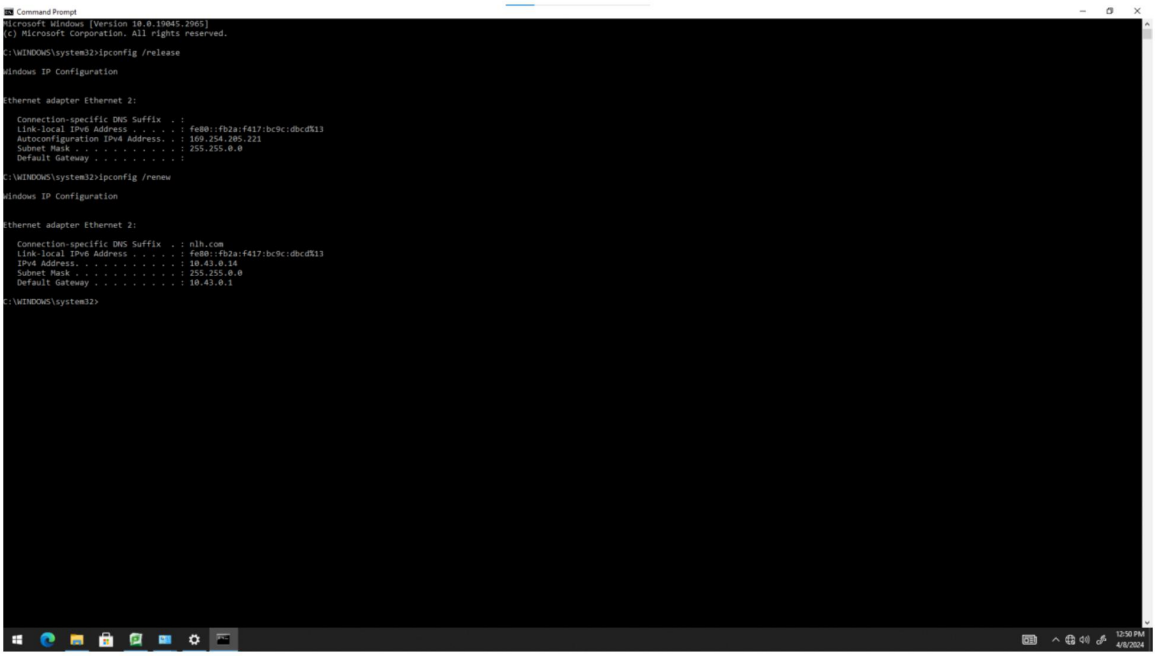


Figure 114
DNS Server

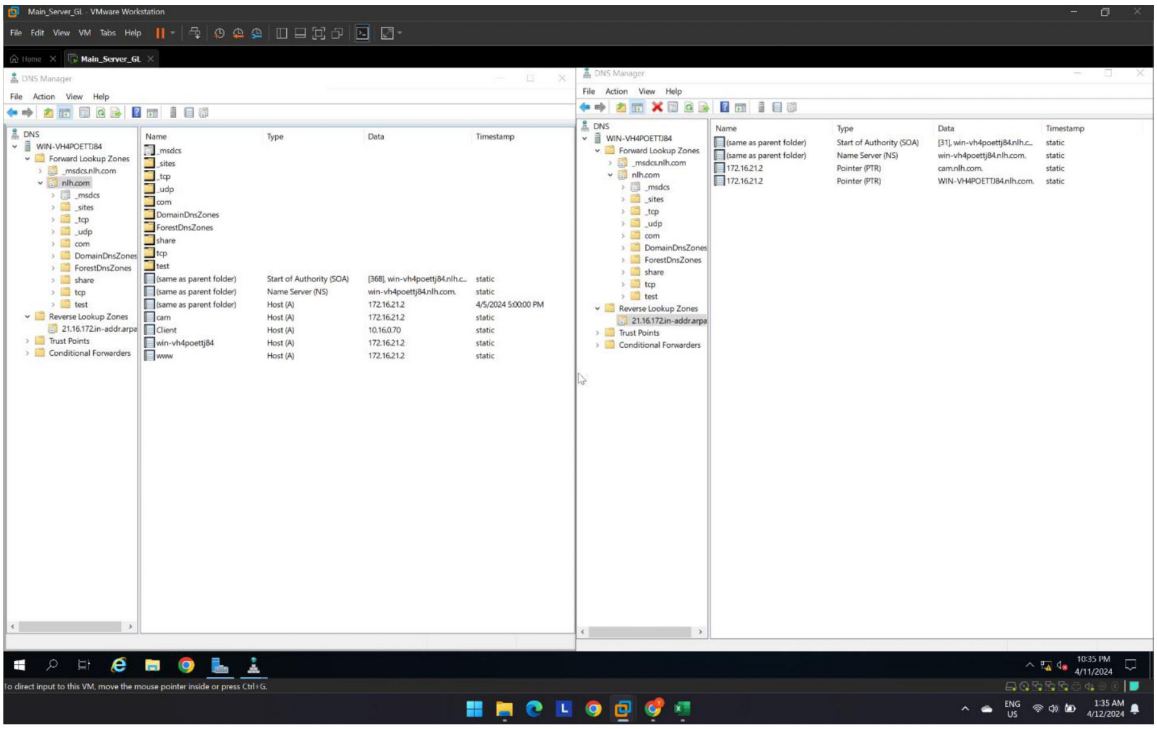


Figure 115
DNS Website On Client Side

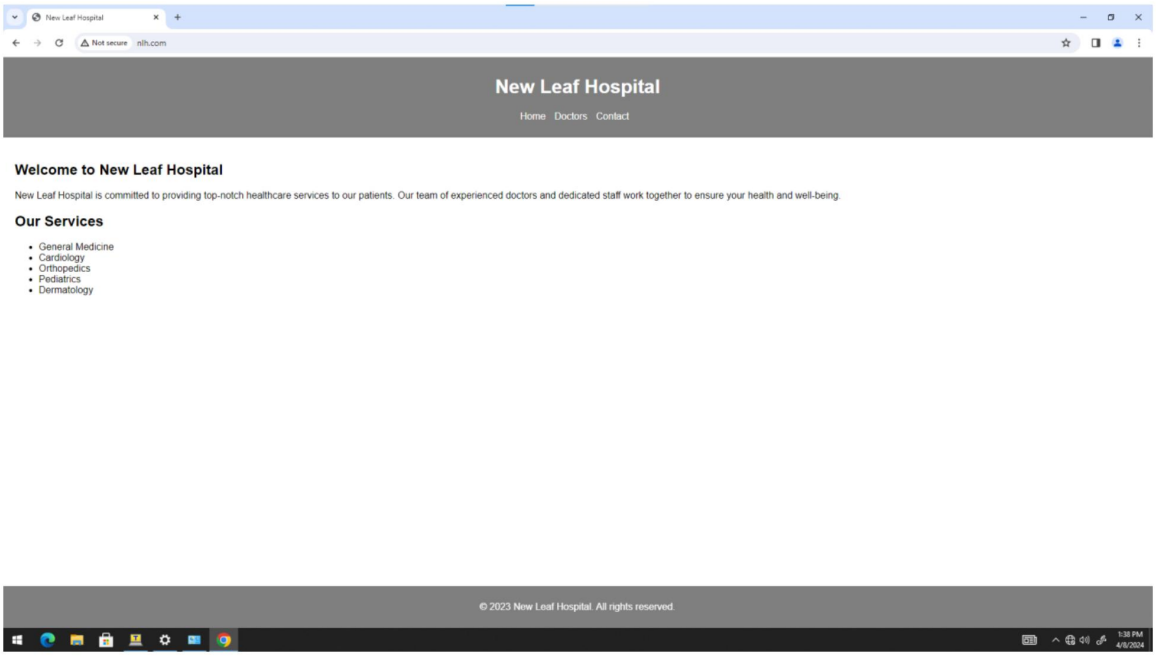


Figure 116
IIS Service

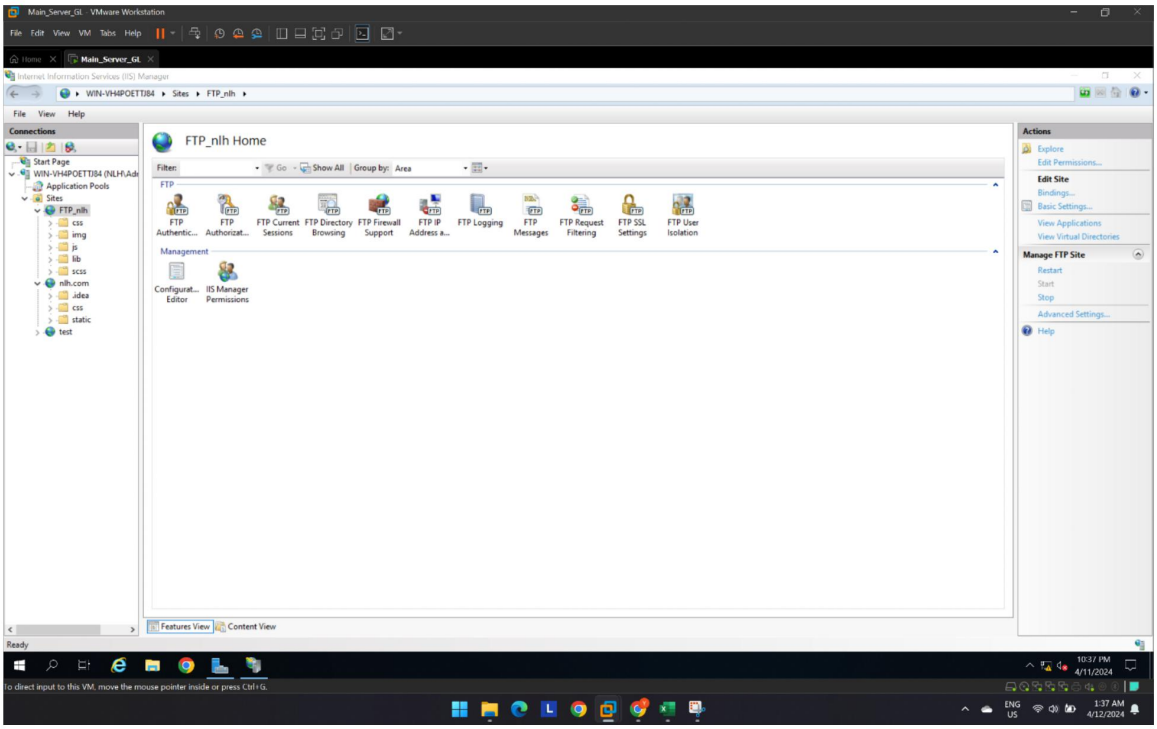


Figure 117
FTP Access Authentication

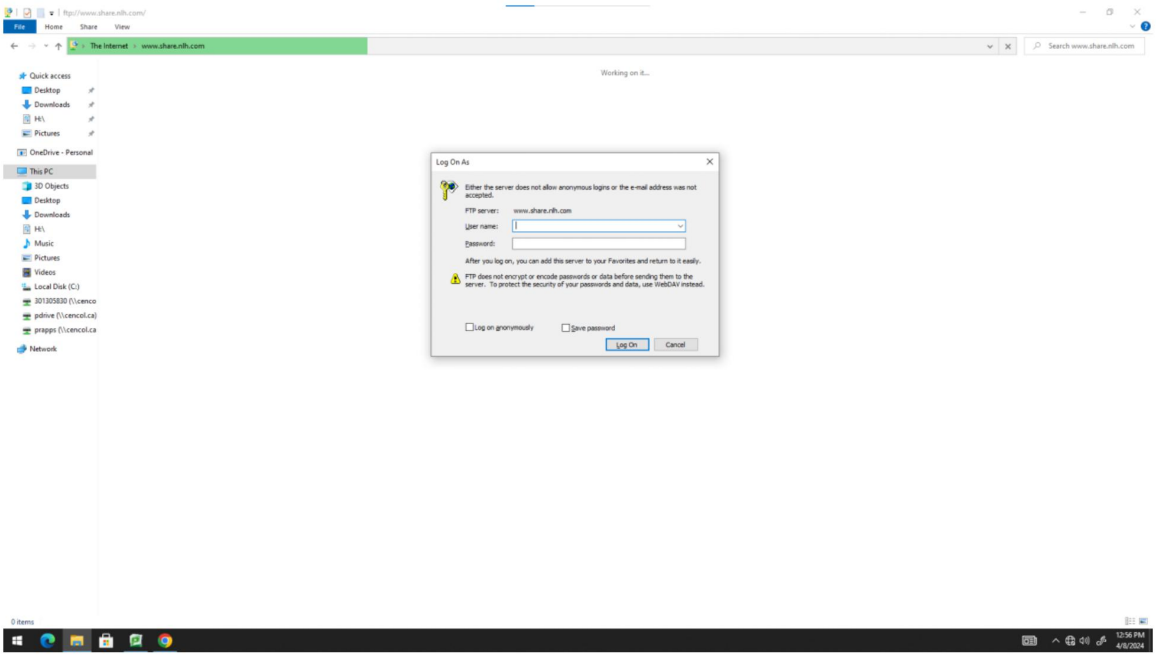


Figure 118
FTP Access Authentication User

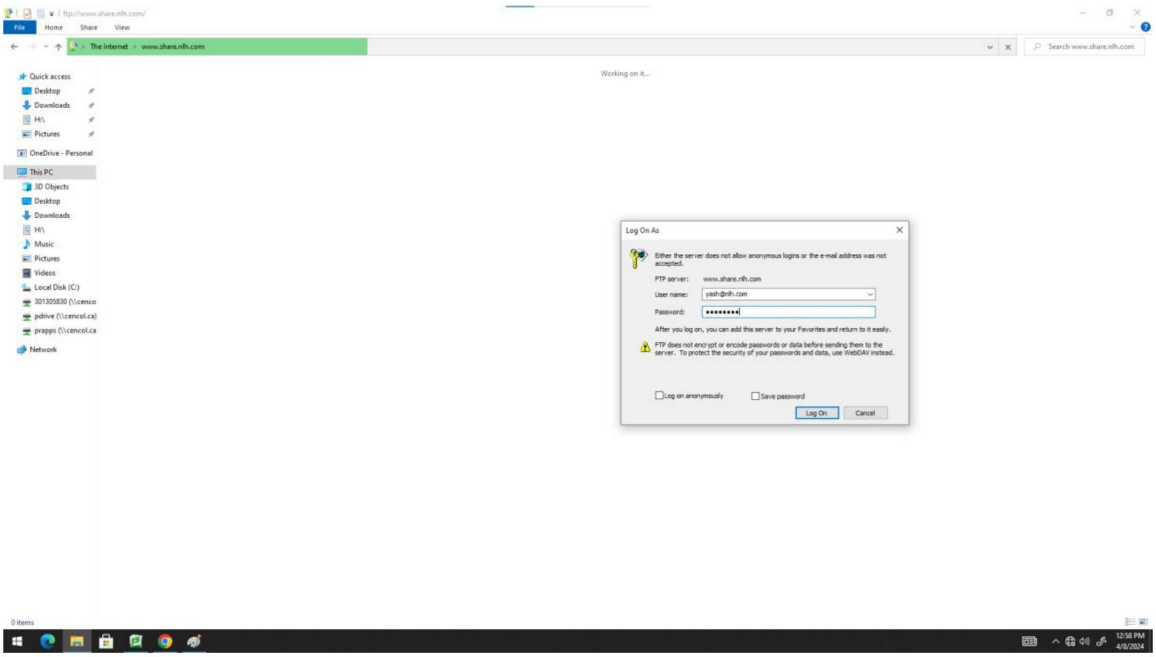


Figure 119
FTP Access Authentication User Accessed

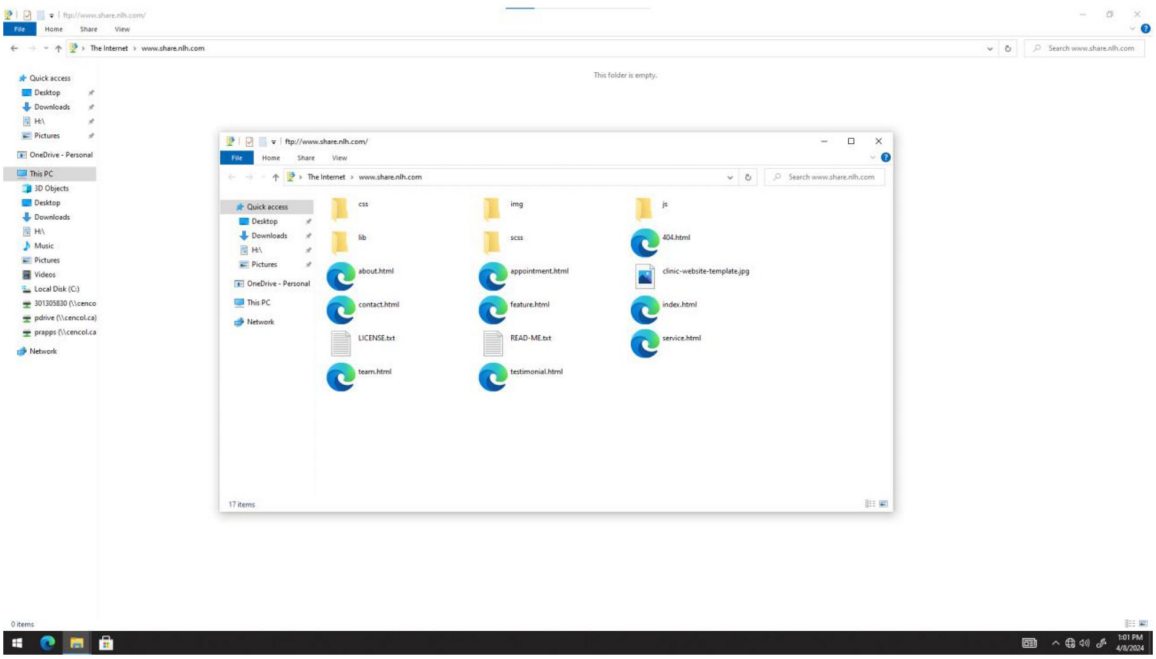


Figure 120
FTP Session

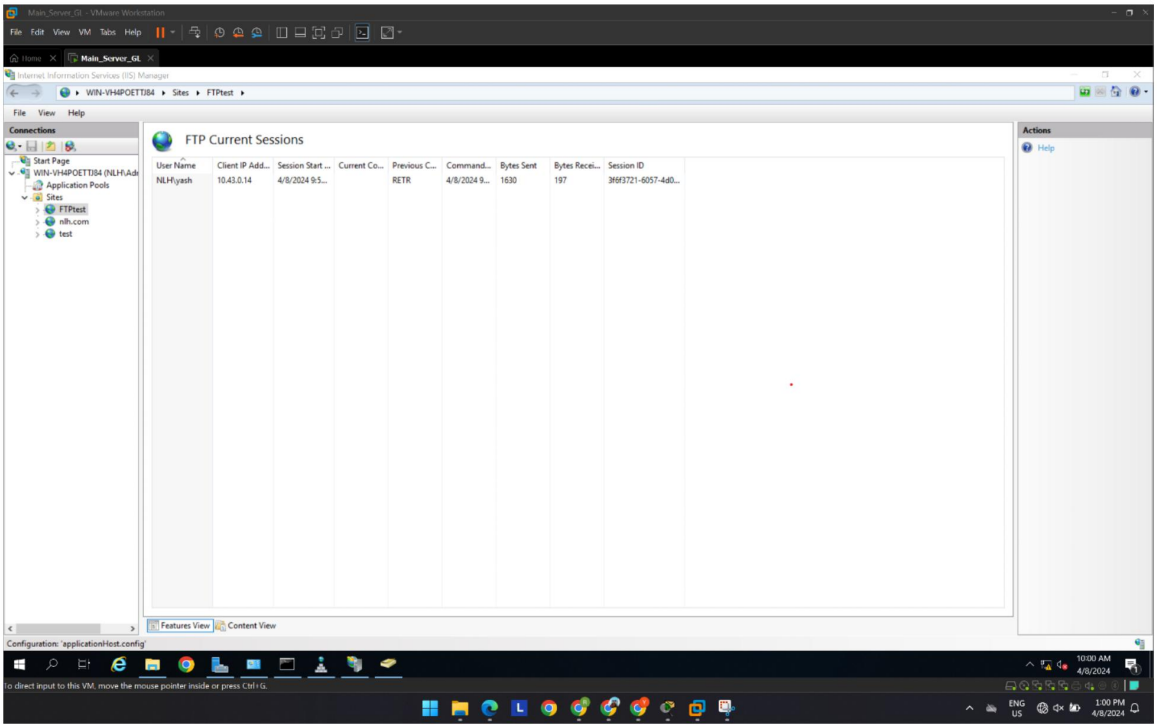


Figure 121
IOT YAWCAM Administrator

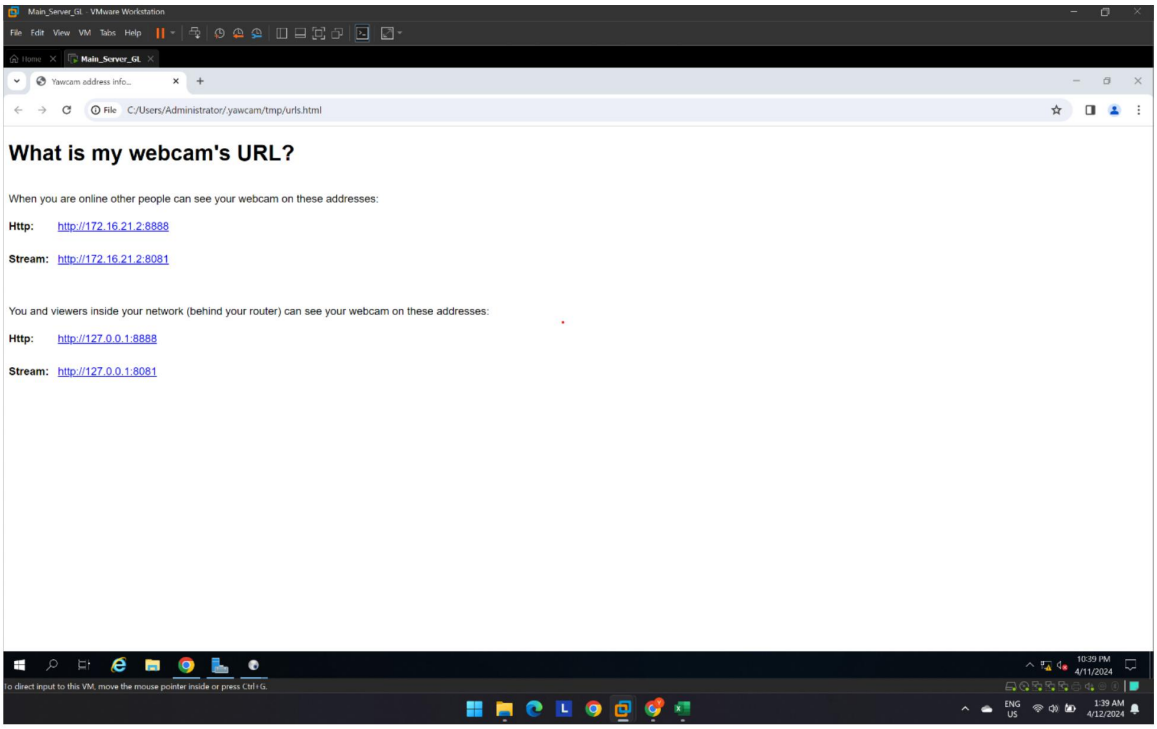


Figure 122
IOT CAM Accessed from Client Side

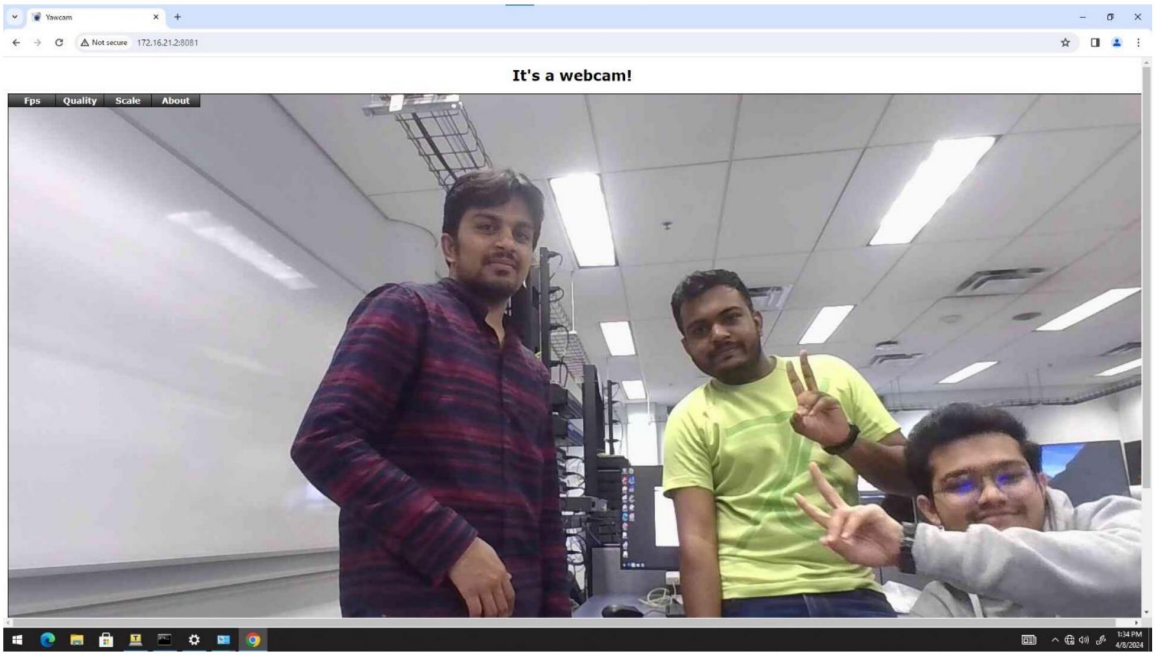


Figure 123
VOIP Client 1 IP address

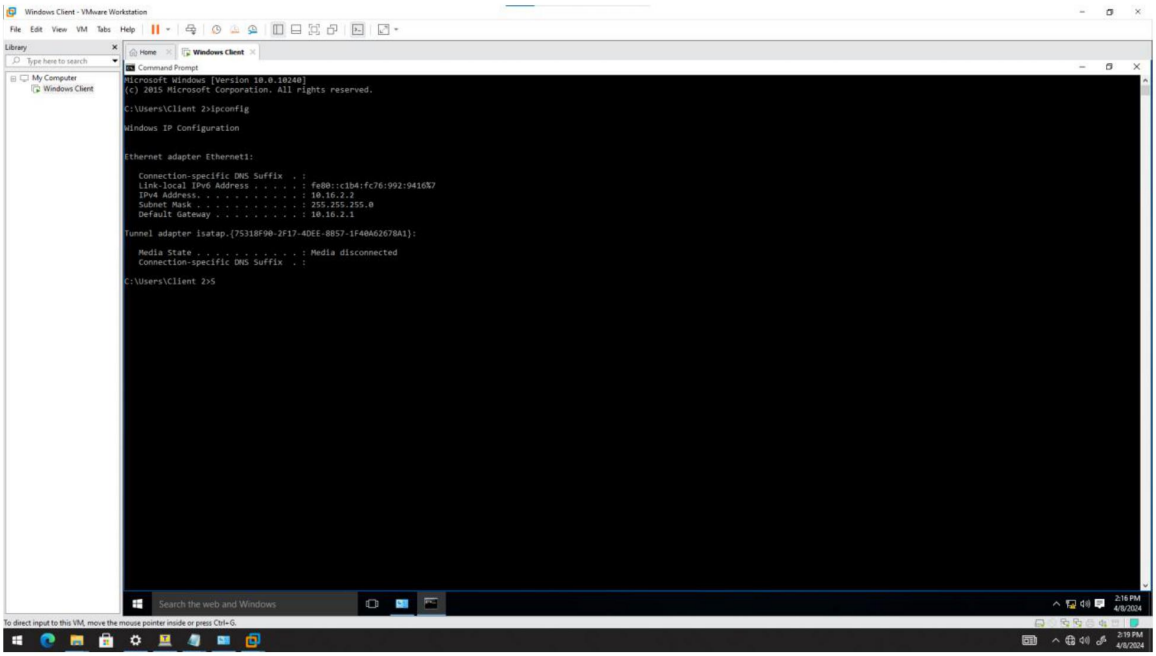


Figure 124
VOIP Client 2 IP address

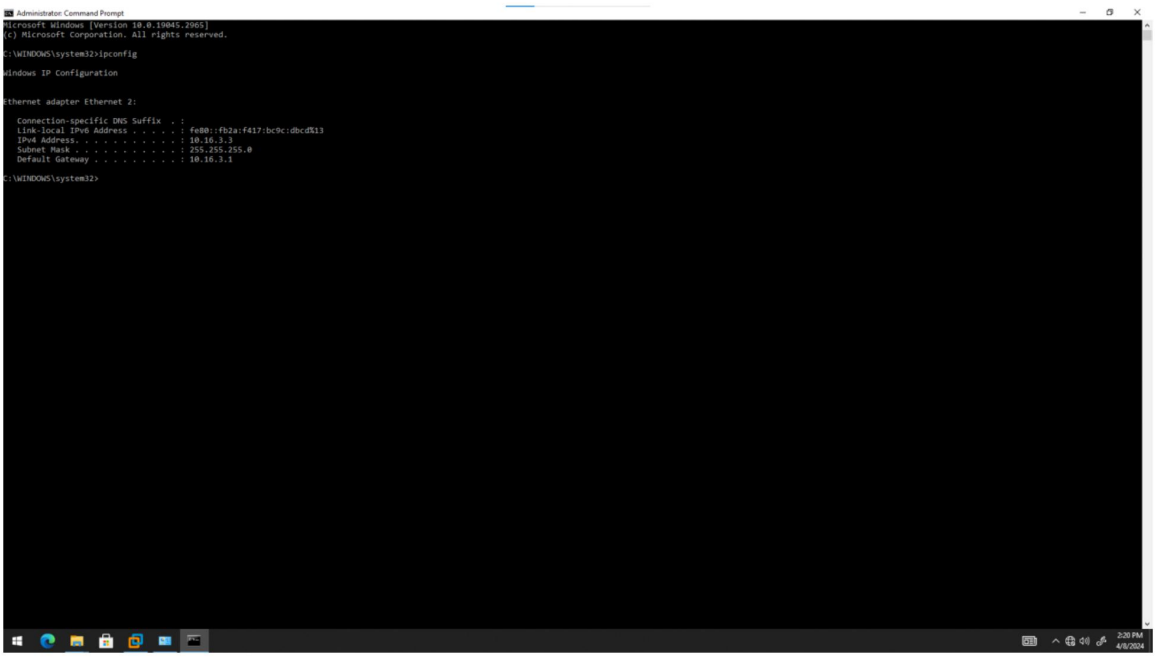


Figure 125
Telephony Session

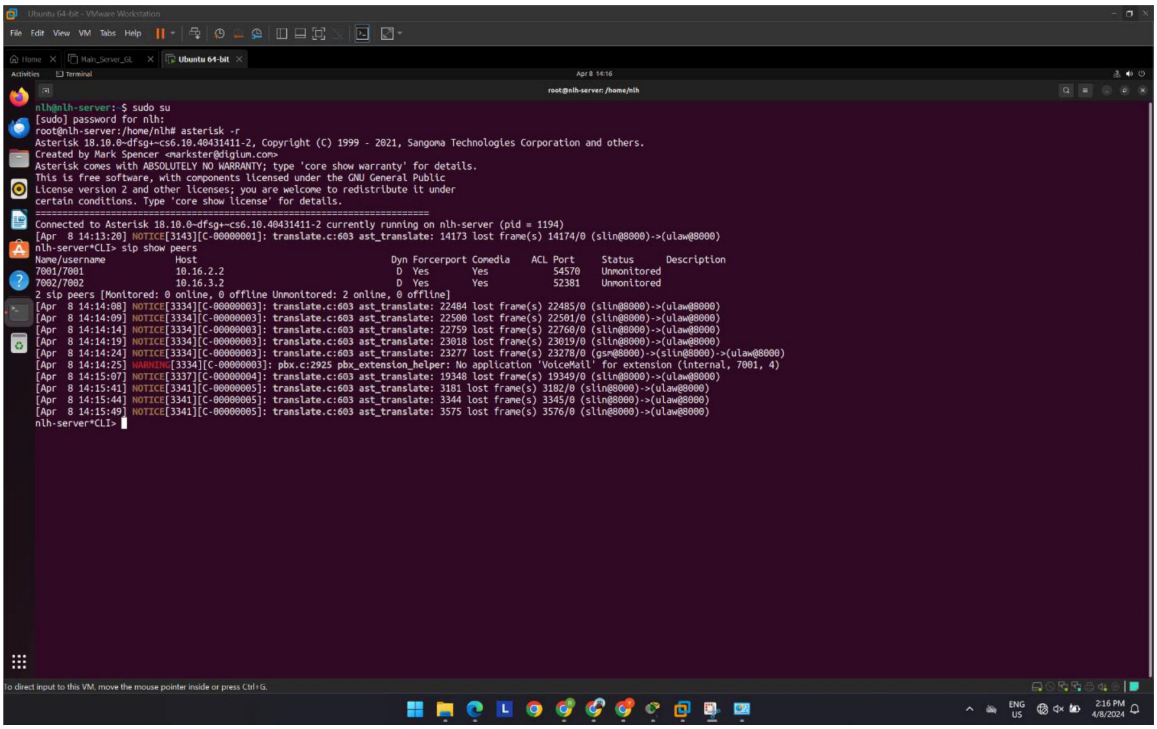


Figure 126
VOIP Client 1 Calling Client 2

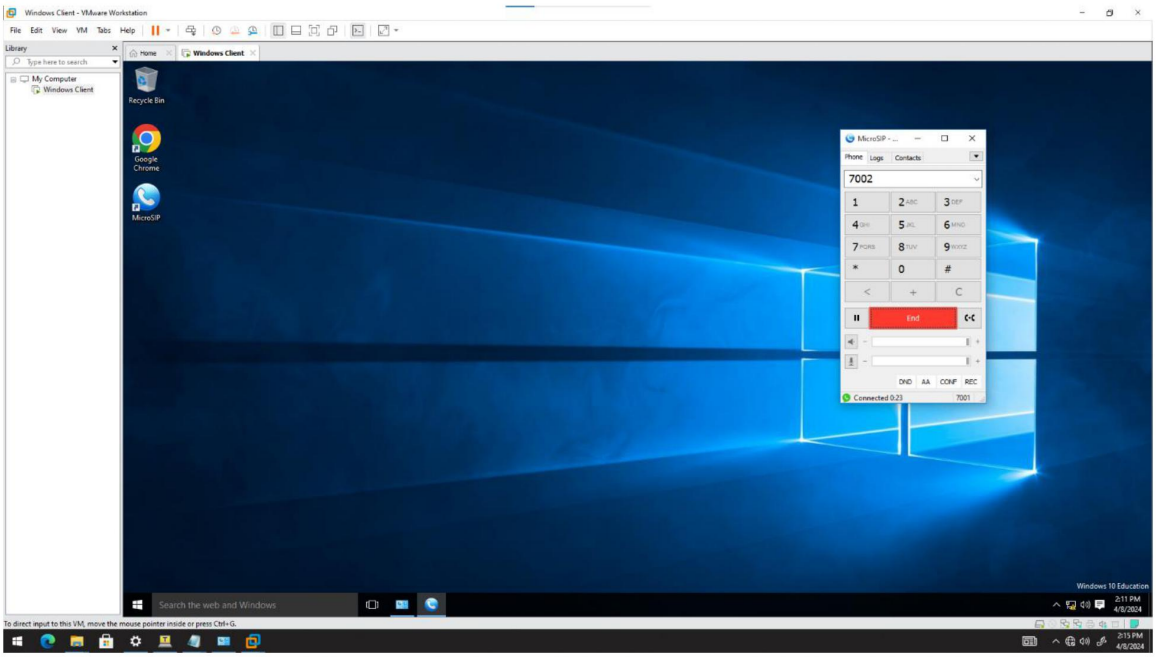
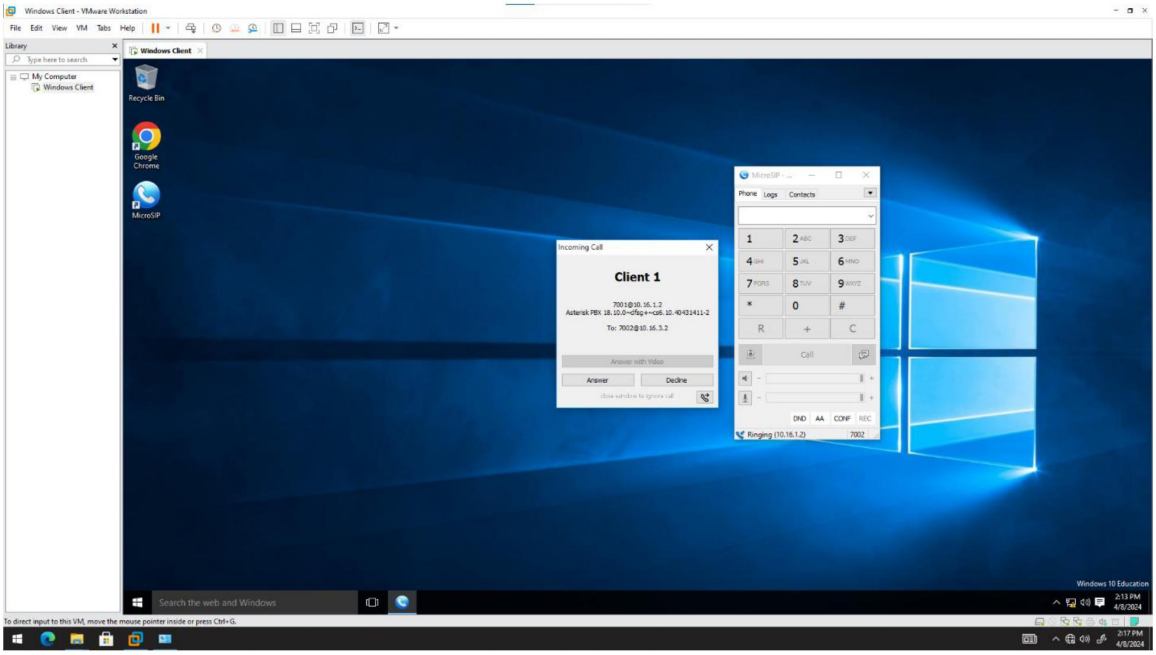


Figure 127
VOIP Client 2 Receiving Call from Client 1



References

FS. (n.d.). *Fiber Optic Cable*. Retrieved from fs.com: https://www.fs.com/products/40191.html

FS. (n.d.). *Layer 3 Switch*. Retrieved from fs.com: https://www.fs.com/products/185426.html

HID. (n.d.). *HID Proximity Plus 6005*. Retrieved from hidglobal.com: https://www.hidglobal.com/products/6005

Kits, C. &. (n.d.). *Cat 6 Cable*. Retrieved from cable&kits.com: https://www.cablesandkits.com/mc/cabling/data-console-cables/console-cables/cabconusb/fam-334/fp-9900/

reolink. (n.d.). *Smart 4K Ultra HD PoE Camera*. Retrieved from reolink.com: https://reolink.com/product/rlc-820a/?attribute_pa_version=1-pack-white

Router-Switch. (n.d.). *Palo Alto PA-800 Series Firewalls*. Retrieved from Router-Switch.com: https://www.router-switch.com/palo-alto-pa-800-series-price.html

Technologies, D. (n.d.). *OptiPlex 3000 Micro Form Factor*. Retrieved from dell.com: https://www.dell.com/en-ca/shop/dell-desktops-workstations/optiplex-3000-micro-form-factor/spd/optiplex-3000-micro

Warehouse, i. (n.d.). *IP Phones*. Retrieved from ipphonewarehouse.com: https://www.ipphone-warehouse.com/yealink-t33g-ip-phone-p/sip-t33g.htm