TRIBHUVAN UNIVERSITY

INSTITUTE OF ENGINEERING

THAPATHALI CAMPUS

CASE STUDY

ON

MERAKI TECHS OFFICE NETWORK

Submitted By:

Bibek Joshi (THA079BEI007)

Submitted To:

Department of Electronics and Computer Engineering

Thapathali Campus, Kathmandu, Nepal

August 15, 2025

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to **Meraki Techs Pvt. Ltd.**, where I am currently employed, for allowing me full access to the office network and providing the necessary support and cooperation to conduct this case study. Their willingness to share information about network infrastructure, devices, and operations made it possible to prepare a detailed and practical analysis.

I would also like to thank our lab instructor **Er. Jalauddin Mansur** and the Department of Electronics and Computer Engineering, Thapathali Campus, for their guidance, encouragement, and constructive feedback throughout the preparation of this report.

Finally, I extend my appreciation to my colleagues at Meraki Techs who assisted in providing information, clarifying technical details, and sharing their experiences regarding the company's network operations.

Table of Contents

INTRODUCTION

A company network is a private computer network designed to connect various departments, workstations, servers, and devices within an organization. It facilitates internal communication, resource sharing, internet access, and secure data exchange between employees, enabling smooth day-to-day operations.

Meraki Techs, a growing IT service and software development company based in Kathmandu, operates with a typical small-to-medium-sized office network setup commonly seen in Nepali companies. The network connects multiple departments such as Administration, Software Development, Design, Sales & Marketing, and Technical Support. The infrastructure includes both **wired Ethernet connections** for desktop workstations and **Wi-Fi access points** for laptops, mobile devices, and visitors.

The network also supports shared access to resources like file servers, a local intranet, printers, and a project management portal. Internet connectivity is provided through a high-speed fiber line from a local ISP, distributed across the office through managed switches and a central router. Security measures such as a firewall, WPA2-protected Wi-Fi, and antivirus software are in place to ensure safe and reliable operations.

This case study aims to document and analyze the design, structure, and functioning of the Meraki Tech's office network, identify its current capabilities, outline the challenges, and provide recommendations for improvement.

OBJECTIVES

- To analyze the structure and functioning of Meraki Techs’ office network.
- To identify and study the network topology, devices used, and configuration details and IP addressing scheme and VLAN/subnetting approach.
- To evaluate the performance, security measures, and reliability of the network, highlight challenges faced and suggest possible improvements.

METHODOLOGY

The methodology for this case study involved a combination of on-site observation, technical analysis, and reference to industry best practices to ensure a comprehensive understanding of Meraki Techs' office network.

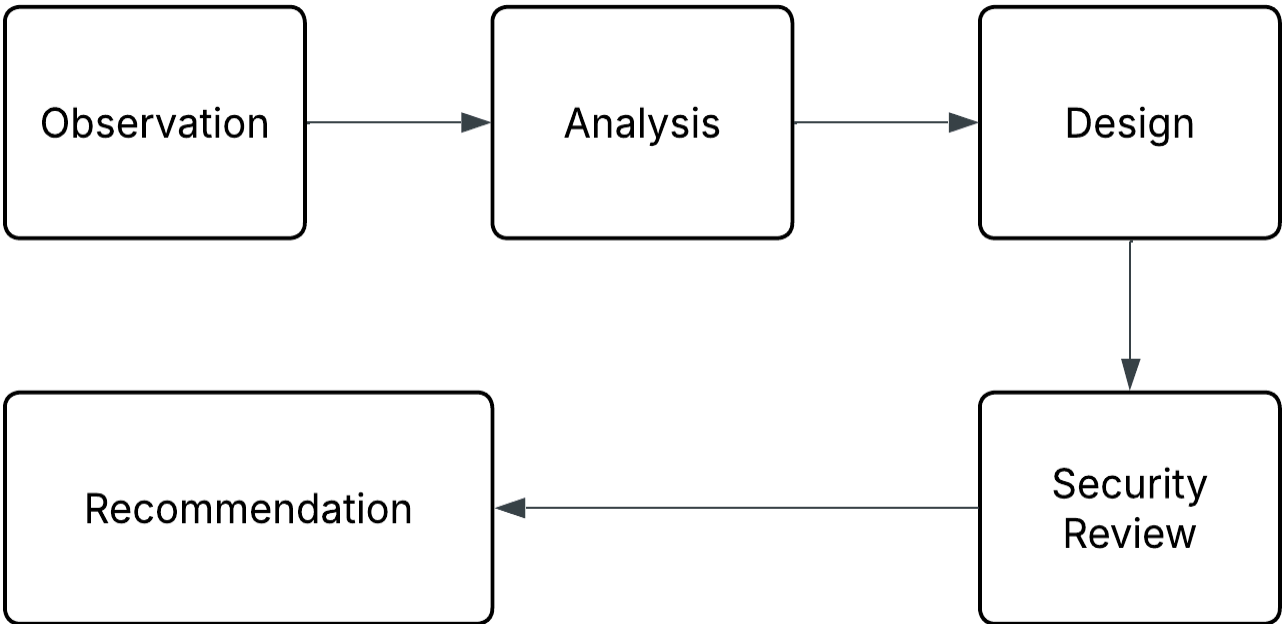

Figure 1: *Methodology flow for Meraki Tech's network analysis.*

1. **Information Gathering**

   The first step involved observing the existing network infrastructure within the office premises. Discussions were held with the IT support staff to understand the current network setup, daily operational requirements, and any known issues. In addition, standard small business network layouts and industry best practices were referred to in order to make realistic design assumptions where direct data was unavailable.

2. **Analysis of Network Components**

   A detailed analysis was conducted to identify both the physical and logical topology of the network. All major networking devices, including routers, switches, access points, servers, and endpoint devices, were documented. The IP addressing scheme, DHCP configurations, and VLAN segmentation were reviewed to understand network organization and traffic isolation practices.

3. **Network Diagram & Design Tools**

   Conceptual network diagrams were created using **Cisco Packet Tracer** and **draw.io** (Lucidchart can also be used) to visualize connections between departments, servers, and network devices. These diagrams helped illustrate both the physical layout and logical structure of the network for analysis and reporting purposes.

4. **Security & Performance Review**

   The network's existing security measures were examined, including firewall rules, Wi-Fi encryption, and antivirus deployment. Performance challenges, such as bandwidth spikes during peak usage and Wi-Fi coverage gaps in certain office areas, were also identified and documented.

5. **Recommendations for Improvement**

   Finally, recommendations were formulated based on observed issues and best practices. Suggestions included optimizing access point placement, upgrading switches for better throughput, implementing departmental VLANs, and improving network monitoring and backup procedures.

COMPANY OVERVIEW

Meraki Techs is a Kathmandu-based IT service and software development company established in 2018. The company offers a range of technology solutions, including custom software development, web and mobile app design, IT consulting, and network support services for both local and international clients.

Currently, Meraki Techs operates with a medium-sized team of **75 employees** across five main departments:

- **Administration & HR:** Handles office management, finance, human resources, and client coordination.
- **Software Development:** Focuses on coding, testing, and maintaining client projects.
- **Design & Creative:** Works on UI/UX design, graphics, branding, and promotional content.
- **Sales & Marketing:** Manages lead generation, client acquisition, and social media campaigns.
- **Technical Support:** Provides troubleshooting and after-sales technical assistance for clients.

The office is located in a commercial building in **Shantinagar, Kathmandu,** and is organized into departmental work zones, a server room, a small meeting/conference room, and a reception area. The network infrastructure is centralized in the server room, where core devices such as the router, managed switches, and servers are housed in a secure rack cabinet. The network combines wired Ethernet connections for desktops with secure Wi-Fi for laptops, mobile devices, and visitors.

With steady growth over the years, network performance, scalability, and security have become increasingly important to support daily operations efficiently. The availability of firsthand access to the network provides a valuable opportunity to analyze and document its design, functioning, and areas for improvement.

NETWORK OVERVIEW

The Meraki Tech's office network is designed to support the company's multi-department workflow, enabling efficient communication, secure data sharing, and reliable internet connectivity for day-to-day operations.

The network follows a **star topology** with a central server room acting as the hub. All wired Ethernet connections from different departments terminate at **managed switches** in the server room, which connect to the main **router/firewall** linked to the Internet Service Provider (ISP). This setup ensures centralized management, easier troubleshooting, and scalability for future expansion.

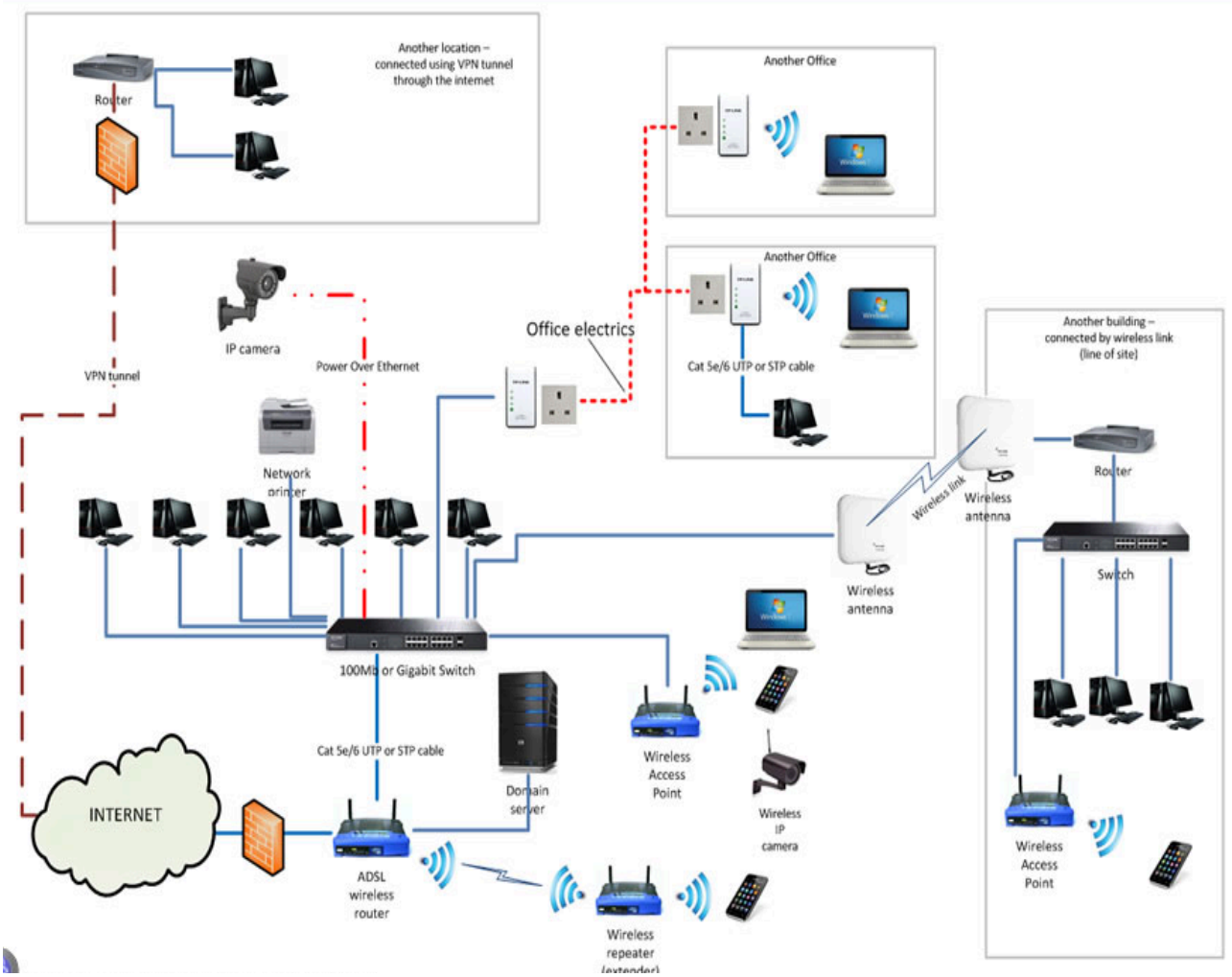

Figure 2: *High Level Overview of the Network Setup*

Key Features of the Network Setup

- **Internet Connectivity**: A high-speed fiber-optic connection from a local ISP (250 Mbps dedicated line) provides stable internet access to all users.
- **Wired & Wireless Access**: Desktop workstations in Administration, Development, and Design departments use **Cat6 Ethernet connections** for better stability, while laptops and mobile devices connect via **secure Wi-Fi**.
- **Server Room Infrastructure**: Houses the core router, 24/48-port managed switches, local application/file server, and backup storage system.
- **Departmental Segmentation**: VLANs are implemented to logically separate traffic between departments, improving both security and performance.
- **DHCP & IP Scheme**: The router handles DHCP for dynamic device assignment, while key servers and printers have **static IP addresses**.
- **Security Measures**: Network traffic passes through a firewall, and Wi-Fi uses WPA2-Enterprise encryption with unique staff logins.

This hybrid wired-wireless network design provides the speed and reliability needed for development work while ensuring flexibility for mobile users and guests. With the centralization of core devices in the server room, the company can maintain a controlled and secure networking environment while being ready to scale as the business grows.

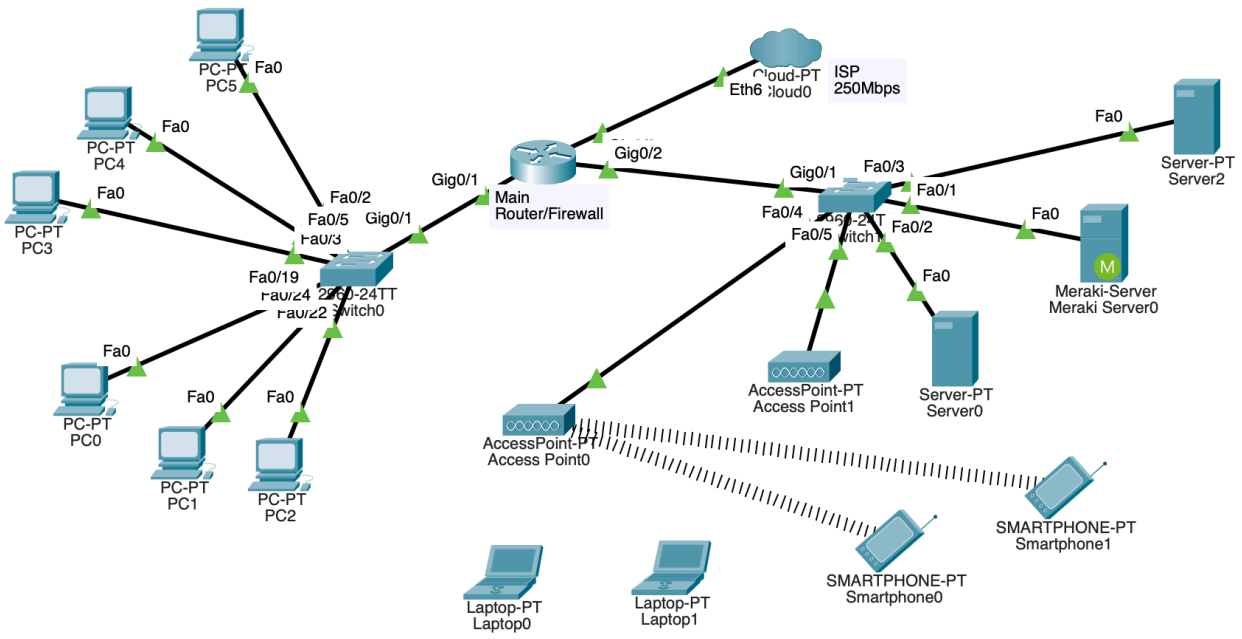

Figure 2: *Meraki Tech's office network with centralized server room, wired desktops, and wireless access points.*

NETWORK TOPOLOGY

Meraki Techs' office network follows a star topology, where all network devices are connected to a central hub located in the server room. This centralization simplifies management, enhances scalability, and makes troubleshooting easier.

- The core router/firewall connects directly to the ISP's fiber line.
- The router connects to managed switches in the server rack, which distribute network connections to all departments.
- Wired connections (Cat6 cables) are used for stationary workstations, while wireless access points provide coverage for laptops, mobile devices, and visitors.
- VLANs are configured on the managed switches to logically separate departmental traffic, improving security and network efficiency.

- The server room also hosts file/application servers, a backup server, and a network-attached storage (NAS) system.

Departmental Connectivity

- **Administration & HR**: Connected via managed switch ports, VLAN 10.
- **Software Development**: Connected via high-speed Ethernet to VLAN 20 for code repository access and testing environments.
- **Design & Creative**: Connected via VLAN 30 with higher bandwidth allocation for large media file transfers.
- **Sales & Marketing**: Connected via VLAN 40 with access to CRM and marketing tools.
- **Technical Support**: Connected via VLAN 50 for remote troubleshooting and support tools.
- **Guest Wi-Fi**: Separate VLAN 60 with internet-only access for visitors.

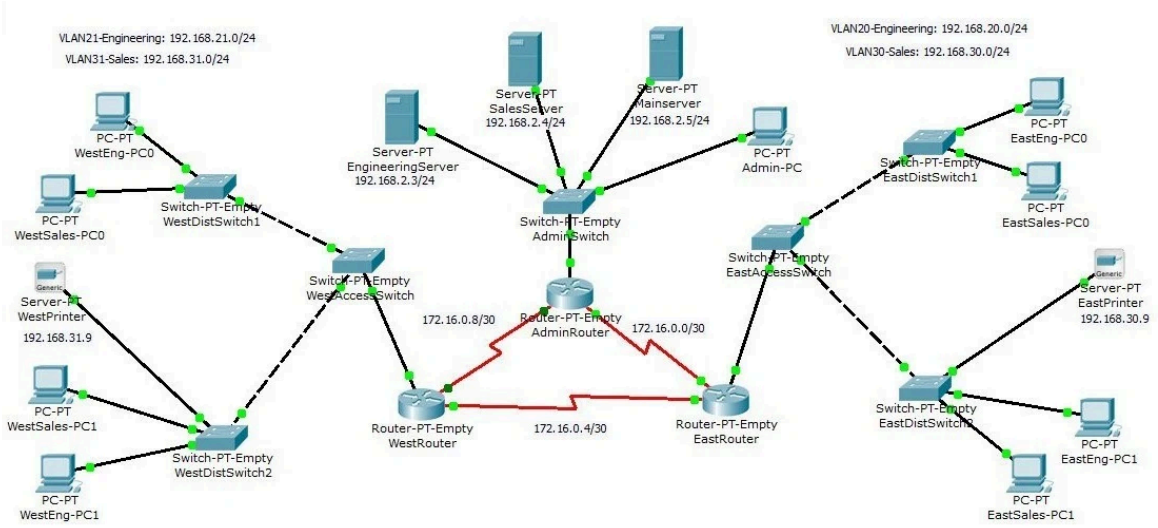

Figure 3: *Star Topology, Network controlled from Centralized Server*

DEVICES USED

The Meraki Tech's office network consists of enterprise-grade networking and computing equipment designed for reliability, scalability, and secure communication. The devices are housed primarily in the **server room**, with access points and endpoint devices distributed throughout the office.

Router / Firewall

The core of Meraki Techs' network is a **MikroTik CCR1009-7G-1C-1S+ router**, which acts as the main gateway between the ISP's dedicated fiber connection and the office LAN. It manages routing, applies firewall rules for network security, handles VLAN segmentation for departmental traffic separation, and provides Quality of Service (QoS) to prioritize business-critical applications. The router also supports VPN connectivity, allowing remote employees to securely access company resources from outside the office, a feature that has become increasingly useful for hybrid work setups in Nepal.

Figure 4: *Main Router*

Managed Switches

Two **Cisco Catalyst 2960X-48FPD-L managed switches** form the backbone of the wired network. They distribute Ethernet connections to all departments while supporting VLANs for traffic isolation, PoE+ for powering wireless access points and IP phones, and link aggregation for faster backbone links. These switches are rack-mounted in the server room and connected using Cat6 UTP cables for desktops and fiber patch cables for high-speed interconnects.

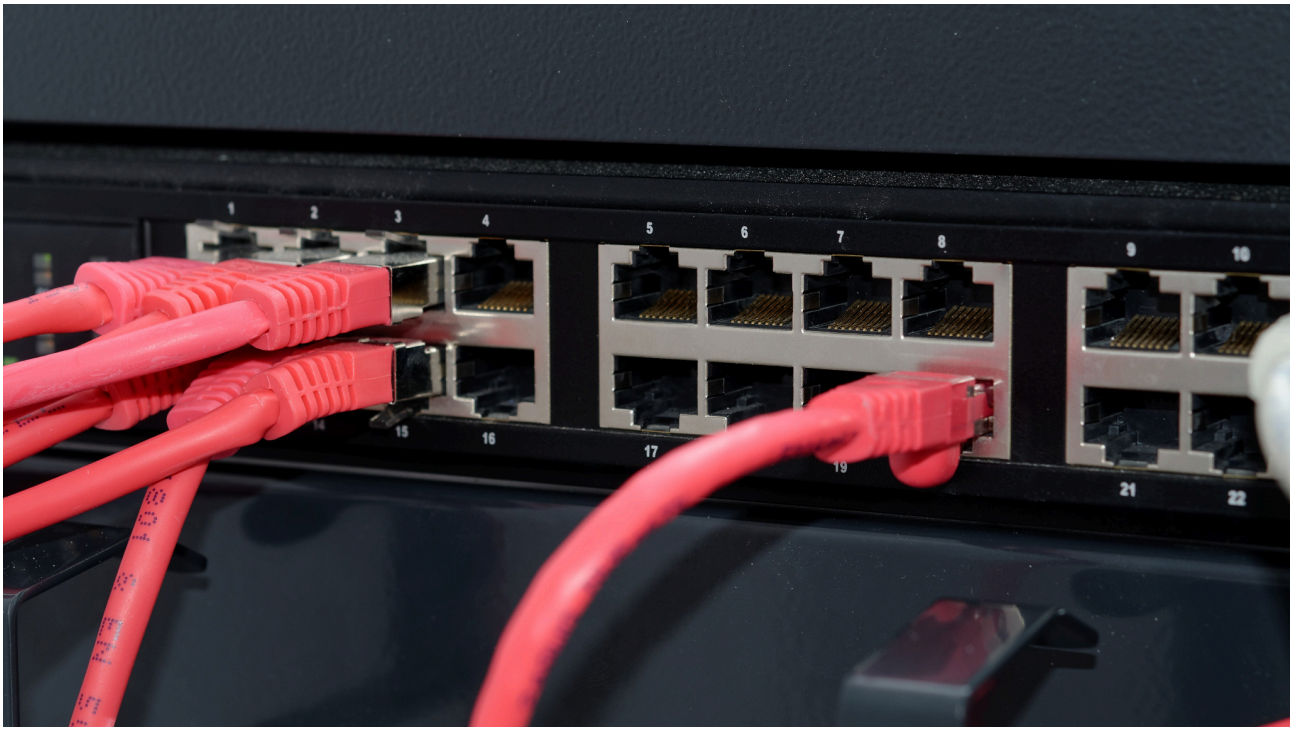

Figure 5: *Network Distribution Switch*

Wireless Access Points

Office-wide wireless coverage is delivered by four **Ubiquiti UniFi 6 Lite (Wi-Fi 6) access points**, positioned strategically to eliminate dead zones. Each AP supports dual-band connectivity for improved speed and efficiency, uses WPA2-Enterprise encryption with RADIUS authentication for staff, and broadcasts a separate guest SSID that is VLAN-isolated to prevent access to internal resources.

Figure 6: *Wifi 6 Access Points*

Servers

The primary server is a **Dell PowerEdge T440**, which hosts internal applications, file storage, Git repositories, and project management tools. It is configured with 8TB of RAID 5 storage for redundancy. A **Synology DS920+ NAS** serves as the backup server, performing automated nightly backups of essential company data and configuration files, ensuring business continuity in case of hardware failure or data loss.

Other Networking Components

A **42U lockable server rack** with cooling fans houses all core networking devices in the server room. An **APC Smart-UPS 3000VA** provides backup power during outages, a common concern in Kathmandu. Structured cabling uses Cat6 UTP for workstations and fiber links for high-speed backbone connections, ensuring minimal latency and reliable performance.

Figure 7: *Central Server of whole network*

Endpoint Devices

The network supports 60 desktop workstations running Windows 11 Pro for Administration, Development, and Design teams. These are connected via gigabit Ethernet for stability and speed. Ten laptops are issued to Sales, Marketing, and remote-capable staff for mobility. Additionally, three multifunction printers/scanners are connected with static IP addresses, allowing all employees to access printing and scanning services over the network.

IP ADDRESSING SCHEME & VLAN DESIGN

The Meraki Techs network uses a **private IPv4 addressing scheme** to ensure secure internal communication while avoiding conflicts with public IP addresses. A **Class C** private range (192.168.x.x) is allocated and further segmented into VLANs to isolate traffic between departments. This approach enhances network security, reduces broadcast traffic, and allows better bandwidth management.

The **MikroTik CCR1009 router** acts as the central DHCP server for each VLAN, assigning dynamic IP addresses to client devices while keeping certain devices (servers, printers, network storage) on static IPs for consistent accessibility. VLAN tagging is implemented on the Cisco managed switches, and access points are configured to broadcast SSIDs mapped to their respective VLANs.

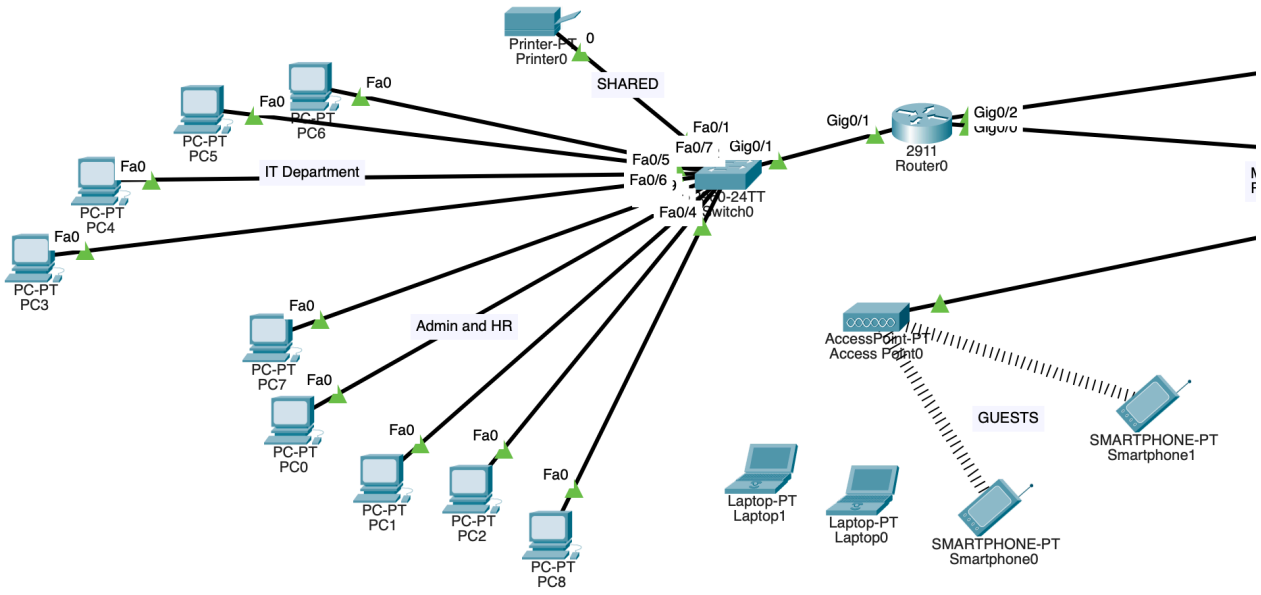

Figure 9: *VLAN Setup and Network Division*

VLAN & IP Scheme Table

VLAN ID	Department	Subnet	IP Range	Gateway
10	Administration & HR	192.168.10.0/24	192.168.10.10 to 192.168.10.200	192.168.10.1
20	Software Development	192.168.20.0/24	192.168.20.10 to 192.168.20.200	192.168.20.1
30	Design & Creative	192.168.30.0/24	192.168.30.10 to 192.168.30.200	192.168.30.1
40	Sales & Marketing	192.168.40.0/24	192.168.40.10 to 192.168.40.200	192.168.40.1
50	Technical Support	192.168.50.0/24	192.168.50.10 to 192.168.50.200	192.168.50.1
60	Guest Wi-Fi	192.168.60.0/24	192.168.60.50 to 192.168.60.200	192.168.60.1
100	Server & Infrastructure	192.168.100.0/24	192.168.100.10 to 192.168.100.50	192.168.100.1

- **Subnetting:** Each VLAN uses a /24 subnet mask (255.255.255.0) to allow up to 254 usable host addresses per department.
- **Static IPs:** Servers, printers, and NAS devices are manually assigned IPs in the .10–.50 range of their VLAN for easy management.

- **DHCP:** The router assigns addresses dynamically for workstations and laptops within the defined ranges.
- **Isolation:** VLANs are restricted using switch configuration and router ACLs (Access Control Lists), ensuring sensitive data is not accessible across departments except where explicitly allowed.

SECURITY MEASURES

Meraki Techs' network security framework is designed to protect sensitive company data, ensure uninterrupted operations, and safeguard against both internal and external threats. The approach combines hardware-based protections, software safeguards, and administrative policies.

1. **Firewall & Network Protection**

   The MikroTik CCR1009 router serves as the primary firewall, implementing strict filtering rules to block unauthorized inbound traffic and restrict outbound access to only necessary services. Access Control Lists (ACLs) are applied to VLANs to ensure departmental isolation, preventing users from accessing resources outside their designated network segment. Port forwarding is restricted to essential services, and all remote access occurs over encrypted VPN tunnels.

2. **Wireless Network Security**

   All staff Wi-Fi connections use WPA2-Enterprise encryption integrated with a RADIUS authentication server, ensuring that only authorized employees can connect. Each employee has unique login credentials, which are revoked immediately when they leave the organization. Guest Wi-Fi is VLAN-isolated, allowing internet access without any route to internal resources. Access points

are configured to limit broadcast power, reducing the chance of signal leakage outside office premises.

3. **Endpoint & Server Protection**

   All desktop workstations and laptops run licensed antivirus software (ESET Endpoint Security) with regular signature updates. The Dell PowerEdge T440 server uses built-in security features such as secure boot, OS hardening, and restricted administrator access. File servers require authentication with strong passwords, and multi-factor authentication (MFA) is enabled for remote logins to critical systems.

4. **Data Backup & Disaster Recovery**

   A Synology DS920+ NAS is configured for automated nightly backups of essential business data, stored separately from live production systems. Weekly backups are also mirrored to an offsite storage location via a secure encrypted connection, ensuring data is recoverable in case of hardware failure, ransomware attacks, or natural disasters.

5. **Password & Access Control Policies**

   Meraki Techs enforces strong password policies, minimum 12 characters with a mix of uppercase, lowercase, numbers, and symbols, and requires password changes every 90 days. Administrator accounts are limited to IT staff, and all access to network devices is logged and monitored.

6. **Physical Security**

   The server room is locked at all times, accessible only to authorized IT staff. CCTV surveillance covers the server room and main office areas, and biometric access control is installed at the server room entrance to prevent unauthorized physical access.

These combined measures create a multi-layered defense system, ensuring the network remains resilient against cyber threats, internal breaches, and physical security risks, a necessity for maintaining client trust and meeting professional IT service standards in Nepal's competitive tech industry.

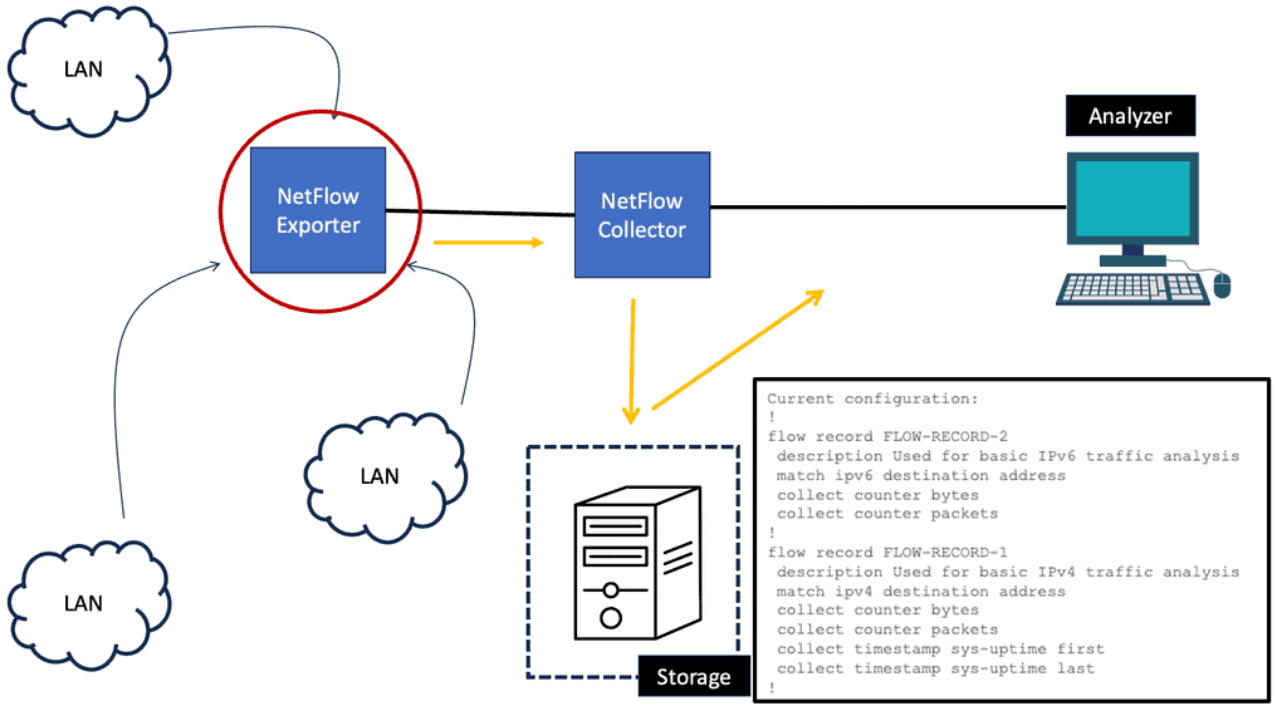

***Figure 10**: Network Security Monitoring*

CHALLENGES

Despite having a well-structured and secure network, Meraki Techs faces a number of operational and technical challenges that impact performance, efficiency, and scalability. These challenges were identified during on-site inspection, staff interviews, and analysis of network performance logs.

1. **Bandwidth Management Issues**

   The company currently uses a single 250 Mbps fiber internet connection shared across all departments. During peak working hours, especially when multiple teams are uploading large design files to cloud platforms, network speeds drop significantly. While the MikroTik router supports bandwidth shaping, no Quality of Service (QoS) rules are actively enforced, allowing non-priority traffic (e.g., social media, YouTube) to consume bandwidth alongside critical business applications.

2. **Wireless Coverage Gaps**

   Although the UniFi UAP-AC-LR access points provide decent coverage in most areas, signal strength drops in far-end corners of the office and meeting rooms with thick concrete walls. This leads to unstable video conferencing connections and reduced productivity for staff working in these zones.

3. **Outdated Endpoints**

   Some workstations are running on hardware over 7 years old, equipped with HDDs instead of SSDs, and limited RAM. These devices struggle with modern software requirements, causing delays in application loading, slow file transfers, and frequent freezing during multitasking.

4. **Limited Network Monitoring**

   The IT team relies mainly on reactive troubleshooting rather than proactive monitoring. Although the router and switches support SNMP and logging, no

centralized network monitoring system is implemented. This means issues like abnormal traffic spikes or potential security breaches may go unnoticed until they cause significant disruption.

5. **Backup Dependency on Manual Checks**

   While the NAS backup system is in place, its success logs are not automatically reviewed. In cases where automated backup jobs fail, detection is delayed until a manual check is performed, creating a risk of unprotected data in the event of a sudden failure.

6. **Scalability Concerns**

   With the company growing steadily, the current network infrastructure, especially the single-layer switch configuration, may become a bottleneck. As more departments are added, VLAN complexity, broadcast traffic, and switch port limitations will require an upgrade to a more hierarchical network design.

RECOMMENDATIONS

Based on the network analysis and identified challenges at Meraki Techs, the following recommendations are proposed to improve performance, reliability, and scalability:

1. **Upgrade Internet Bandwidth and Implement QoS**

   To address bandwidth bottlenecks, the company should consider upgrading its fiber connection to a higher speed plan, such as **500 Mbps or 1 Gbps**, depending on future growth. Additionally, configuring **Quality of Service (QoS)** on the MikroTik router will prioritize critical business applications like project management tools, Git repositories, and video conferencing over non-essential traffic, ensuring consistent performance during peak hours.

2. **Enhance Wireless Coverage**

   Adding 2–3 additional UniFi access points in weak signal areas, particularly in far-end corners and meeting rooms, will eliminate dead zones. Optimizing AP placement and conducting a Wi-Fi site survey will ensure balanced coverage and minimal interference.

3. **Upgrade Aging Workstations**

   Replacing older desktops with modern machines equipped with SSDs and at least 16GB RAM will significantly improve application performance, file transfer speeds, and overall productivity. Alternatively, selective upgrades (e.g., RAM/SSD additions) can be applied to critical machines to reduce immediate costs.

4. **Implement Centralized Network Monitoring**

   Deploying a network monitoring solution like PRTG, Zabbix, or the UniFi Controller will allow IT staff to proactively monitor bandwidth usage, detect abnormal traffic patterns, and receive instant alerts for potential security

threats. This proactive approach will reduce downtime and improve troubleshooting efficiency.

5. **Automate Backup Verification**

   Integrating automated backup verification tools with the Synology NAS will ensure that any failed backup jobs are immediately flagged and corrected. Offsite replication of critical data should continue, but with automated checks to confirm integrity and completeness.

6. **Plan for Future Scalability**

   To support company growth, consider a hierarchical network design with core, distribution, and access layers. Upgrading to modular or stackable switches will allow additional ports and easier VLAN management as new departments or devices are added. Regular review of VLAN segmentation and IP addressing will maintain performance and security as the network expands.

7. **Strengthen Security Practices**

   Continuous employee training on password hygiene, phishing awareness, and safe internet usage will complement existing technical measures. Periodic firewall rule reviews and patch updates for all network devices will ensure ongoing protection against evolving threats.

CONCLUSION

This case study analyzed the office network of Meraki Techs, a Kathmandu-based IT service and software development company. Through observation, discussions with IT staff, and reference to standard small-to-medium business network practices, we documented the network's design, devices, topology, IP addressing, VLAN segmentation, and security measures.

The network follows a star topology with a centralized server room hosting core switches, routers, and servers, ensuring efficient communication, resource sharing, and reliable internet access for all departments. The combination of wired connections for desktops and wireless access points for laptops and mobile devices provides both stability and flexibility. VLANs are implemented to logically separate departments, enhancing performance and security.

Our analysis identified key strengths, including centralized management, adequate bandwidth for current operations, and basic security measures like firewall protection and WPA2-Enterprise Wi-Fi. Challenges such as limited Wi-Fi coverage in certain areas, occasional network slowdowns, and aging hardware were also highlighted. Recommendations were provided, including optimizing AP placement, upgrading switches, and implementing better cable management to improve performance and scalability.

Overall, this case study demonstrates a practical approach to understanding, analyzing, and improving a real-world office network. It highlights the importance of structured network design, proper device deployment, and security planning in ensuring smooth day-to-day operations and readiness for future growth.