HDNETS1.docx

by Y4Z YASIRU PRABODHA

Submission date: 07-Mar-2025 08:01AM (UTC+0000)
Submission ID: 251983986
File name: 156359_Y4Z_YASIRU_PRABODHA_HDNETS1_2528557_723672229.docx (260.29K)
Word count: 4548
Character count: 28560

Wisdom of Networking

Created by: L.H.G. Yasiru Prabodha

CMU ID: st20330308

ICBT ID: CL/HDNET/CMU/51/14

Course: HD in Network Technology and Cyber Security

Lecturer: Ms. Hashini

Submit Date: 2024/03/06

Acknowledgment

I would also like to extend my gratitude at this moment to our esteemed lecturer Miss Hashini in all sincerity for her incessant guidance and counseling, which were crucial for the success of this project. Her thought-provoking lectures, clear explanation, and true passion for teaching us have not only enhanced our comprehension of intricate networking principles but also motivated us to deliver high levels of performance in every facet of our work.

Miss Hashini's dedication to the students and her love for the topic have rendered learning a lively and encouraging journey. Her talent for explaining topics, giving valuable feedback, and stimulating critical thinking has enabled us to conquer challenges and attain academic success. With her mentorship, we gained a good understanding of the strategic value of network architectures, implementations of security measures, and how to troubleshoot—knowledge that will surely stand us in good stead in the future.

It has been a learning experience par excellence for this project, and we know that the success of it is a reflection of the painstaking efforts of Miss Hashini herself. We gratefully acknowledge her priceless contributions to our learning process and practical capabilities. Thank you, Miss Hashini, for being such a great mentor and for your limitless devotion to making us successful.

Sincerely,

Yasiru Prabodha

Executive summary

This paper presents an extensive networking plan for ZoomTech Corporation to improve operational efficiency, simplify communication, and protect information across its operations throughout the country. The model presented is a WAN-LAN hybrid architecture that integrates fast, localized connections with secure, wide-area communications, where every branch from the main headquarters in Kandy to distant offices can have the capability to exchange vital resources seamlessly and work in real time.

At the center of the strategy is a centralized IT infrastructure that utilizes client-server models, centralized sharing of resources, and optimized file transfer. Local Area Networks (LANs) are deployed at every location to ensure high-speed, secure internal networking, while a Wide Area Network (WAN) connects these locations via encrypted VPN tunnels. This setup reduces data redundancy, lowers operational costs, and enables scalable growth by making it easy to add new branches without replacing the current infrastructure.

The main networking devices, including VPN routers, Layer 2/3 switches, centralized servers, and Wi-Fi 6 access points, are installed to enable important functions. The report explains how each of the devices corresponds to the OSI model to use protocols like IPsec, VLAN, and TCP/IP in the optimal manner in order to maintain data integrity and achieve maximum communication efficiency. The proposal also calls for a wired-wireless hybrid approach, balancing the reliability of the wired network for mission-critical functions with the flexibility provided by wireless connections for customer-facing activities.

Apart from infrastructure, proactive troubleshooting and maintenance are also emphasized as key elements. Through the use of SolarWinds, PRTG, and Wireshark, ZoomTech can identify and fix issues even before they lead to serious problems, thus ensuring smooth operations, safeguarding revenue, and establishing trust with customers. Generally, the strategy sets up ZoomTech for improved performance, superior security, and long-term growth in a competitive business environment.

Introduction

In today's business landscape, seamless communication and data-driven operations are crucial for success. ZoomTech Corporation, a mid-sized office supply distributor in Sri Lanka, finds itself at a pivotal juncture. The company's expansion across the nation has highlighted inefficiencies in its fragmented IT infrastructure, characterized by isolated systems, communication breakdowns, and inadequate security measures. These challenges threaten to impede progress in a competitive market. To address these issues, ZoomTech plans to overhaul its operations by implementing a centralized client-server network. This new infrastructure will link its Kandy headquarters with offices nationwide, facilitating improved collaboration, enhanced security, and scalability.

This report provides a comprehensive roadmap for ZoomTech's network transformation, structured around four critical pillars:

1. **Networking Fundamentals**: Establishing the core concepts, network types, and architectures that underpin ZoomTech's operations.
2. **Devices and Protocols**: Selecting hardware and protocols aligned with the OSI model to ensure efficiency and security.
3. **Network Design**: Proposing a hybrid topology to connect branches securely while optimizing local performance.
4. **Monitoring and Troubleshooting**: Implementing proactive strategies to safeguard business continuity.

By integrating WAN and LAN infrastructures, VPN and VLAN implementations, and implementation of enterprise-class security tools, this architecture not only meets ZoomTech's current requirements but also provides for future growth scalability. The suggestions in this report conform to ZoomTech's objectives of containing operational expenses, enhancing inter-departmental collaboration, and protecting confidential information critical enablers to keep its leadership in Sri Lanka's office supply market.

TASK 01

1.a. Concept of Computer Networking and Benefits for ZoomTech Corporation

Computer networking is the process of interconnecting devices such as computers, servers, printers, and IoT gadgets via wired or wireless channels. For instance, Wikipedia notes that a network is a set of computers sharing resources located on or provided by network nodes , while TechTarget defines networking as the practice of transporting and exchanging data between nodes over a shared medium.

This interconnected environment facilitates resource sharing, data exchange, and collaboration across geographically dispersed locations. Cisco defines computer networking as the practice of connecting computing devices to communicate with one another, emphasizing the critical role of standardized protocols like TCP/IP and hardware components such as routers, switches, and firewalls. Similarly, virtual private networks (VPNs) enable devices to share data and network resources securely over public networks by utilizing encryption and tunneling protocols.

For enterprises like ZoomTech Corporation, a robust network serves as the backbone of modern IT infrastructure, supporting centralized management, real-time collaboration, and streamlined operations. As artificial intelligence (AI) usage increases, it places considerable stress on network capabilities, necessitating upgrades to support the anticipated traffic. Companies such as Cisco are focusing on revamping current network systems by upgrading equipment and implementing new tools to support this demand. (ComputerNetworkingNotes, 2024)

Benefits for ZoomTech Corporation

1. **Centralized Resource Sharing**

   A **client-server network architecture** centralizes critical resources (files, databases, applications) on dedicated servers at ZoomTech's headquarters. Departments like Finance and HR can access these resources securely from any branch, eliminating data silos and ensuring consistency.

   Example

- **File Servers**: Host shared documents (e.g., company policies, sales reports).
- **Database Servers**: Manage centralized inventory and customer records accessible to Sales and Logistics teams in real time.
- **Print Servers**: Allow employees to share printers across departments, reducing hardware costs.

Impact

- Reduces data duplication (e.g., a single customer database instead of multiple spreadsheets).
- Ensures all teams work with the latest information, minimizing errors in order processing or payroll.

2. **Improved Communication**

Networking enables seamless communication between ZoomTech's headquarters in Kandy and its branches through digital tools and protocols.

Example Tools & Protocols

- **Unified Communication Systems**: VoIP (Voice over IP) for cost-effective internal calls between branches.
- **Instant Messaging Platforms**: Microsoft Teams or Slack for real-time collaboration on projects.
- **Email Systems**: Exchange Server for secure corporate email communication.

Impact

- Accelerates decision-making (e.g., HR can quickly approve leave requests from branch employees).
- Reduces travel costs by enabling virtual meetings between departments.

3. **Efficient File Sharing**

A centralized network significantly streamlines interdepartmental data exchange, particularly for large files like invoices and delivery schedules. By establishing a central server, organizations create a unified platform that eliminates the inefficiencies and security risks associated with outdated manual transfer methods, such as USB drives or email attachments. This centralized approach fosters instant and reliable data sharing, enhancing operational efficiency and collaboration. (UGREEN NAS, 2024)

Example Workflow

- **Sales Team**: Uploads updated product catalogs to a shared server accessible to all branches.
- **Logistics Team**: Automatically syncs delivery schedules with the central server to avoid shipment delays.

Protocols & Tools

- **FTP/FTPS**: Securely transfers bulk files (e.g., daily sales reports).
- **Cloud Integration**: Hybrid cloud storage (e.g., SharePoint) for remote access to files.

Impact:

- Eliminates delays in updating inventory data, preventing stockouts or overordering.
- Ensures Customer Support teams have immediate access to order status updates.

4. **Enhanced Security**

Centralized control enables ZoomTech's IT department to enforce uniform security policies across all locations. (Vaishnavi, 2024)

Security Measures:

- **Firewalls & IDS/IPS**: Monitor and block malicious traffic at network entry points.
- **Data Encryption**: TLS/SSL for securing emails and VPNs for encrypted inter-branch communication.
- **Automated Backups**: Daily server backups to prevent data loss during hardware failures.

Impact:

- Protects sensitive data (e.g., employee payroll details, customer payment information).
- Mitigates risks of cyberattacks targeting branch offices.

5. **Cost Savings**

Networking reduces operational costs by consolidating resources and optimizing infrastructure.

Example Savings

- **Shared Hardware**: Fewer printers and servers needed due to centralized resource pooling.
- **Reduced IT Overheads**: Centralized software licenses (e.g., Microsoft Office 365) instead of individual purchases.
- **Lower Communication Costs**: Free VoIP calls between branches instead of traditional phone lines.

Impact

- Cuts capital expenditure (CapEx) by up to 30% through resource sharing.
- Lowers energy costs by reducing redundant hardware.

6. **Scalability**

ZoomTech's network can expand effortlessly as the company grows, supporting new branches, users, and technologies.

Scalability Features

- **Modular Hardware**: Add switches or APs to accommodate new employees.
- **Cloud Integration**: Scale storage or computing power on demand (e.g., AWS for seasonal sales spikes).
- **VPNs**: Connect new branches to HQ within hours using pre-configured VPN routers.

Impact

- Supports ZoomTech's nationwide expansion without overhauling existing infrastructure.
- Enables adoption of future technologies (e.g., IoT sensors in warehouses).

7. **Business Continuity & Disaster Recovery**

A robust network ensures uninterrupted operations during emergencies (e.g., power outages, natural disasters).

Strategies

- **Redundant Servers**: Failover servers automatically take over if the primary server crashes.
- **Offsite Backups**: Cloud backups ensure data recovery if HQ faces a physical disaster.

1.b. Types of Networks and Recommendation

Types of Networks

❖ **LAN (Local Area Network)**

A LAN connects devices within a limited geographic area, such as a single building, office, or campus. It is characterized by **high-speed connectivity** (up to 10 Gbps) and **low latency**. (lifewire, 2019)

Key Features

- Uses Ethernet (wired) or Wi-Fi (wireless) technologies.
- Managed by switches and routers for efficient traffic routing.
- Ideal for internal departmental collaboration (e.g., HR, Finance).

Example For ZoomTech

- **Kandy Headquarters**: All devices in the Finance department share files via a LAN connected to a central server.
- **Branch Offices**: Sales teams in a Colombo branch use a LAN to access local printers and shared drives.

❖ WAN (Wide Area Network)

A WAN spans large geographic distances, connecting multiple LANs across cities, countries, or continents. It relies on leased lines, fiber optics, or VPNs over the internet. (Cloudflare, n.d.)

Key Features

- Lower speed compared to LANs (due to distance and infrastructure).
- Requires routers and modems to manage long-distance data transmission.
- Supports secure, real-time communication between dispersed locations.

Example For ZoomTech

- Connects the Kandy HQ to branches in Galle, Jaffna, and Matara via encrypted VPN tunnels.

❖ MAN (Metropolitan Area Network)

A MAN covers a metropolitan area (e.g., a city like Kandy) and interconnects multiple LANs. It is larger than a LAN but smaller than a WAN. (chtips, 2021)

Key Features

- Uses fiber-optic cables or wireless technologies like microwave transmission.
- Suitable for organizations with multiple buildings in a single city.

Relevance to ZoomTech

- **Not recommended**, as ZoomTech’s branches are spread **nationwide**, not confined to a single city

Recommendation for ZoomTech

1. **LANs at Each Location**
   - Deploy high-speed LANs at the Kandy HQ and every branch for internal operations.

- **LAN Components**
    - **Layer 3 Switches**: Segment departments into VLANs (e.g., Finance, Sales).
    - **Wi-Fi 6 Access Points**: Enable wireless connectivity for mobile teams.
    - **Local Servers**: Host frequently accessed files (e.g., branch-specific sales data).

2. **WAN for Inter-Branch Connectivity**

- Use site-to-site VPNs over the internet to securely link all branches to the central HQ server.
- **WAN Components**
    - **VPN-Enabled Routers**: Encrypt data using IPsec or SSL protocols.
    - **Leased Lines (Optional)**: For critical branches requiring guaranteed bandwidth (e.g., MPLS connections).

Justification for Hybrid WAN-LAN Architecture

1. LAN Benefits for ZoomTech

- **High-Speed Operations**
    - Enables real-time access to central servers for tasks like payroll processing (Finance) and inventory updates (Logistics).
- **Enhanced Security**
    - VLANs isolate sensitive departments (e.g., HR data) from general traffic.
- **Cost Efficiency**
    - Reduces reliance on WAN bandwidth for internal tasks (e.g., printing, local file sharing).

2. WAN Benefits for ZoomTech

- **Nationwide Connectivity**
    - Securely transfers sales reports, customer data, and HR records between HQ and branches.

- **Centralized Control**
  - IT teams in Kandy can monitor and manage all branch networks remotely.
- **Scalability**
  - New branches can be added by configuring VPNs without overhauling the core network.
  -

3. Cost-Effective VPN Solution

- **Internet-Based VPNs**
  - Cheaper than leased lines (e.g., MPLS) and sufficient for a medium-sized business like ZoomTech.
  - Trade-off: Slightly lower reliability compared to leased lines, mitigated by redundant ISP connections**.**

4. Exclusion of MAN

- **Why Not MAN?**
  - ZoomTech's branches are distributed across Sri Lanka, not concentrated in a single metropolitan area.
  - WANs better serve nationwide connectivity needs.

1.c. Wireless vs. Wired Networks and Practical Solutions for ZoomTech

Comparison

Wired Networks (Ethernet)	**Wireless Networks** (Wi-Fi)
Pros: - Faster speeds (1 Gbps+). - More secure (physical access needed).	**Pros**: - Mobility for employees (e.g., Sales use tablets). - Easier to expand (no cabling).

- Stable connectivity.	- Lower installation cost.
Cons: - Inflexible (requires cabling). - Higher installation cost.	**Cons**: - Slower speeds (1 Gbps max). - Vulnerable to interference and security breaches.

Recommendation for ZoomTech

A **hybrid wired-wireless network** is optimal.

1. **Wired Networks**
    - Deploy in critical departments (Finance, HR, IT) for high-speed, secure connections to the central server.
    - Use fiber optics for backbone links between floors/buildings. (Velocenetwork, 2023)
2. **Wireless Networks**
    - Implement Wi-Fi in customer-facing areas (Sales, Customer Support) for mobility.
    - Use WPA3 encryption to secure wireless traffic. (Fortinet, 2024)
3. **Branches**
    - Use wired connections for servers and wireless for staff devices.

Justification

- Wired networks ensure reliability for sensitive tasks (e.g., payroll processing).
- Wireless flexibility supports dynamic departments like Sales.
- Hybrid setups balance cost, performance, and scalability.

TASK2

2.a. Roles of Key Networking Devices and Recommendations

Key Networking Devices:

Routers, switches, hub, and servers form the backbone of the network, enabling secure, centralized connectivity and efficient communication between headquarters and branches. (Jennifer, 2022)

1. **Router**

Routers function as essential gateways, connecting disparate networks like local area networks (LANs) to wide area networks (WANs), and directing data packets via IP addresses. Leveraging routing tables, they determine optimal data transfer paths. Modern routers often incorporate advanced functionalities, including virtual private network (VPN) support, Quality of Service (QoS) for prioritized traffic, and integrated firewall protection, enhancing network security and performance. These devices are critical for efficient and secure data flow across complex network infrastructures.

Use Case for ZoomTech

- Connects headquarters (HQ) in Kandy to nationwide branches via IPsec VPN tunnels over the internet.
- Prioritizes critical traffic (e.g., VoIP calls for Customer Support) using QoS.

Example: Cisco ISR 1000 Series or FortiGate routers with built-in VPN and threat detection.

2. **Switch**

Switches function within a LAN, connecting devices like computers and printers while directing data using MAC addresses. Unlike hubs, they deliver data only to the intended device, minimizing network collisions and enhancing efficiency.

Layer 2 Switches: Manage MAC addressing and VLAN segmentation.

Layer 3 Switches: Combine switching and routing for inter-VLAN communication.

Use Case for ZoomTech

- **Layer 3 switches** at HQ segment departments (e.g., Finance, HR) into VLANs for security.
- **Layer 2 switches** in branches connect local devices (Sales, Logistics).

Example: Cisco Catalyst 9200 (Layer 3) for HQ, TP-Link JetStream (Layer 2) for branches.

3. **Hub**

Hubs are legacy [1] devices that broadcast data to all connected devices in a network, leading to collisions, inefficiency, and security risks.

Drawbacks

- No traffic prioritization or MAC address filtering.
- Obsolete in modern networks due to performance limitations.

Recommendation

Avoid hubs entirely; replace them with switches for better performance and security.

4. **Server**

Servers are centralized systems that host resources (files, databases, applications) for client devices. Types include:

- **File Servers**: Store shared documents (e.g., sales reports, HR policies).
- **Database Servers**: Manage inventory, payroll, and customer data.
- **Application Servers**: Host centralized software (e.g., ERP systems).

Use Case for ZoomTech

- **Centralized servers** at HQ provide real-time access to critical data for all branches.

- **Redundant servers** with RAID configurations ensure high availability.

Example: Dell PowerEdge or HPE ProLiant servers with failover clustering.

5. **Access Point (AP)**

APs bridge wireless devices (e.g., laptops, tablets) to a wired network using [12] Wi-Fi standards (e.g., Wi-Fi 6). Advanced APs support:

- **Multiple SSIDs**: Separate networks for employees and guests.
- **Band Steering**: Direct devices to less congested [13] frequency bands (2.4 GHz vs. 5 GHz).

Use Case for ZoomTech

- Provide wireless connectivity in customer-facing areas (Sales, Customer Support).
- Support IoT devices (e.g., inventory scanners in Logistics).

Example: Aruba AP-500 Series or Cisco Aironet Wi-Fi 6 APs with WPA3 encryption.

Recommended Components for ZoomTech

- **Core Components**
  - **Routers:** Deploy VPN-enabled routers to securely connect branches over the internet (WAN).
  - **Switches:** Use Layer 2/3 managed switches for LANs at HQ and branches (supports VLANs for departmental segmentation).
  - **Servers**: Implement centralized servers (file, database, and application servers) at HQ.
  - **Access Points**: Install Wi-Fi 6 APs for high-speed wireless access in customer-facing areas.
- **Exclusions**: Avoid hubs due to their inefficiency. (modems2, 2024)
-

Justification

1. **Routers**:

- **VPN Support**: Encrypts sensitive data (e.g., HR records, financial reports) during transmission between branches.
- **QoS**: Prioritizes VoIP and video conferencing traffic for Customer Support teams.

2. **Switches**:

- **VLAN Segmentation**: Isolates Finance and HR data from general traffic, reducing breach risks.
- **Layer 3 Capability**: Enables inter-VLAN routing without additional hardware.

3. **Servers**:

- **Centralization**: Eliminates data silos; Sales teams in Galle access the same inventory data as HQ.
- **Redundancy**: RAID configurations prevent data loss during hardware failures.

4. **Access Points**:

- **Wi-Fi 6**: Supports 4x more devices than Wi-Fi 5, ideal for high-density areas.
- **WPA3 Encryption**: Protects against brute-force attacks on wireless networks.

5. **Exclusion of Hubs**:

- Switches provide **dedicated bandwidth** per device, improving speed and security compared to hubs.

2.b. Mapping Devices to the OSI Model and Protocols

OSI Model Layers and Device/Protocol Mapping:

OSI Layer	**Function**	**Devices**	**Protocols**	**Relevance to ZoomTech**
Layer 1: Physical	Transmits raw bitstreams over hardware.	Cables, APs (radio signals)	Ethernet (Cat 6/7), Wi-Fi (802.11ax)	Cat 6 cables ensure high-speed wired

				connections. Wi-Fi 6 reduces latency in APs.
Layer 2: Data Link	Manages MAC addressing and frame delivery.	Switches, APs	MAC, VLAN (802.1Q), PPP, WPA3	VLANs isolate HR/Finance traffic. WPA3 secures wireless data.
Layer 3: Network	Routes packets using IP addresses.	Routers, Layer 3 switches	IP, ICMP, IPsec (VPN), OSPF	IPsec VPN encrypts inter-branch traffic. OSPF optimizes routing paths.
Layer 4: Transport	Ensures reliable end-to-end data delivery.	Servers (software-based)	TCP (reliable), UDP (fast)	TCP guarantees delivery of payroll data. UDP streams real-time VoIP calls.
Layer 5: Session	Manages connections between applications.	Servers (authentication tools)	NetBIOS, TLS/SSL	TLS/SSL secures HTTPS sessions for ZoomTech's internal portals.
Layer 6: Presentation	Translates data formats (encryption, compression).	Servers	HTTP/HTTPS, FTP/FTPS	HTTPS encrypts web traffic. FTPS secures file transfers.
Layer 7: Application	Provides user-facing services.	Servers, client devices	HTTP, FTP, SMTP, DNS, DHCP	DNS resolves domain names (e.g., zoomtech.lk). DHCP automates IP assignments.

Device to Layer Relevance

1. **Routers (Layer 3)**

- **Protocols**
    - **IPsec (VPN)**: Encrypts data between branches and HQ.
    - **OSPF**: Dynamically routes traffic to avoid network congestion.
- **Justification**
    - Ensures secure and efficient WAN connectivity for ZoomTech’s nationwide operations. (Williams, 2020)

2. **Switches (Layers 2 & 3)**
    - **Protocols**
        - **VLAN (802.1Q)**: Segments departments (e.g., HR, Sales) to limit unauthorized access.
        - **IP Routing**: Enables inter-VLAN communication without a dedicated router.
    - **Justification**
        - Reduces network complexity and enhances security for sensitive departments.
3. **Servers (Layers 4 - 7)**
    - **Protocols**
        - **TCP**: Ensures error-free delivery of payroll data (e.g., TCP’s acknowledgment mechanism).
        - **HTTPS/SSL**: Secures ZoomTech’s internal employee portal.
        - **FTP/SFTP**: Facilitates secure file sharing between Logistics and Sales teams.
    - **Justification**
        - Centralizes critical services (e.g., HR databases, inventory management) while ensuring protocol-level security.
4. **Access Points (Layers 1 – 2)**
    - **Protocols**
        - **WPA3**: Provides military-grade encryption for Wi-Fi traffic.
        - **802.11ax (Wi-Fi 6)**: Supports high-density device connectivity in customer support areas.
    - **Justification**
        - Balances performance and security for mobile staff and IoT devices. (Airheads Community, 2015)

TASK 03

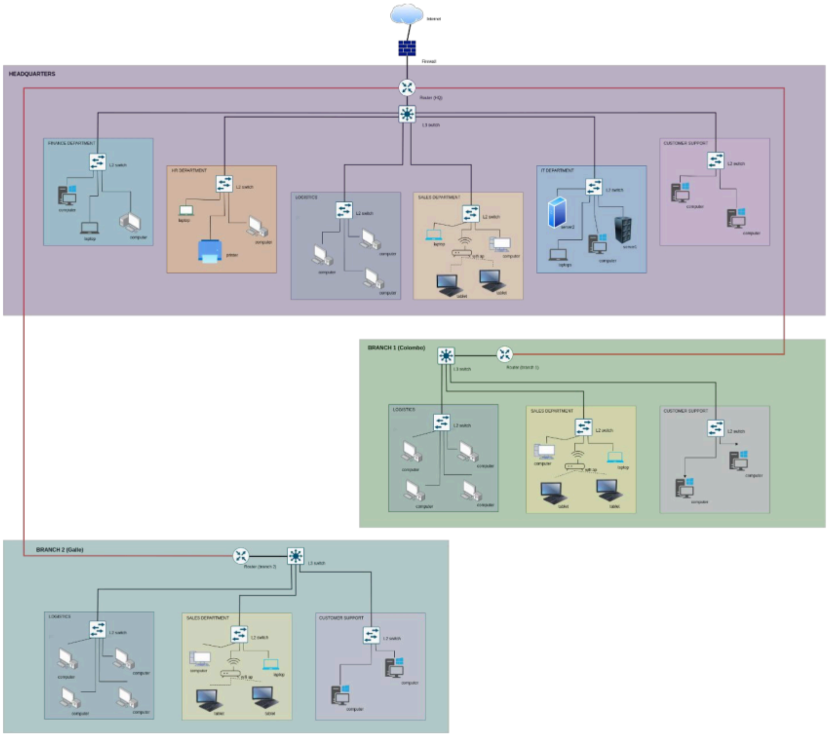
3.a. Network Topology Diagram and Explanation

Recommended Topology

The backbone of a centralized network relies on key hardware components: routers, switches, hubs, and servers. Routers act as traffic directors, guiding data between distinct network segments, while switches and hubs facilitate internal data flow among connected devices within those segments. Centralized servers offer secure and accessible storage and application services, forming the core of data management. This integrated infrastructure ensures efficient and secure connectivity between main offices and remote branches, promoting seamless communication and resource sharing throughout the entire organization. (Staff Contributor, 2019)

Topology Components

1. **HQ in Kandy (Central Hub)**
   - **Core Layer**
     - **Enterprise Firewall**: Acts as the security gateway (e.g., FortiGate 600E).
     - **Core Router**: Connects to branches via VPN tunnels.
   - **Distribution Layer**
     - **Layer 3 Switches**: Segment departments into VLANs (Finance, HR, IT, etc.).
   - **Access Layer**
     - **Layer 2 Switches**: Connect end-user devices (PCs, printers).
     - **Wi-Fi 6 Access Points**: For Sales and Customer Support mobility.
   - **Central Servers**
     - File, database, and application servers hosted in a secured data center.
2. **Branches (Remote Offices)**
   - **Edge Router**: Establishes VPN tunnels to HQ.
   - **Layer 2 Switches**: Connect local devices (Sales, Logistics, Customer Support).
   - **Wireless APs**: For staff mobility.
3. **WAN Connections**:
   - **Site-to-Site VPNs**: Encrypted tunnels over the internet for secure HQ-branch communication. (Fortinet, 2025)



3.b. Network Security Implementation

1. **Firewalls**

   - **Deployment**
     - **HQ:** Next-Generation Firewall (NGFW) with IDS/IPS to monitor and block malicious traffic. (IBM, 2021)
     - **Branches:** Firewall-enabled routers (e.g., Cisco ASA) for basic threat prevention.
   - **Features**
     - Application-aware filtering (block unauthorized apps).

        - Stateful inspection for inbound/outbound traffic.

2. **VPNs (Virtual Private Networks)**
    - **Implementation**
        - **Site-to-Site IPsec VPNs**: Encrypt all data between HQ and branches.
        - **Remote Access VPNs**: For secure employee access from external locations (e.g., SSL VPN).
    - **Benefits**
        - Prevents tapping on sensitive data (e.g., financial records).
3. **Encryption**
    - **Data in Transit**
        - **TLS 1.3**: Encrypts web traffic (e.g., HTTPS for internal portals).
        - **AES-256**: Secures VPN tunnels and file transfers (FTP/SFTP). (Cisco, 2023)
    - **Data at Rest**
        - **BitLocker/FileVault**: Encrypts server and endpoint storage.
4. **Access Control Measures**
    - **Role-Based Access Control (RBAC)**
        - Restrict database/server access by role (e.g., HR managers only access payroll systems)
    - **Multi-Factor Authentication (MFA)**
        - Required for accessing servers or sensitive applications.
    - **Network Access Control (NAC)**
        - Ensures devices comply with security policies (e.g., updated antivirus) before granting network access. (SentinelOne, 2024)
5. **Additional Security Tools**
    - **Endpoint Protection:** Antivirus/anti-malware on all devices.
    - **Regular Audits:** Penetration testing and vulnerability scans.
    - **Physical Security**: Biometric access to server rooms.

TASK04

4.a. Importance of Monitoring and Troubleshooting

Why Proactive Monitoring is Crucial

ZoomTech relies on strong network monitoring and fast troubleshooting for smooth operations. With a centralized IT structure supporting distributed offices, even small network issues disrupt collaboration, slow orders, and hurt customer trust. Proactive network management is crucial to maintain connectivity and business continuity across all locations. (Rapid7, 2024)

Key Reasons for Proactive Monitoring:

1. **Early Detection of Issues**
   - Identifies problems like bandwidth congestion, hardware failures, or security breaches **before they escalate**.
   - Example: Detecting a failing switch at a branch before it causes a complete network outage.
2. **Minimized Downtime**
   - Reduces unplanned downtime, ensuring departments like Sales and Logistics can operate uninterrupted.
   - Example: Real-time alerts for a VPN tunnel failure allow immediate remediation.
3. **Performance Optimization**
   - Monitors traffic patterns to optimize resource allocation (e.g., prioritizing VoIP calls for Customer Support).
4. **Security Threat Mitigation**
   - Flags unusual activity (e.g., unauthorized access attempts) to prevent data breaches
5. **Compliance with SLAs**
   - Ensures ZoomTech meets service-level agreements with clients and partners.

Impact on Business Continuity

- **Revenue Protection**: Downtime in Sales or Logistics could delay order fulfillment, directly affecting revenue.

- **Reputation Management**: Consistent network reliability builds trust with clients and suppliers.
- **Compliance**: Proactive monitoring ensures adherence to data protection regulations (e.g., GDPR).
- **Scalability**: Monitoring tools provide insights for future network upgrades as ZoomTech expands. (Huang et al., 2023)

4.b. Common Network Issues and Resolution Strategies

Common Issues Affecting ZoomTech:

Issue	**Causes**	**Diagnostic Strategies**	**Resolution**	**Recommended Tools**
Latency	- Bandwidth congestion - Faulty hardware	- Use `ping/traceroute` to identify delays - Analyze traffic with Wireshark	- Upgrade bandwidth - Implement QoS policies	SolarWinds NPM, Wireshark
Connection Drops	- Unstable ISP links - Misconfigured VPN	- Check physical cabling - Monitor VPN logs	- Redundant ISP links - Reconfigure VPN tunnels	PRTG Network Monitor, podman
Device Failures	- Aging hardware - Overheating	- Review SNMP alerts - Perform hardware diagnostics	- Replace faulty devices - Deploy redundant hardware	Nagios, Cisco Prime Infrastructure
Security Breaches	- Unpatched systems - Phishing attacks	- Analyze firewall/IDS logs - Conduct vulnerability scans	- Patch systems - Isolate infected devices	Snort (IDS), Nessus (Vulnerability Scanner)

DHCP/IP Conflicts	- Duplicate IP addresses	- Check DHCP server logs - Use IP scanning tools	- Reserve static IPs - Expand DHCP scope	Advanced IP Scanner, Infoblox

Proactive Troubleshooting Strategies

1. **Regular Audits**
   - Conduct monthly network health checks (e.g., testing backup systems, updating firmware).
2. **Automated Alerts**
   - Configure tools like **Zabbix** or **SolarWinds** to send SMS/email alerts for critical events (e.g., server downtime). (Chelsea, 2023)
3. **Documentation**
   - Maintain a network topology map and asset inventory to speed up fault isolation.
4. **Redundancy**
   - Deploy backup power supplies (UPS) and redundant links for critical devices.

Tools for Effective Management

- **Monitoring**
  - **SolarWinds Network Performance Monitor (NPM)**: Tracks bandwidth usage, device health, and application performance.
  - **PRTG**: Monitors VPN stability and WAN/LAN traffic in real time. (Staff Contributor, 2025)
- **Diagnostics**
  - **Wireshark**: Analyzes packet-level data to pinpoint latency or misconfigurations.
  - **PingPlotter**: Maps network paths to identify bottlenecks.
- **Security**
  - **Snort**: Detects and blocks intrusions in real time.
  - **Cisco Umbrella**: Secures DNS queries to prevent phishing attacks. (Crowdstrike.com, 2023)

Conclusion

ZoomTech Corporation's network design integrates a hybrid Wide Area Network (WAN) and Local Area Network (LAN) architecture, effectively combining high-speed local connectivity with secure long-distance communications. This approach ensures efficient data transfer and collaboration across all company locations.

Strategically deploying key networking equipment including VPN-capable routers, Layer 2/3 switches, centralized servers, and Wi-Fi 6 access points optimizes both performance and security. Mapping these devices to the OSI model underscores the importance of robust protocols such as IPsec for encryption, VLAN segmentation for isolating sensitive traffic, and TCP/IP for reliable data delivery. This structured approach simplifies troubleshooting, enhances network management, and preserves the integrity of the IT infrastructure.

Proactive monitoring and troubleshooting are essential to maintain uninterrupted functionality. ZoomTech employs sophisticated tools like SolarWinds, PRTG, and Wireshark to swiftly identify, diagnose, and resolve networking issues before they escalate. Additionally, maintaining comprehensive system documentation, implementing regular network backups, and conducting routine audits further bolster network resilience, ensuring business-critical operations continue smoothly, even during adverse conditions.

Collectively, this network strategy achieves significant cost savings, enhances operational effectiveness, and establishes a secure foundation for future growth. By emphasizing performance, security, and scalability, ZoomTech is well-positioned to address current challenges and capitalize on future opportunities. This robust strategy not only safeguards the company's revenue and reputation but also fosters a culture of ongoing innovation and excellence, ensuring long-term success in an increasingly competitive marketplace.

HDNETS1.docx

ORIGINALITY REPORT

5%	3%	0%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Wales Institute, Cardiff Student Paper	2%
2	Submitted to K12 Incorporated Student Paper	<1%
3	Submitted to SIM Global Education Student Paper	<1%
4	Submitted to Texas A&M University, College Station Student Paper	<1%
5	Submitted to Australian Institute of Higher Education Student Paper	<1%
6	files.wimaxforum.org Internet Source	<1%
7	careers.frieslandcampina.com Internet Source	<1%
8	fastercapital.com Internet Source	<1%
9	www.bartleby.com Internet Source	<1%
10	www.slideshare.net Internet Source	<1%
11	syshen.blogspot.com Internet Source	<1%
12	www.coursehero.com Internet Source	<1%

13	www.electronicshub.org Internet Source	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		