Enterprise Network Architecture Design

Faculty of Computer Networks and Communications
University of Information Technology - VNU-HCM

1 General Introduction

O-UIT Outsourcing Company currently operates two main facilities in Ho Chi Minh City: the headquarters in Thu Duc and a branch in District 3. The headquarters is located in a modern 5-story building equipped with a large-scale Data Center to handle and store data for international projects. The building houses management departments and specialized teams, including the CEO, HR, Project Manager, Technical Manager, Business Analyst, IT Manager, as well as developer and tester teams. These teams are responsible for implementing software projects and advanced technological solutions for international markets, particularly projects with strict standards and complex technical requirements. They also handle domestic projects.

The District 3 branch primarily focuses on projects for domestic clients, ensuring flexibility and alignment with local market demands and requirements. Both locations collaborate to ensure the quality and progress of projects while supporting each other in deploying technological solutions for domestic clients.

2 Customer Requirements Analysis

2.1 Headquarters

Requirement	Details
Devices Used	- Developers and Testers: Only use company desktop computers; personal laptops are not allowed to access the company network. - CEO, HR, Project Manager, Technical Manager, Business Analyst, IT Manager: Allowed to use personal laptops and access the internal Wi-Fi via authenticated accounts.
Internal Wi-Fi	- Provide an internal Wi-Fi system with user authentication (using authenticated accounts). - This Wi-Fi is dedicated to employees such as the CEO, HR, Project Manager, Technical Manager, Business Analyst, and IT Manager.
Public Wi-Fi	- Provide a public Wi-Fi system for guests or non-security-sensitive needs. - This Wi-Fi has a separate Internet connection from the internal Wi-Fi.
Server Virtualization Hardware	- Deploy hardware infrastructure to support application deployment during the testing phase. - The system must ensure high performance and scalability for future work requirements.
Cloud Service Usage	- Use cloud services for application deployment during the staging phase, allowing clients to test applications before official release. - Ensure security and safety during cloud deployment.
Internal Network Connectivity	- Establish an internal network to ensure connectivity between departments, development and tester teams, as well as between servers and internal applications.

Table 1: Headquarters Requirements for Network Architecture

Requirement	Details
Devices Used	- Developers and Testers: Only use company desktop computers; personal laptops are not allowed to access the company network.
Site-to-Site VPN Connection	- Use a site-to-site VPN connection to deploy applications to the Data Center at the headquarters. - The connection must ensure high security and stable connectivity between the two locations.
Wi-Fi	- Provide a separate Wi-Fi system at the District 3 branch with a dedicated Internet connection to separate work traffic from public connections.
Data Center Connectivity	- Ensure stable connectivity between the branch and the Data Center at the headquarters for application deployment.
Security System	- Implement appropriate security solutions to ensure secure connections and access between the branch and headquarters, especially with the use of site-to-site VPN.

Table 2: Branch Requirements for Network Architecture

2.2 District 3 Branch

3 Network System Design

3.1 Logical Network Model Design

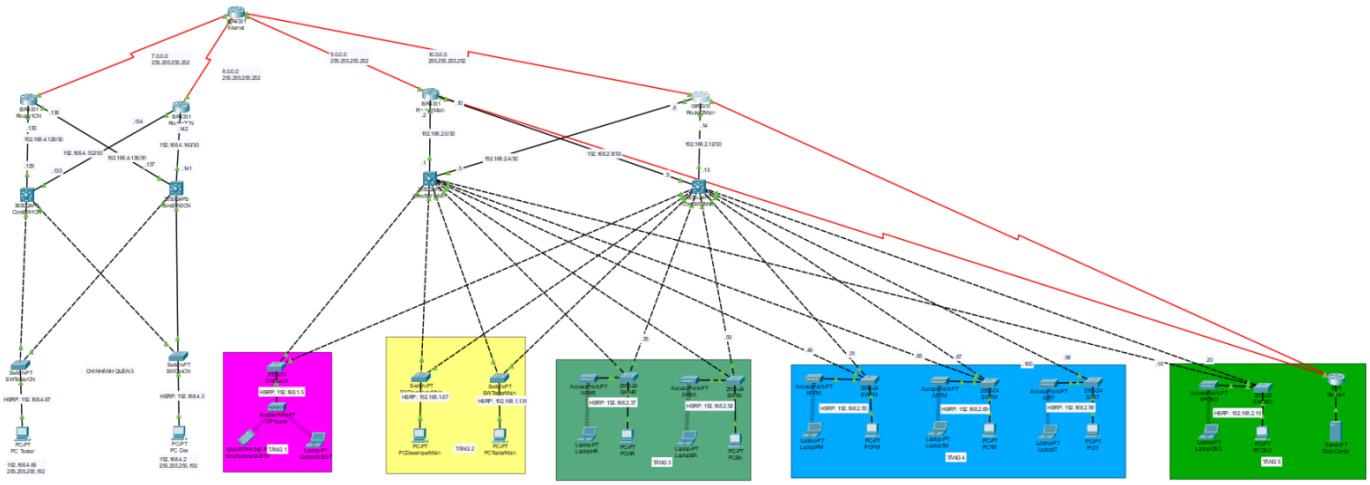

Figure 1: Logical Network Design for O-UIT Compan

Layer Diagram at Headquarters:

- Layer 1: Guest
- Layer 2: Developers and Testers
- Layer 3: HR and Business Analyst
- Layer 4: Project Manager, Technical Manager, and IT Manager
- Layer 5: CEO and Data Center

3.2 Physical Network Model Design

This section only provides estimated hardware costs based on research into the prices of devices listed in the equipment table.

3.2.1 Physical Diagram

Table 3: Router Equipment Specification and Cost Estimation

Device Type	**Model/Product Line**	**Ports and Interfaces**	**Function Description**	**Quantity**	**Unit Price**	**Total Cost**
Router	Cisco ISR4331-AX/K9	3 Gigabit Ethernet WAN/LAN ports (RJ45 and SFP), 2 NIM slots, 1 SM-X slot, 1 Console port, 1 Aux port	Supports throughput from 100 Mbps to 300 Mbps, suitable for high-bandwidth applications. Supports advanced security features like firewall, VPN, and threat management (with upgraded licenses). Integrates VoIP, video, and SD-WAN services. Supports NIM and SM-X modules for network function expansion. Provides monitoring and configuration via web interface or CLI.	4	$7,850.92	$31,403.68
Layer 3 Switch	Cisco Catalyst C9200-48P-A	48 RJ-45 ports with PoE+, 4 10Gbps SFP+ uplink ports	Powers devices like IP cameras, IP phones, and Wi-Fi access points without separate power cables. Integrates security measures to ensure hardware, software, and data integrity. Supports StackWise-80 technology for combining multiple switches into a single manageable entity with 80 Gbps stacking bandwidth, up to 8 switches per stack. Ensures high-performance inter-layer connectivity with 4 10G uplinks. Runs Network Advantage software, supporting advanced routing (OSPF, EIGRP, BGP), QoS, and VLAN segmentation.	4	$8,252.00	$33,008.00

Continued on next page

Table 3: Router Equipment Specification and Cost Estimation (Continued)

Device Type	**Model/Product Line**	**Ports and Interfaces**	**Function Description**	**Quantity**	**Unit Price**	**Total Cost**
Layer 2 Switch	Cisco Catalyst C1000-48FP-4G-L	48 PoE+ ports (10/100/1000 Mbps), 4 SFP uplink ports (1G)	Supports IEEE 802.3at (PoE+) with up to 740W total power, suitable for powering IP cameras, IP phones, and wireless access points. Supports Gigabit SFP modules for extended bandwidth and long-distance connectivity. Provides wire-speed forwarding for high performance in multi-device environments. Supports CLI and web GUI for easy configuration and management, integrable with tools like CNA or SNMP. Features Storm Control to limit Broadcast, Multicast, and Unicast traffic, protecting against traffic storms. Prevents network loops with Spanning Tree Protocol (STP). Supports resilient power supply (RPS) for continuous operation during power failures.	11	$3,332.00	$36,652.00
Wireless Router	Cisco Catalyst 9800-L	4 1G/10G Ethernet uplink ports, 2 1G RJ-45 service ports, 1 Console port, 1 USB port	Manages up to 250 wireless access points and 5,000 users. Supports automation features and open APIs (NETCONF, RESTCONF) based on YANG data models for integration with third-party or custom management tools. Provides high-speed wireless connectivity with support for Wi-Fi 6 and Wi-Fi 6E, improving performance with faster data rates, lower latency, and wider coverage.	7	$3,758.00	$26,306.00

Continued on next page

Table 3: Router Equipment Specification and Cost Estimation (Continued)

Device Type	**Model/Product Line**	**Ports and Interfaces**	**Function Description**	**Quantity**	**Unit Price**	**Total Cost**
Access Point	Cisco Aironet 2802i	2 Gigabit Ethernet ports, 1 Console port, 1 USB 2.0 port, Kensington lock slot	Theoretical speed up to 5.2 Gbps, four times faster than 802.11ac Wave 1 devices. MU-MIMO technology (4x4) enhances performance, allowing multiple devices to connect simultaneously without bandwidth reduction. Optimizes signals for mobile device stability and performance. Monitors and mitigates wireless interference. Flexible Radio Assignment automatically switches between 2.4 GHz and 5 GHz based on the environment. Supports wireless security monitoring to detect threats.	7	$640.00	$4,480.00
					Total	**$131,849.68**

3.2.2 Devices Used in the System

- Cisco ISR4331-AX/K9 Router
- Cisco Catalyst C9200-48PB-A Layer 3 Switch
- Cisco Catalyst C1000-48FP-4G-L Layer 2 Switch
- Cisco Catalyst 9800-L Wireless Controller
- Cisco Aironet 2802i Access Point

3.2.3 Required Services

- Internal Network: Lux800 (FPT Telecom): 1,000,000 VND/month
- Public Network: Lux500 (FPT Telecom): 800,000 VND/month
- Cloud Service: Azure Dev/Test (Microsoft): $2.67/hour

3.3 IP Address Assignment for Network and Devices

Table 4: IP Allocation Table for Headquarters

Subnet	Size	Address	Subnet Mask	Broadcast
Guest Network	50	192.168.1.0	255.255.255.192	192.168.1.63
Developer	50	192.168.1.64	255.255.255.192	192.168.1.127
Tester	50	192.168.1.128	255.255.255.192	192.168.1.191
Server IO – Data Center	248	192.168.1.192	255.255.255.0	192.168.10.255
Core Switch 1 – Router Hawkins	2	192.168.2.0	255.255.255.252	192.168.2.3
Core Switch 1 – Router 2	2	192.168.2.4	255.255.255.252	192.168.2.7
Core Switch 2 – Router 1	2	192.168.2.8	255.255.255.252	192.168.2.11
Core Switch 2 – Router 2	2	192.168.2.12	255.255.255.252	192.168.2.15
CEO	10	192.168.2.16	255.255.255.240	192.168.2.31
HR	10	192.168.2.32	255.255.255.240	192.168.2.47
Project Manager	10	192.168.2.48	255.255.255.240	192.168.2.63
Technical Manager	10	192.168.2.64	255.255.255.240	192.168.2.79
Business Analyst	10	192.168.2.80	255.255.255.240	192.168.2.95
IT Manager	10	192.168.2.96	255.255.255.240	192.168.2.111
Router 1 – RouterDC	2	192.168.2.112	255.255.255.252	192.168.2.115
Router 2 – RouterDC	2	192.168.2.116	255.255.255.252	192.168.2.119
VPN	2	192.168.5.0	255.255.255.192	

Table 5: IP Allocation Table for Branch (Quarter 3)

Subnet	Size	Address	Subnet Mask	Broadcast
Developer	50	192.168.4.0/26	255.255.255.192	192.168.4.63
Tester	50	192.168.4.64/26	255.255.255.192	192.168.4.127
Core Switch 1 – Router 1	2	192.168.4.128/30	255.255.255.252	192.168.4.131
Core Switch 1 – Router 2	2	192.168.4.132/30	255.255.255.252	192.168.4.135
Core Switch 2 – Router 1	2	192.168.4.136/30	255.255.255.252	192.168.4.139
Core Switch 2 – Router 2	2	192.168.4.140/30	255.255.255.252	192.168.4.143

Table 6: IP Assignment Table for Headquarters

Device	Interface	Address	Subnet Mask	Default Gateway
Router1Main	G0/0/0	192.168.2.2	255.255.255.252	N/A
	G0/0/1	192.168.2.10	255.255.255.252	N/A
	Se0/2/0	9.0.0.1	255.255.255.252	N/A
	Se0/2/1	192.168.2.14	255.255.255.252	N/A
	Tunnel0	192.168.5.2	255.255.255.0	N/A
Router2Main	G0/0/0	192.168.2.14	255.255.255.252	N/A
	G0/0/1	192.168.2.6	255.255.255.252	N/A
	Se0/2/0	10.0.0.1	255.255.255.252	N/A
	Se0/2/1	192.168.2.18	255.255.255.252	N/A
CoreSW1Main	G1/0/1	192.168.2.1	255.255.255.252	N/A
	G1/0/2	192.168.1.65	255.255.255.192	N/A
	G1/0/3	192.168.1.129	255.255.255.192	N/A
	G1/0/4	192.168.2.33	255.255.255.240	N/A
	G1/0/5	192.168.2.91	255.255.255.240	N/A
	G1/0/6	192.168.2.49	255.255.255.240	N/A
	G1/0/7	192.168.2.65	255.255.255.240	N/A
	G1/0/8	192.168.2.100	255.255.255.240	N/A
	G1/0/9	192.168.2.18	255.255.255.240	N/A
	G1/0/10	192.168.1.1	255.255.255.192	N/A
	G1/0/11	192.168.2.5	255.255.255.252	N/A
CoreSW2Main	G1/0/1	192.168.2.13	255.255.255.252	N/A
	G1/0/2	192.168.1.68	255.255.255.192	N/A
	G1/0/3	192.168.1.132	255.255.255.192	N/A
	G1/0/4	192.168.2.35	255.255.255.240	N/A
	G1/0/5	192.168.2.93	255.255.255.240	N/A
	G1/0/6	192.168.2.51	255.255.255.240	N/A
	G1/0/7	192.168.2.67	255.255.255.240	N/A
	G1/0/8	192.168.2.98	255.255.255.240	N/A
	G1/0/9	192.168.2.20	255.255.255.240	N/A
	G1/0/10	192.168.2.9	255.255.255.252	N/A
	G1/0/11	192.168.1.6	255.255.255.192	N/A
HSRP Virtual Gateway				
	Guest	192.168.1.5	255.255.255.192	N/A
	DevMain	192.168.1.67	255.255.255.192	N/A
	TesterMain	192.168.1.131	255.255.255.192	N/A
	HR	192.168.2.37	255.255.255.240	N/A
	Business Analyst	192.168.2.92	255.255.255.240	N/A
	Project Manager	192.168.2.50	255.255.255.240	N/A
	Technical Manager	192.168.2.69	255.255.255.240	N/A
	IT Manager	192.168.2.99	255.255.255.240	N/A
	CEO	192.168.2.19	255.255.255.240	N/A
SmartphoneGuest	NIC	192.168.1.2	255.255.255.192	192.168.1.5
LaptopGuest	NIC	192.168.1.3	255.255.255.192	192.168.1.5
PCDeveloperMain	NIC	192.168.1.66	255.255.255.192	192.168.1.67
PCTesterMain	NIC	192.168.1.130	255.255.255.192	192.168.1.131
LaptopHR	NIC	192.168.2.39	255.255.255.240	192.168.2.37
PCHR	NIC	192.168.2.34	255.255.255.240	192.168.2.37
LaptopBusinessAnalyst	NIC	192.168.2.94	255.255.255.240	192.168.2.92
PCBusinessAnalyst	NIC	192.168.2.90	255.255.255.240	192.168.2.92
LaptopProjectManager	NIC	192.168.2.53	255.255.255.240	192.168.2.50
PCProjectManager	NIC	192.168.2.52	255.255.255.240	192.168.2.50
LaptopTechnicalManager	NIC	192.168.2.70	255.255.255.240	192.168.2.69
PCTechnicalManager	NIC	192.168.2.71	255.255.255.240	192.168.2.69
LaptopITManager	NIC	192.168.2.102	255.255.255.240	192.168.2.99
PCITManager	NIC	192.168.2.101	255.255.255.240	192.168.2.99
LaptopCEO	NIC	192.168.2.22	255.255.255.240	192.168.2.19
PCCEO	NIC	192.168.2.21	255.255.255.240	192.168.2.19
DataCenter	NIC	192.168.13.193	255.255.255.0	192.168.1.194

Table 7: IP Assignment Table for Branch (Quarter 3)

Device	Interface	Address	Subnet Mask	Default Gateway
Router1CN	G0/0/0	192.168.4.130	255.255.255.252	N/A
	G0/0/1	192.168.4.138	255.255.255.252	N/A
	S0/2/0	7.0.0.1	255.255.255.252	N/A
Router2CN	G0/0/0	192.168.4.133	255.255.255.252	N/A
	G0/0/1	192.168.4.142	255.255.255.252	N/A
	S0/2/0	8.0.0.1	255.255.255.252	N/A
	Tunnel0	192.168.5.1	255.255.255.0	N/A
CoreSW1CN	G1/0/1	192.168.4.129	255.255.255.252	N/A
	G1/0/2	192.168.4.133	255.255.255.252	N/A
	G1/0/3	192.168.4.65	255.255.255.192	N/A
	G1/0/4	192.168.4.1	255.255.255.192	N/A
CoreSW2CN	G1/0/1	192.168.4.137	255.255.255.252	N/A
	G1/0/2	192.168.4.141	255.255.255.252	N/A
	G1/0/3	192.168.4.68	255.255.255.192	N/A
	G1/0/4	192.168.4.4	255.255.255.192	N/A
HSRP Virtual Gateway				
	TesterCN	192.168.4.67	255.255.255.192	N/A
	DevCN	192.168.4.3	255.255.255.192	N/A
PCTester	NIC	192.168.4.66	255.255.255.192	192.168.4.67
PCDev	NIC	192.168.4.2	255.255.255.192	192.168.4.3

4 System Services and Operating Costs

4.1 Provided Services

4.1.1 Advantages

- **Reasonable Cost:** The system is designed with cost-effectiveness in mind, suitable for companies that need to balance budget constraints while maintaining a high-quality and efficient network system.
- **Complete System:** The system is fully equipped with features and services that effectively meet work requirements, ensuring the ability to serve the needs of both the headquarters and the branch.
- **Simple and Scalable Model:** The network model is designed with a simple yet effective structure, making it easy to manage, upgrade, or expand as business needs grow. This ensures the system can flexibly adapt to future changes without requiring a complete rebuild.
- **Redundant Transmission Lines for Continuity:** Implementing redundant transmission lines ensures system continuity and stability in case of network failures or interruptions, a critical factor in maintaining uninterrupted business operations.

4.1.2 Disadvantages

- **Overload with Large Data Volumes:** Due to the lack of detailed investment in virtual server infrastructure optimization, the system may face challenges when processing large data volumes or sudden increases in user numbers, potentially affecting overall performance, especially under high load.
- **Restrictions on Personal Device Usage at District 3 Branch:** The policy prohibiting employees from using personal devices to access the company network at the District 3 branch may reduce work flexibility. This is particularly inconvenient for employees needing to work remotely or quickly access the network for urgent tasks.
- **Complex Configuration and Difficult Troubleshooting:** The network system's complex configurations may pose challenges in maintenance and error resolution. When issues arise, the troubleshooting process may take longer, potentially disrupting business operations if not addressed promptly.

4.2 Costs for the Entire System

4.2.1 Equipment Costs

- The initial investment cost for the necessary equipment to deploy the entire system is $131,849.68, as detailed above. This figure includes the hardware costs but does not cover additional expenses such as installation fees, transportation costs, or auxiliary materials like network cables or other necessary accessories. Businesses should allocate additional budget for these items to ensure the system is fully and effectively deployed.

4.2.2 Service Costs

- The monthly service costs to maintain the system (internal network, public network, and cloud services) amount to 5,200,000 VND.

4.3 Proposed Protocols, Services, and Network Configurations

4.3.1 ACL (Access Control List)

- Configuring ACLs is critical for enhancing security and controlling traffic in the network model. It allows management of packets based on criteria such as IP address, protocol, and destination port, enabling the blocking or allowing of access as required. In a VLAN-segmented network, ACLs ensure security by controlling communication between VLANs. Additionally, ACLs provide flexible, customizable security solutions tailored to the specific needs of the headquarters and branch, effectively protecting network resources.

4.3.2 HSRP (Hot Standby Router Protocol)

- HSRP plays a vital role in ensuring high availability and continuous connectivity. It allows a group of routers to function as a virtual default gateway, with one router acting as the primary (active) and another as the backup (standby). If the primary router fails, the standby router automatically takes over, ensuring devices in the network remain connected without interruption. This is particularly valuable in systems requiring high reliability, reducing downtime and improving user experience.

4.3.3 DHCP (Dynamic Host Configuration Protocol)

- DHCP automatically assigns IP addresses and network parameters such as subnet mask, default gateway, and DNS to end devices. This reduces manual configuration efforts, minimizes configuration errors, and enhances system management efficiency. DHCP is especially useful in large networks with frequently changing device connections, ensuring each device receives a valid IP address while optimizing IP address resource usage.

4.3.4 VPN (Virtual Private Network)

- VPNs are critical for securing remote connectivity. They create a secure data transmission channel over public networks by encrypting information, ensuring data safety and integrity. VPNs also protect user privacy, enhance security, and optimize network connectivity efficiency.

5 Conclusion

5.1 Performance and Feasibility Evaluation

The network system designed for O-UIT Company demonstrates stable performance, effectively meeting the operational and management needs of both the headquarters and the branch. The model's feasibility is highly rated, as it is entirely implementable in practice due to the harmonious integration of hardware and software, ensuring operational flexibility. To ensure stable operation in real-world environments, specific strategies should be implemented, including:

- **Cable and Physical Device Planning:** Place devices such as routers, switches, and access points in appropriate locations to optimize connectivity.
- **Regular Maintenance and Inspections:** Conduct routine system maintenance to promptly detect and address potential issues, maintaining high performance and extending device lifespan.
- **Performance Evaluation:** Establish a periodic performance evaluation plan to measure critical metrics such as latency, bandwidth, and network reliability.

5.2 Future Development Directions

To meet the growing demands of the business and enhance competitiveness, the network system should be improved and expanded in the following directions:

5.2.1 Enhancing Security and Data Safety

- Deploy advanced Next-Generation Firewalls (NGFW) to prevent external attacks and control internal access traffic.
- Regularly update security software and apply patches to mitigate system vulnerabilities.
- Implement Role-Based Access Control (RBAC) to ensure only authorized personnel can access critical resources.

5.2.2 Scaling and Integrating Modern Technologies

- Enhance cloud service integration for application deployment and data storage to improve performance and system scalability.
- Adopt SD-WAN to optimize connectivity between the branch and headquarters, reducing latency.
- Upgrade hardware to modern devices supporting Wi-Fi 6 or advanced network protocols to enhance performance and data transmission speeds.

5.2.3 Human Resource Development

- Organize training programs on cybersecurity, network tool usage, and system administration.
- Build a dedicated IT team to monitor, manage, and quickly resolve network issues.

5.2.4 Improving Internal User Experience

- Optimize the internal network to ensure all employees, from management to developer and tester teams, can access the system with high speed and low latency.
- Use intelligent management tools like SolarWinds or Zabbix to monitor and manage network performance, optimizing user experience.