CBA College Of Business Administration كلية إدارة الأعمال

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

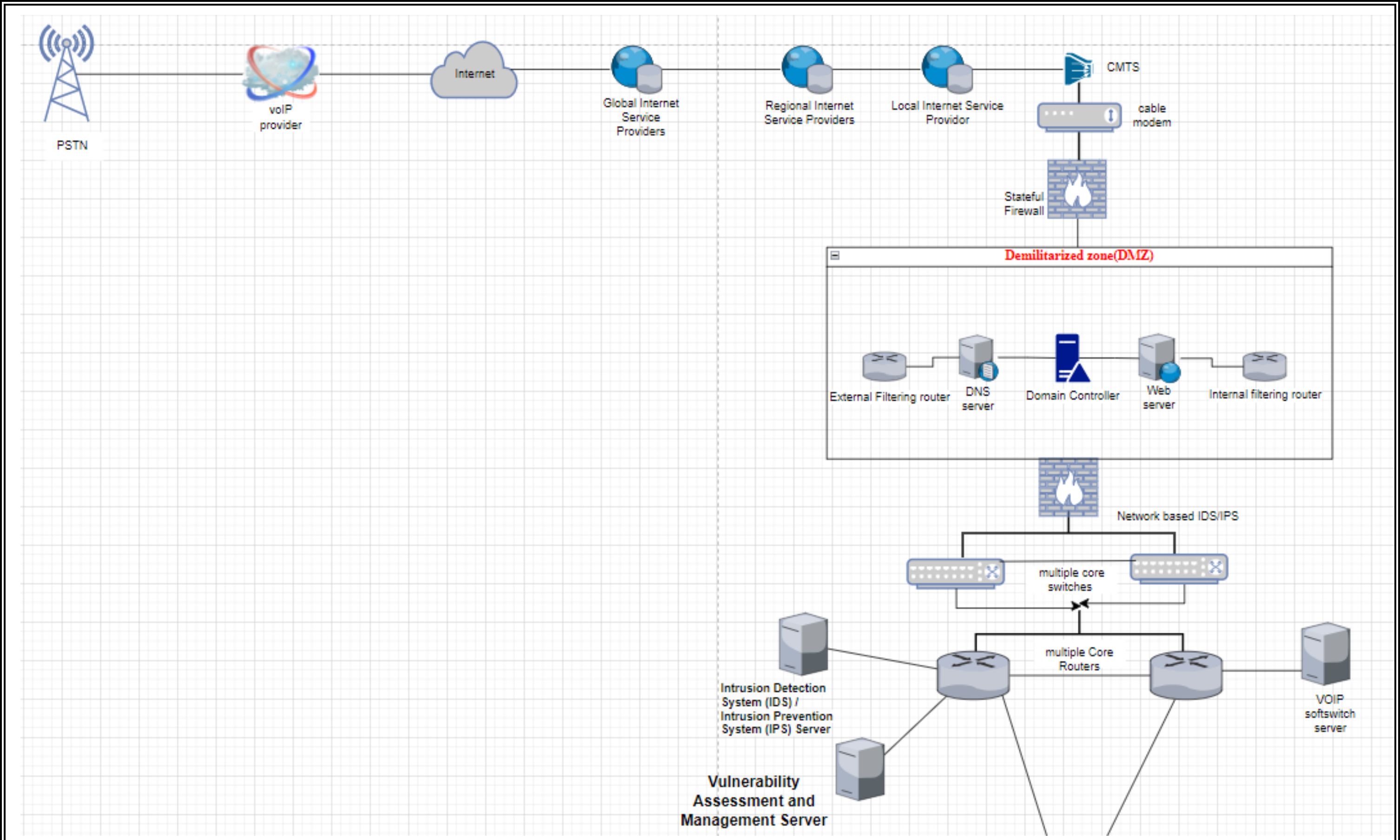
Course title: MIS 411: Network Management

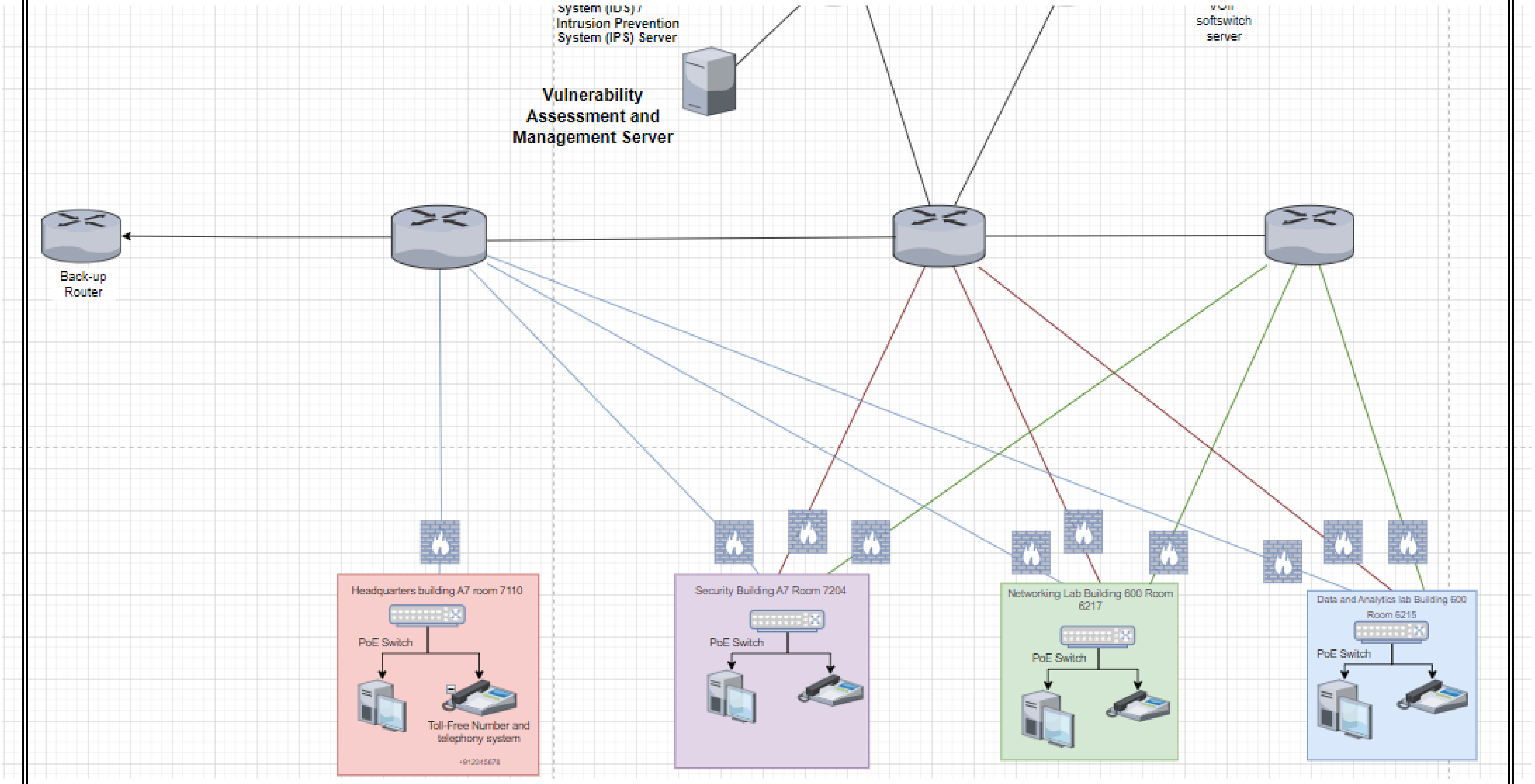
Instructor: Dr. Shaista Rashid

Group project: Second Semester 2023-2024

Section: 3207; Group 1

ID	Student name
2210003293	Rafaa Yagoob Alghamdi
2210002794	Aliah Hammad Alshammari
2210006230	Ghada Turki Almutairi
2210003096	Mais Raji Alabdulaal


PSTN
voIP provider
Internet
Global Internet Service Providers
Regional Internet Service Providers
Local Internet Service Providor
CMTS
cable modem
Stateful Firewall
Demilitarized zone(DMZ)
External Filtering router
DNS server
Domain Controller
Web server
Internal filtering router
Network based IDS/IPS
multiple core switches
multiple Core Routers
Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) Server
VOIP softswitch server
Vulnerability Assessment and Management Server


System (IDS) / Intrusion Prevention System (IPS) Server
softswitch server
Vulnerability Assessment and Management Server
Back-up Router
Headquarters building A7 room 7110
PoE Switch
Toll-Free Number and telephony system
+912345678
Security Building A7 Room 7204
PoE Switch
Networking Lab Building 600 Room 6217
PoE Switch
Data and Analytics lab Building 600 Room 6215
PoE Switch

The Public Switched Telephone Network (PSTN) serves as the traditional telephone network, utilizing physical infrastructure, such as copper wires, to transmit voice signals over long distances. However, with the emergence of Voice over Internet Protocol (VoIP) technology, a new approach to voice communication has been introduced. A VoIP provider offers the necessary infrastructure and services to transmit voice signals over the internet, diverging from the use of conventional phone lines. Within the digital consultancy service network, the VoIP provider plays a crucial role as an intermediary, facilitating the conversion of voice signals from the PSTN into data packets suitable for transmission over the internet.

For this connection to be established, the VoIP provider relies on an internet connection, which is typically established in collaboration with Internet Service Providers (ISPs). By connecting to the internet through ISPs, the VoIP provider ensures the transmission of voice data between the PSTN and the network. The internet serves as the medium through which voice data is transmitted, enabling global connectivity and seamless data transfer between various locations. Through the internet, the VoIP provider efficiently transmits the converted voice data packets, facilitating communication between the PSTN and the network. By establishing a connection with the VoIP provider, the PSTN gains the capability to transmit and receive traditional phone calls. This integration of the PSTN with the VoIP provider and the network allows for a unified and efficient communication system within the digital consultancy service.

Global ISPs are responsible for establishing connections between networks and the expansive internet infrastructure on a global scale. Regional ISPs act as intermediaries between global and local ISPs, facilitating internet access within specific geographic regions. Local ISPs, represented in the network diagram serving the College of Business Administration, provide tailored internet connectivity at a localized level to meet the unique requirements of their immediate community. Collectively, these ISPs ensure uninterrupted access to the internet, facilitating global communication for networks.

High-speed internet access for the network is made possible by accessing the internet through the local Internet Service Provider with a connection to the cable modem and CMTS (Cable Modem Termination System). Lin et al. (2018) state that CMTS acts as an interface to facilitate data transfer via cable infrastructure by acting as a bridge between the cable modem and the ISP's network. According to Lin et al. (2018), this configuration provides dependable connectivity, which is necessary for using online resources and enabling digital services inside the network. The first line of defense for protecting the network from outside threats is the firewall, which is installed after the cable modem. As in a switch or router failure, traffic can be diverted via other pathways. Scalability makes it possible to expand the network seamlessly to handle more devices and increase traffic volumes. To further improve overall network speed and stability, traffic is also distributed over several core routers and switches to avoid congestion and bottlenecks. In addition to facilitating effective load distribution and traffic control, this configuration

guarantees the best possible use of network resources. In general, robustness, flexibility, and efficiency are provided in providing essential network applications and services by the integration of numerous core switches and routers. (Xie et al., 2017).
The headquarters router connects to the headquarters and the three labs, and 2 other routers connect to the 3 labs to minimize work overload on the routers (Kurose & Ross, 2021).

Servers connected to the core routers: VOIP softswitch, IDS/IPS, Vulnerability Assessment and Management Server.
VoIP softswitches, which are software applications running on specialized server hardware, are connected to the core routers and are an essential part of VoIP networks (Meng et al., 2016). They oversee invoicing, media conversion, call routing, and user authentication (Meng et al., 2016). VoIP softswitches are software-based, but they require server hardware server to function well (Meng et al., 2016). They put a high priority on instantaneous communication and optimize call routing to reduce waiting times (Meng et al., 2016). VoIP simulation software mimics the functionality of a typical phone, making call features like audio transmission and initiation easier (Dinh et al., 2019). This server is best suited for large network infrastructures, and it provides a realistic atmosphere for VoIP experimentation by simulating network circumstances for interoperability testing and QoS (quality of service) assessments (Dinh et al., 2019).

By adopting VOIP, the network would enjoy several luxuries. For example, VoIP saves costs by utilizing existing internet infrastructure for voice communication, eliminating the need for separate phone lines and related hardware. VoIP includes sophisticated capabilities like voicemail, call forwarding, video conferences, and connection with other digital applications, which improves the DCSC's efficiency and collaboration (Rashid et al., 2020). in addition, utilizing a toll-free number with a VoIP phone enables the DCSC to give a simple and cost-effective means for consumers to reach them, regardless of their location or phone service. It also provides scalabilityand flexibility for overseeing and managing incoming calls and responding to changing requirements.
The Intrusion Prevention System (IPS) / Intrusion Detection System (IDS) Server improves network security by continually monitoring and analyzing network traffic for signals of suspicious or malicious activities (Islam et al., 2017). The IDS/IPS server detects possible security violations, unauthorized access attempts, and malicious activity in real-time using signature-driven detection algorithms and anomaly detection approaches (Islam et al., 2017). Furthermore, the IDS/IPS server can prevent attacks by blocking or mitigating suspicious traffic, protecting the entire network against cyber vulnerabilities and threats (Islam et al., 2017).

Additionally, the Vulnerability Assessment and Management Server (VAM) is critical in discovering and addressing security vulnerabilities in the network architecture that attackers may exploit (Amoroso, 2012). VAM systems do not immediately prevent assaults. They generate reports outlining detected weaknesses, misconfigurations, and entry points for attackers by scanning and analyzing devices, systems, as well as applications automatically (Amoroso, 2012). It enables network administrators to prioritize patching or remediation actions to improve their network security posture (Amoroso, 2012). Furthermore, VAM improves patch management, configuration strengthening, and compliance adhesion, lowering the chance of successful cyber assaults and data breaches (Amoroso, 2012).

In terms of the subnets, the subnets inside the digital consultancy service network are connected to each other using routers.

- Headquarter Lab Router:

The headquarter lab subnet has a router that acts as a central connection point for the other subnets. This router is responsible for directing traffic between the headquarter lab subnet and the other divisional lab subnets.

- Divisional Labs (Subnet) Routers:

Each divisional lab subnet has its own router. These routers oversee directing traffic within their own divisional lab subnets and sending traffic to the headquarter lab subnet router when needed.

To ensure that the divisional lab subnets can communicate with each other, the routers in each divisional lab are connected together. This connection allows them to share information about the best paths for traffic and enables the routing of traffic between the divisional lab subnets.

The Security framework

1-stateful firewalls: Stateful firewalls provide sophisticated inspection of packets and filtering capabilities, according to Xie et al. (2017), guaranteeing that only permitted traffic passes through the network perimeter. It examines packet content, keeps track of active network connections, and looks for any security risks in the context of network traffic.

2- (IDS) / (IPS) Server: As stated previously, The IPS/IDS server continually analyzes network traffic for indicators of unusual or malicious activities.

3-VAM Server: performs automated scans and inspections of networking equipment, systems, and applications to detect security vulnerabilities and weaknesses.

4-VOIP softswitch: The VoIP Softswitch server performs call navigation, authorization of users, and media conversion operations in the VoIP network (Chai et al., 2019).

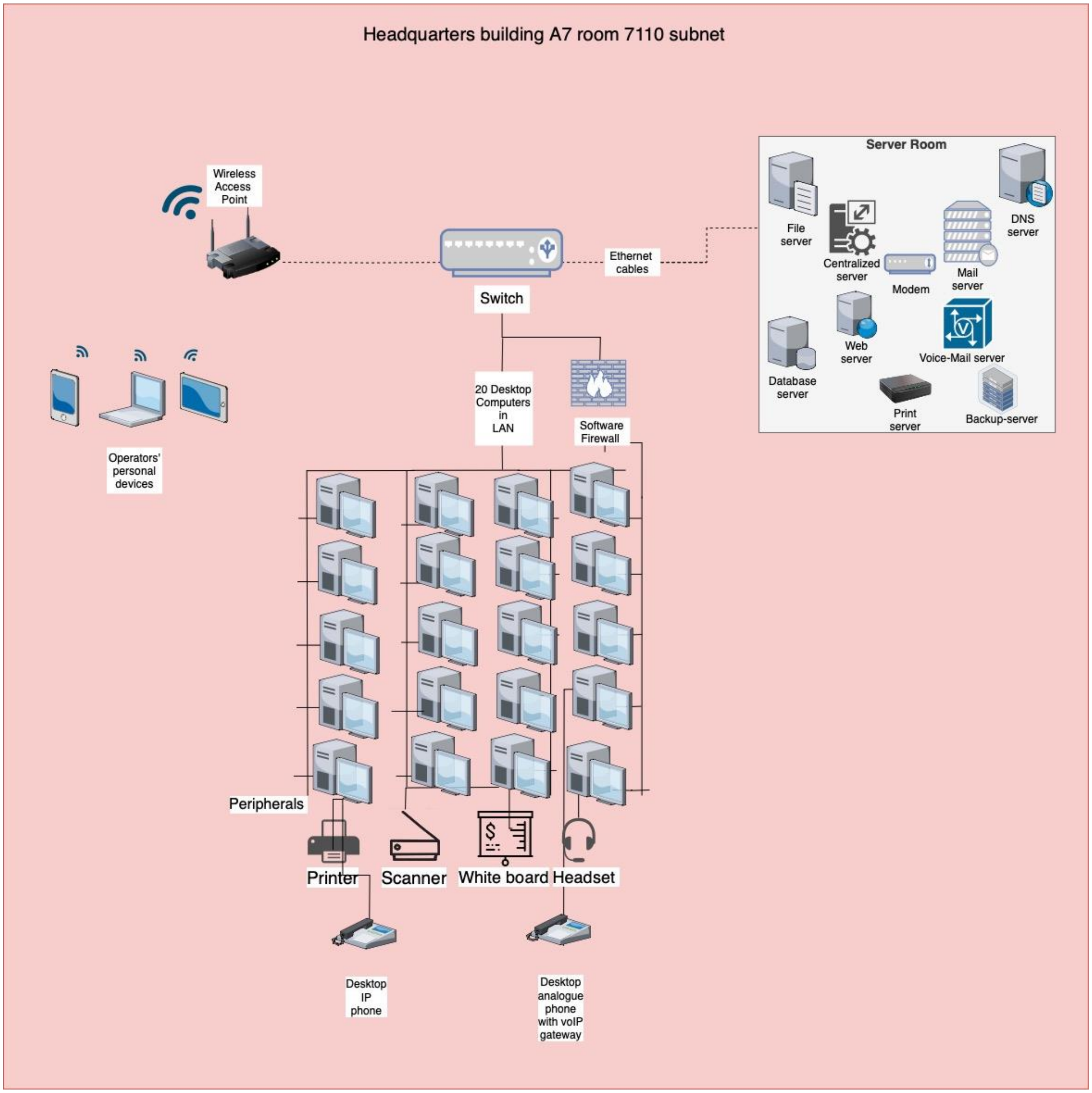
5- Email Security Measures (SPF, DKIM, DLP): Email authentication technologies like Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) are integrated into the mail server to confirm senders' legitimacy and stop email spoofing (Sukadev et al., 2018). Furthermore, Data Loss Prevention (DLP) algorithms in the mail server identify and prohibit the unlawful delivery of sensitive information via email, improving data safety and compliance (Sukadev et al., 2018).

6-https://www.dcsc.cba.edu.sa: To ensure the security and integrity of information shared, the DCSC website employs Secure Sockets Layer (SSL) / Transport Layer Security (TLS) protocols to encrypt data communicated between clients and the server (Xiao et al., 2018). The DCSC website secures online connections with SSL/TLS encryption, protecting confidential information from eavesdropping and manipulation and increasing user trust and confidence (Xiao et al., 2018).

7-user education: User education initiatives increase understanding of best practices in cybersecurity, and the need to abide by security rules and procedures (Alghamdi et al., 2020). Education programs have an important role in reducing human-related risks to safety and improving overall security by empowering users via regular emails or messages to properly notice and respond to privacy risks (Alghamdi et al., 2020).

8- Biometrics and Passwords: Employing biometric authentication (fingerprints or facial recognition) and password-based controlled entry methods at labs and headquarters entrance points improves physical security by validating individuals' identities when they enter restricted locations (Singh et al., 2019). Biometrics are a strong and dependable form of authentication, whereas passwords offer an extra layer of protection to prevent unwarranted entry (Singh et al., 2019). Plus, entrance security measures can be created and programmed to prevent access to the divisions beyond the operational hours, which are set from Sunday to Thursday between 10:00 a.m. and 6:00 p.m.

9-subnets: Subnets provide an essential security precaution by logically splitting networks into smaller portions. This segmentation minimizes the effect of possible breaches of security while improving network security management. Subnets allow CBA to regulate traffic flow and prevent unwanted access to important resources, improving entire network security (Hu et al., 2018).



Headquarter subnet

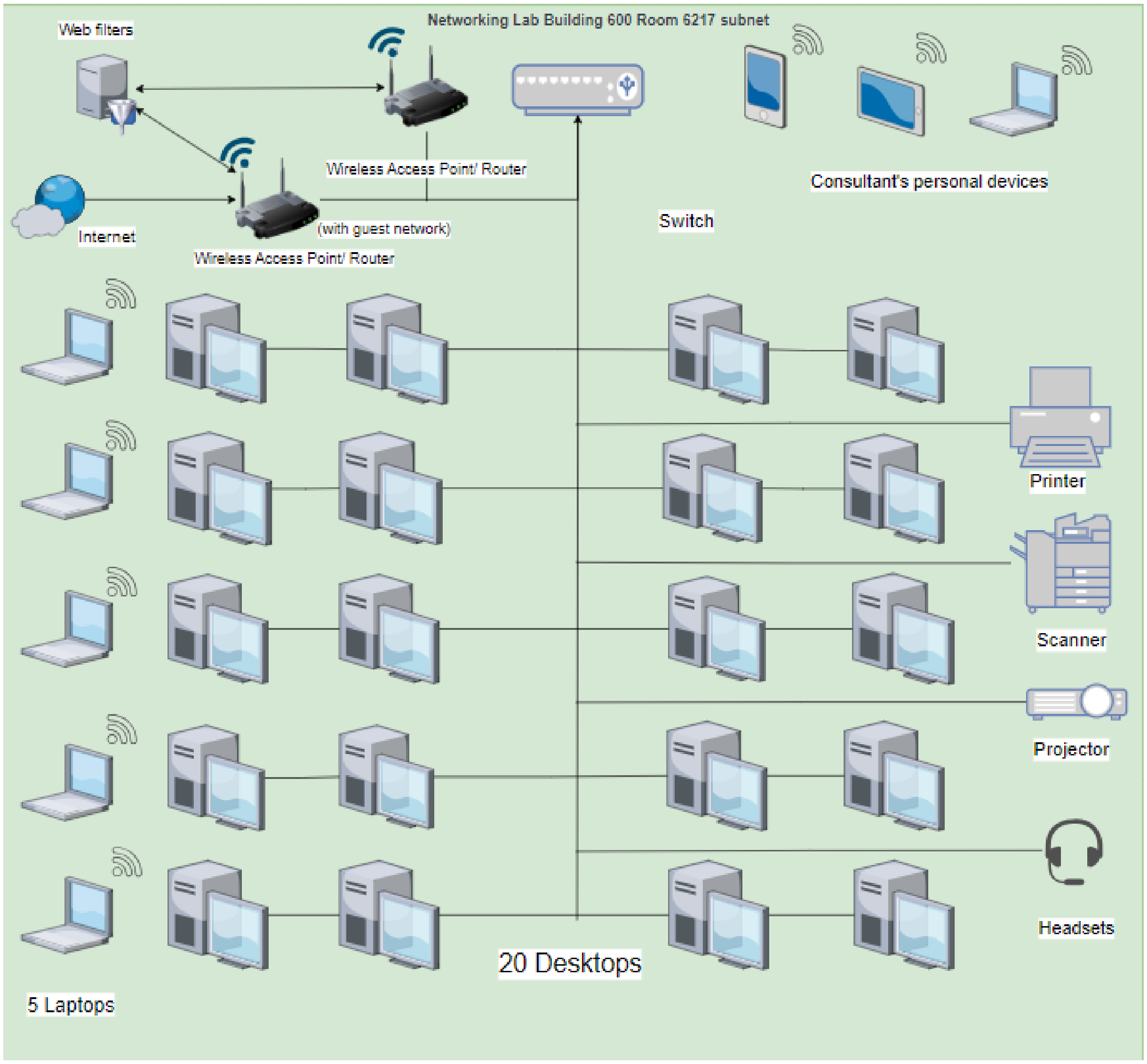
The headquarter lab depicts a well-designed network infrastructure that supports speed and scalability. The design is in a hierarchy that enhances communication and connection throughout

the infrastructure. The central switch is at the core of the infrastructure and among all the other components as the main hub managing all connectivity in the system (Cisco, 2021). The backbone of the network is the server's room, and the facility is a server that supports the activities of the lab. The servers in the server room include a file server that hosts the files and allows access to others within the network, a centralized server for authentication, web server for internal and external website configuration, along with a database server that stores data. Other servers include a print server, mail server which is for managing email communications, voicemail server, since the digital consultancy service in question offers voice-mail services, they will be required to utilize voicemail servers in this regard. Voicemail servers are computer-based systems that enable the handling of voicemail services, and a Backup server, every business, organization, or institution has a backup server. A backup server is responsible for data protection and recovery. A DNS Server, which is a digital infrastructure that translates domain names to IP addresses. For example, the DNS server makes sure the digital consultancy service and its online resources are accessible online by translating their domain names to their IP address, enhancing communication and engagement through their domain names (Cisco, 2021).

The server room is connected to the Internet using a modem (Cisco, 2021) to enable the lab to access external resources and communicate with other networks remotely. Additionally, the server room will be connected to the central switch using Ethernet cables to ensure reliable and high-speed communication among the server and other network components. Lastly, a software firewall will also be installed between the desktop computers and the central switch to control traffic between the various components and protect the lab’s data and resources (Cisco, 2021).

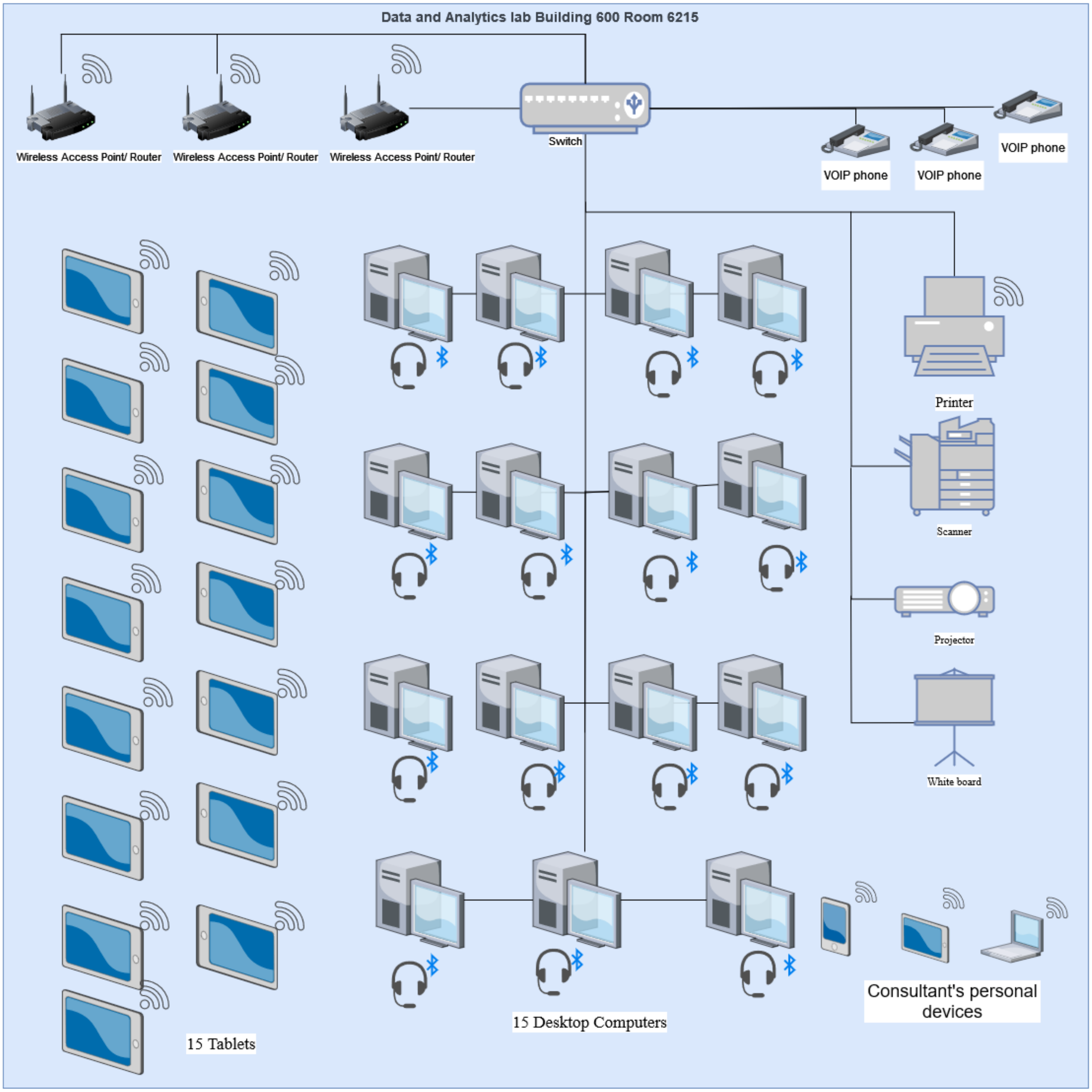
The central switch at the headquarters lab is connected to 20 desktop computers that make up the local area network (LAN). These computers were carefully set up and tuned to fulfill the facility's operating needs. To improve efficiency and cooperation even more, the lab's peripherals, such as printers, scanners, whiteboards, and headsets, are also linked to the local area network (LAN) (Cisco, 2021).

The lab uses desktop analog phones and IP phones and desktop computers for phone calls by utilizing A softphone software, it allows users to utilize computers or mobile devices for making calls instead of traditional landline phones (Feng et al. 2010). This technology uses the existing internet connections to send voice data using Voice over Internet Protocol (VoIP) (Kurose & Ross, 2017). Advanced functions including call forwarding, conference calling, voicemail, and interaction with other communication programs are available on IP phones, which are linked to the IP network. In contrast, the VoIP gateway that connects to the desktop analog phones transforms analog voice signals into digital data packets that may be sent over the IP network (Rouse, 2023). Moreover, wireless communication is available throughout the lab due to the access point linked to the main switch via Ethernet cables. This enables operators to conveniently access resources and complete their responsibilities by allowing them to utilize their personal devices and connect to Wi-Fi (Cisco, 2021). Given the circumstances, the network infrastructure in the headquarters lab assures data integrity, enables effective communication, and offers dependable connectivity (Cisco, 2021). A strong and extremely effective network environment is created by the central switch, room server, desktops connected via Ethernet cables, and the wireless access point. The lab's ability to integrate traditional and modern communication methods is further enhanced with the addition of IP phones and desktop analog phones with a VoIP gateway (Rouse, 2023).


Networking Lab Building 600 Room 6217 subnet
Web filters
Wireless Access Point/ Router
Internet
(with guest network)
Wireless Access Point/ Router
Switch
Consultant's personal devices
Printer
Scanner
Projector
Headsets
20 Desktops
5 Laptops

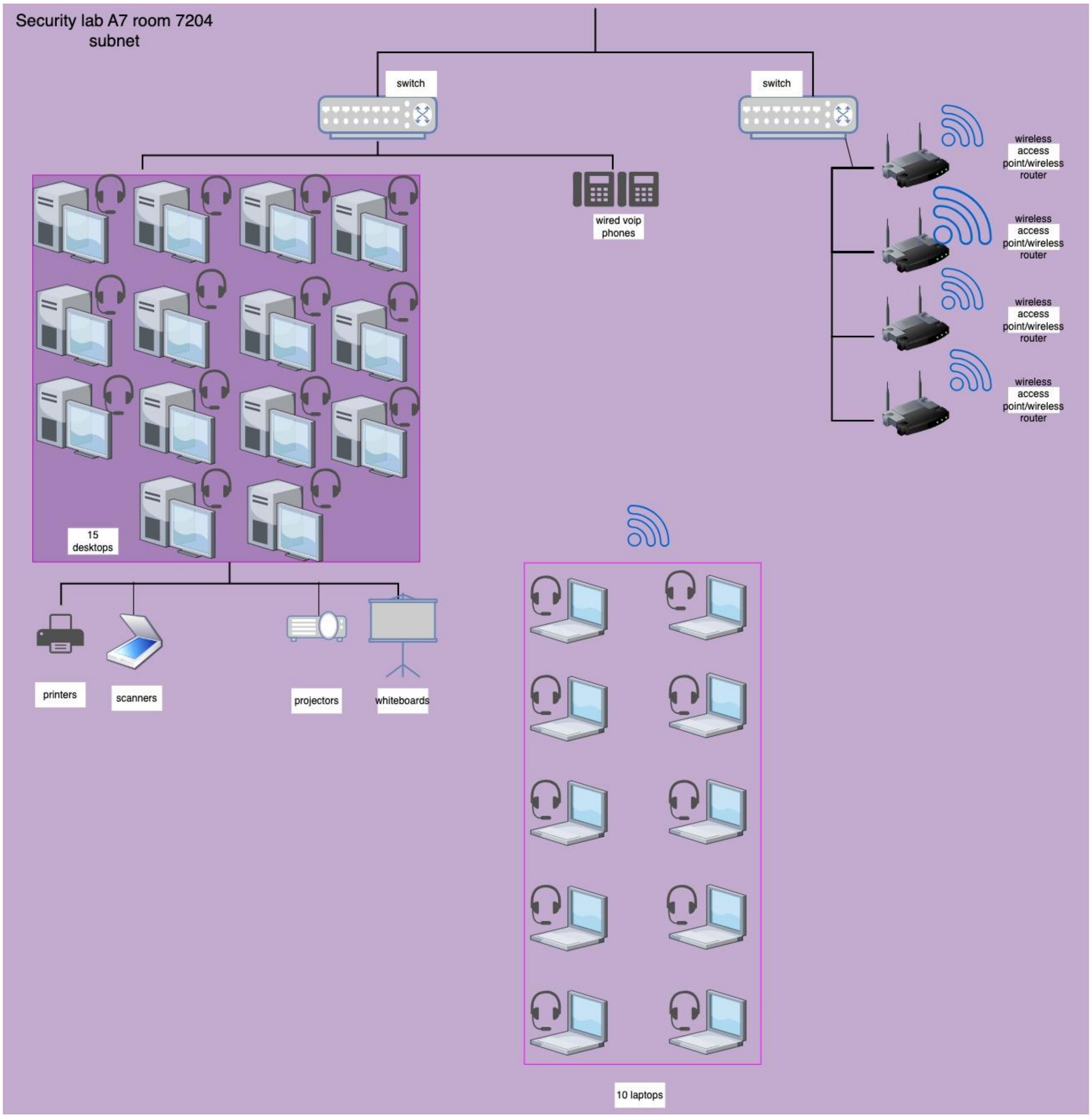
Networking lab subnet

The wireless access point in the networking lab enables internet access to 20 desktops and 5 laptops while maintaining restricted internet access for consultants' personal devices through web filters that limit consultants from accessing certain services, the router is connected to a switch that connects to 20 desktops while laptops have wireless connections, peripherals like projectors, printers, or scanners are also connected to the switch with headsets connected with a wire to the desktops for the softphone software for easy calls handling process.


Data and Analytics lab Building 600 Room 6215
Wireless Access Point/ Router
Wireless Access Point/ Router
Wireless Access Point/ Router
Switch
VOIP phone
VOIP phone
VOIP phone
Printer
Scanner
Projector
White board
15 Tablets
15 Desktop Computers
Consultant's personal devices

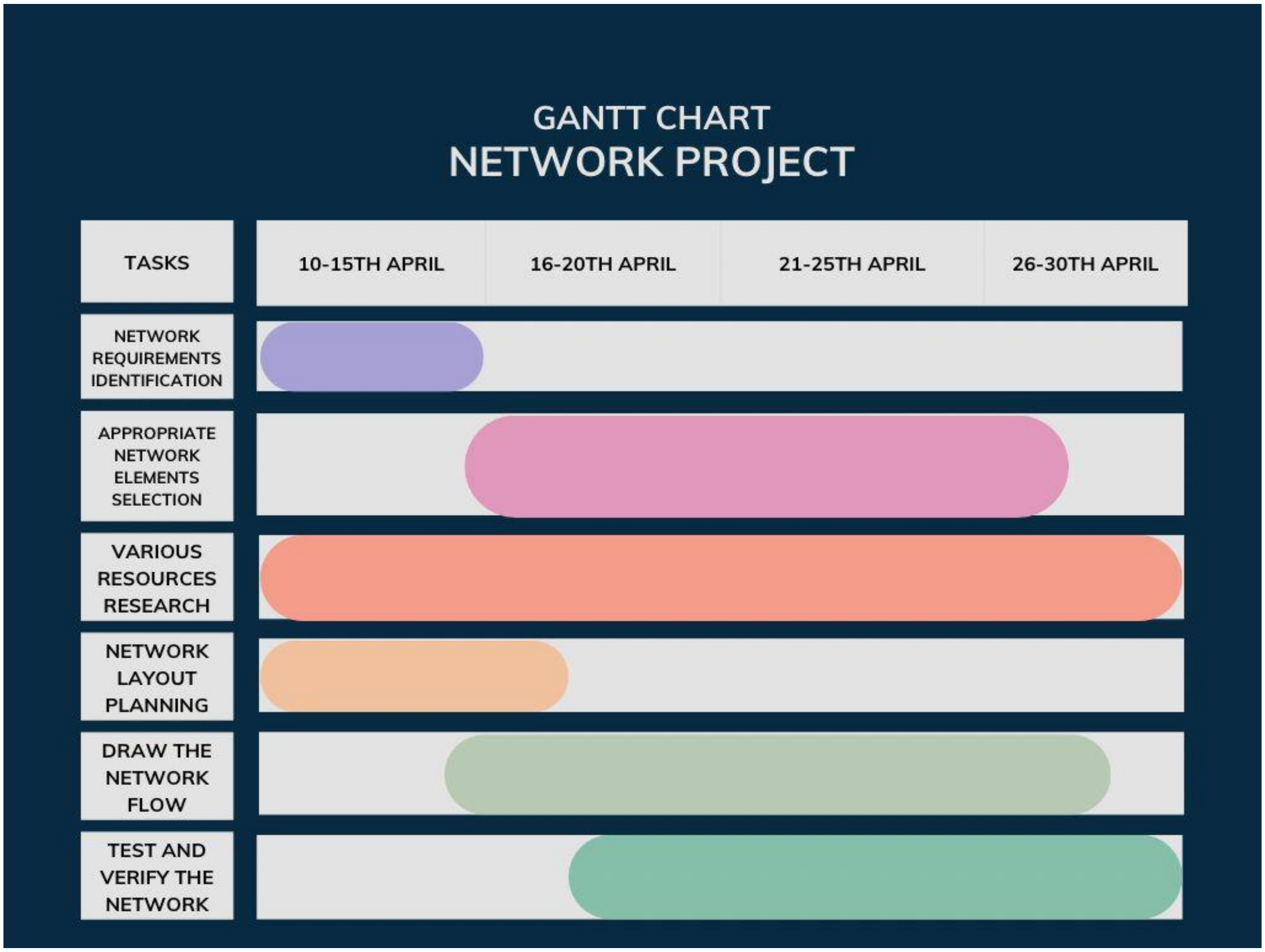
Data and Analytics lab subnet

This diagram represents a subnet that is the Data and Analytics lab. The Data Analytics lab consists of 15 desktop computers connected by wire to a POE switch that is connected to routers. Each desktop computer is connected to a headset by Bluetooth, a wired connection can also be considered. The lab has 15 tablets connected to the network via wireless access point/ router that is then connected to the switch, this allows them to gain access to the network and internet. The office also has VOIP phones for communication between divisions. However, forwarded customer calls by the head department are received on their desktop pc using Softphone Software and carried by the headset. Consultants can use their personal devices without restricted access, connecting to the wireless access point. Other peripherals like scanners, projectors, printers, and white boards are connected to the switch. However, printing can also be done wirelessly by using Air printer features.


Security lab A7 room 7204 subnet
switch
switch
wired voip phones
wireless access point/wireless router
wireless access point/wireless router
wireless access point/wireless router
wireless access point/wireless router
15 desktops
printers
scanners
projectors
whiteboards
10 laptops

Security lab subnet

The security lab subnet is thoroughly built to enable effective communication and smooth functioning throughout the division. Two switches act as the network's backbone, connected to the outside subnet routers over Ethernet. The first switch connects four wireless access points, providing extensive connectivity across the lab. On the other hand, the second switch links all 15 desktop computers and a few wired VoIP static phones, allowing for data and voice transmission throughout the network. Each desktop has a headset connected to it by wire for the softphone software, making it easier to handle calls from clients forwarded from the other divisions. Furthermore, wired VoIP phones are provided for inter-divisional communication. Additionally, the lab has 10 laptops with similar functionality to desktop computers, each with its headset. These laptops provide mobility, enabling users to roam flexibly within the lab while remaining wirelessly connected to the network.



Record of meetings held within the group:

April 10th: Discussing project requirements.

April 11th: Project work division.

April 14th: Sharing related references and research.

April 16th: Drawing the first draft.

April 21st-23rd: Developing an enhanced version of the draft.

April 24th-26th: Writing the report.

April 26th-30th: Finalizing and verifying the project.

References:

Cisco (2021) 'Campus LAN and wireless LAN Solution Design Guide', Cisco. Available at: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html (Accessed: 30 April 2024).

Rouse, M. (2023) 'What is voice over internet protocol (VoIP)? - definition from Techopedia', Techopedia. Available at: https://www.techopedia.com/definition/5406/voice-over-internet-protocol-voip (Accessed: 30 April 2024).

Kurose, J. & Ross, K. (2021) Computer Networking. 8th ed. New York: Pearson.

Lin, C. H., Lai, C. F., Tsai, H. J., & Chu, W. T. (2018). Intelligent cable modem termination system for improving the efficiency of HFC networks. Journal of Optical Communications and Networking, 10(2), A250-A259.

Xie, Y., Yu, J., Huang, H., Zhang, S., & Wang, J. (2017). A novel stateful firewall design for high-speed networks. IEEE Transactions on Network and Service Management, 14(1), 236-248.

Dinh, T. N., Qiu, T., & Thai, M. T. (2019). A survey of network simulation tools: Current status and future development. ACM Computing Surveys, 52(3), 1-43.

Meng, L., Shi, J., & Jin, X. (2016). A study on VoIP QoS model and its implementation. In International Conference on Computer Science and Technology (pp. 329-333). Springer, Singapore.

Rashid, A., Akram, N., & Azam, S. (2020). VoIP Technology: A Cost-Effective Communication Solution for Organizations. Journal of Advanced Research in Dynamical and Control Systems, 12(Special Issue), 1239-1247.

Alghamdi, S., Liu, L., & Orgun, M. A. (2020). A Review of Cybersecurity Education. In The Impact of Security Culture on Security Compliance in Health Care in the USA (pp. 131-152). Springer, Cham.

Chai, J., Wang, J., & Zhu, Q. (2019). A reliable distributed architecture for VoIP service based on softswitch. Journal of Ambient Intelligence and Humanized Computing, 10(5), 2013-2023.

Durai, P., & Manivannan, D. (2017). An efficient vulnerability assessment model for network security using fuzzy logic and computational intelligence algorithms. Wireless Personal Communications, 94(3), 1629-1649.

Sari, M. I., Nugroho, A. S., & Iswanto, D. H. (2018). The implementation of intrusion detection system using machine learning and signature-based approach for early warning system in the network. In 2018 International Conference on Information and Communications Technology (ICOIACT) (pp. 330-335). IEEE.

Singh, A., Garg, A., & Gupta, A. (2019). A biometric authentication framework for securing e-transaction in e-commerce. Journal of King Saud University-Computer and Information Sciences, 31(4), 480-489.

Sukadev, M. E., Mani, D., & Raghavan, V. S. (2018). Detection of Email Spoofing Attacks Using Email Authentication Techniques. Procedia Computer Science, 132, 1038-1045.

Xiao, L., Liu, H., & Sun, X. (2018). An Improved TLS Protocol Based on Hybrid Key Exchange. In 2018 International Conference on Networking and Network Applications (pp. 99-103). IEEE.

Hu, J., Cai, Z., & Yang, C. (2018). Research on the Security Strategy of Subnet Segmentation. In 2018 International Conference on Computer Science and Application Engineering (CSAE) (pp. 64-68). IEEE.

Zhang, J., Zhou, Y., Yu, Y., & Wang, H. (2019). Research on the Application of Stateful Firewall in Network Security. In 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) (pp. 301-305). IEEE.

Feng, H., Zhu, W., Zhang, H., & Guo, L. (Eds.). (2010). Unified communications and collaboration (UCC) handbook. Springer Science & Business Media. (Chapter 12 by Khalil discusses softphones specifically)