FMDB *Transactions on Sustainable Computer Letters*

Planning and Designing Different Types of Surveillance Networks for Enhanced Security and Monitoring

Wycliffe Kanyimama[1,*], Musa Sule Argungu[2], Danlami Gabi[3], Hassan Umar Suru[4]

[1,2,3,4,] Department of Computer Science, Kebbi State University of Science and Technology, Aliero, Nigeria.
2ukidy@gmail.com[1], sm279arg@gmail.com[2], gabsonley@gmail.com[3], suruhassan@yahoo.com[4]

Abstract: Networks must be planned and designed to fulfill client needs. Good networks require planning. Planning involves analyzing the network's physical and logical settings and comparing them to the client's needs and the network's goals. According to the report, planning is crucial when creating surveillance networks. Most research never considers network kinds when designing networks. Our study demonstrates that planning is the first and most significant component of network design, requiring time, ability, and awareness of the client's needs. The study examines how planning affects network design. The paper discusses the Access, Distribution, and Core layers, which complicate network architecture and technology. The study discusses Ethernet, Wireless, Power or Phone Line, and Hybrid surveillance network designs, as well as Local Area Networks (LAN), Metropolitan Area Networks (MAN), Wide Area Networks (WAN), and Global Area Networks (GAN) as the backbone for any surveillance network. This paper defines network topology as nodes and links' physical and logical organization. However, IP structure appears to be significant for creating a long-term monitoring network. The study finds that the network life cycle is an important process criterion for architecture and development.

Keywords: Surveillance Networks; Enhanced Security and Monitoring; Network Architecture and Development; Local Area Networks (LAN); Metropolitan Area Networks (MAN); Wide Area Networks (WAN); Global Area Networks (GAN).

Received on: 09/11/2023, **Revised on:** 03/01/2024, **Accepted on:** 25/02/2024, **Published on:** 07/03/2024

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSCL

DOI: https://doi.org/10.69888/FTSCL.2024.000181

Cite as: W. Kanyimama, M. S. Argungu, D. Gabi, and H. U. Suru, "Planning and Designing Different Types of Surveillance Networks for Enhanced Security and Monitoring," *FMDB Transactions on Sustainable Computer Letters*., vol. 2, no. 1, pp. 52–62, 2024.

1. Introduction

This paper will discuss the planning of different networks and the design of various types of surveillance networks. Most studies never consider network types when it comes to network design. Study shows that planning is the first and most important part of network design, which requires a lot of skill and understanding of what exactly is required by the client that uses the infrastructure; however, previous designer limited their study to either Home Surveillance Network, Campus surveillance Network or Airport Surveillance Network, without considering the planning aspect of it. The planning and survey will analyze networks and network gaps that satisfy the general description and study how their system works. The methodology was then compared to a larger surveillance system, which this study encapsulates by using IP cameras, sensors, and IP scanners within the same large network.

[*]Corresponding author.

The concept of a surveillance IP Network means moving from the manual surveillance operation to a more digitalized surveillance policing aspect. IP surveillance networks use information and communication technology (ICT) to enhance surveillance. It could be argued that there is no general agreement on what the concept of really means different thing to different people. For instance, “surveillance” could mean critical looking, astute or intelligent. The Bureau of Justice Assistance regards IP surveillance networks as broad-based interventions that apply evidence-based, data-driven policing practices, strategies, and tactics to prevent and control crime. According to Shamsi and Davies [1], (IP Surveillance) is the transaction of services and information between the police and citizens via ICT. A recent review of surveillance service models and call management revealed that using the Internet to report calls for service was an emerging trend. This can be described as electronic transactions between the IP machine and the client system. Usually, the use of network technology and ICT delivers a central access point for public safety.

However, according to Ariel [3], surveillance networks prioritise proactive rather than reactive law enforcement in their fight against crime. In order to implement proactive policing, the author goes on to say that surveillance initiatives should include the use of information and communication technology (ICT)-driven tools like analytical software, DNA forensics, and technology in addition to surveillance capabilities for crime control and prevention. In a similar vein, Santoso et al. [4] contend that data and analytics are becoming more influential in decision-making across all societal sectors in this era of information. Government agencies are just as busy as private companies when it comes to gathering, analysing, and interpreting data—both quantitative and qualitative—in order to make their surveillance operations better and more efficient. From this, one could deduce that a Surveillance IP network is the implementation of diverse high-impact technologies or ICT for the purpose of conducting policing operations outside of the realm of internet-only communication and surveying of the public. Moreover, despite the abundance of definitions, surveys and surveillance are considered essential components of e-government, which is defined as the use of information and communication technologies by governments to guarantee efficient and effective service delivery in order to fulfil the needs for greater transparency and to appease the information demands of outside organisations [12].

Smart policing is another name for a surveillance network. It is generally described as the integration of current policing strategies like Intelligence-led, Hotspot, Problem-oriented, Community, and Sector Policing with cutting-edge technological advancements in order to better and more efficiently execute these strategies. A striking feature of these explanations is that, instead of focusing on crime prevention and control, the phrase "smart policing initiatives" is used to describe efforts to enhance the overall effectiveness of the police force. The efficacy, efficiency, and cost-effectiveness of these endeavours, however, require additional focus.

The security industry has moved on from closed circuit television (CCTV) to IP cameras, which are now the craze. Through the use of a built-in web server and network technology, IP cameras allow for video surveillance monitoring from any location and at any time using a web browser. It is common practise to link the system to either an existing or a design network. IP cameras have the capability to do intelligent calculations, and there is a growing supply of related equipment and services. Furthermore, compared to CCTV, the installation costs of IP cameras are lower [5]. In a well-designed and installed network, IP cameras include a web server, encoder, and CCTV camera, making them easy to manage. You can access it in real-time from any location using your smartphone or the web. On the other hand, there are some issues with IP cameras that need to be addressed, such as the need to certify users and design access to the IP camera web server, as well as newly installed IP cameras on the network.

The technology behind networking systems is advancing at a rapid pace. The system is increasingly incorporating more complex network topologies to facilitate the connection of end devices like PCs, routers, switches, smart devices, Internet of Things (IoT) devices, etc. They have introduced new networking technologies. One of these is the Local Area Network, or LAN. As a result, it facilitates the connection of end devices at closer spatial distances. Therefore, it is suitable for use in medium to small businesses. This paves the way for rapid expansion of monitoring systems. Another advancement in technology that originated from LAN is the Wide Area Network (WAN). In comparison to other comparable technologies, the WAN facilitates the merging of multiple local area networks (LANs) into a single, larger network. Data and traffic communication is facilitated by computer networks, which are a crucial concept. Routing, system design for networks, and strategy development, including visual network learning, are common components of computer networks. When information needs to go from one node in a network to another, routing is what makes that possible.

A Smart Airport Surveillance Network was developed by Dash and Sharma [6] to track the arrival and departure of aircraft at the airport. This study found that the air control room, which oversees all airport operations, is one of the most crucial areas. With a default mask of 255.255.255.0, the IP address of the PC in the air control room is 192.168.20.0. In order to fulfil the needs of the client, this surveillance network has been meticulously designed and organised. Nonetheless, the correct survey and need analysis were conducted during the network's planning stages, making this possible.

After that, there are two sections to the arrival room. Both the staff and the customers will need one. Here, the two pieces are partitioned into separate routers. Employees can stay informed about flight status updates and other important traffic by connecting their routers to the airport control room. Security reasons prohibit guests from transmitting or accessing data to or from the Air Control Room. In order to secure the arrival room and control the data transmission system, the study employed static routing.

There are two sections to the departure room: the staff and the customers. Accordingly, two separate routers serve distinct purposes in each component. Additionally, the router used by the staff can communicate with the Air Control Room, allowing them to stay informed about any changes or new flight information. For safety reasons, guests are still unable to transmit or receive data from the Air Control Room. Computers in the Departure Room have an IP address range of 192.168.40.2 to 192.168.40.10. When using a subnet mask, all of the computers have the same DNS server and default gateway. All of the computers use 0.0.0.0 as their DNS server, and the IP address of the router that links the computers in the air control room to the internet is known as the default gateway IP.

2. Hierarchical Network Design

When it comes to network architecture, there are no hard and fast rules or "one size fits all" answers. Follow the rules of the network; that is the only guiding principle. Nevertheless, when confronted with intricate network architecture, it is helpful to be familiar with the critical design factors. This will allow you to prioritise the components necessary to address the network's complexity and create a solution that satisfies those factors. Three separate hierarchies or layers of functionality make up the network design, according to a recent study by an academic specialising in Cisco networking. Different functions and purposes are met by each layer. Layers consist of:

- Access layer
- Distribution layer
- Core layer

Users, in this case the scanners and cameras, are connected through the access layer. The distribution layer is responsible for the transmission of data between different local networks. Here you may find the network technology and the connector. The core layer, meanwhile, stands in for the fast backbone layer that connects all the other networks. The access layer is the usual starting point for user traffic, which then proceeds to traverse the levels as needed.

What this means is that the hierarchical design model divides the design into modular groups or layers, as shown in the study by Kang et al. [7]. Eliud claims that the network design may be simplified and made easier to deploy and administer by breaking it into layers, with each layer focusing on specialised functions. According to his research, one can make design components that can be repeated all throughout the network by using modularity in network architecture. With replication, you may easily scale the network and distribute it consistently. The many levels of network architecture are illustrated in Figure 1.

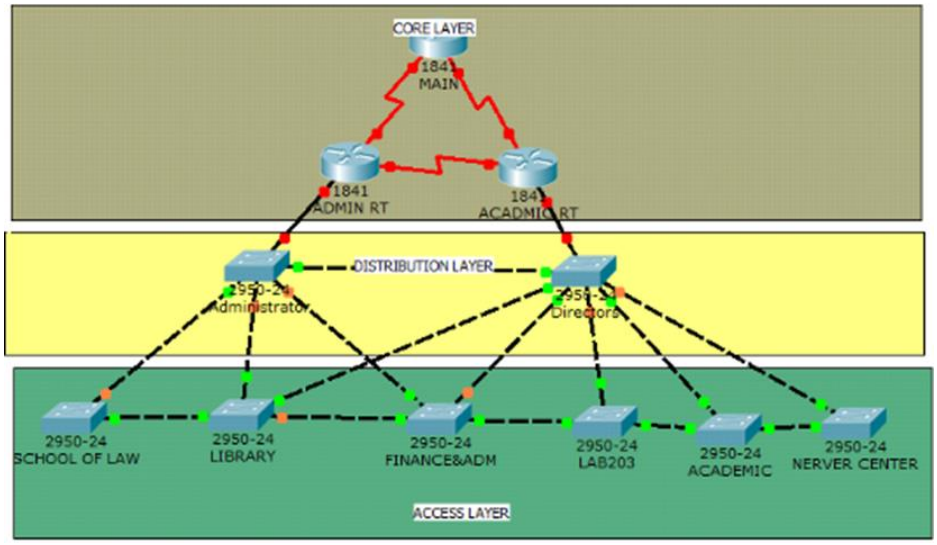

Figure 1: Hierarchical design layers

At the very centre of every network or system is the core layer. The core layer, located at the very top of the stack, is in charge of the fast and reliable transfer of massive data sets. Streamlining traffic switching is an important function of the network's foundational layer. Most users experience the traffic being transferred over the core. An other name for the distribution layer is the workgroup connector layer, and it is responsible for facilitating communication between the core and the access layer. The distribution layer is responsible for a number of things, including filtering, routing, and wide area network (WAN) access, as well as determining how packets can reach the core when necessary. The access layer manages which network resources can be accessed by users and groups within an organisation. One name for the access layer is the desktop layer. Nearby servers will house the majority of users' network resources. The distribution layer is responsible for managing all traffic related to connectivity and remote services [8]. Although there are three levels in the hierarchical architecture, a two-tiered hierarchical network design may be used by smaller enterprises. Networks with a two-tier hierarchical design may be simpler and cheaper to build since the core and distribution layers are combined into one.

3. Types of Network Design

According to Khalifeh et al. [9], the four main types of smart network designs are embedded in any network architecture, whether it's a local area network (LAN), metropolitan area network (MAN), wide area network (WAN), or global area network (LAN). These designs include Ethernet smart home network, wireless network, power or phone line smart network, and hybrid smart network (GAN).

3.1. Ethernet Smart Home Network Design

There are a variety of network designs that can be used to plan home area networks. The benefits and drawbacks of each network design are different. The key point is that the architecture is long-lasting, inexpensive, and adaptable to future changes in the network. Using Ethernet cables, every computer in an Ethernet Design communicates with a central router or modem. In comparison to wireless networks, which can only manage speeds of up to 100 Mbps, Ethernet networks are far more advantageous due to their ease of setup, speed, and capacity to reach speeds of up to 1000 Mbps. But this technology has an issue with running the cables and isn't very mobile (Figure 2).

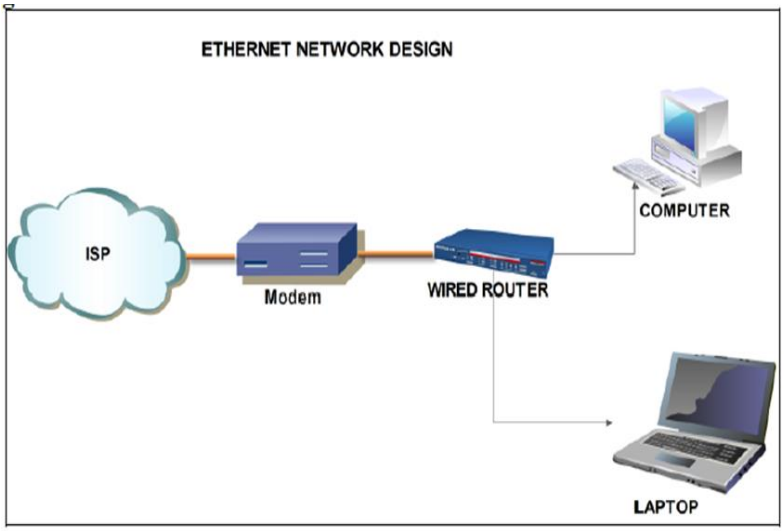

Figure 2: Ethernet Network Design

3.2. Wireless Network Design

Computers using this technology link up wirelessly with a wireless router or other wireless devices. The fundamental benefit of a wireless network architecture is the reduction or elimination of cable clutter, allowing users greater freedom of movement within the home or within the range of the network while carrying out various tasks. Also, the most recent development in wireless technology is Wi-Fi, which allows any device with Wi-Fi capabilities to connect to a wireless network with ease. One major issue with wireless networks is the restricted coverage they provide. Data security is not a given; it is something that needs to be maintained. Setting up such a network also requires some technological know-how (Figure 3).

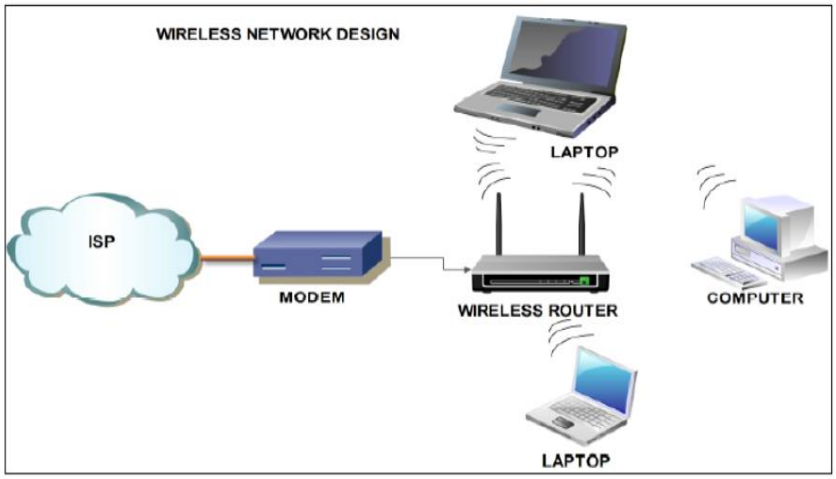

Figure 3: wireless network design

3.3. Power or Phone Line Smart Network Design

The data and traffic carried by an internet signal can be sent to additional computers in a home using power or phone lines in this network arrangement. With this setup, it's possible to add more computers and Wi-Fi-enabled devices to an existing home network, increasing the network's capacity and allowing more people to access the internet (Figure 4).

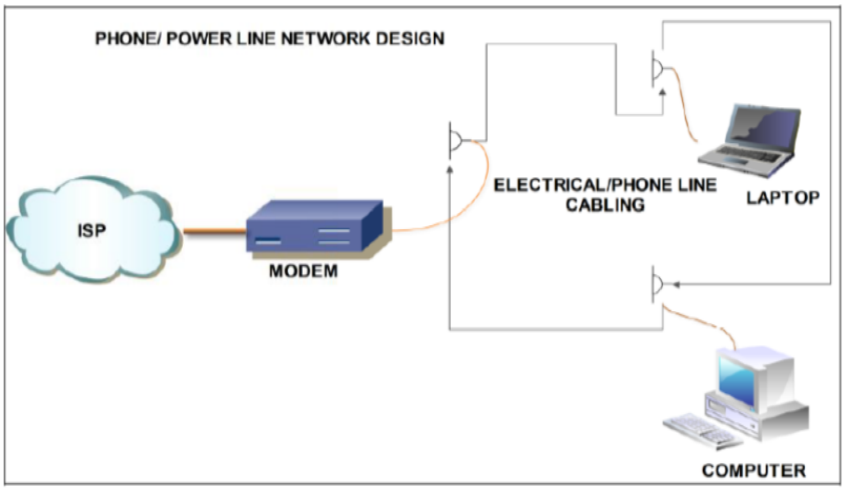

Figure 4: Phone/Power Line Network Design

3.4. Hybrid Smart Network Design

The basic premise behind hybrid network designs is to integrate the best parts of several types of networks. It is possible to expand the network's capacity and connect all of a home's PCs to the internet. This layout is compatible with either wired or wireless technology, or even a combination of the two in a single network configuration. Accessing the Internet using power or phone line connections is an option for computers that are unable to connect to a router. So, if you're looking for a way to develop a network design for your home or business that's both efficient and affordable, a hybrid approach is a great choice (Figure 5).

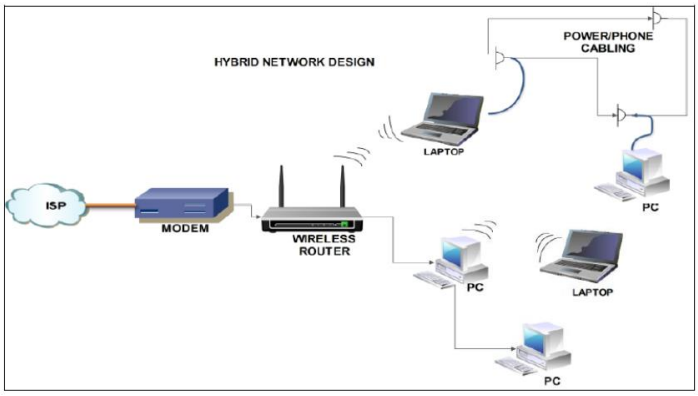

Figure 5: Hybrid network design

Additionally, the network can be subdivided into four main geographical sections. Tri-Level Networks: LANs, MANs, and WANs (WANs). Network for the Whole World (GAN) [10]. Any collection of interconnected local networks that are managed by the same administrative body is called a local area network (LAN). Local area networks (LANs) were originally characterised as tiny networks that resided in a single physical location in the early days of networking. A WAN is a vast system of interconnected computer networks that are not limited to a certain physical location. More than local area networks (LANs), wide area networks (WANs) allow for communication and data sharing. Wide area networks (WANs) can also mean networks that span a lot of land (Figure 6).

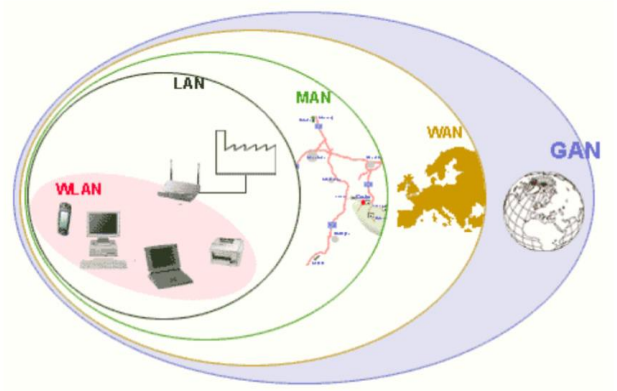

Figure 6: Types of Network

Computers and users in one place can communicate with those in another location thanks to wide area networks (WANs), which link smaller networks like metro area networks (MANs) and local area networks (LANs). Computers in a metropolitan area (MAN) are linked by a network. A metropolitan area might be a single large metropolis, a collection of smaller cities and towns, or any significant area with numerous buildings. In most cases, a MAN will be bigger than a LAN but less than a WAN. Simultaneously, there is an infinitely large network called the Global Area Network (GAN) that is made up of interconnected networks. The phrase is often used interchangeably or in connection with the Internet, which is a worldwide network.

3.5. VLAN (Virtual Local Area Network)

To facilitate data flow without the initial conventional physical limitations imposed on the network, a virtual local area network (VLAN) simulates a typical LAN in network technology. The LAN devices that make up an administrative group can form a VLAN. Rather than geographical location, administrative policies and setup criteria determine who can join the VLAN Group. Even though they may be on separate physical LAN segments, members of a virtual local area network (VLAN) communicate with each other as though they were on the same wire or hub. Users on the same switch can nevertheless participate in virtual local area networks (VLANs) and communicate with each other as though they were on separate portions of the network. Virtual Local Area Networks (VLANs) are more adaptable due to their foundation in logical rather than physical links [11]. Figure 7 is the source.

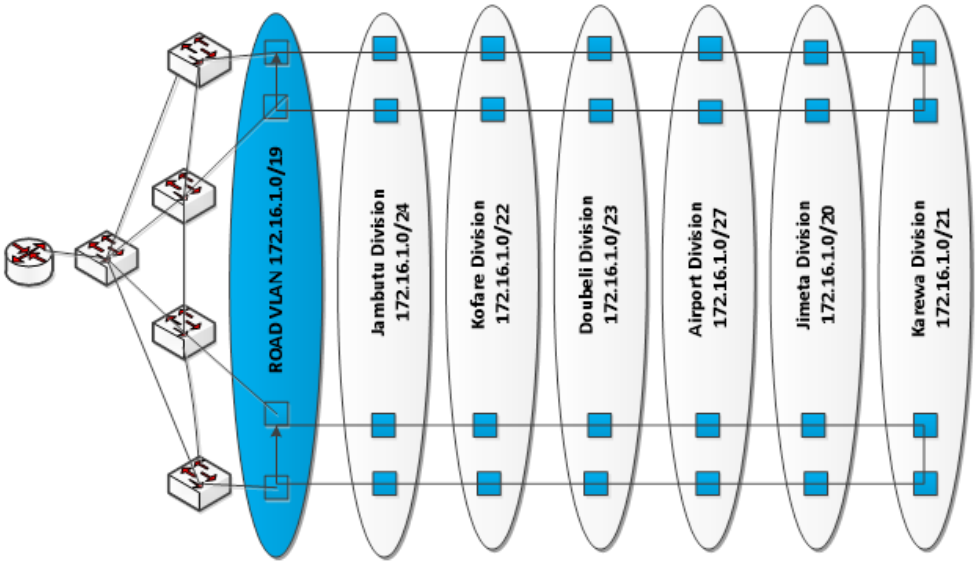

Figure 7: VLAN showing group members

The switches in the above VLAN configuration are set to identify the following VLANs: road, Jimeta, Karewa, Dobeli, and airport. Through the connection link, frames can be exchanged, and the receiving switch can check the VLAN tag to see which frames to send. One name for the connection between the two switches is a trunk, while another is a trunk link. The network designer can use the Trunk links to create VLANs that span numerous switches, as demonstrated above.

4. Network Design Topology

The physical and logical configuration of a network's nodes and links is called its topology. Common node types include switches, routers, and the capabilities of routers. It is common practise to use a graphical model to depict network topologies. The arrangement of hardware components, such as computers, cables, and other peripherals, is known as physical topology. Logical topologies, on the other hand, detail the locations of network services like routing and address resolution as well as the paths that data takes inside a network. The physical topology diagram of a wired network depicts the cabling closet as well as the cabling leading to each user's station. The physical topology of a wireless network consists of an access point and a wiring closet. The physical topology confines the wireless signal inside the coverage area due to the absence of wires.

Having a logical understanding of the network topology is occasionally important in addition to the physical topology map. Hosts are grouped in a logical topology map according to their network usage, regardless of their physical location. The logical topology map can document host names, addresses, group details, and applications [13]. Figure 8 shows the graphical representation of the two topologies, which can help you comprehend the differences between them.

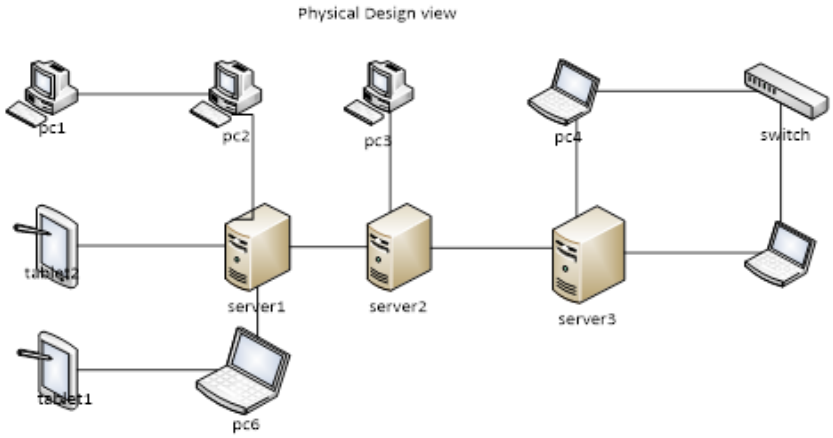

Figure 8: Physical Design View

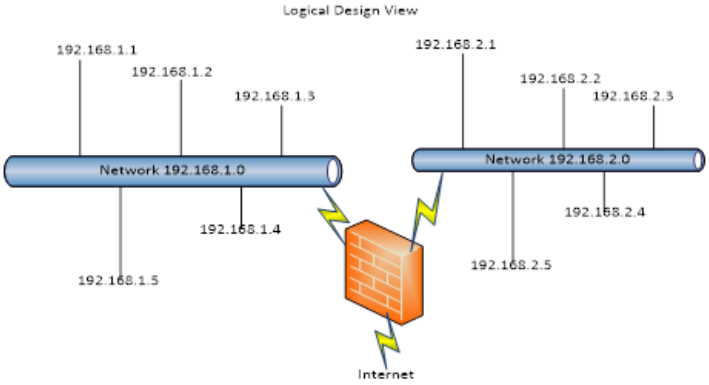

Figure 9: Logical Design View

Research on web-based video dashboards was conducted by Siagian and Fernando [14]. An OpenStack topology design is presented in the study. This design incorporates API technology services, a web-based dashboard interface, and the servers of compute, storage, and data centre data source networks (Figure 9). Based on the amount of visualisation pictures (VM) requested by the task, the study developed a topology that may be modified to make this more adaptable. Nova, Keystone, Horizon, Cinder, Glance, Swift, and Neutron are some of the primary components that make up OpenStack. This part has an additional purpose as well. The Nova is responsible for controlling how the network's computing resources are used; the Neutron is in charge of managing all of the network's resources and providing image storage services; the Cinder is in charge of the block storage area; and the Keystone is in charge of providing certificate services and horizontal functions to help with the operation's interface. You can see OpenStack's IP and network architecture below (Figure 10).

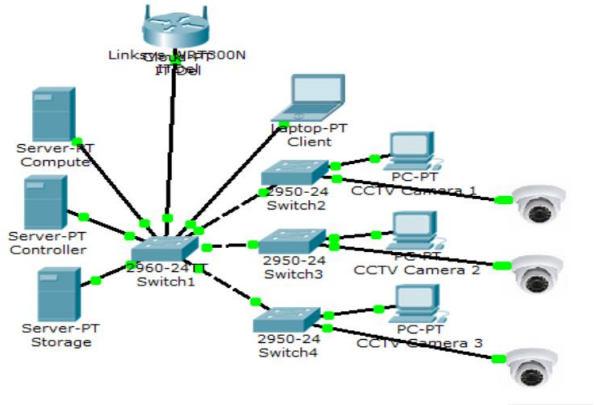

Figure 10: Physical Network topology for OpenStack

Table 1: IP address structure for OpenStack

s/n	Police Division		Network IP	Subnet mask	CIDR	Total Host
1	**Jimeta Division**	Network1	172.16.1.0	255.255.240.0	/20	2^12=4,096
		Network2	172.16.16.0	255.255.240.0	/20	2^12=4,096
		Network3	172.16.32.0	255.255.240.0	/20	2^12=4,096
	Up to	Network32	172.16.**248**.0	255.255.**248**.0	/21	2^11=2,048
2	**Double Division**	Network1	172.16.2.0	255.255.254.0	/23	2^9=512
		Network2	172.16.4.0	255.255.254.0	/23	2^9=512
		Network3	172.16.6.0	255.255.254.0	/23	2^9=512
	Up to	Network128	172.16.**254**.0	255.255.**254**.0	/23	2^9=512
3	**Airport Division**	Network1	172.16.1.32	255.255.255.224	/27	2^5=32
		Network2	172.16.1.64	255.255.255.224	/27	2^5=32
		Network3	172.16.1.96	255.255.255.224	/27	2^5=32
	Up to	Network8	172.16.1.**224**	255.255.255.**224**	/27	2^5=32
4	Road Network	N	172.16.**224**.0	255.255.224.0	/19	2^13=8,192

The network topology mentioned before can be accurately represented by the IP addresses in Table 1. By utilising Integrated Multiple Camera Surveillance, the table's simulated IP address was created (MCS). Utilizing OpenStack Swift on IaaS, the web application for video surveillance is linked to MCS and the data centre through PC-PT. Using MCSs, the object storage fast acquires nine nodes for network-based original video recording storage. Using OpenStack Swift, it integrates all the benefits of a web-based dashboard system.

5. Security Camera System

In comparison to human security guards, modern security camera systems are far more effective and efficient. Nowadays, cameras come equipped with high-definition sensors that can identify and recognise objects. Using a powered system, Aishwarya and Lande [2] created a wireless camera system. Charging their batteries from the sun, the wireless cameras record footage in real time and transmit it to a central station via a wireless network. This technology allows the system to function both during the day and at night. During the day, the solar panel provides power and charges the device. In the evening, the system battery provides backup for the camera operating system. To record footage in motion, they utilised a Raspberry Pi 3 module that had a camera attached to it. Raspbian, the operating system that the Raspberry Pi 3 runs on, is typically freely available online. They utilise sudo apt-get to create and install motion commands on Raspbian Pi's command line, and then they use the motion daemon 'Motion' library to detect motion.

Setting up port forwarding in the modem or router is a must for setting up an internet capture camera and for monitoring a webcam from any location over the Internet. Port 80 must be forwarded in order for Raspberry Pi's private IP address to be used. Since all incoming connections to port 80 are processed at the local address, this allows one to view the live streaming by inputting their public IP address. In order to connect to the Raspberry Pi from the outside world, you'll need a public IP address that won't change when you restart it.

An algorithm that takes into account the use of a Raspberry Pi and a camera to establish a low-cost surveillance camera was also created by Aishwarya and Lande [2]. The algorithm chart can be found below. In order to activate motion detection, you'll see a decision box on the chart. Once you confirm that there is movement, the camera will take a picture, store it in system memory, and then transfer it to your phone over Wi-Fi. That is to say, the systems go back to square one if they don't find any images. The iterative nature of these procedures (Figure 11).

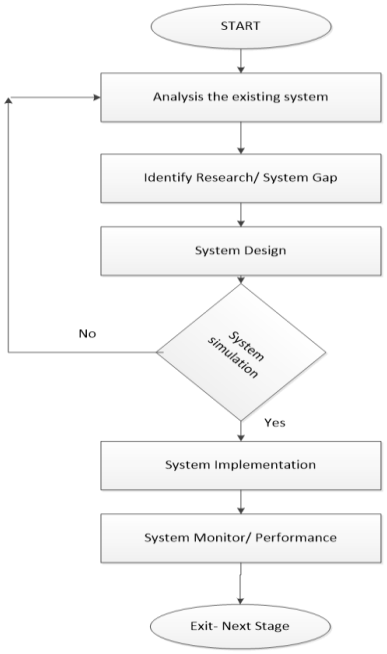

Figure 11: surveillance camera algorithm

6. Network Development Life Cycle

When working on a network development project, the network life cycle is a crucial set of procedural standards that helps with network architecture. The cycle provides a systematic approach to accomplishing a task. There are six stages to the network lifespan. Figure 2 shows the phases of the Network Development Life Cycle (NDLC) that Javid and Pervez [15] divided into

analysis, design, simulation, prototype, implementation, monitoring, and management. The NDLC is considered to be highly appropriate for research pertaining to network design. The researcher begins the design and research phase by assessing the current structure or system in order to make improvements to it, and this analysis serves as a foundation for future research that can be helpful as a reference [16]. Prior to beginning the design process, all hardware, including routers, client devices, and servers, is configured. This architecture is based on the protocols. To avoid reconfiguring the network every time there's an issue, maintenance, or an update, it's important to document the configuration. This is because adding or changing a device without affecting its previous configuration means that all of the devices will continue to communicate as if they were on the same network (Figure 12).

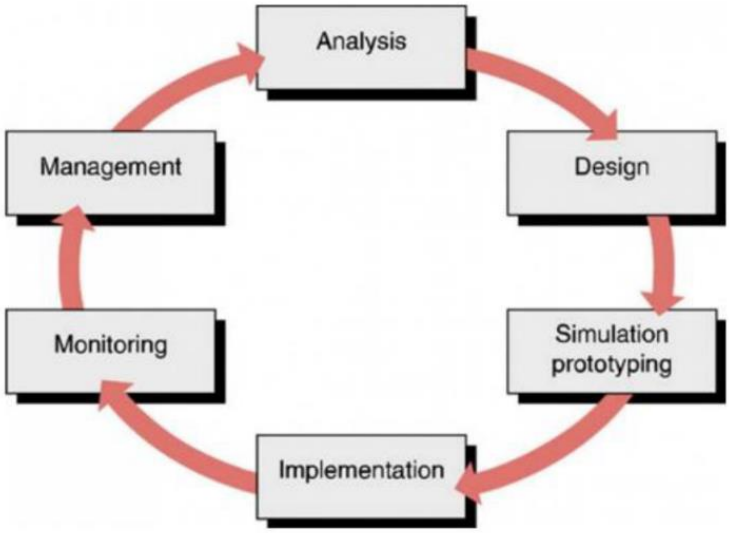

Figure 12: Network Development Life Cycle

The following step is simulation prototyping, which involves deploying software to verify the system's connectivity and ensuring it functions as expected by the designer. All of the previously planned and prepared stages will be put into play during the implementation stage. The success or failure of the project will be determined at the implementation stage, which will test the team's abilities in both technical and non-technical areas.

Computer and communication networks must be able to function in accordance with the user's original desires and objectives established during analysis in order for the implementation phase to go to the monitoring phase. The monitoring stage must be executed. The last step is to oversee the new system to make sure it's optimised, up-to-date, working, and carrying out its intended function.

7. Conclusion

The concentration of research in surveillance networks has been notable, with various studies focusing on distinct types of systems, including Home Surveillance Networks, Smart Surveillance City Networks, Airport Surveillance Networks, and Campus Surveillance Networks. Each of these studies has contributed valuable insights, yet they remain isolated in their applications and designs. This study, titled "Planning Surveillance Network," seeks to integrate these diverse surveillance systems into a comprehensive framework that consolidates all existing networks into a unified structure. The proposed Smart Surveillance Network encompasses elements from Smart Surveillance homes, airports, and campuses, creating an interconnected ecosystem designed for enhanced monitoring and management. By integrating these systems, the study aims to address the existing gaps in network design, particularly in terms of interoperability and scalability. Moreover, this research underscores the necessity for further investigation into the planning and architecture of surveillance networks. As technology evolves, the demand for robust, efficient, and cohesive systems becomes increasingly critical. Future studies should focus on developing a comprehensive surveillance network that not only enhances monitoring capabilities but also facilitates the control of various policing activities through advanced network technologies. This holistic approach is essential for creating a more secure and efficient environment, ultimately paving the way for smarter and more responsive surveillance solutions that can adapt to the needs of modern society.

Acknowledgment: We are deeply grateful to the Kebbi State University of Science and Technology, Aliero, Nigeria.

Data Availability Statement: The data for this study can be made available upon request to the corresponding author.

Funding Statement: This manuscript and research paper were prepared without any financial support or funding

Conflicts of Interest Statement: The authors have no conflicts of interest to declare. This work represents a new contribution by the authors, and all citations and references are appropriately included based on the information utilized.

Ethics and Consent Statement: This research adheres to ethical guidelines, obtaining informed consent from all participants.

References

1. A. Shamsi and A. S. Davies, “Smart policing: Abu Dhabi police AI/GPS-based initiative to reduce heavy vehicle driver violations,” Policing: A Journal of Policy and Practice, vol. 16, no. 2, pp. 260–269, 2022.
2. S. Aishwarya and B. P. Lande, “Wireless security camera system,” International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 2751-2754, 2019.
3. B. Ariel, “Technology in policing,” University of Cambridge, United Kingdom, pp. 485-516, 2019.
4. B. Santoso, A. Sani, T. Husain, and N. Hendri, “VPN site to site implementation using protocol L2TP and IPSec,” TEKNOKOM, vol. 4, no. 1, pp. 30–36, 2021.
5. R. Catte and R. Linden, “Leadership and change in Winnipeg’s Smart Policing Initiative,” Polic. J. Policy Pract., vol. 15, no. 1, pp. 181–196, 2021.
6. B. Dash and P. Sharma, “Role of artificial intelligence in smart cities for information gathering and dissemination (A review),” Academic Journal of Research and Scientific Publishing, vol. 4, no. 39, pp. 58-35, 2022.
7. J. Kang, J. Han, and J. Park, “Design of IP camera access control protocol by utilizing hierarchical group key,” Symmetry (Basel), vol. 7, no. 3, pp. 1567–1586, 2015.
8. S. K. A. Imran, S. Mitra, R. Islam, and S. S. Das, “Developing a network design for a smart airport using Cisco Packet Tracer,” Informatica Economica, vol. 25, no. 1, pp. 25-38, 2022.
9. A. Khalifeh et al., “Wireless sensor networks for smart cities: Network design, implementation, and performance evaluation,” Electronics (Basel), vol. 10, no. 2, p. 218, 2021.
10. K. Gakis and P. Pardalos, Network Design and Optimization for Smart Cities, University of Florida, USA: World Scientific Publishing, vol. 8, no. 6, pp. 404, 2017.
11. M. Ekaabi, K. Khalid, and R. Davidson, “The service quality and satisfaction of smart policing in the UAE,” Cogent Bus. Manag., vol. 7, no. 1, p. 10, 2020.
12. R. L. G. Matlala, “Defining e-policing and smart policing for law enforcement agencies in Gauteng Province,” Int. J. Soc. Sci. Humanit. Invent., vol. 3, no. 12, pp. 3058-3070, 2016.
13. M. Ji, “Designing and planning a campus wireless local area network,” International Journal Information Technology, vol. 1, no. 5, pp. 1-40, 2017.
14. P. Siagian and E. Fernando, “The design and implementation of a dashboard web-based video surveillance in OpenStack Swift,” Journal of International Conference on Computer Science and Computational Intelligence, vol. 179, no. 10, pp. 448-457, 2020.
15. S. R. Javid and S. M. Pervez, “Planning a smart network design in home networking: A survey,” International Journal of Advanced Research, vol. 3, no. 5, pp. 1308-1312, 2013.
16. T. Lammle, Cisco Certified Network Associate Study Guide, SYBEX Inc., Alameda Press, Alameda, 2000.