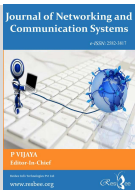
Vol.6 No.4 Oct 2023

Journal of Networking and Communication Systems

Received 16 September, Revised 11 October, Accepted 21 October



Design of Logical and Physical View of IP Surveillance Network

Wycliffe Kanyimama
Kebbi State University of Science and Technology Aliero (KSUSTA), Kebbi State Nigerian.

Musa M. S. Argungu
Kebbi State University of Science and Technology Aliero (KSUSTA), Kebbi State Nigerian.

Abstract: At times of failure, problems,or upgrading network topology mapping becomes paramount. Tounderstand the possible failure occurrence, the topology views of the network become the first step to use asa solution. Such practice helps network engineersreduce the downtime to restore the falling network link through the logical and physical design view of the network. Inthe design phase, the designer failstodifferentiate and specify the physical topology from the logical topology view of the network this will reduce the network efficiency. The study aimsto design the logical and physical view of a security surveillance network system to provide network management in times of failure. Most designers are not taking into consideration the views as the backbone and foundation of building a network. The study used IP Vision 4 classes C (192.168.1.0/27) andsubnetted into units to enable manageable networks and hosts to meet up with future growth. The logical and physical view of the network is identified to differentiate in times of failure and upgrading. The tools used to achieve the goal are Microsoft Visio and Smart Draw for Network Architectural Design for the logical design view. A packet Tracer simulation machine is been deployed for the physical design view and also to detail the network information. The designed network is subdivided into sub-management units (from networks 1 -8) which provide flexible, scalable, and cost-effective solutions suitable for Local Area Networks (LAN). However, the study uses existingliterature to gather primary and secondary data. Study shows that IP surveillance network technology are taking over the manual policing system and Countries like America, British and others were able to implement them in other to reduce crime using IP Surveillance Networks. The designer recommends full system deployment and implementation when it comes to network design methodas operational requirements for standard performanceand also encouragesfurther research on network design mapping

Keywords: SurveillanceNetwork, security, Logical view, physical view, Internet Protocol, Network, subnetting

Nomenclature

Expansion	Abbreviation
Internet Protocol	IP
Closed Circuit Television	CCTV
Physical Topology View	PTV
Logical Topology View	LTV
Cisco Certify Network Academic	CCNA
Transmission Control Protocol	TCP
Sub Networks	Subnetting
Network Development Life Cycle	NDLC
Power over Ethernet	PoE
Network Hosts	H
Network Bits Host Part	NBHP
Routing Information Protocol 2	RIP2
Main Distribution Facility	MDF
Network Address Translation	NAT
Virtual Local Area Network	VLAN
Application Programming Interface	API
Network Interface Card	NIC
Information Communication Technology and Security	ICTS
Spanning Tree Protocol	STP
Pan Tilt Zoom	PTZ

https://doi.org/10.46253/jnacs.v6i4.a1

1. Introduction

IP surveillance networks are criticalbecause they attract worldwide attention to track many crimes and terror attacks.The recent was the tracked movements of two attacks on9th January 2015 in the office of Charlie Hebdo inParis that left 12 persons dead in France [10]. Despite their usefulness, most current IP surveillance Networksare designed with one missing part, which is the logical and physical view to allow for flexibility.The most common technology used in surveillance is the CCTV. A CCTV system is one in which many video cameras are connected through a closed circuit or loop and the image taken by the cameras is sent to a television monitor or recorder [8]. The term close circuit highlights the private nature of the system and distinguishes it from television broadcasting from which anyone can receive signals. There is little or no doubt that CCTV is a powerful crime-managing tool producing huge amounts of visual data [1].Some solutions may yield valuable intelligence which can lead to successful prosecutions [15]. Increasingly, CCTV technology is becoming more of a former rather than new technology in terms of surveillance networks. Nowadays, modern CCTV cameras exist which use digital technology commonly known as IP.Cameras are no longer closed circuits but are usually networked with digital cameras [13]. The IP camera surveillance is combined in a network with software capable of better storage, access to events, and detection of security breaches[23]. For example, digital surveillance systems can track individuals with a camera image that carries explosive devices.

A physical topology is the real physical location of cabling, computers, and other network devices that are placed within the network. Where the logical topology documents the pathways that data is taken through a network and the location addresses where network functions, like routing, occur. In a wired network, the physical topology mapconsists of the wiring closet, as well as the wired to the individual end-user stations. In a wireless network, the physical topology consists of the wiring closet and an access point. Since there are no wires, the physical topology contains the wireless signal of the area covered within the network, and this includes the names and Layer 3 addresses of end stations, router gateways, and other network devices, regardless of the physical location. Itindicates the location of routing, network address translation, and firewall filtering is usually placed on topology mapping of the network [14].Therefore, it is clear that any network designer who fails to separate the logical and physical mapping would eventually lead to confusion when it comes to network maintenance and upgrading [25].

Network documentation is paramount especially when there is a problem or failure within the network, the engineer first consults with the network document for a speedy solution. For one to understand where the possible failure occurs, the topology views of the network become the earlier step to use for a solution base that is well documented at the design phase. This practice helps to reduce the time for restoring a falling network link through the logical and physical design view of the network. If from the design phase, the designer identifies the physical and logical topology view of the network this will increase the network efficiency.

Many network designs have mission-critical tasks, so it is clear that the physical and logical view of the network needs to be taken into consideration at design time. Security and response time is paramount for most network applications for the following reasons. Most Surveillance networks actively monitorpublic spaces and therefore, when the network is down this can allow for threat and security windows, which often deduce wrong perceptionof information other than the data monitored [5]. Such unwanted information leakage results in privacy breaches of the people in the environment. The combination of these factors demands adequate design measures for Surveillance networks to ensure smooth operation. Secrecy of sensitive data and privacy for people within the network environments can only be achieved through the prepared design and operation of the surveillance system [22].The network downtime is always reduced through well-designed network documentation, the network documentation here entails the design of both the physical and logical view of the network to understand how and where each device is connected.

This paper provides proactive measures tohelp network designersconsider building a network with various views or mapping as this would improve the design and subsequently in terms of a network management system. The study has been provento be of value to network securitypersonnel in the aspect of managing network infrastructure as this will reduce maintenance and operational cost. In this age, building a surveillance networkis a promising approach for a variety of applications such as monitoring the safety and security of public spaces, measuring traffic flows, and tracking unguided behaviors by person. Over the years IP Surveillance Networks have played an essential role in various aspect of pervasive computing technology, as even our personal mobile devices interact with IP Surveillance networks in our environment which eliminate distance[17].

The main contribution of the project is to designa logical and physical view of a security surveillance network system to improve network management when there isa failure. Most designers don'ttake into consideration the different views as the backbone and foundation for building a reliable network.

This study designed a logical view and physical view of an IP surveillance network that proved for different views even when the network is at the implementation stage. These views allow for management and maintenance phases easy with the network, this is because the views serve as a key through which the system operates. The study adoptsthe Network Life Cycle development method to achieve the said goal. It is expected that at the end of the paper, a clear network mapping or view will be proven for IP surveillance Networks.

The paper is organized as follows: Section 2 covers the Literature review. Section 3 details the Methodology, and Section 4 emphasizes the Results and Discussion. Section 5 mentions the Advantages and Disadvantages of the proposed method. The conclusion is recapitulated in Section 5.

2. Literature Review

This section focuses on similar works undertaken by different researchers, organizations, or companies to have a clear insight into previous and present studies in this area of interest. The section reviews related works on physical and logical views of network surveillance technology and the level to which IP surveillance design has grownto effectively prevent crimes and terrorism.

2.1 Physical and Logical Network Design View

CCNA describes Physical and Logical as the two design views or mapping commonly to aid network design. A physical mapping is said to be the actual physical location of cables, computers, and other devices. A logical mapping or view documents the path and address that data takes through a network and the location where the network functionsincludingrouting. When networks are designed, a physical topology map is created to record where each host is located and how it is connected to the network. The physical topology map also shows where the wiring is installed and the locations of the networking devices that connect the hosts. Icons are used to represent the actual physical devices within the topology map [6].

Fig. 1 graphically illustrates the physical design view of the network and Fig. 2 represents the logical topology maps.

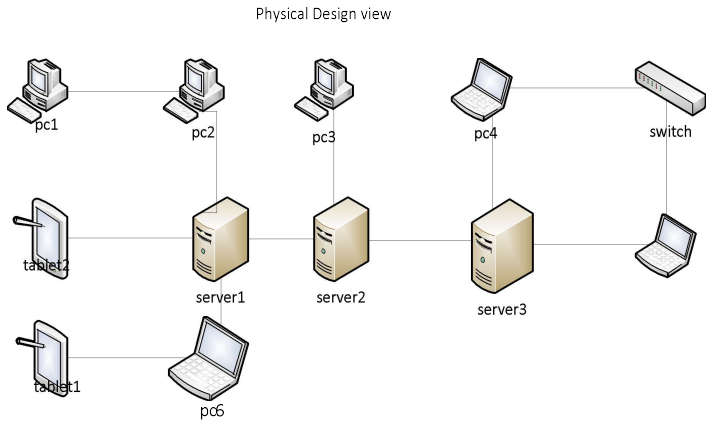


Fig. 1. *Physical Design View (CCNA Discovery4 2014).*

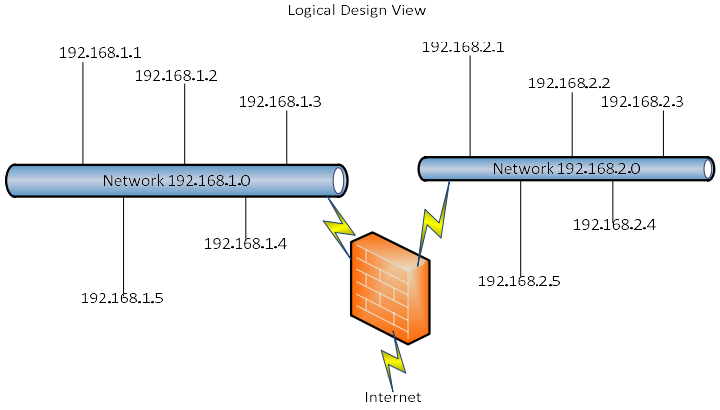


Fig. 2. *Logical Design View (CCNA Discovery4 2014).*

According to CCNA, the physical topology map is sometimes necessary to also have a logical view of the network topology. Logical topology groups host by how they use the network, no matter where they are physically placed or located. Host names, addresses, group information, and applications can be recorded on the logical topology map.

2.2 IP Surveillance Network Design

There is no particular format of network design but the guiding principle is to consider the topology and physical area of the design scope and how the devices will be interconnected within the area. When it comes to network design study of the physical and security setting must be put in place, also the economic consideration which is also important. To this point, many designs will be reviewed to give us the overall technology used by different designers[17].

In a different study,In 2019, Sholihah, *et al*., [21]havereplaced a CCTV with a VLAN access client they achieved this using client VPCS technology. They deployeda layer 2 switch, layer 3 switch, and Cisco routers for the Client vpcsas an access point on the Cameras. These Access points and Cameras wereconnectedto the layer 2 switch using VLAN system technology.The cables that were used for connecting the access points and cameras to layer 2 switches werefiber optic cables with 1 GB/s speed. The layer 2 switch was connected to the layer 3 switches in NIC.

In 2021, Budi,*et al.,*[4]have developedNDLC.According to the authors, it was very suitable for researchrelated to network design whichrequires stages of analysis, design, simulation, prototype, implementation, monitoring, and management as shownin Fig.3. The analysis wasthe basisfor research that wasuseful forreferencepoints in the design and research stage.The researcher analyzesthe existing structure or the system with the view of improvingthe existing networksystem. In the design phase which wasthe architecture based on the protocols where all the hardware (such as router, client device, and server) will be configured beforemoving.The configuration must also be documented so that when there isa problem or trouble in maintainers or device updates, no need to reconfigure it again, It was usually made on the addition of a device or if there was a change inthe device this still hada previous configuration were each device will communicate as if it were in the same network through, the below Fig.3 explain this in detail.

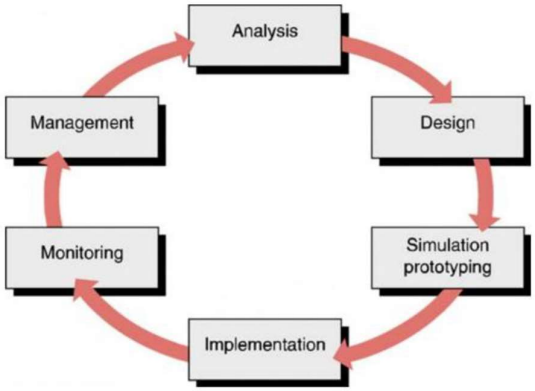


Fig. 3. *Network Development Life Cycle [4]*

The next phase wasthe simulation prototyping phase where particular application software wasused to carry out the testing of the connectivity to ensure the system wasworking as expected. The implementing stage will apply all the stages that have been planned and designed beforehand. Implementationwasa very decisive stage for the success or failure of the project building, and the teamwork will test both technical and non-technical requirements.

After the implementing stage, it continues to the monitoring stage. Thisstage wasessential so that computer and communication networks couldrun in accordance with the initial wishes and designgoals of the user from the analyzing stage.It wasimportant to carry out the monitored stage. The last stage wasthe management of the new system to ensure optimization of the system, up-to-date running, and performing the task it was designed for.

In 2020, [19]have used video surveillance design toprovide an OpenStack topology to their design whichwasintegrated between servers of computing, storage, and data center, the data source network deployed theAPI services and control through a Web-base dashboard interface. This process is demonstrated in Fig. 4.

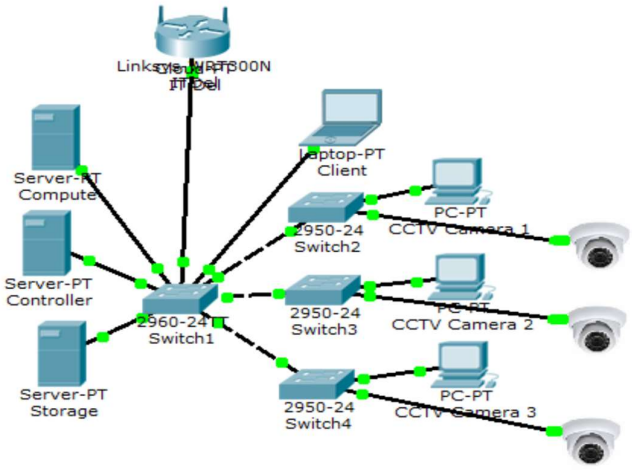


Fig. 4. *Video Surveillance Network Design(Pandapotan and Erick, 2020)*

2.3 Camera Systems with Internet Protocol (IP)

IP cameras are network cameras thatuse IP identification for communication. Unlike CCTV models, the IP enables video surveillance monitored through a web browser anywhere and anytime, whichisusually connected to the Internet or an existing network. IP cameras contain a CCTV camera, encoder within, and web server with itself so that it can be easily managed and communicate even if the IP cameras are dispersedly installed [13]. The IP cameras lack in terms of access authority and user certification for the IP camera to work in a web server or certification of IP cameras whichwas newly installed on the network [2]. IP camera transmits video based onthe IP network.It was open to its expandability and flexibility which is better than the CCTV systems. In addition, IP cameraweredesigned in a close way with the network technology not being exposed outwards. However, when one IP camerais installed at a distant place or a few cameras are installedforuse, vision, detection, and blocking systems, are usually generalized [11].

The existence of IP cameras contains overall weaknesses like the absence of a management system for accessing authority and plain text transmission of passwords. The access control system always suggests that the IP camera in this paper has some advantages compared to thenonIP camera system. First, it can control and monitor the system safely by grouping them in one position using a hierarchical grouping network technology key. Second, designinga protocol thatprovides mutual authentication between the IP camera and the systems is critical for surveillance[25].

2.4 IP AddressingSubnetting and Internet Protocol

An IP address is a series of 32 binary bits (ones and zeros) which is commonly a computer language. Using binary times is very difficult for humans to read a binary IP address and therefore is converting into real numbers for human understanding. For this reason, the 32 bits are grouped into four 8-bit bytes called octets. An IP address in this format is hard for humans to read, write, and remember. Therefore, when a camera host is configured with an IP address, it is enteredas a dotted decimal number such as 192.168.1.5. Imagine if you had to enter all the 32-bit binary equivalent of this 11000000101010000000000100000101. If just one bit is missing or mistyped, the address would be different and the host may not be able to communicate on the network.The IP address of 192.168.18.57 (group C) the first three octets, (192.168.18), identifiesthe network portion of the address, and the last octet, which is (57) identifies the host. This is known as a hierarchical address because the network portion indicates the network on which each unique host address is located. Routers only need to know how to reach each network, rather than knowing the location of each camera.

When a camera or host receivesan IP address, it will be looking at all 32 bits as they are receivedby the NIC. Humans on the other way, need to convert those 32 bits into their four octet decimal places or equivalent for understanding. Each octet is made up of 8 bits and each bit has a value. The four groups of 8 bits have the same set of values. The rightmost bit in an octet has a value of 1 and the values of the remaining bits from right to leftare 2, 4, 8, 16, 32, 64, and 128, where the value is all 1s this produce 255.

The author [24] revealed that Internet Protocol IPv4 is a 32-bit number, normally writtenas four 8-bit numbers expressed in decimal places and separated with periods. Examples of IP addresses are 10.0.17.1, 192.168.1.1, or 172.16.5.23. If oneenumeratesevery possible IP address, they would range from 0.0.0.0 to 255.255.255.255, which yields a total of more than four billion possible IP addresses (255 x 255

x 255 x 255 = 4,228,250,625).Many of these are reserved for special purposes and should therefore not be assigned to cameras or hosts. Each of the usable IP addresses is unique identifying differentiates one network node from another. Interconnecting networks must agree on an IP addressing plan. IP addresses must be unique and generally cannot be used in different places on the Internet at the same time.Otherwise, routers would not know how best to route packets to them. IP addresses are allocated by a central numbering authority that provides a consistent and coherent numbering method. This ensures that duplicate addresses are not used by different networks. The authority assigns large blocks of consecutive addresses to smaller authorities, who in turn assign smaller consecutive blocks within these ranges to other authorities or their customers. These groups of addresses are called sub-networks or subnets.

For short, large subnets can be further subdivided into smaller subnets. A group of related addresses is referred to as an address space.

TCP/IP is the protocol stack most commonly used on the global Internet. It refersto a whole family of related communications protocols. TCP/IP is also called the Internet protocol suite and it operates at layers three and four of the TCP/IP model[19]

IP addresses are grouped into 5 classes. Classes A, B, and C are commercial addresses and are assigned to hosts. Class D is reserved for multicast use and Class E is for experimental use. Class C addresses have three octets for the network portion and one for the hosts. The default subnet mask is 24 bits (255.255.255.0). Class C addresses are usually assigned to small networks. Class B addresses havetwo octets to represent the network portion and two for the hosts. The default subnet mask is 16 bits (255.255.0.0). These addresses are typically used for medium-sized networks. Class A addresses have only one octet to represent the network portion and three to represent the hosts. The default subnet mask is 8 bits (255.0.0.0). These addresses are typically assigned to large organizations [24]. The class of an address can be determined by the value of the first octet. For instance, if the first octet of an IP address has a value in the range 192-223, it is classified as a Class C address. As an example, 200.14.193.67 is a Class C address.

2.5 Network Surveillance and Crime Prevention

As [26] has argued there are three main types of crime prevention activity: primary, secondary, and tertiary. Primary crime prevention is focused on the offense rather than the offender and is often associated with situational crime prevention strategies thatfocus on the immediate and localized context of the offense. Secondary crime prevention is concernedwith offenders rather than offenses and seeksto intervenein the lives of those who are most at risk of offending. To prevent them from committing such crimes in the future. Tertiary crime prevention strategies focus on reducing or preventing the criminality of already known offenders, and this will typically involve forms of rehabilitation programs with convicting criminals. As a crime prevention strategy surveillance has generally found its theoretical justification insituational crime prevention and, as such, is neither concerned with the wider social structural causes of crime nor interventions aimed at fundamentally altering the individual. Indeed, as disillusion with both social welfare approaches and the efficacy of criminal justice measures in prevention have prevailed, the appeal of situational crime prevention has increased. The appeal comes not just from its supposed efficacy, but also in its de-politicization of the problem of crime. As Ron Clarke, one of the leading exponents of situational crime prevention has noted, it relies ‘not on improving society or its institutions, but simply on reducing opportunities for crime’ [7].

Situational crime theorists draw on rational choice theory to see crime as being committed by individuals who have weighed up the cost of benefits of crime. It is an evaluation by the potential offender of two questions: Will I going to succeed in carrying suchacrime? If I do succeed, will I get to be caught? Situational crime prevention strategies attempt to decrease the potential offenders’ belief that they are likely to be successful and increase their belief that they are likely to be caught. Situational strategies do not therefore try to change the basic motivation of the offender but instead try to increase the costs and risks associatedwith when such crime is committed [22]. However, all these crime isconsidered as the result of the better installation of a surveillance network.

2.6 Information Communication Technology and Security(ICTS)

ICTs have been gradually adopted to address security challenges in developed and developing countries. ICTs can assist security agencies in achieving more efficiency and effectiveness in their operations [1]. One of those areas in which ICT has played a significant role is the domain of surveillance. According to [1], surveillance is a deliberate system of keeping a close watch on behaviors or activities of persons, groups, institutions, and organizations suspected of doing something illegal or warehousing information capable of causing breaches by government security agencies. The ICT usually used for surveillance is

CCTV. The surveillance network is a video camera that plays a significant role in the detection and prevention of crime or security-related vices in any society that isdeveloped or developing. The surveillance system comprises of fixed or PTZ camera that could be mounted on a wall, a street Light Pole, a fence, or the roof of a building, a monitoring centerthat comprises of wall mounted monitors and desktop monitors, a recording facility, data processing area and communication area and also available response teams to act on the available information received via the cameras and communicated via the communication to prevent, deter or apprehend offenders. The motive of installing surveillance network cameras by the government (at whatever level), organizations,or private individuals is to reduce crime and increase public safety.

2.7 Surveillance Network in Developing Nations

In recent times, the crime rate in Nigeria has risen to the level in which public outcries are urging the government for urgent and concrete solutions. The government has adopted various security policies to secure the lives and properties of its citizens but none of these policies have yielded positive results. Human abduction, armed robbery, terrorism, bomb attacks, and lots more have been the order of the day in the Country [18]. Many surveillance network systems are deployedto deter crime and terrorism in the country but little has been achieved to stop these crimes. This is because the deployment of surveillance network systems is not fully digitalized to support all the public areas in the country as such many crimes are taking place without the surveillance network cameras capturing them. However, most of the sensitive governmentagencieslike banks, federal ministries, and some cities now use the systems and this hasdeterred some potential offendersfrom becomingaware of the presence of surveillance networks in which they assess the risks of offending in this location to outweigh the benefits and chooses either not to offend or to offend elsewhere.

There is limited focus on the evaluation of Surveillances projects in developing countries [12]. Hence, there is a call for more theory-driven approaches to the evaluation of surveillance network system projects in developing countries [9]. Thereforethe study has shown that most developing countries like Nigeria are yet to enjoy the full benefit of Information Technology and this is so because of the slow nature of the deployment of ICT. In this study, we want to design a surveillance network system that will provide security to the citizens of countries like Nigeria. According to Zheng,ICTs are seen either as an industry or a motor for industrialization, with much attention focused on how ICTs can enhance productivity and competitiveness [27]. Here Zheng associates ICT with the economic development of any nation that is coming like Nigeria.

3. Methodology

There are no fixed rules or “one size fits all” solutions when it comes to network design. However, when faced with complex network design, understanding the key design considerations hashelped in identifying the most important components thatareneeded to tackle the complexity of the network and design a solution that meetsthose key design considerations [17].This study describes the procedure and methods that wereused to achieve the set objectives. The highlight technologies and specific tools needed to achieve the goal of designinga surveillance network system.

The study is an action research design, where a new system or technology is introduced to solve an existing problem, action research design focuses on finding a solution, making it more practical for the system user to appreciate the real-time problem. ANDLC [4]is suitable for this type of related research.Itis a network design methodology thatdeployed a series of stages for network design, from system analysis, System Design, system prototyping, and then the implementation phases.

The surveillance system is a technology that cuts through these problems associated with manual security surveillance systems. The design objective is to design a logical and physical view of a network surveillance system thatcan record, recognize, and baggage imagery.Itcanmonitora person's movement at checkpoints and prevent security threatswithin the surveillance area.

The tools to bedeployed to achieve the said goal are Microsoft Visio and Smart Draw for Network Architectural Design are used in the logical design view. A Packet Tracer is also used in the physical design view of the study and to detail the simulation of the network.

3.1 Network Requirements

Network requirements should be communicated and well-defined before a network design starts, though in some cases a network designer needs to clarify additional details along the network design process. The basic objective is to design an IP Surveillance network thatconnects all the IP cameras with a server in the security Administration center. The IP cameras are installed within an interval of 50 meters from

each other, starting from the gateway of the area to the public space. Each camera has its clear standing video zone that has to cover, capture, and record a particular space based on the topological nature of the area. Other requirements are:

The IP cameras can receive power through the same data cable in the Network, PoE.The IP Vision 4 classes C (192.168.1.0) is adopted. This is to enable for manageable subnet and host to meet up with the future growth.

4. Results and Discussion

4.1 Network IP Addressing Structure and Subnet

The IP address is the backbone of any well-designed network.It is important because a host needs an IP address to participate in the sensor surveillance network. The IP address is a logical network address that identifiesa particular host or camera. It must be properly configured and unique to communicate with other devices on the network. The IP allows for the logical breakdown of the network into smaller forms for easy management and good design practice, because of these benefits the researcher, therefore subnets the network into many smaller units.

A subnet is a way of making a single IP network address that is logically andlocallysplit into several small units ofnetworks that can be managed in a local network. Remember, a single IP network number can only be used on a single network. The subnet enables the designerto manage huge amounts of video stream traffic and if not properly subneted the network would certainly collapse due to traffic load in a single network.The designer used a class C network address (192.168.1.0) the study worked through some steps to subnet this Class C network.

The study revealed that the historical growth trends of host and sub-network arereal for any organization.It is determined that an organization needs at most 20 hosts (H) on any subnets(S). In the future, the subnet size is expected to pass 25 hosts after integrating the network with other networks. Hence, set H at 32.

With this Class C network address, there are 27 total bits to work with. Only borrow up to 3 of these and determine the number of bits to borrow (bb) from the host ID such that

$$2^{bb} - 2 \geq S \quad (1)$$

The inequality can berewrittenas:

$$2^{bb} \geq S + 2 \quad (2)$$

Since S = 4,this becomes:

$$2^{bb} \geq 2 + 2 = 2^{bb} \geq bb \quad (3)$$

Using the formula $2^{bb} - 2$ = Number of usable S can easily be seenthat the researcher needs to borrow bb bits.The number of bits in the host ID portion (NBHP) of the address is:

NBHP (27 bits) = 11111111.11111111.11111111.**111**00000

But 5hostbits are needed (hb) to meet up with the required 32 hosts per S, such that:

Which is less than NBHP= 27, certainly the study hasbits left (bl).

255.255.255.0 = 11111111.11111111.11111111.00000000

To ensure 5 of the host bits (0) *remain* host bits to satisfy the requirements. All the other bits can become network bits.

New Mask = 11111111.11111111.11111111.**111**00000

Note the 5 host bits that are saved. In decimal format, after studying the 128, 64, and 32 bits in the last octet for a value of 224.

128+64+32 = 224

If the mask is back to decimal, the subnet mask that would be used on all the new networks, so the new subnets mask – 255.255.255.**224**

Hence the custom subnet mask for this network is

255.255.255.**224**

192.168.1.0 (First valid subnet ID)

After adding 32 to 192.168.1.0 until either reaches the value of the custom subnet mask (255.255.255.**224**) or until network addresses for $2^{bb} - 2$ subnets (these two conditions are equivalent and so would occur at the same time).

Ina Class C network, there are 24 bits in the network portion of the address and eight bits in the host portion of the address which differentiates it from other network address classes. Each bit in a binary IP address has only one of two possible values, a zero or a one. The number of host addresses is calculated using the powers of two. Therefore, the number of host addresses available for an eight-bit address is 2^8 or 2x2x2x2x2x2x2x2. With an 8-bit host ID, there is one network with 254 possible host addresses.

In this case, a Class C network is subnetted and 3 bits are borrowedfrom the host ID to use for the subnet ID, there are 5 bits left for host addresses. Five host bits mean that there can be 30 hosts per subnet or 2^5 - 2. Remember that the all-zeros and all-one host addresses are reserved for the network designation and the broadcast address. The number of subnetting is calculated similarly. If three bits are borrowed for the subnet address, the number of subnets is 2x2x2 or 2^3. So, by subnetting in this manner, there are eight subnets with 30 hosts each.

4.2 Subnet and IP Address of Surveillance Network

Each subnet has a network address to which the host is attached. The range of each host is 29. The subnet also has a broadcast address to connect each subnet. Table 1 represents the Surveillance Network Internet Protocol (IP).

Table 1: *Surveillance Network Internet Protocol (IP)*

Subnet	Network Address	Host range	Broadcast Address
1.Network1	192.168.1.0/27	192.168.1.1-192.168.1.30	192.168.1.31
2. Network2	192.168.1.32/27	192.168.1.33-192.168.1.62	192.168.1.63
3. Network3	192.168.1.64/27	192.168.1.65-192.168.1.94	192.168.1.95
4. Network4	192.168.1.96/27	192.168.1.97-192.168.1.126	192.168.1.127
5. Network5	192.168.1.128/27	192.168.1.129 - 192.168.1.158	192.168.1.159
6. Network6	192.168.1.160/27	192.168.1.161 - 192.168.1.190	192.168.1.191
7. Network7	192.168.1.192/27	192.168.1.193 - 192.168.1.222	192.168.1.223
8. Network8	192.168.1.224/27	192.168.1.225 - 192.168.1.254	192.168.1.255

The network address is the first address that identifies a network, which cannot be used by the host. In the above table, the network address for the security room is 192.168.1.0. The host rangeisthe useable addresses that are within the range of the network. The host address are usable address for the cameras and other devices, the host range for the security center is from 192.168.1.1 to 192.168.1.30. While the Broadcast Address is the last address of the network. The Broadcast Address allows all hosts on the network to receive a message when it is used.The Broadcast Address of Gate-security unit is 192.168.1.31.

To determine the valid IP addresses for each subnet, the designer begins with the network ID for the subnet. Which eventually starts with the first subnet whose address is 192.168.1.1to find the first IP address on the subnet, one needs to increase or add 1 to the rightmost octet of the subnet address: Thus the first valid IP address on subnet 1 is 192.168.1.1.

This continues incremented until the value reaches 255, or until the next increment reaches two less than the next subnet addresses, or until generated $2^{hb} - 2$ IP addresses (these last two conditions are equivalent and always occur at the same time). It is expected to have $2^3 = 8$, subnet and $32 - 2 = 30$ IP addresses per subnet.

4.3 Surveillance Area Designed Scope

The above view provides the overall area to be covered under the surveillance network. The designer groups the above geographical area into clusters or small networks (subnet) to allow for the management of the enter surveillance system. From thisview, the designer divides the area into seven logical networks.All thesenetworks cover the roads attached to the network. Network 1 (192.168.1.0/27),Network 2 (192.168.1.32/27), Network 3 (192.168.1.64/27), Network 4 (192.168.1.96/27), Network 5 (192.168.1.128/27), Network 6 (192.168.1.160/27) and Network 7 (192.168.1.192/27). The last network which is network 8 (192.168.1.224/27) is for future expansion. Hence, below is Fig. 5 shows the logical mapping or view.

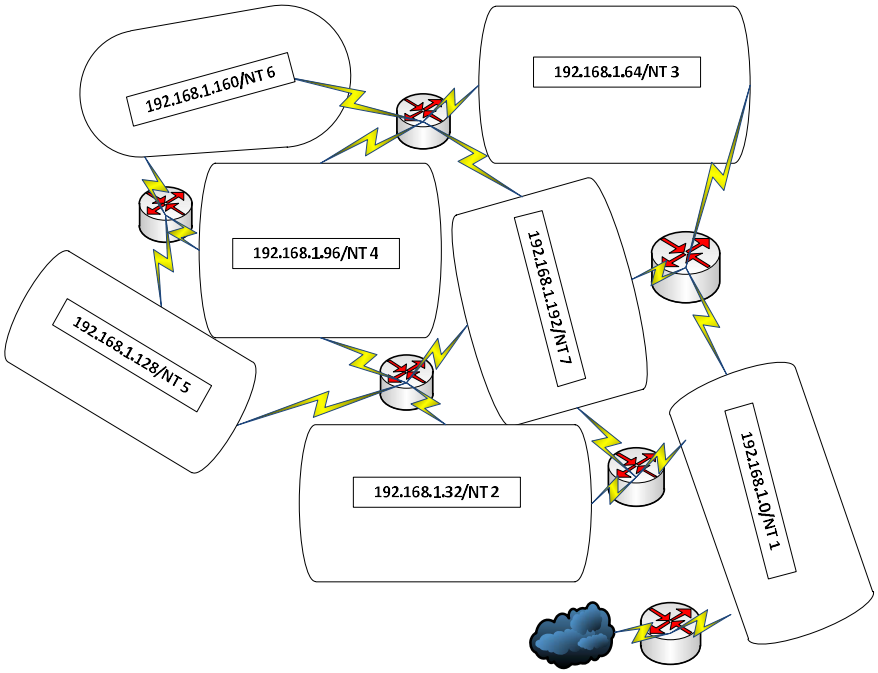


Fig. 5. *Logical Design View of Surveillance Network*

4.4 Routing Information Protocol (RIP2) of the Network

From the above logical designs, there are seven different networks connecting with five routers. Each network hasmore than one gateway and this is too quickly made for recovering from breakdown links or hardware failures. In case thedestination is unreachable through the designated interface the routers need to quickly recover and update routes that arereachable through the routing table generated. Therefore, whenever the topology of a network changes because of reconfiguration or failure, the routing tables in all the routers must also change to reflect an accurate view of the new topology and forward data through another chargeable path to reach the needed destination. The above five routers communicatetheirrouting information to theirneighbors that share a direct connection and all this happensevery 30 seconds. However, this is not so with other network designs that provide for fast recovering time to initiate a different path even if the original path has fallen. One advantage oflogical mapping is tobring the path in which a single router can reach a device through many other paths especially in times of failing link, just as it is described above in Fig. 5. Secondly, another advantage of the above logical view is that it shows different networks by network how each network is connected to the other network and what is the type of connectorand to which of the ports the device is attached to within the network.

These benefit associated with logical mapping can never be over-emphasized, because the logical view as shown above give the designer well skeleton in which a real network with full flesh is designed open. Without this view, the network engineer or administrator works blindly especially when it comes to maintenance and upgrading the entire network system. In fact, from the above view in Fig.5, it is clear that these routerscommunicate and understand the position of each machine within the network including the distance metric and how much time will it take to reach a particular router.

Eventually, each router learns to know about others more remote within the networks based on the information that it receives from its neighbors. Each of the network addresses configured in the routing table has an accumulated distance vector to show how far away that network is in a given direction.The RIP2 distance vector routing algorithm usually passes periodic copies of a routing table data from router to router which makes it easy to remember and understand the actual positioning of the device. These regular updates between routers communicate topology changes. In case a router is removed or added to the network the system regenerates its router table and then broadcasts its table to the next router connected to it and this keeps on going until the last router understands the changes made within the network. The router considers cost, number of hops, and reliability to the next network before sending data or video frame.

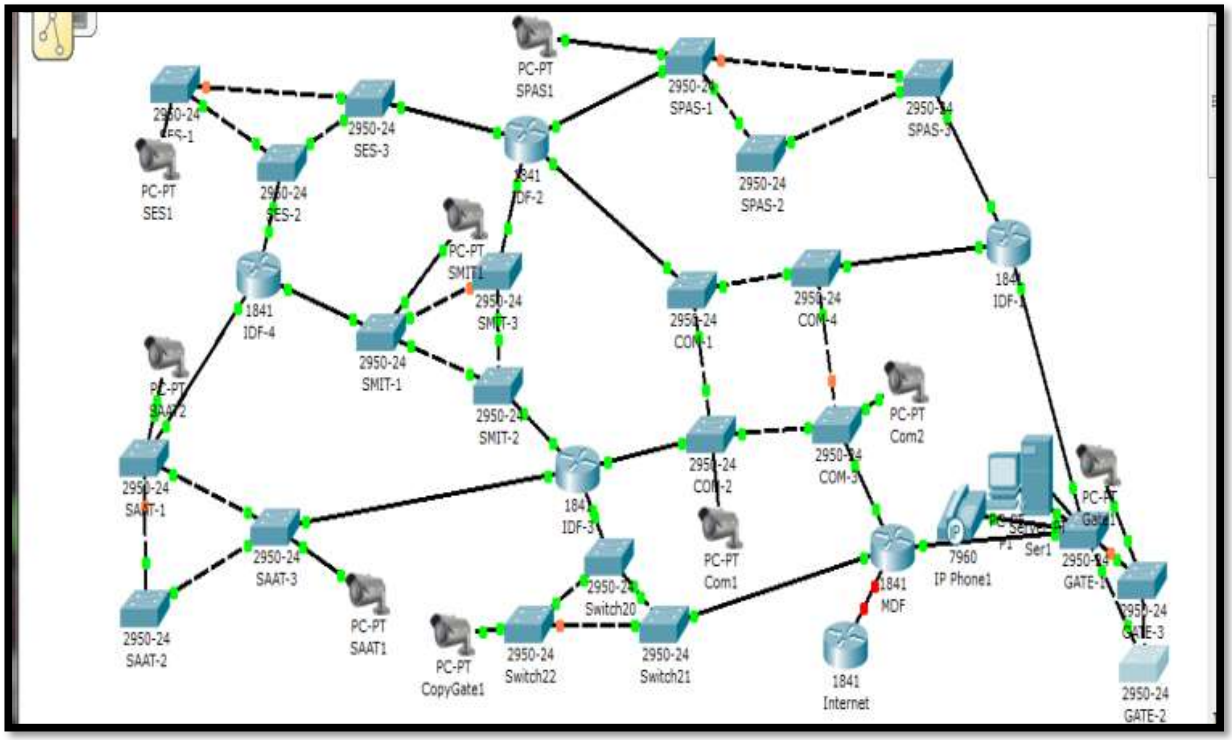


Fig. 6. *Physical Design View Using Packet Tracer Simulator*

4.5 Routing Configuration

The simulated network is sub-divided or segmented into seven different networks deploying five routers that provide eachconnection through these networks. Each sub-network has more than one gateway through which information can move freely in case one link is down. All five routers are configuredwith Router Information Protocol Version 2 (RIP2). This is to ensure the reliability and flow of videos.

TheMDF which is the engine room of the surveillance network is connected to three routers. This first router is connected to the internet and this serves as the gateway of the entire network to the world. The MDF is the viewing center where image and video frames are analyzed and stored for reviewing if the need arises. What makes this design standout is the deployment of STP, a technology that increases network reliability which is not common to other network design.

The entire network is configured with anSTP for moreredundancy.This isintended to increase the network and device performance. The STP redundancy is required in the network to provide and maintain a high degree of reliability byeliminatingany single point of failure. STP in this network (Fig. 6) provides a mechanism for disabling redundant links in a switched network [3]. The protocol is deployed in the above network to provide redundancy and reliability without creating switching looping. Upon initialization of a device, each port generates a BPDUwith the following, the port as the designated port, the device as the root bridge, and 0 as the root path.If a port does not receive any configuration BPDUs within the timeout period as required, the switch port transits to the listening state. From there the device will recalculate the spanning tree [20]. The STP takes the port 50 seconds to transit back to the forwarding state. To ensure a fast topology convergence is ensuredand a different path is taken for communication.

4.6 Network Address Translation (NAT)

NAT is configured on anMDF to enable cameras and devices with internal private addresses (192.168.1.0) to communicate on the Internet. NAT isusually configured at one interface to allow the network to communicate with the internet. To access the Internet, NAT must be configured as the outside and inside interface. When devices on these internal networks communicate through the external interface, the addresses can be translated to 10.168.1.5 or more registered IP addresses to access the internet.

5. Advantages and Disadvantages

Advantages

- The designer network is subdivided into sub-management units (from networks 1-8) which provide flexibility, scalability, and cost-effective solution for LAN.
- Subnetting helps to reduce network traffic, simplify management, optimize network performance, and facilitate the spanning of large geographical distances.
- Power cables are connected along with the data cables of the cameras for easy access.
- Subnetting can manage large amounts of video streaming traffic and it is reliable.
- Each subnet has one or two gateways.
- The potential benefit associated with surveillance network systems is their ability to prevent crime activities, whether through the identification of suspicious persons or packages that are preventing the act from taking place or through the identification, apprehension, and conviction of suspects after the act.

Disadvantages

- Initial investment is required for the cost of installation and maintenance.
- Common issues include power outages, faulty connections, lens distortion, blurry images, and distorted colors will happen in Cameras. Reliability issues may also arise due to improper installation or temperature fluctuations.

6. Conclusion and Recommendations

The study aims to design a physical and logical design view of an IP surveillance network of cameras and subnet the network into manageable units. Asimulatednetwork using a packet tracer test proved the capability of better network response timeand effective video network usage for monitoring people in public spacesfor public safety. This method critically analyzes the requirements and technical approach ofthis study. A well-designed video surveillance system would help in counter-terrorism by providing first-hand information and intelligence gathering to enable security agencies to preventpotential incidents. There is no doubt that video surveillance is a powerful crime management tool thatproduces huge amounts of visual intelligence data that can lead to successful prosecutions of crime.Surveillance networks or computer networks will be a destination of the most important infrastructure for the 21st-century global information and technology society. IP Surveillance network has come to stay as it bringsa lot of advantages. However, this study is conducted onasmall area of the IP surveillance network design and the application that the network system deploy for video streaming which have to be developed in future study.

Therefore, full system deployment and implementation of afew important factors have been recommended as pillars to securing the framework such as operational requirements, decision guidelines, performance standards, evidence base requirements, and importance of surveillance network operators. Also, encouragefurther research on setting up an IP Surveillance Network security master plan that covers the nation.

Compliance with Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

[1] C. F. Agbala, "Security Challenger: *What can ICT do*?", Retrieved December 20 2021 from http://www.punchng.com/business/ictclinic/security-challenges-what-can-ict-do, 2018.

[2] S. A. Ahmad and K. Khalid, "The adoption of M-government services from the user's perspectives: Empirical evidence from the United Arab Emirates", International Journal of Information Management, 2017.

[3] A. Biswas, S. R. Mondal and C. Biswas, "A Review On Loops In A Computer Network & Spanning Tree Protocol (STP)",*Int. Res. J. Mod. Eng. Technol. Sci*, Vol. 4, no. 2, pp. 612-615, 2022.

[4] B. Santoso, A. Sani, T. Husain and N. Hendri. "VPN site to site Implementation using Protocol L2TP and IPSEC", TEKNOKOM, Vol. 4, no. 30-36, 2021.

[5] C. W. Brandon and F. David, "Making public place safer: surveillance and crime prevention", Oxford University Press, 2009.
[6] Cisco Certify Networking Academy http://www.academynetspace.com/ http://CISCO_CCNA\Discovery1_English\index.html, 2019.
[7] R. V. Clarke, "Situational crime prevention. *Strategic Approaches to Crime Prevention", Vol. 19. Crime and Justice: A Review of Research*, Chicago, Illinois: University of Chicago Press, pp. 91-150, 1995.
[8] B. J. Goold, "Surveillance *network and Policing: Public Area Surveillance and PolicePractices in Britain",* New York: Oxford University Press, 2004.
[9] R. Heeks, "Do Information and Communication Technologies (ICTs) Contribute to Development?"', Journal of International Development, Vol. 22, pp. 625-640, 2010.
[10] D. Ortner, "The Terrorist's Veto: Why the First Amendment Must Protect Provocative Portrayals of the Prophet Muhammad", Nw. JL & Soc. Pol'y, Vol. 12, pp. 1, 2016.
[11] J. Kang, J. K.Han and J. H. Park, "Design of IP Camera Access Control Protocol by Utilizing Hierarchical Group Key", 2020.
[12] S. Kamel and M. El-Tawil,"The Impact of ICT investments on Economic Development",Electronic Journal of Information Systems in Developing Countries, Vol. 36, pp. 1, 1-21, 2009.
[13] K. Prasetya, A. Aribowo, A. Satyaputra and J. O. Tjahyadi. "Implementation of Tensorflow in the CCTV-Based People Counter Application at PT Matahari Department Store", Tbk, 2020.
[14] Mengdi Ji, "Designing and planning a campus wireless local area network", 2017.
[15] M. Michael and N. Clive, "Close Circuit Television in London centre for criminology and criminal justice University of Hull Cottingham", Journal of centre for technology and society. Vol. 5, pp. 1-10, 2004.
[16] Moxa.,"CCTV surveillance system Network Design Guide", Retrieved April 2015.
[17] N. Omoregbe, S. Misra, R. Maskeliunas, R. Damasevicius, A. Falade, A. Adewumi, Retrieved October 28 2021, 2019.
[18] P. Ogedebe, S. I. Dasuki and J. Makinde, "Assessing the impact of Closed Circuit Television (CCTV) camera on crime control in developing countries: A Nigeria perspective", African Journal of Computing & ICT, Vol. 7, no. 4, pp. 23-34, 2014.
[19] P. Siagian and E. Fernando, "The Design and Implementation of a DashboardWeb-Based Video Surveillance in OpenStack Swift", International Conference on Computer Science and Computational Intelligence, Retrieved October 02, 2022, from procedia computer science press.
[20] P. A. Rahman, "An algorithm for selection of the preferable root switch for the spanning-tree protocol in computer networks", In Journal of Physics: Conference Series, Vol. 1661, no. 1, pp. 012010, IOP Publishing, 2020.
[21] W. Sholihah, T. Rizaldi and I. Novianty, "Information and communication system technology with VPN site-to-site Ipsec", In Journal of Physics: Conference Series, Vol. 1193, no. 1, p. 012012, IOP Publishing, 2019.
[22] S. Livingston, "Africa's Information Revolution: Implications for Crime, Policing and Citizen Security", Africa Center for Strategic Studies Research Paper No. 5 Washington, D.C, 2013.
[23] A. K. Turnage, "Surveillance and Security: Technological Politics and Power in Everyday Life" by Monahan, T. Illusions of Seurity: Global Surveillance and Democracy in the Post-9/11 World by Webb, M: Book Review: Public Surveillance and the Illusion of Security, 2007.
[24] T. Lammle, "CCNA Cisco certified network associate study guide", Sybex, 2000.
[25] A. Tongkaw, "Multi-Perspective and Low-Cost Coverage Network Design for Implementing in Campus Network: A Case Study", In IOP Conference Series: Materials Science and Engineering, Vol. 551, no. 1, pp. 012031, 2019.
[26] R. Weiss, "The Community and Crime Prevention",Handbook on Crime and Delinquency Prevention, New York: Greenwood Press, 1987.
[27] Y. Zheng, "Different spaces for e-development: What can we learn from the capability approach?", Information technology for development, Vol. 15, no. 2, pp. 66-82, 2009.