Abdulwahid Moalin

Building a small network for a startup

Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Bachelor’s Thesis

30 April 2025

Abstract

Author:	Abdulwahid Moalin
Title:	Building a small network for a startup
Number of Pages:	24 pages + 7 appendices
Date:	30 April 2025
Degree:	Bachelor of Engineering
Degree Programme:	Information Technology
Professional Major:	IoT and Networks
Supervisors:	Aarne Klemetti, Researching Lecturer

This thesis designs a cost-effective and functioning network for a startup. Project aims to determine the most practical way to build a network while keeping in mind the company's network needs. Network infrastructure of startups' country of operation is taken into consideration and there were alternative implementation methods given for this reason.

The project examines two different network approaches: Cisco professional-grade network and SOHO network. Although, Cisco's professional-grade network offers more advanced network features, SOHO approach was chosen as the more practical option for the startup due to its lower cost and easier implementation.

In both approaches, the company's needs were considered, and suitable network components were selected to design a network that meets those needs. The comparison between the two approaches included cost, ease of implementation, required technical skills, and scalability. This decision is also due to consideration that a professional-grade network require professionals to implement and manage it day-to-day and this would not be ideal for a startup.

The decision was also influenced by the fact that the company would not significantly benefit from a professional-grade network if it were to adopt cloud services such as Microsoft 365 Business packages. This project can be used as a reference for other small companies to build an affordable and functioning network.

Keywords: SOHO

Tiivistelmä

Tekijä:	Abdulwahid Moalin
Otsikko:	Verkon rakentaminen pienelle startup-yritykselle
Sivumäärä:	24 sivua + 7 liitettä
Aika:	30.4.2025
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	IoT ja tietoverkot
Ohjaajat:	Tutkijaopettaja Aarne Klemetti

Opinnäytetyö suunnittelee kustannustehokkaan ja toimivan verkon startupille. Projektin tavoitteena on selvittää, mikä on käytännöllisin verkkoratkaisu startup-yrityksen toiminnan aloittamiseksi ja mikä vastaa yrityksen verkkoon liittyviä tavoitteita. Projektissa otettiin myös huomioon yrityksen kohdemaan verkkoinfrastruktuuri, ja tämän vuoksi esitettiin vaihtoehtoisia toteutustapoja verkon pystyttämiseksi.

Projektissa tarkasteltiin kahta eri lähestymistapaa verkon toteuttamiseksi: Ciscon ammattilaiskäyttöön tarkoitettua verkkoa sekä SOHO-verkkoa. Vaikka Ciscon verkko olisi tarjonnut parempia ominaisuuksia, projektissa tultiin siihen lopputulokseen, että SOHO-verkko olisi parempi vaihtoehto yritykselle tässä vaiheessa, sen alhaisemman hinnan ja helpomman käyttöönoton vuoksi.

Molemmissa lähestymistavoissa otettiin huomioon yrityksen tarpeet ja valittiin sopivimmat saatavilla olevat verkkolaitteet. Tähän tulokseen vaikutti se, että Ciscon verkkosuunnitelma vaatisi pysyviä työntekijöitä verkon rakentamiseen ja ylläpitoon. Tämä nostaisi yrityksen kuluja eikä olisi ideaali ratkaisu startupille.

Päätökseen vaikutti myös se, ettei yritys hyötyisi merkittävästi ammattilaiskäyttöön tarkoitetusta verkosta, jos se ottaisi käyttöön pilvipalveluita, kuten Microsoft 365 -businesspaketteja. Tämä opinnäytetyö toimii myös mallina muille pienyrityksille, jotka etsivät edullista ja toimivaa verkkoratkaisua.

Avainsanat: SOHO

Table Of Contents

Appendices

Appendix 1: Configurations

List of Abbreviations

LAN:	Local Area Network
WAN:	Wide Area network
IP:	Internet Protocol
VoIP:	Voice over Internet Protocol
RIP:	Routing Information Protocol
OSPF:	Open Shortest Path First
BGP:	Border Gateway Protocol (BGP).
LTE:	Long Term Evolution
QoS:	Quality of Service
NAT:	Network Address Translation
SOHO:	Small Office Home Office
SIP	Session Initiation Protocol

1 Introduction

In today's world, internet connectivity is an essential part of business operations. A secure, reliable and efficient network infrastructure is critical for a company's success and smooth functioning. This thesis focuses on a small-sized green energy business startup. Its aim is to plan a network, select appropriate components, and implement widely used techniques while ensuring the network's reliability and scalability for future expansions.

The startup is in Somalia, where electricity prices are extremely high, making affordable solar systems a vital alternative for local households. It is of utmost importance to establish a network that meets current operational needs while accommodating future expansions.

This thesis designs a network that considers branches, including various departments such as management, accounting, sales, and technicians. The project also accounts for other office equipment, such as printers and IP phones. The thesis does not focus on the servers that the company might need but rather focuses on the network infrastructure and connectivity between offices.

The goal of this project is for the network infrastructure designed in this thesis to serve as a complete guide for implementation, allowing any small-sized company to use it as a blueprint for a network. The objective is to provide a solution that addresses the company’s current needs while also preparing for future growth.

The study aims to determine the most practical network design for a startup to begin operations, while ensuring affordability and meeting the company’s network-related goals.

2 Theory

This chapter explains essential theory parts to build network. It goes over different computer networks and explains what different network components do, as well as topics such as IP addressing and VPNs.

2.1 Different types of computer networks

This section explains terms used to classify computer networks based on their geographic scope such as Local Area Networks (LANs) and Wide Area Networks (WANs). Understanding these two networks is of utmost importance when designing and implementing networks.

2.1.1 LAN

A Local Area Network (LAN) is a group of different devices, such as computers and other devices, connected together either physically or wirelessly in a single location, whether it’s an office building or a home. There are many benefits of Local Area Networks. For example, LANs enable resource sharing, from emails to printers and files. LANs cover small geographicarea while also offering high speeds for data transfers. [1]

To give a better picture of a Local Area Network (see Figure 1), a small company’s setup is comprised of a router, switch, firewall, wireless access points, IP phones, and PCs. Each of these components has a specific purpose, which will be explained further in this project. Additionally, all these components will be utilized in this project.

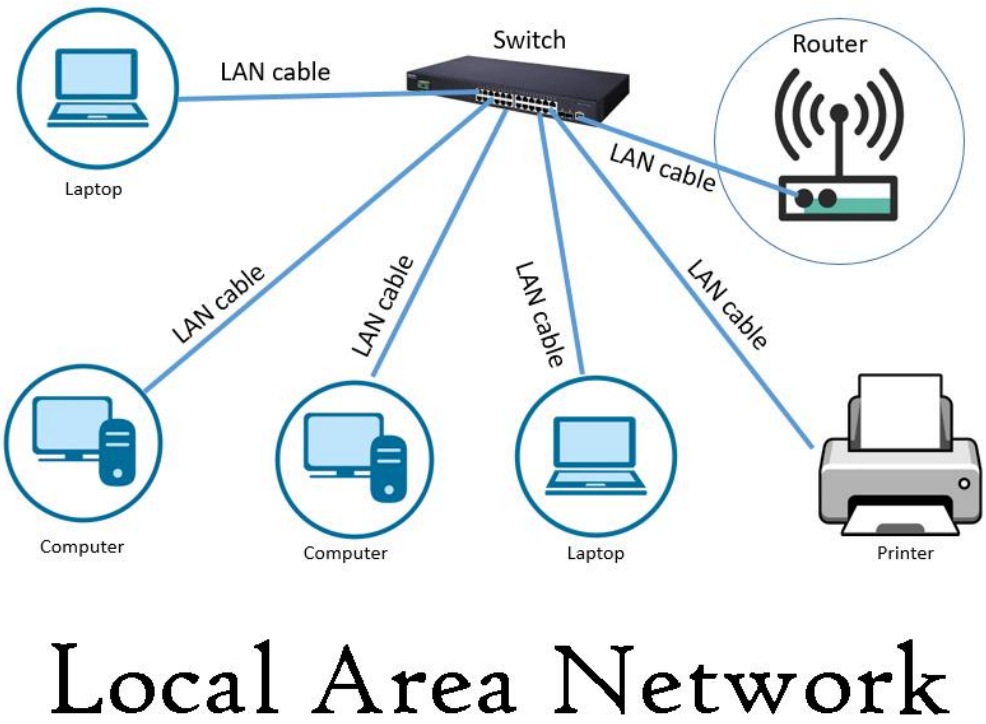

Figure 1. Illustration of LAN [25]

2.1.2 WAN

A Wide Area Network (WAN) is essentially one or more LANs connected. WANs covers large geographic area and are not restricted in one location. WANs enable access for users who are in different locations to share and access applications and files as if they were in the same location. This is widely used when connecting main office to branches. [2] See Figure 2 below.

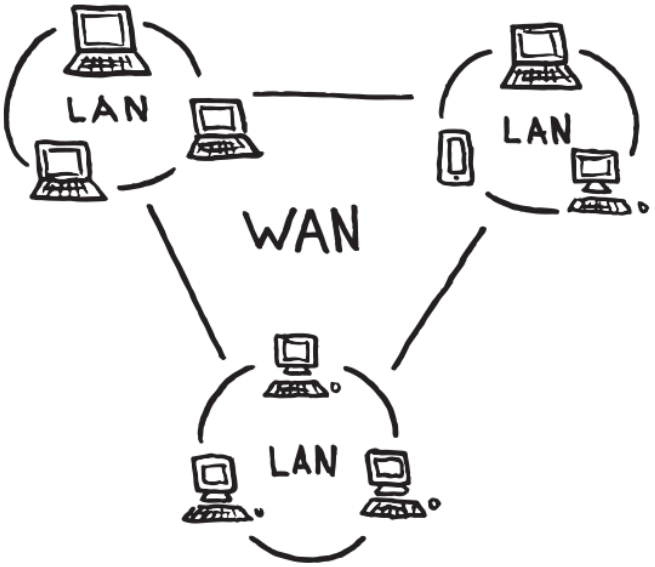

Figure 2. Illustration of WAN [2]

2.2 Component

This section presents components used in this project and explains the function of each component. The specific models chosen for implementation are not revealed in this part but on further chapters.

2.2.1 Router

A router is necessary device in the network for connecting to the worldwide internet. Routers also enable communication between two or more separate LANs. Routers operate in layer 3 in the OSI model, and they are responsible for forwarding packets based upon IP addresses. Routers pass packets between networks by checking IP address and calculating best way to reach the destination. [3, 4]

Routing is managed by several different protocols including RIP, OSPF and BGP. Each of these protocols have their own unique strengths. These are different protocols that enable to manage network traffic while also ensuring data reaches its destination quickly and reliably. For this projects those mention protocols are

not used since the network is small and the router doesn’t need to communicate with other routers in the network. Mainly BGP is used by the ISP as routing protocol. [3]

There are different types of routers, each of them is designed for a different purpose in a network environment. For example, edge routers are placed at the edge of a network. It works as a bridge between the internal network and outside internet. They are responsible for managing network traffic that enters and leaves the network while also providing security and addressing. [4]

Another type of router is the SOHO router. SOHO combines edge router and wireless access point functionalities into one device. These are commonly used in homes and small offices, and it provides both wired and wireless connections to a network. Other types of routers include Core Routers, which are primarily used by ISPs for handling large amounts of data traffic, and Distribution Routers, which receive data from edge routers and distribute it within larger networks.[4]

2.2.2 Switch

A switch is a network device that connects multiple devices within the same LAN. By directing data packets to their intended targets using MAC addresses, switches ensure efficient and accurate communication between devices. Switches enable resource sharing within the LAN. [6]

When a switch receives a data frame from a connected device, it checks the destination MAC address in the frame and forwards it to the corresponding port. If the switch does not know the location of the destination device, it automatically broadcasts the frame to all ports except the one it received it from. Once the destination device replies, the switch updates its MAC address table by recording the MAC address and the port it is connected to, and this allows it to forward future frames directly to that correct port. In a small office, a switch connects all devices, such as computers, IP phones, and printers, together. See Figure 3.

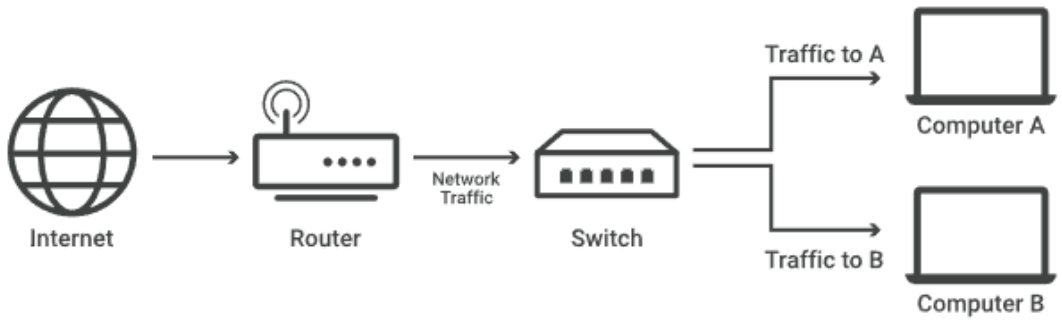

Figure 3. Illustration of switch operating [6]

There are two types of switches: unmanaged and managed. Unmanaged switches are designed to be plugged into the network, and they don't require any configuration. They typically lack advanced features such as QoS and enhanced security capabilities. Unmanaged switches can be used for homes and small businesses where advanced features are not necessary, and devices are minimal. Both types of switches are used in this project. [5]

Traditional switches operate in layer 2 of OSI-model. There are layer 3 switches that are capable of routing IP packets and are capable doing such tasks as inter-VLAN routing. Layer 3 are also known as multilayer switches, because they operate in both layer 2 and layer 3 of OSI-model.

2.2.3 Firewall

A firewall is an essential part of network security. It serves as a barrier that separates an outside network, which is deemed unsafe, from an internal network, which is trusted. This is achieved by using preset security rules to control incoming and outgoing traffic, determining what passes through and what is blocked. [8, 9] See Figure 4 below.

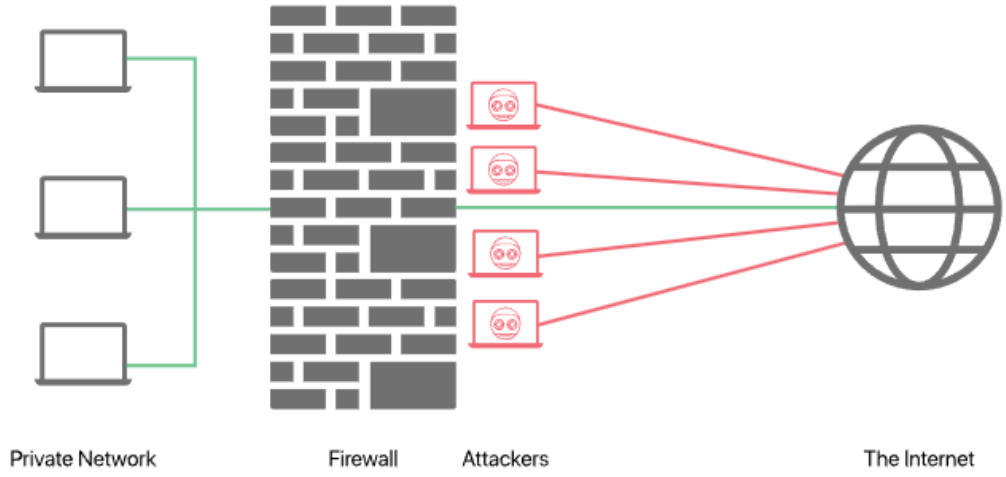

Figure 4. Firewall protecting a network from attackers [8]

Firewall can be physical hardware or software based. Firewall hardware usually is designed to protect the entire network while software firewall is designed to protect individual devices from cyber threats such as unauthorized access and malware attacks. This project uses routers firewall capabilities instead of physical firewall. [8, 9]

2.2.4 Wireless access points

Wireless access points are devices that enable wireless using devices to connect to wired networks. They are used for creating wireless networks where there is already existing wired network infrastructure. [7]

2.2.5 IP phone

An Internet Protocol phone (IP phone) is a phone that uses Voice over Internet protocol (VoIP) to make and receive calls rather than traditional phone lines. An IP phone converts analog audio signals into small digital data packets, which then are sent over the internet using different kind of protocols such as SIP. After that the receiving end will convert digital packet into audio. [10, 11]

There are many advantages in IP phones. They are easily scalable as businesses grow while also ensuring that calls can be made anywhere with internet connection Additionally, they are more affordable when making standard calls, and this cost-effectiveness is especially noticeable when making international calls.

While IP phones offer numerous advantages, it’s important to take into account network infrastructure around it. Many businesses make many phone calls concurrently, which could lead to dropped calls, jitter, and poor audio quality. These problems could be easily avoided with enough bandwidth and proper configuration of network. Each IP phone call requires 100kbps. [12]

If IP phones experience issues due to internet congestion, QoS can be implemented. QoS is mechanism that allows to give priority to certain types of traffic, such as voice and video.

2.3 IP address

IP address is identification number that is unique to device in a public network and a private network. There are two IP address versions: IPv4 and IPv6. IPv4, was introduced in 1980s. When IPv4 was introduced, it was not foreseen that all the IPv4 addresses would be used. This happened because of exponential growth of devices connected to the internet. For this reason, IPv6 was rolled out. [13]

IPv6 uses a 128-bit addressing system that is written in hexadecimal format, which provides approximately 340 undecillion unique addresses. This large address space enables that there will be enough of IP addresses available to accommodate the growing number of internet-connected devices in the future. Despite its advantages over IPv4, IPv6 is still not widely adopted all over the world. IPv6 is not used in this project for that particular reason. [13, 14]

IPv4 uses 32-bit addressing system and the numbers are expressed as set of four numbers and they are separated with dots. These numbers range from 0 to 255 making full IP address range from 0.0.0.0 to 255.255.255.255. This means IPv4 provides only over 4 billion unique addresses. IPv4 quite limited address space led to the introduction of private IP scheme.

Public IP is assigned by ISP and are always unique across the internet. This ensures that devices could be identified and communicated with globally. IP addresses are [14]

Private IP addresses are unique in LANs and are not recognized over the internet and they are assigned by the LAN administrator. To communicate with the internet this IP address must be translated into public IP addresses using NAT. Using this method all the private IP addresses in the same LAN can communicate on the internet while using the same public IP address. This network design uses Class C private IP addresses (192.168.x.x range), which are suitable for small and medium-sized business networks. The following table shows the reserved IP address ranges for private networks. First bits are reserved for the network addresses and the rest are for host addresses. [14, 15] See Table 1 below.

Class	**Usable Private IP Address Range**	**CIDR Notation**
Class A	10.0.0.0 – 10.255.255.255	10.0.0.0/8
Class B	172.16.0.0 – 172.31.255.255	172.16.0.0/12
Class C	192.168.0.0 – 192.168.255.255	192.168.0.0/16

Table 1. Usable private IP address classes [15]

2.4 VPN

Virtual Private Network is a connection that is established digitally between a server and a computer. VPN Is commonly used both for personal privacy and corporate network security. When browsing the internet without VPN, ISP can access browsing data and give it to advertisers and law enforcement. VPN adds extra layer of protection on the internet, it encrypts data between computer and the VPN server thereby making user anonymous. When using VPN, service providers can see your browser data, but the difference is that most of the paid services have no-log policy which keeps you secure. [18]

Generally, the usage of VPNs in corporate world differs from personal use. For example, VPN is used in the corporate world to give remote access to employees to use internal applications or to create one big network which is used in different branch offices to connect to the main branch office, and this ensures secure communication and protection of company data. This is the aim for the VPN usage in this project. [16]

There are two ways to connect the main office for example to branch office or home. The two primary ways to connect remote office to the main office. Leased lines or VPN.

Leased line is a dedicated physical connection between the offices. These are not usually encrypted but they offer faster speeds than VPNs. Leased lines are rented by the ISP. The other option to connect the offices is through VPN. In this project site-to-site IPSEC is preferred to be used to allow remote location to use servers on the main site that maybe added such as FTP. [17] See Figure 5 below.

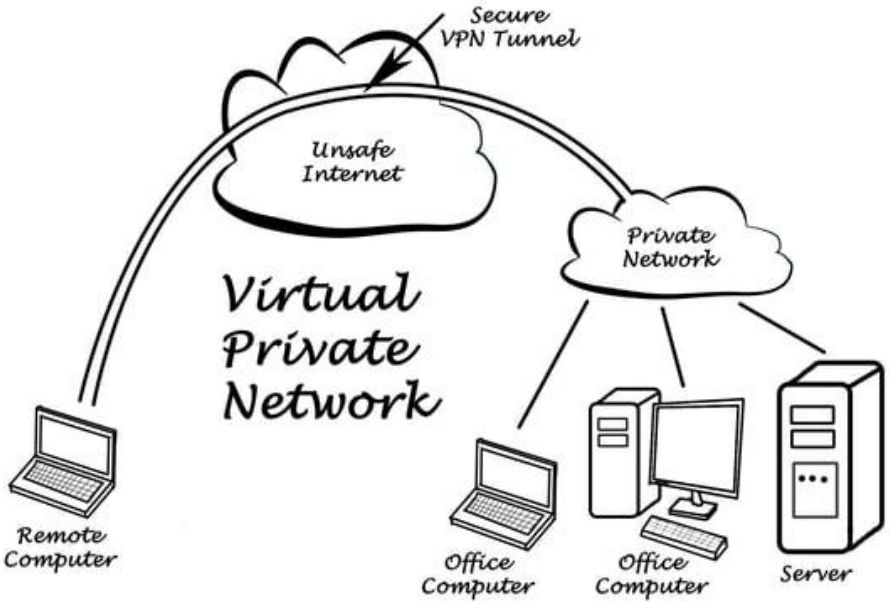

Figure 5. Illustration picture of VPN [16]

3 Network design

This chapter specifies what does this network supposed to accomplish and the minimum requirements. The chapter discusses two different methods to build network, one professional grade and the other is small office/home network which doesn’t take much skill.

3.1 Network Departments and Infrastructure

There are several different departments in this business. The departments are the following:

- Management
- Accountants
- Sales

- Technicians
- IT

Each department has computers and IP phones, and they also have access to printers. There is also another sales point outside the city this company is located which needs access to company's network. Other necessary equipment includes security cameras to ensure safety and surveillance.

These are the minimum requirements that the network infrastructure should accommodate. It would also be beneficial to have a VPN connection from the remote office to the main office. Security will not be a primary focus in this project.

3.2 Network implementation approaches

This section considers two network implementation approaches: a commercial network build and a SoHo approach, while also evaluating their advantages and disadvantages.

3.2.1 Cisco build

This approach involves using Cisco networking equipment to build a high-performance, secure, and scalable network that is designed for businesses. Cisco is the biggest networking company in the world, and it is known for its network solutions.

One of the tools used in this project is Packet Tracer, which is developed by Cisco Systems. It's a network simulation tool that was created as an educational tool. It's used by students and professionals to create network topologies, configure devices, and simulate real-world networking scenarios without needing physical hardware.

This network build is designed to be as cost-effective as possible while still meeting the minimum requirements. This comes with trade-off such as the network doesn't have redundant hardware such as backup router and switches and this could cause network to be downtime if one of the critical network components happen fail.

For this network build, different departments are separated into different VLANs for enhanced security and network segmentation (see Figure 6). Devices such as IP phones, printers and security cameras are each on their own VLANs. Table 1 provides an overview of the VLAN assignments by department.

Department	Number of Devices	VLAN ID
Sales	3 PCs	VLAN 20
Management	2 PCs	VLAN 30
Accountants	2 PCs	VLAN 50
Technicians	2 PCs	VLAN 60
IP Phones (All Departments)	7 IP Phones	VLAN 70
Office Printers	1 Printer	VLAN 80
Security Cameras	3 IP security cameras	VLAN 90
Network admin	1 PC	VLAN 5
Remote Sales Office	1 PC, 1 Printer, 1 IP Phone	N/A

Table 2. Each department's VLAN ID and number of devices.

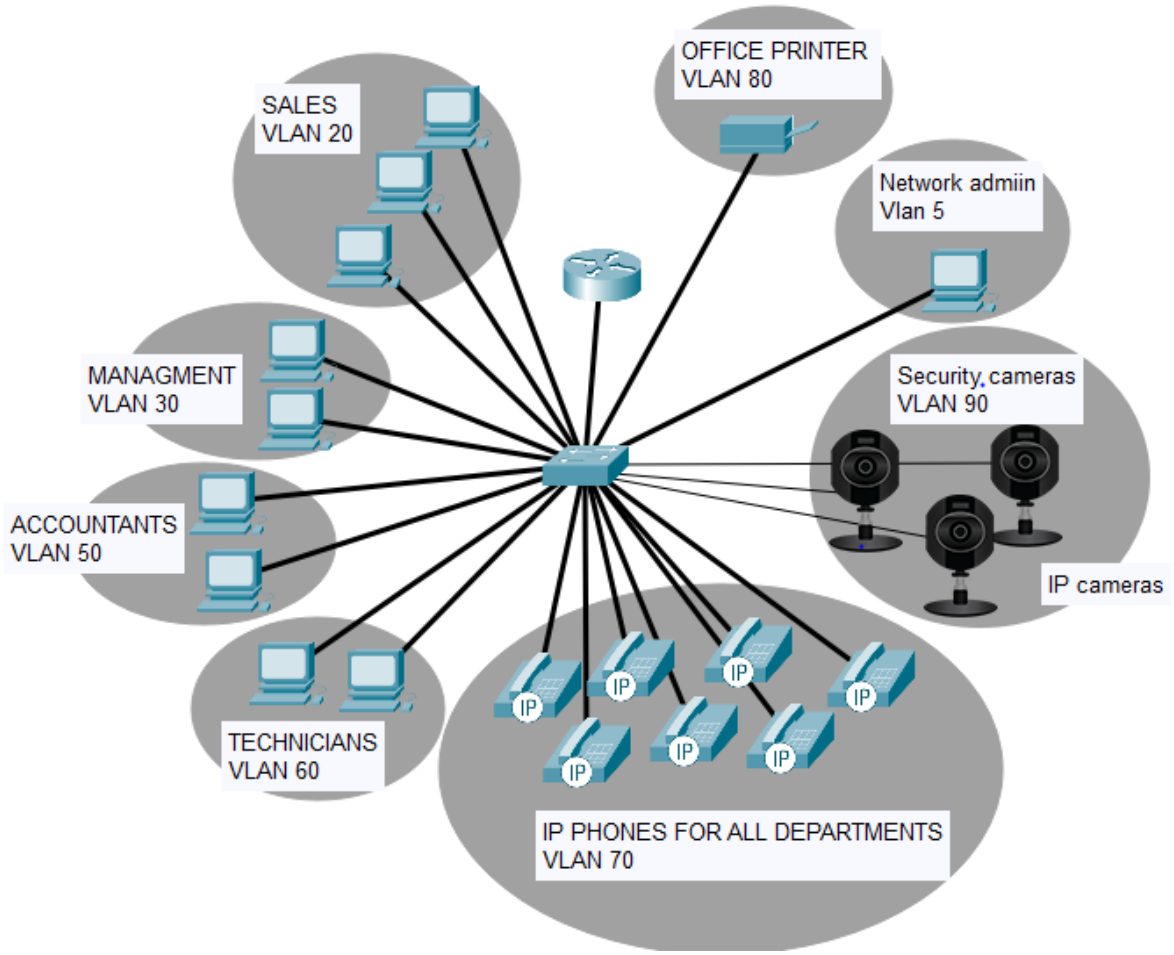

Figure 6. Illustration of the network plan for the main office

Network device choices

There are many options to choose from. The aim is to be as cost efficient as possible, while also reaching the goals set for the small office network. Network devices must support following things:

Router requirements:

- VPN
- DHCP
- Inter-VLAN routing
- Future scalability

When designing network in developing countries, it’s important to consider the current state of internet access. Somalia has fiber optic internet available in major cities such as the city where this network is built. The most common way how internet reaches homes in Somalia is through mobile broadband, particularly via LTE networks provided by local telecom companies.

Both homes and businesses in major cities can get fiber optic connection instead of mobile broadband. This project is designed for fiber optic connection , but in case it’s not available in the remote office, then LTE model of the chosen router can be used as a backup.

Since routers are exposed to the internet, they are frequent targets for cyberattacks. Therefore, in addition to meeting technical requirements, it is essential that the chosen router has active vendor support and is commercially available at the time of the network build.

For this reason, the Cisco ISR 1000 Series is an ideal choice for this project — unlike older models such as the Cisco 2911, which has already reached end-of-life status. At the time of writing this thesis, the Cisco C1101-4P is available for approximately €600 and fully meets the network’s needs. [20] See Figure 7 below.

Figure 7. Main office router choice C1101-4P [19]

This router comes with 4 LAN ports capable of speeds 1 Gbps each and 1 WAN port. It allows fast communication between local devices such as computers, IP

phones, and printers. There are variants of this model such as C1101-4PLTEP and C1101-4PLTEPW which include additional features such as LTE and built-in WI-FI. These features are integrated into the hardware and cannot be added later. [19]

There is also a more budget-friendly option, the Cisco ISR 921-4P, which offers basic routing features. The router has 2x Gigabit Ethernet WAN ports, 4x Gigabit Ethernet LAN ports. In this project, both router models are used: the C1101-4P is deployed in the main office, while the 921-4P Series router is used at the remote sales office to establish a secure VPN connection. There is also a LTE variant of this model. [21] See Figure 8 below.

Figure 8. remote office router 921-4P [21]

Switch requirements:

- VLAN
- QoS
- Sufficient port count
- Security

For this project, a Layer 2 managed switch is enough since inter-VLAN routing is handled by the router. Layer 2 switches are more cost-effective than Layer 3 switches while still supporting VLANs, port security, and QoS.

For the both offices, the recommended device is the Layer 3 switch Cisco Catalyst 9200L, with a 24-port configuration. It meets all project requirements. It is future-proof, supports advanced features such as stacking. This switch was picked over the Layer 2 model C1000-24 because of its better scalability, future proofing and considering that the C1000-24 model is approaching its end of life. If C1000-24 is available at the time of building this network, it could be used in the remote office. [22, 23]

The Cisco Catalyst 9200L (Figure 9) supports stacking. It is possible to add multiple switches in the future, which can be connected to the existing one and managed centrally from it. All the stacked switches act as one logical switch, simplifying management and increasing scalability. The layer 2 model C1000-24P does not support stacking. [22, 23]

Figure 9. Main/remote office switch: Catalyst 9200L 24-port [22]

In this project, the network was configured using the simplest and most straightforward approach possible to ensure easy implementation. For this reason, a /24 subnetting style was chosen, assigning each VLAN its own full Class C subnet. This makes IP planning easier and avoids calculations. Below is the VLAN and subnet mapping used.

VLAN ID	Subnet	Devices	Switch ports
VLAN 5	192.168.5.0/24	1	G1/0/23
VLAN 20	192.168.20.0/24	3	G1/0/1- G1/0/3
VLAN 30	192.168.30.0/24	2	G1/0/4-G1/0/5
VLAN 50	192.168.50.0/24	2	G1/0/6- G1/0/7
VLAN 60	192.168.60.0/24	2	G1/0/8- G1/0/9
VLAN 70	192.168.70.0/24	7	G1/0/10- G1/0/16
VLAN 80	192.168.80.0/24	1	G1/0/17
VLAN 90	192.168.90.0/24	3	G1/0/18- G1/0/20

Table 3. VLAN and switch port assignment plan

The detailed configuration commands for both the switch and router are included in the appendix 1 for reference.

3.2.2 SOHO build

This approach is much simpler and more affordable than enterprise grade network. This SOHO network is designed with ease of implementation and management in mind. While this network design lacks advanced network features and long-term scalability. This network design can still be scaled for certain extent until the hardware cannot handle anymore.

The issue with the professional grade network is that not only it is more expensive than the SOHO approach but also a professional needs to build it, which could even cost more than the network equipment itself. This approach tries to eliminate needing professionals of the field and minimize the equipment cost.

There are many great options to choose from with this approach. TP-Link's Deco X60 Mesh is excellent choice and can handle up to 150 devices simultaneously. It's a mesh system that is designed to provide seamless wireless connectivity through the whole premises. For example, the 3-pack. cover up 790 sqm. The price of this particular mesh system of 3-pack is 240€ at the time of writing this thesis. [26, 27] See Figure 10 below.

Figure 10. Picture of TP-Link’s Deco X60 3-pack [27]

The Deco units communicate wirelessly together or could be wired for faster communication. Only one deco unit must be connected to the Internet through ISP. This system allows devices to switch between access points based up to the strongest signal received from access point. For example, when moving from one floor 1 to floor 2 device will stay connected to floor 1 access point until floor 2 becomes stronger signal which it will automatically connect to it. This ensures smooth connectivity and uninterrupted internet connection. [26]

While the Deco X60 offers great wireless connectivity it has some limitation for this specific project. The main challenge for this project is that many of the connections are designed for wired networks such as IP phones and PC’s while the Deco X60 only has 2 ethernet ports. One of the ports may be used as backhaul between nodes, which leaves only one port available to other devices

The solution for this issue is to add a switch such as TP-Link’s. It’s unmanaged 24-ports Gigabit switch. At the time of writing, the TL-SG1024 costs approximately 110€. See Figure 11 below.

Figure 11. Picture of the chosen switch TL-SG1024 [28]

Deco X60 offers some of the features that were used in the professional network design such as QoS for the IP phones and free basic firewall. In addition to that, Deco X60 allows to segregate network between internal office network and guest network for extra security.

The Deco X60 Mesh system is managed from Deco app which provides easy to use graphic user interface. The app is available for Android and IOS devices. All configurations and monitoring are done within the app, allowing to manage the network without requiring advanced technical skills. See Figure 12 below.

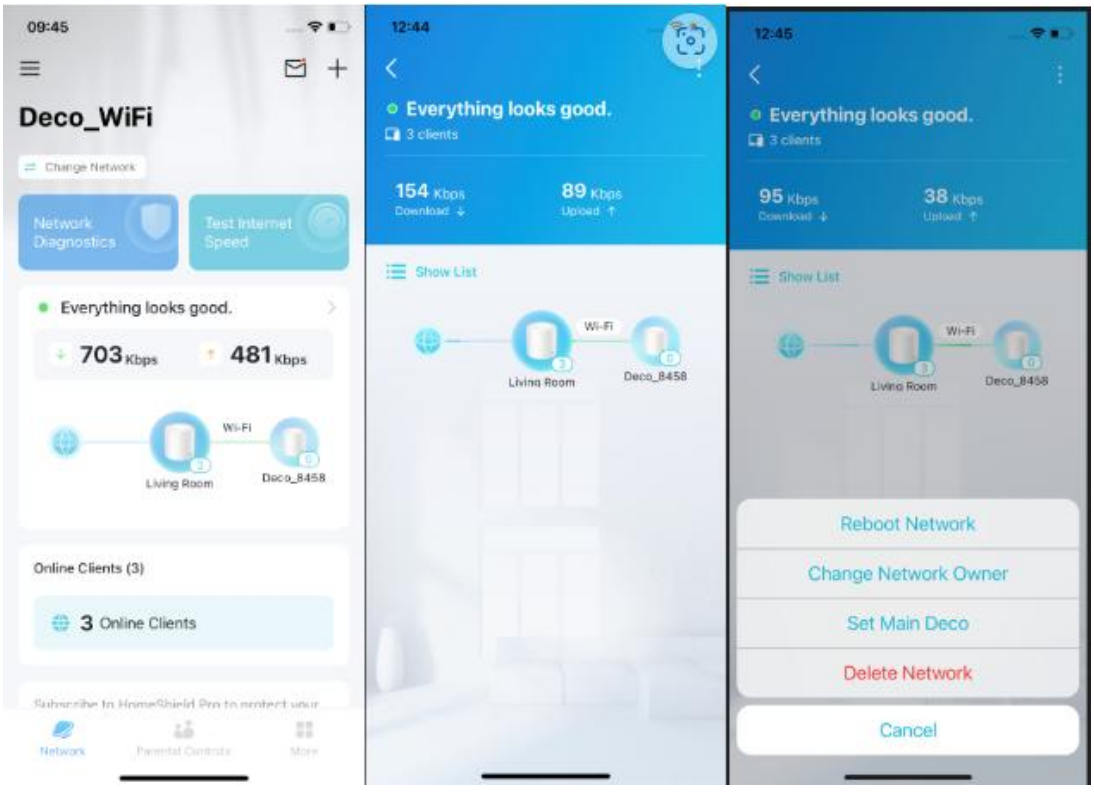

Figure 12. Mobile application's user interface [29]

For security Deco X60 has built-in firewall and comes with network protection kit (HomeShield) which is meant to protect the network. TP-Link also offers extra features with paid version of HomeShield. [26]

The remote office is not connected to the main office using a VPN in this network plan. Remote office has the same Mesh system but instead uses smaller 8 devices switch, like TP-Links TL-SG108, since it doesn't need all those ports. Since the plan of this build was easy deployment and management adding a VPN would have defeated the purpose.

Collaborating with the main office happens through the cloud, as it is easier to manage and set up. Instead of setting up an FTP server for collaboration, this can be done by using cloud-based solutions such as Microsoft 365 Business subscriptions.

3.2.3 Chosen implementation approach

After carefully comparing Cisco's professional network approach with a simple SOHO network, this project chooses the SOHO approach as the more practical option for initial deployment. This decision is due to the significantly higher costs of the professional network build. It was also taken into consideration that this type of network requires a professional to implement and manage it, which may not be feasible for a startup with limited technical resources and budget.

It's important to note that the case company does not really have need for professional-grade network infrastructure at this stage. Advanced features and future scalability are not very useful as of now. It's more reasonable financially to start as SOHO network and later when business grows, upgrade it to professional network.

3.3 Challenges

The biggest challenge in this project has been getting reliable information from Somalia, because it's not available in the web. When building network, it is important to know internet speed among other information such as reliability of electricity and the availability of network in certain rural areas.

Just before returning this project, it was announced that Somalia has officially granted a licence to operate to Starlink by SpaceX. Starlink is an internet service provider that uses low earth orbit satellites to deliver high-speed internet connection, and it's perfect for rural areas and developing countries in general, offering better speeds than most local ISPs. [24]

Each Starlink customer gets a small satellite dish that communicates with Starlink's low earth orbit satellite in Ku-band frequencies (Figure 13). The satellite then relays the signal down in Ka-bands to a ground station (gateway) that is connected to the worldwide internet. [30]

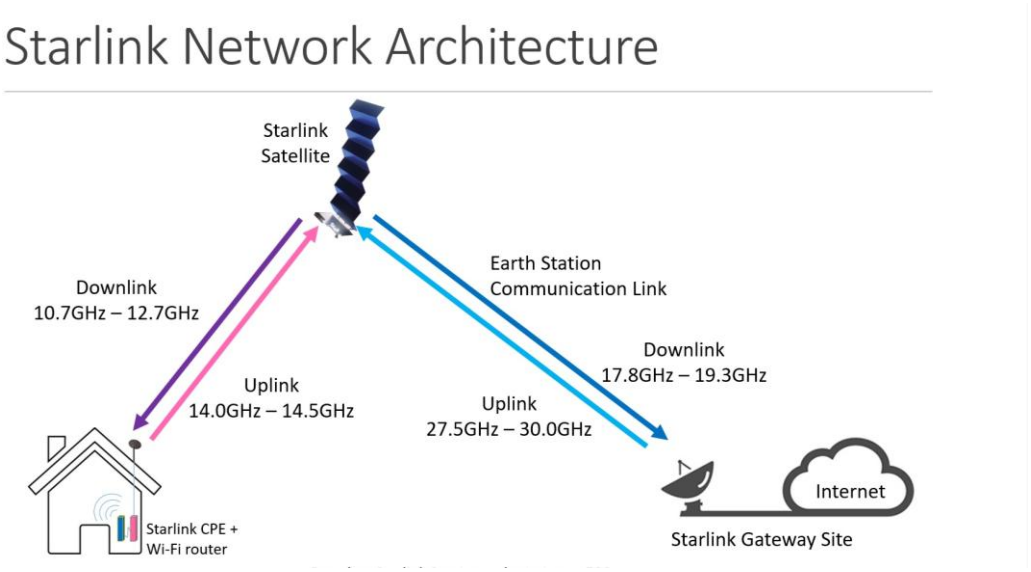

Figure 13. How Starlink operates. [25]

Another problem in developing countries which must be taken into consideration when building network is unreliable electricity supply. It's common that electricity

goes out because of poor infrastructure, even though it is getting better in big cities, and it has become less frequent. Since this project is for green energy company assumption is made that they have reliable electricity.

Since this project focuses on planning the network, testing was not done on physical devices to verify connectivity. Instead, some of the project was tested on network simulation tool. Even though there were no exact same device models available in the network simulator tools, the closest matches were used to test the hardware configuration. The mentioned configurations all reached the desired goal and network connectivity worked.

The local pricing of the network devices was not found on the web in Somalia. Therefore, the prices mentioned in this project were based on Finland's prices.

4 Conclusion

The aim of the thesis was to design a cost-effective and fully functional network for a startup operating in Somalia. The network design had to consider local network infrastructure, electricity reliability, current business needs and future scalability. The project reached its main goal to give a blueprint that meets these needs.

The thesis took two different approaches to design and implement a network, for a small company to examine which one would be better approach for case company. One approach was professional Cisco based network, and the other was SOHO approach. SOHO approach was chosen as the more practical option for the startup due to its lower cost and easier implementation.

Although all the goals were not reached on the professional network design, such as VPN implementation and due to the limitation of the simulation tool, the project met its primary goal. This project can be used as a reference for other small companies in similar environments that are looking to build an affordable and efficient network.

References

1.What is a LAN, https://www.cloudflare.com/learning/network-layer/what-is-a-lan/ Accessed 3.8.2024

2.WAN vs LAN, https://www.truecable.com/blogs/cable-academy/wan-vs-lan Accessed: 3.8.2024

3. What is a router, https://www.cloudflare.com/learning/network-layer/what-is-a-router/ Accessed 4.10.2024

4. What is a router, https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-a-router.html#~types-of-routers Accessed 4.10.2024

5. What is network switching, https://www.cisco.com/c/en/us/products/switches/what-is-network-switching.html Accessed 5.10.2024.

6. What is a network switch, https://www.cloudflare.com/learning/network-layer/what-is-a-network-switch/ Accessed 5.10.2024.

7. What is an access point, https://www.cisco.com/site/us/en/learn/topics/small-business/what-is-an-access-point.html Accessed:10.11.2024

8. What is a firewall, https://www.cloudflare.com/learning/security/what-is-a-firewall/ Accessed 10.11.2024

9. What is a firewall, https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-firewall.html Accessed 10.11.2024

10. VoIP phone
https://www.techtarget.com/searchunifiedcommunications/definition/VoIP-phone
Accessed 15.11.2024

11.What is ip telephony, https://www.nextiva.com/blog/what-is-ip-telephony.html
Accessed 15.11.2024

12. VoIP data usage, https://www.nextiva.com/blog/voip-data-usage.html
Accessed:28.11.2024

13.What is an IP address, https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address Accessed: 28.12.2024

14. .What is IP address,
https://www.fortinet.com/uk/resources/cyberglossary/what-is-ip-address
Accessed 28.12.2024

15. Address filter,
https://www.arin.net/reference/research/statistics/address_filters/ Accessed 10.1.2025

16.VPN for business, https://www.foxpass.com/vpn-for-business Accessed 20.2.2025

17 What Are Leased Lines, https://www.gradwell.com/guides/leased-lines-guide/ Accessed 20.2.2025

18. What Is a Virtual Private Network,
https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-virtual-private-network-vpn.html Accessed 20.2.2025

19. Cisco 1000 Series Integrated Services Routers Data Sheet
https://www.cisco.com/c/en/us/products/collateral/routers/1000-series-

integrated-services-routers-isr/datasheet-c78-739512.html - Cisco110xISRsRoutingfundamentalsperfected Accessed 1.4.2025

20. Services Router 1101, https://www.multitronic.fi/fi/products/2344418/services-router-1101?srsltid=AfmBOoo_DyXg5oSptA7l_G2oEvnl9Z6fYtmz8_AscN371DNWEtgGz4v_bIc Accessed 1.4.2025

21. Cisco 900 Series Integrated Services Routers Data Sheet, https://www.cisco.com/c/en/us/products/collateral/routers/900-series-integrated-services-routers-isr/datasheet-c78-741615.html Accessed: 1.4.2025

22Cisco Catalyst 9200 Series Switches Data Sheet, https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html Accessed:1.4.2025

23. Cisco Catalyst 9200 Series Switches Data Sheet, https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-1000-series-switches/nb-06-cat1k-ser-switch-ds-cte-en.html Accessed 1.4.2025

24. Mohamed Sheikh Nor, Published 13.4.2025, Somalia Gives Elon Musk’s Starlink Permit to Operate in Country – Bloomberg, https://www.bloomberg.com/news/articles/2025-04-13/somalia-gives-elon-musk-s-starlink-permit-to-operate-in-country Accessed 23.4.2025

25. What is Local Area Network, https://www.heavy.ai/technical-glossary/local-area-network image Accessed 4.10.2025

25.Why Starlink is a gamechanger, blog, https://www.connectivity.technology/2021/03/why-starlink-is-already-gamechanger.html Accessed 23.04.2025

26.Deco X60 | AX5400 Whole Home Mesh Wi-Fi 6 System, https://www.tp-link.com/nordic/home-networking/deco/deco-x60/ Accessed: 23.05.2025

27 TP-Link Deco X60 WiFi 6 mesh-järjestelmä (3 kpl), https://www.gigantti.fi/product/tietokoneet-ja-toimistotarvikkeet/reitittimet-ja-verkkolaitteet/reitittimet/tp-link-deco-x60-wifi-6-mesh-jarjestelma-3-kpl/150301 Accessed 5.4.2025

28. TP-LINK TL-SG1024 -24-porttinen kytkin https://www.verkkokauppa.com/fi/product/300476/TP-LINK-TL-SG1024-24-porttinen-kytkin Accessed 5.4.2025

29. Getting to know your Deco app | TP-Link Nordic https://www.tp-link.com/nordic/support/faq/1593/ Accessed 13.4. 2025

30. Starlink, https://www.starlink.com/satellites Accessed 25.4.2025

Appendix 1: Configurations

Configuration on the switch:

1.Creating VLANs.

```
enable
configure terminal

vlan 5
name Network_Admin
exit
vlan 20
name Sales
exit
vlan 30
name Management
exit
vlan 50
name Accountants
exit
vlan 60
name Technicians
exit
vlan 70
name IP_Phones
exit
vlan 80
name Printers
exit
vlan 90
```

```
name Cameras
exit
```

2. Assigning ports to VLANs and turning switch ports to access only for security purposes.

```
interface range GigabitEthernet1/0/1 - 3
switchport mode access
switchport access vlan 20
exit

interface range GigabitEthernet1/0/4 - 5
switchport mode access
switchport access vlan 30
exit

interface range GigabitEthernet1/0/6 - 7
switchport mode access
switchport access vlan 50
exit

interface range GigabitEthernet1/0/8 - 9
switchport mode access
switchport access vlan 60
exit

interface range GigabitEthernet1/0/10 - 16
switchport mode access
switchport access vlan 70
exit

interface GigabitEthernet1/0/17
switchport mode access
```

```
switchport access vlan 80
exit

interface range GigabitEthernet1/0/18 - 20
switchport mode access
switchport access vlan 90
exit

interface GigabitEthernet1/0/23
switchport mode access
switchport access vlan 5
exit
```

3. Configuring trunk port that connects to the router.

```
interface GigabitEthernet1/0/24
switchport mode trunk
exit
```

3. For security purposes, all unused switch ports are administratively shut down. The switch has two ports that are unused. These can be used for future additions. The unused ports are GigabitEthernet1/0/21 and GigabitEthernet1/0/22. These ports could be later used for servers or any additional devices.

```
interface range GigabitEthernet1/0/21 - 22
shutdown
exit
```

After these configurations are done, devices in the same VLANs can communicate with each other. This was tested with network simulation tool using ping command. For full communication between devices in different VLANs, inter-VLAN routing must be done.

Configuration on main office router

In this project, main router is configured to act as DHCP server. For network this small, this way is practical and cost-effective solution as it doesn't require dedicated DHCP server. This means there will be no extra hardware costs thus keeping costs minimal.

The router is also responsible for inter-VLAN routing. While this could have been implemented on the Layer 3 switch, routing is instead handled by the router for the sake of simplicity and ease of configuration. Another reason why this approach is chosen is to enable usage of this project with layer 2 switch. This method, commonly known as router-on-a-stick, uses subinterfaces on a single physical interface to manage traffic between VLANs.

1.Creating subinterfaces for each VLAN.

```
enable
configure terminal

interface GigabitEthernet0/0.5
encapsulation dot1Q 5
ip address 192.168.5.1 255.255.255.0
exit

interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
exit

interface GigabitEthernet0/0.30
```

```
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
exit

interface GigabitEthernet0/0.50
encapsulation dot1Q 50
ip address 192.168.50.1 255.255.255.0
exit

interface GigabitEthernet0/0.60
encapsulation dot1Q 60
ip address 192.168.60.1 255.255.255.0
exit

interface GigabitEthernet0/0.70
encapsulation dot1Q 70
ip address 192.168.70.1 255.255.255.0
exit

interface GigabitEthernet0/0.80
encapsulation dot1Q 80
ip address 192.168.80.1 255.255.255.0
exit

interface GigabitEthernet0/0.90
encapsulation dot1Q 90
ip address 192.168.90.1 255.255.255.0
exit
```

2. Enabling the physical router interface that connects to the switch.

```
interface GigabitEthernet0/0
no shutdown
exit
```

3. Before creating DHCP address pools, it's important to exclude the default gateway addresses of each VLAN. These addresses are assigned to the router's subinterfaces and must not be allocated to devices.

```
ip dhcp excluded-address 192.168.5.1
ip dhcp excluded-address 192.168.20.1
ip dhcp excluded-address 192.168.30.1
ip dhcp excluded-address 192.168.50.1
ip dhcp excluded-address 192.168.60.1
ip dhcp excluded-address 192.168.70.1
ip dhcp excluded-address 192.168.80.1
ip dhcp excluded-address 192.168.90.1
```

4. Creating DHCP pools to assign IP addresses to devices in each VLAN. A DNS server is to Google's public DNS server because it is fast, reliable, and globally accessible and for that reason it makes an excellent choice for a small network.

```
ip dhcp pool VLAN5
network 192.168.5.0 255.255.255.0
default-router 192.168.5.1
dns-server 8.8.8.8

ip dhcp pool VLAN20
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
dns-server 8.8.8.8

ip dhcp pool VLAN30
network 192.168.30.0 255.255.255.0
default-router 192.168.30.1
dns-server 8.8.8.8
```

```
ip dhcp pool VLAN50
network 192.168.50.0 255.255.255.0
default-router 192.168.50.1
dns-server 8.8.8.8

ip dhcp pool VLAN60
network 192.168.60.0 255.255.255.0
default-router 192.168.60.1
dns-server 8.8.8.8

ip dhcp pool VLAN70
network 192.168.70.0 255.255.255.0
default-router 192.168.70.1
dns-server 8.8.8.8

ip dhcp pool VLAN80
network 192.168.80.0 255.255.255.0
default-router 192.168.80.1
dns-server 8.8.8.8

ip dhcp pool VLAN90
network 192.168.90.0 255.255.255.0
default-router 192.168.90.1
dns-server 8.8.8.8
```