CMPG315 PROJECT DOCUMENTATION

Group: 20

Abstract

This project focused on designing a secure, scalable, and efficient LAN network for a medium-sized detached office building. Using Cisco Packet Tracer, we developed a network that provides internet access, section isolation, and wireless connectivity for employees and guests. The network allows seamless remote access while prioritizing security and expansion capabilities. The project also assessed budgeting, work-from-home infrastructure, and group dynamics in a hybrid working model.

Group Members: CS, Tsetsa [42010225], O Khechane [34285180], EM Machete [38123908], MP Thabane [38697505], K Thobejane [35819685], TB Mlambo [40451720], DL Zame [41362918], LS Mavhungu [44418450]

CONTENTS

1. Group and Project Details

1.1. List of participating group members

The following participants contributed to completing the project, and the members of this group believe they all deserve to be listed as equal contribution members:

Role	Name	Student number
Networking Setup	CS Tsetsa	42010225
Topology Design	O Khechane	34285180
Documentation	MP Thabane	38697505
Budget Research	EM Machete	38123908
Networking Setup	K Thobejane	35819685
Topology Design	TB Mlambo	40451720
Documentation	LS Mavhungu	44418450
Budget Research	DL Zame	41362918

1.2. List of dismissed members

None.

1.3. Major Unresolved Problems

The group experienced the following unresolvable problems:

- We experienced some small scheduling issues because of remote work but sorted them out by using asynchronous updates.
- It was sometimes tricky to find meeting times that worked for everyone due to schedule clashes.
- We also ran into a few technical problems with different versions of Packet Tracer.
- Despite these challenges, everything was resolved, and the project was completed without any major setbacks.

1.4. Overview of Project

The project involved creating a complete network setup for a standalone office building measuring 100x50 meters. The layout included various areas such as multiple offices, a reception area, a technicians' room, a kitchen, a meeting room, an open-plan office space, and a machine room. The network needed to support both wired and wireless connectivity, include isolated sections using VLANs, provide internet access via a single ISP connection point, and ensure strong support for remote access.

2. Network Topology and Setup

In this section, the detailed setup of the designed network is discussed. The layout of the building, the specific needs of each area, and the work-from-home requirements have all been carefully considered. The network was designed to ensure reliable high-speed connectivity, strong security, and scalability for future growth. Each decision regarding hardware selection and network structuring is motivated based on these goals.

2.1. Overview of Topology

The hierarchical star topology was selected for this project because it allows for easy expansion, efficient management, and better fault isolation. In this design, all access switches are connected to distribution switches, which in turn connect to core switches located in the machine room. The centralized design allows for efficient management of network traffic and ensures that a single access point failure doesn't disrupt the entire network.

This topology has a number of advantages over other topology designs, such as simplifying troubleshooting procedures, enhancing network performance, and supporting better scalability for future expansions, like increasing users and devices. The distinct separation of core, distribution, and access layers helps keep the network well-organized and improves security by enabling effective VLAN segmentation. This approach does, however, require that a number of issues be kept in mind, namely:

- A failure in the core switch could affect a significant part of the network.
- Core and distribution switches can be expensive, so it’s important to plan the budget carefully.
- Good VLAN planning and correct routing setup are key to keeping different sections properly isolated and managing access effectively.

2.2. Design considerations per section

In this section the physical network design, produced using Packet Tracer version 8.2.0, will be introduced. The presentation in this section builds on the contents of Section 2.1, and the manner in which the design considerations were addressed will also be discussed. The section will conclude with a discussion on how the network will handle remote connections, with a focus on the application of remote work principles.

2.2.1. Reception

The reception area functions as the first point of contact for both staff and visitors. It features two permanent reception desks, each needing wired internet connectivity for administrative use. Additionally, staff require wireless access for their mobile devices, while guests should be provided with restricted internet access via a secure guest Wi-Fi network.

- 2 wired access points connected to an 8-port switch.
- Networked printer made available via Ethernet.
- Dual-band wireless AP supporting staff VLAN and isolated guest VLAN.

2.2.2. Section 1: Offices and Open Plan Space

This section consists of 12 private offices and one large open-plan workspace accommodating 75–120 staff members. The offices are used by administrative and managerial personnel, while the open floor hosts general staff with flexible workstations.

- Each private office is served by an 8-port switch.
- 100 wired access points placed in floor panels in the open-plan area.
- High-density Wi-Fi APs mounted strategically.
- 5 networked printers available near the machine room.
- VLAN partitioning ensures departmental and user group isolation. This section consists of 12 offices used by administrative and managerial staff. Each office needs 2–4 wired access points for laptops or desktops, and strong Wi-Fi for personal devices.
- Each office is served by an 8-port switch.
- Wi-Fi APs installed in central corridors.
- VLAN division ensures departmental isolation.

2.2.3. Section 2: Technicians' Office and Machine Room

This area is used by two technical staff for diagnostics, repairs, and server maintenance. It includes both the technicians' workspace and the centralized machine room.

- 2 wired access points for technician computers.
- 4 additional wired access points for testing hardware.
- Wi-Fi to support up to 16 technician devices.
- Direct cabling path to the machine room.
- Machine room hosts all servers, firewall, router, and two core switches.
- Inter-VLAN routing and external internet access handled here.
- No Wi-Fi in the machine room for security reasons. This area is used by two technical staff for diagnostics and repairs. It requires robust connectivity to the server room for internal testing, remote administration, and equipment maintenance.
- 2 wired access points for technician computers.
- 4 wired access points for technical devices under repair or testing.
- Wi-Fi to support up to 16 devices.
- Direct cabling path to the server room switch.

2.2.4. Section 3: Meeting Room and Kitchen

The meeting room supports up to 30 users during presentations and includes hardware for teleconferencing. The kitchen includes IoT-enabled appliances that must be connected to the network.

- 2 wired ports in the boardroom for conferencing equipment.
- Wireless AP in boardroom for laptops and tablets.
- Kitchen has 4 wired access points for IoT, and one AP for staff Wi-Fi.

The machine room serves as the central hub of the network infrastructure.

- Contains all servers (DHCP, DNS, File, Intranet, VPN), two core switches, one router, and the firewall.
- All external connections and inter-VLAN routing are processed here.
- Server access restricted to authorized devices and technician VLAN only.
- No Wi-Fi needed; cabling and rack-mounted equipment only. The meeting room supports up to 30 users during presentations and includes hardware for teleconferencing. The kitchen includes IoT-enabled appliances that must be connected to the network.

- 2 wired ports in the boardroom for conferencing equipment.
- Wireless AP in boardroom for laptops and tablets.
- Kitchen has 4 wired access points for IoT, and one AP for staff Wi-Fi.

2.3. Network Design

In this section, the physical network design, produced using Packet Tracer version 8.2, will be introduced. The layout follows the design considerations discussed earlier, ensuring that each requirement is fulfilled. The section will also explain how remote connectivity and security were implemented in the design.

2.3.1. Design of Reception Network

- Two wired access points connected to a nearby 8-port switch.
- Staff Wi-Fi configured using WPA2-Enterprise.
- Guest Wi-Fi on a separate VLAN, restricted to internet access only.
- Printer connected via Ethernet and made available to reception PCs.

2.3.2. Design of Section 1 Network

- Each office is connected to an 8-port access switch, linked to a central distribution switch.
- Wired Ethernet ports are available for 2–4 desktop or laptop devices in each office.
- In the open-plan area, 100 Ethernet ports are pre-installed in the raised flooring and connected to floor-based access switches.
- High-density Wi-Fi access points provide robust coverage for personal mobile devices.
- 5 networked printers are installed adjacent to the machine room and shared across the VLAN.
- VLANs segment different office groups and departments to ensure traffic isolation.
- Offices connected to 8-port access switches linked to distribution switches.
- Each office configured for 2–4 wired devices.
- Staff Wi-Fi access via APs in each hallway.
- VLANs ensure that each office's traffic remains isolated.

2.3.3. Design of Section 2 Network

- Technician desktops are connected via two wired access ports linked to the distribution switch.
- Four wired ports are reserved for equipment diagnostics and hardware maintenance.
- A dedicated switch ensures these devices remain isolated but have access to core services.
- Wi-Fi access supports multiple devices used for technical testing.

The machine room includes the core of the network infrastructure:

  - One Cisco 4321 router
  - Two Cisco Catalyst 9500 core switches
  - Centralized servers providing DHCP, DNS, file storage, VPN, and intranet services
  - Cisco ASA firewall
  - Inter-VLAN routing is performed at the core, and all internet traffic passes through the firewall.
  - There is no wireless connectivity in the machine room for security and stability reasons.
  - Dedicated high-speed wired connections to the server room.
  - Two switches manage access to technician PCs and equipment ports.
  - Multiple Wi-Fi devices supported for diagnostics.
  - Access to internal servers is unrestricted within VLAN.

2.3.4. Design of Section 3 Network

- Two wired ports in the boardroom for conferencing hardware.
- Wi-Fi available for laptops and mobile devices.
- Kitchen equipped with 4 Ethernet ports for IoT devices and one AP.

2.3.5. Handling of Remote Connections

The network is capable of offering access via remote connection through the use of OpenVPN and Microsoft Remote Desktop Protocol (RDP). This allows for the following features to be offered to the stakeholders:

- Secure login via VPN before accessing internal systems
- Access to intranet services and shared drives remotely
- Compatibility with both Windows and Linux clients
- Reduced risk of lateral attacks due to strict VLAN enforcement

- VPN traffic is routed through the firewall for monitoring and control.
- Remote Software: OpenVPN, Microsoft RDP
- Security Measures: Endpoint protection for all devices
- Virtual Workspace: Microsoft Teams and OneDrive recommended for collaboration.

2.4. Reflection on Network Design

The group is confident in the design of this network, and believes that it will function should it be implemented in a real world environment. This belief is based on the following observations:

- The network design follows solid networking principles, so implementation is expected to go smoothly.
- Both the wired and wireless configurations meet the necessary speed requirements.
- The centralized Machine Room helps ensure that all critical equipment is securely housed and protected.
- Secure remote access has been successfully integrated to support remote work.
- Possible future improvements include adding a second fibre line for ISP redundancy and installing extra access points if Wi-Fi demand increases in the open office area.

3. Budget

In this section the budget for the project will be discussed. The basic considerations and assumptions will be explained first, followed by an overview of the budget. The section will conclude with the full budget, and a discussion of any factors that may impact the budget, but have not been considered.

3.1. Budget Considerations and overview

The following assumptions were made with regards to the budget:

- A 20% contingency on the final cost should be included;
- Servers are already owned, and printers and PCs are excluded from the network hardware budget.

The total of the budget is R1 034 357.64 and includes the use of the best affordable equipment that could be fund by querying Amazon. This is believed to be a reasonable price for this project because it balances cost efficiency with quality, ensuring the team has access to reliable equipment while staying within financial constraints.

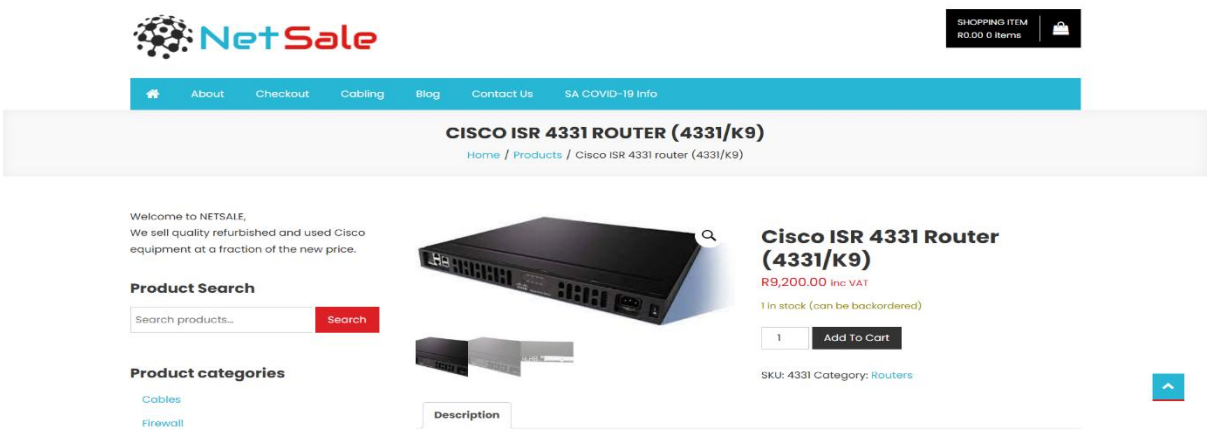
3.2. BUDGET

The following table presents the budget.

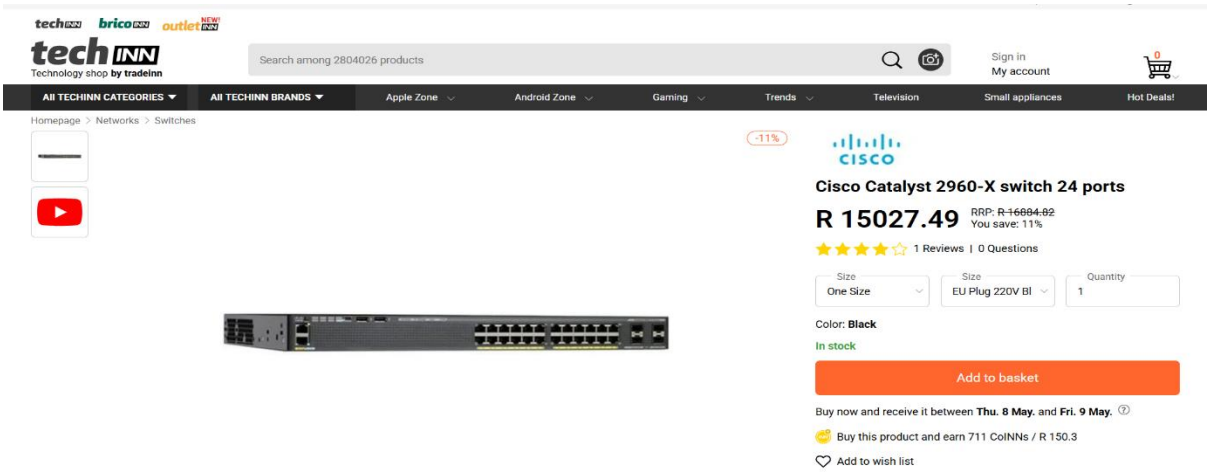
Item	Quantity	Unit Price (R)	Total Price (R)
Cisco ISR 4331 Router	2	R9,200	R18,400
Cisco Catalyst 2960X Core Switch	3	R15,027.49	R45,082.47
Cisco Catalyst 1000 8-Port Switch	20	R7,095.99	R141,919.80
Cisco WAP581 Access Point	40	R7,622.50	R304,900
CAT6 Ethernet Cable (100m rolls)	30 rolls	R889	R26,670
Patch Panels, Racks	5	R1,081	R5,405
Fortinet Fortigate 40F Firewall	1	R27,231	R27,231
UPS Backup Systems	2	R33,879	R67,758
VPN License (Cisco AnyConnect)	100 Users	R188,791.37	R188,791.37

PROOF OF PRICES

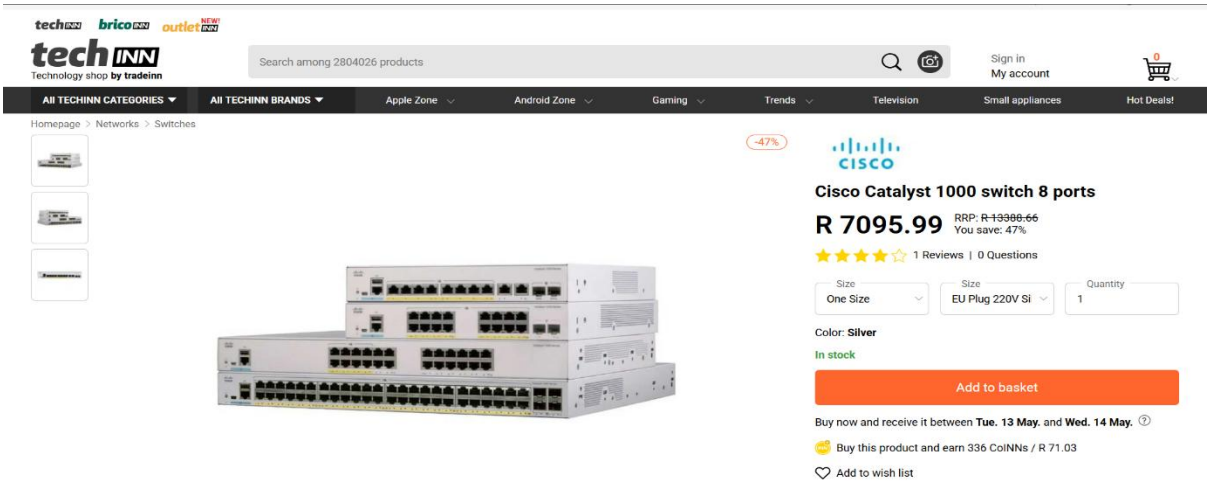
1. Cisco ISR 4331 Router



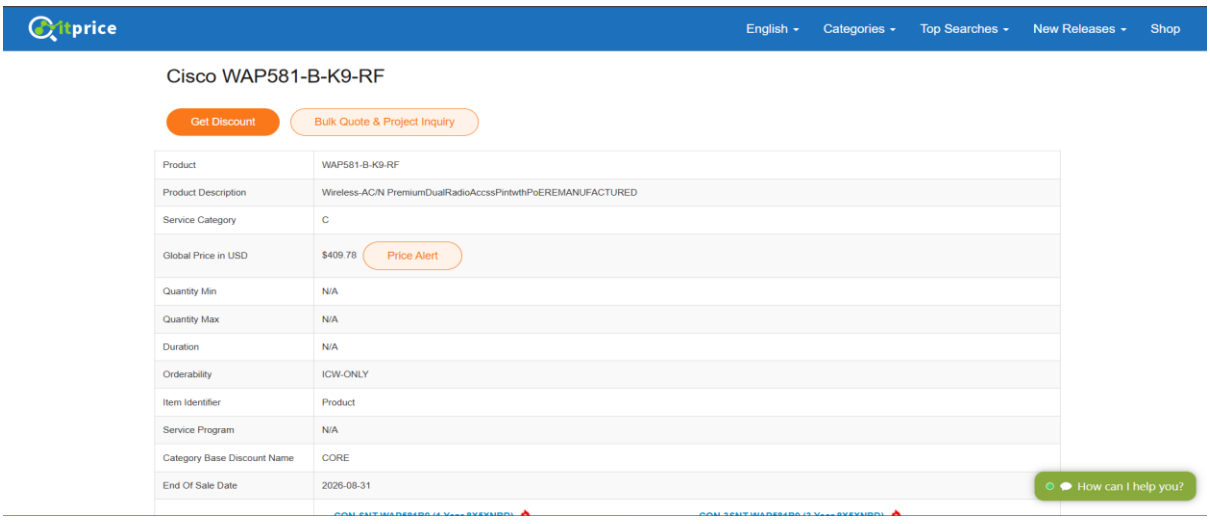
2. Cisco Catalyst 2960X Core Switch



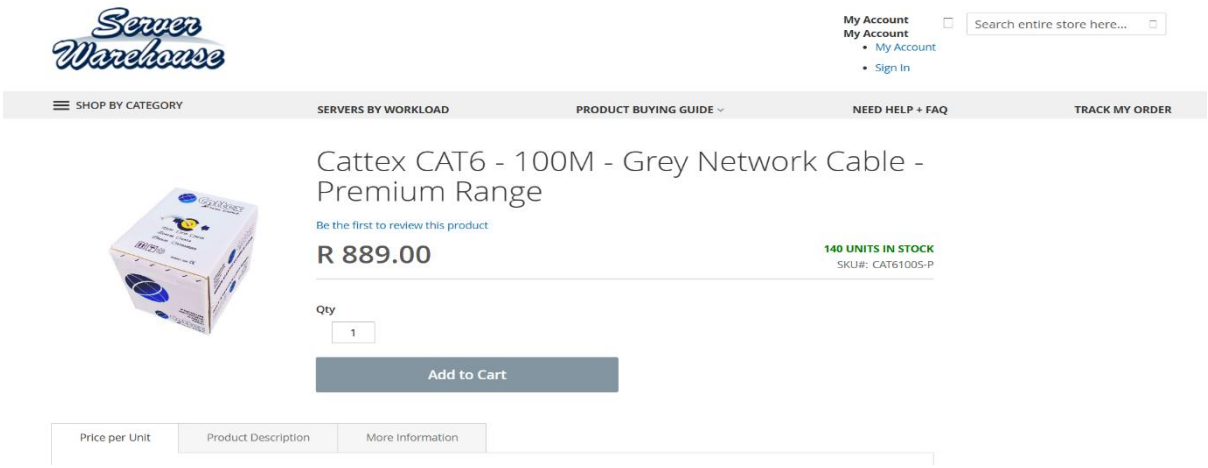
3. Cisco Catalyst 1000 8-Port Switch



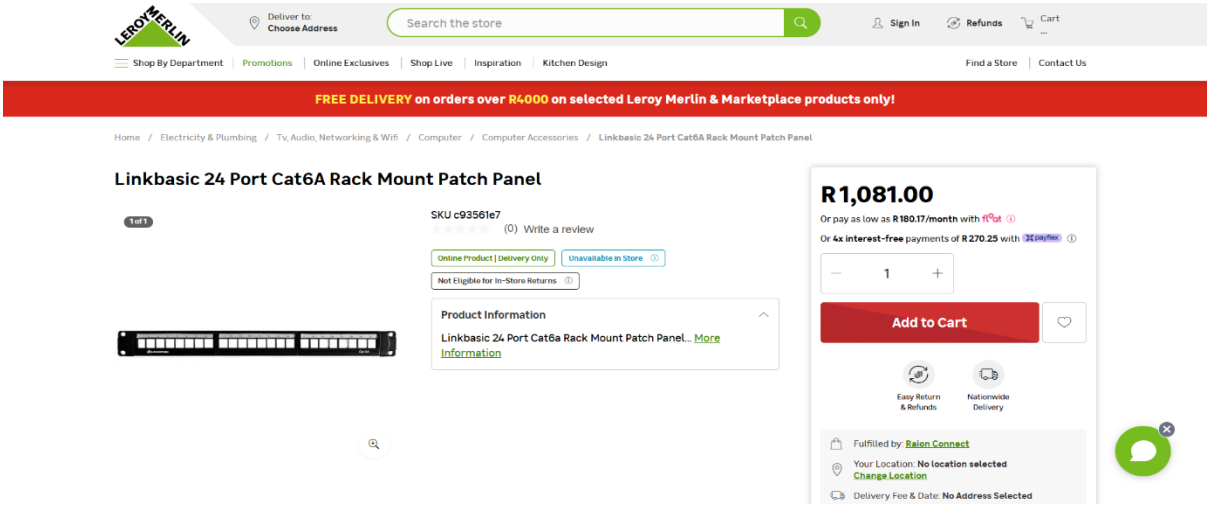
4. Cisco WAP581 Access Point



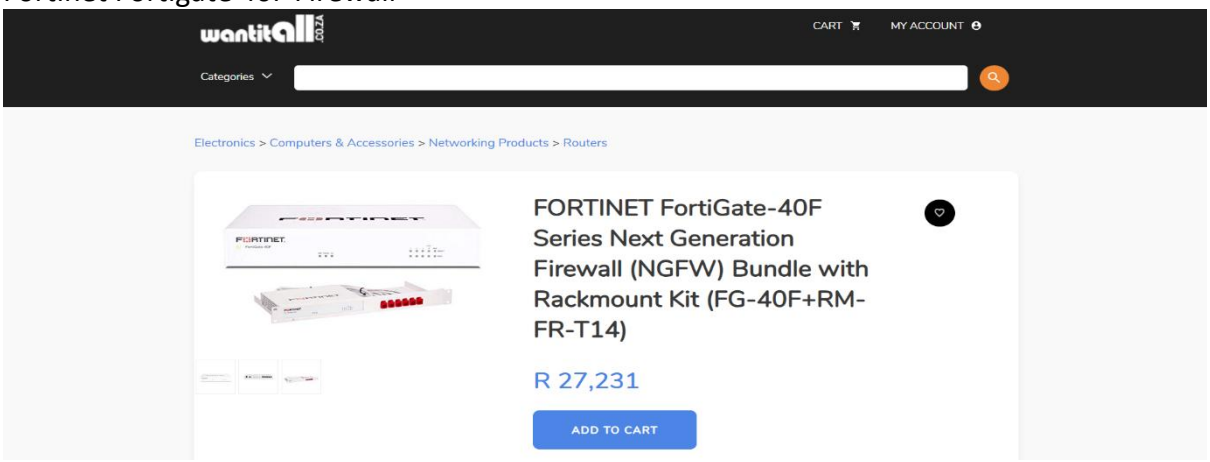
5. CAT6 Ethernet Cable (100m rolls)



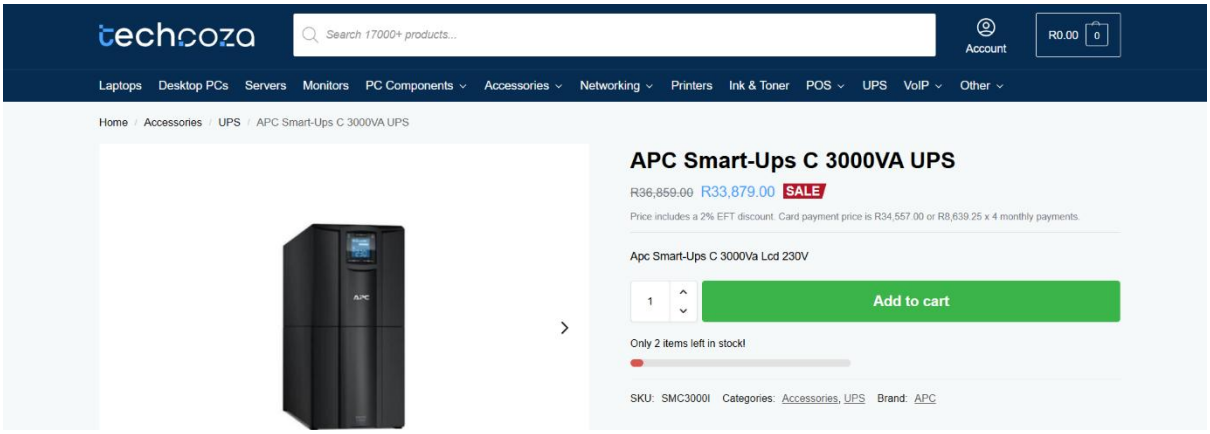
6. Patch Panels, Racks



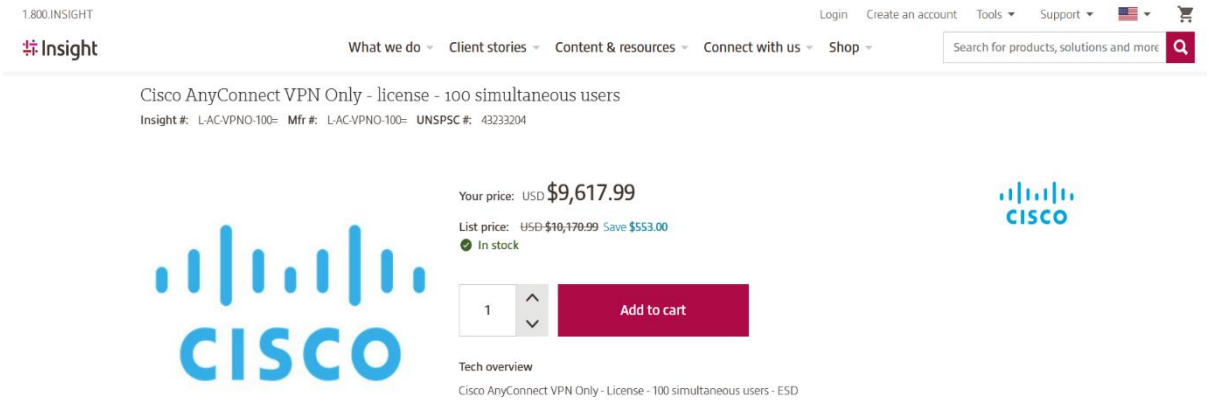
7. Fortinet Fortigate 40F Firewall



8. UPS Backup Systems



9. VPN License (Cisco AnyConnect)



- Subtotal: R826 157.64
- Labour Costs (Technicians 150 hours @ R500/h): R75,000
- Contingency (20%): R133,200

Total Budget: **R1 034 357.64**

4. Remote Group Work

This section contains details on the project group's experiences with conduction the work for this project remotely. The section will start with a discussion of the working procedures/habits/philosophies/assumptions/etc. use/followed/applied by the group, followed by a reflection of the experience.

4.1. Group Modus Operandi when working Remotely

The group had the following methods and procedures when it came to working remotely. Firstly, the group used the following methods:

- Weekly virtual meetings using Microsoft Teams (every Thursday).
- WhatsApp group for quick communication.
- Google Drive for file and document sharing.
- Task allocation: **K Thobejane**
- Networking Setup**: CS Tsetsa** and **K Thobejane**
- Documentation: **LS Mavhungu** and **MP Thabane**
- Budget Research: **DL Zame** and **EM Machete**
- Topology Design: **O Khechane** and **TB Mlambo**

A full record of communications was kept, with meeting dates and summaries.

4.2. Reflection on Remote Group Work Experiences

The group as a whole has difficulties with the remote work aspect of this project. This is due to difficulty in finding times when everyone was free, most group members also struggled with unstable internet connectivity which caused delays.

Although there were some difficulties with the remote work, there are some advantages to it which includes working flexibly from anywhere.

There was one member that liked the collaborative aspect of remote group work and had the following comments: “Being able to contribute at my own pace without needing to commute made the experience more efficient and enjoyable."

4.3 Multiple-solution issues addressed

During the network design process, our group encountered several situations where multiple technical solutions were possible. Below are key examples:

1) **Topology Design – Star vs. Mesh vs. Bus**
   We considered mesh and bus topologies but ultimately chose a hierarchical star topology because it provides better scalability, easier troubleshooting, and stronger fault isolation. While mesh offers redundancy, it was deemed too costly and complex for the size of our network.

2) **Wi-Fi Coverage – Individual APs per room vs. High-Density Centralized APs**
In Section 1 (Open Plan area), we discussed installing one access point per workstation cluster. However, this would be too costly. Instead, we chose strategically placed high-density APs that support more users with minimal performance loss.
3) **Remote Access – VPN Options**
We debated between using OpenVPN, Cisco AnyConnect, and IPSec tunnelling. OpenVPN was selected due to its cross-platform compatibility, ease of configuration, and community support. Cisco AnyConnect was included in budgeting to support enterprise licensing.
4) **Printer Deployment – Centralized vs. Section-Based**
We considered placing all printers in the machine room for central access. However, to reduce congestion and improve user convenience, we installed printers in key sections (e.g., Section 1, Reception), each connected to their respective VLANs.

4.4 ADDITIONAL FEATURES NOT IN PT BUT IMPLEMENTABLE IN REAL-WORLD

In addition to the features implemented in Packet Tracer, the following real-world enhancements are practical, achievable, and contribute to a production-ready network environment:

1) **Endpoint Security and Antivirus Management**
Each device on the network would have centrally managed antivirus software (e.g., Bitdefender or Microsoft Defender). This cannot be simulated in PT but is vital for preventing malware threats.
2) **User Authentication and Access Control**
Real-world deployment would use Active Directory or LDAP for centralized user authentication, with VLAN access policies based on user roles through 802.1X and RADIUS.
3) **Monitoring and Alerting Systems**
A system like Zabbix or SolarWinds would monitor network health and trigger alerts for any anomalies or device failures.
4) IoT Device Management
IoT appliances in the kitchen would be managed via Cisco Kinetic or AWS IoT Core, which are outside PT simulation capabilities.
5) **Firewall Rule Sets and URL Filtering**
The firewall would use intrusion prevention, deep packet inspection, and enforce web content filtering via UTM profiles.
6) **Backup and Disaster Recovery**
File servers and config files would be regularly backed up using cloud or off-site systems like Veeam or AWS Backup to ensure continuity.