**Network Design Project Documentation**

**Group members:**

**Tamandani Stima 42956706**

**Nhlanhla Nwariwe 43511139**

**Sinovuyo Sondara 41434366**

**Panashe K Tarusenga 45204756**

**Orinea Mulaudzi 47639717**

**Siyabonga Mnguni 40987167**

**Kainga Malinga 46583092**

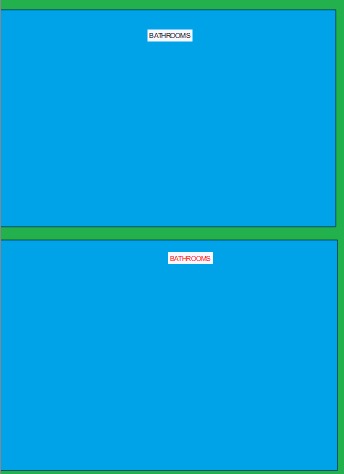
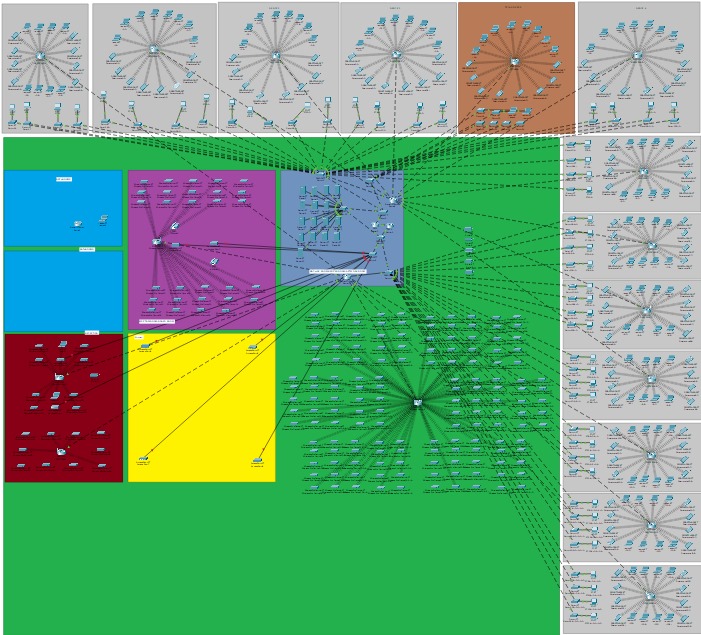
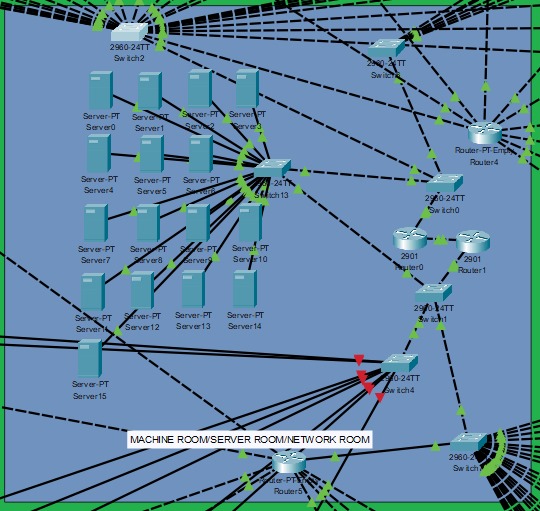
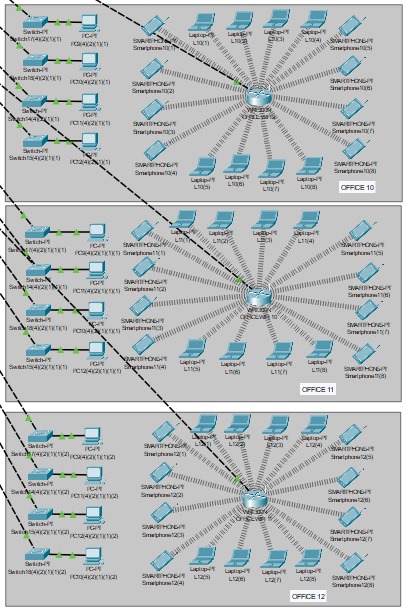
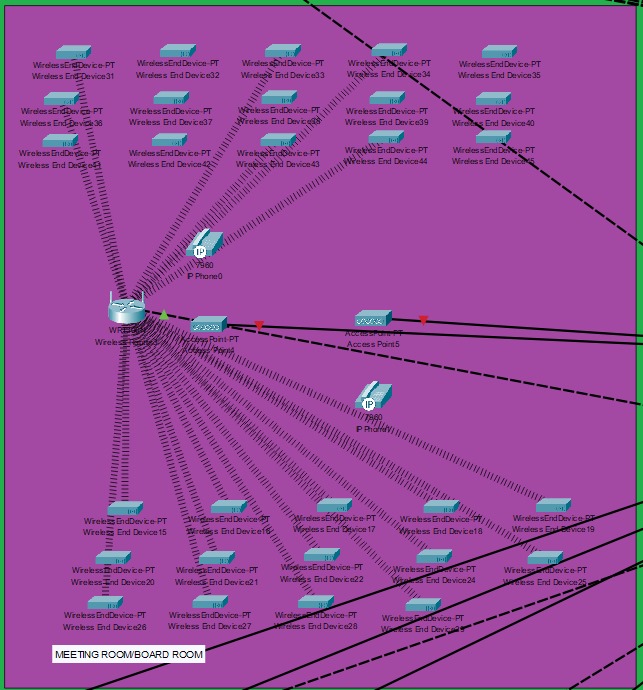
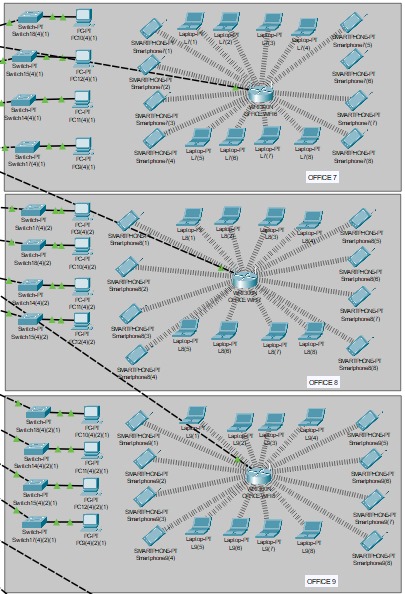
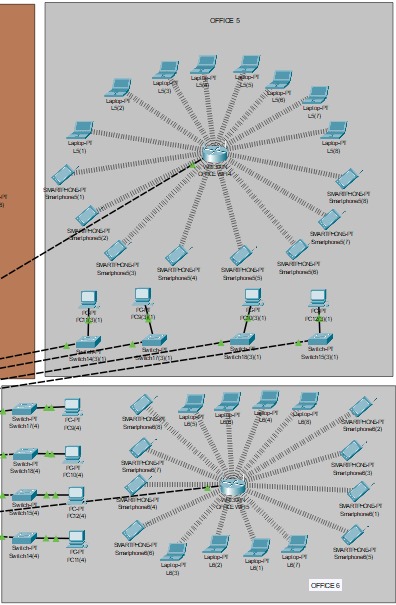
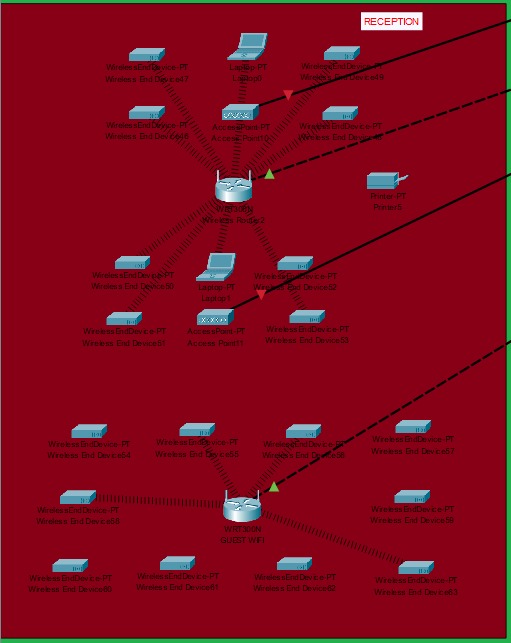
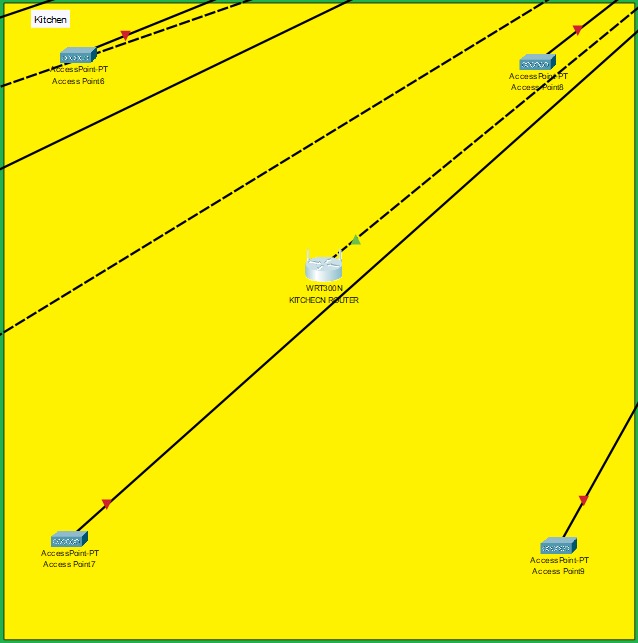
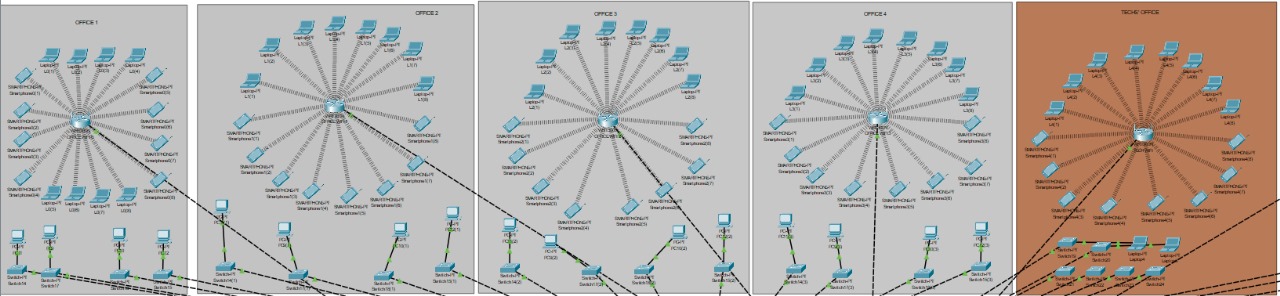
**1. Overview of the Problem**

The company requires a robust and scalable network infrastructure to support approximately **180 employees** and **850–880 total devices** (170 wired and 700 wireless). The network must accommodate:

* **Wired connections** for desktops, printers, IoT devices, and conferencing systems.
* **High-density Wi-Fi** for employees and guests.
* **Remote work capabilities**, including secure access for technicians and staff.
* **Future growth** in device count and bandwidth demands.

**Key Challenges:**

* **Device Density:** Ensuring sufficient wireless coverage for up to 700+ devices.
* **Security:** Segmenting guest and employee traffic to prevent lateral movement threats.
* **Remote Access:** Secure VPN or Zero Trust solutions for work-from-home employees.
* **Scalability:** The network must handle additional devices without major reconfiguration.

**Network Diagrams:** 

**2. Network Topology Design**

The network follows a hub-and-spoke topology for structured communication and efficient resource sharing.

Key Features:

**Dual-Router Redundancy:**

* + Router 1 manages the north section of the building.
  + Router 2 manages the south section.
  + If one router fails, the other ensures partial network availability.

**Centralised Switching:**

* + Each router connects to a core switch, which distributes traffic to departmental switches.

**VLAN Segmentation:**

* + Departments (e.g., Reception, Offices, Guest Wi-Fi) are isolated using VLANs + ACLs.
  + Example: Reception PCs cannot access office networks for security.

**Scalability:**

* + New sections (e.g., a future expansion floor) can be added by connecting to the core switch.

**Device Selection Justification:**

| **Device** | **Reason for Selection** |
| --- | --- |
| **Netgear GS724T Switch** | 24-port Gigabit, VLAN support, and cost-effective. |
| **Ubiquiti UniFi AP AC Pro** | High-density Wi-Fi, seamless roaming, easy management. |
| **Cat6 Cabling** | Future-proofing for 10Gbps, better noise resistance. |

*(Printers and PCs were excluded as they are pre-existing.)*

**3. Budget & Cost Analysis**

**Group Assumptions:**

* Employees: Approximately 180
* Wired Devices: 170
* Wireless Devices: 700
* Total Devices: 850 – 880

### **Tabulated Budget:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Quantity** | **Unit Price (R)** | **Total Price (R)** | **Source** |
| Netgear GS724T 24-Port Gigabit Smart Switch | 10 | 3,400.00 | 34,000.00 | Netgear (2024) |
| Ubiquiti UniFi AP AC Pro | 30 | 2,500.00 | 75,000.00 | Ubiquiti (2024) |
| Cat6 Ethernet Cable (305m roll) | 5 | 627.00 | 3,135.00 | Takealot (2024) |
| HP LaserJet Pro Printer | 6 | 5,599.00 | 33,594.00 | HP Online (2024) |
| Logitech Rally Plus Video Conferencing System | 1 | 96,999.00 | 96,999.00 | FirstShop (2024) |

**Subtotal:** R242,728.00

### **Labour Cost Estimation *(TechTribe IT Solutions – R650/hour)***

|  |  |  |  |
| --- | --- | --- | --- |
| **Task** | **Hours** | **Rate (R)** | **Cost (R)** |
| Network Design and Planning | 10 | 650 | 6,500.00 |
| Hardware Installation | 25 | 650 | 16,250.00 |
| Cabling and Infrastructure Setup | 35 | 650 | 22,750.00 |
| Testing and Troubleshooting | 15 | 650 | 9,750.00 |
| Documentation and Handover | 7 | 650 | 4,550.00 |

**Total Labour Cost:** R59,800.00

Contingency (10% of subtotal): R24,272.80

Grand Total: R326,800.80

**4. Remote Access Solutions**

**Recommended Software:**

* **Remote Desktop (RDP) + VPN (OpenVPN/WireGuard)** for secure internal access.
* **Microsoft Teams/Logitech Rally Plus** for virtual meetings (already budgeted).

**Security Considerations:**

* **BYOD Policy:** Guest Wi-Fi is isolated; employee devices require a VPN.
* **Lateral Movement Prevention:** VLAN segmentation, firewall rules.
* **Zero Trust Option:** Future-proofing with multi-factor authentication (MFA).

**Virtual Workspace Setup:**

* Cloud-based collaboration (Teams, SharePoint) for hybrid work.

**5. Network design**

**Strengths:**

* Scalable for future growth (VLANs, spare ports).
* High-reliability hardware (Ubiquiti, Netgear).
* Secure remote access options.

**Weaknesses & Maintenance Concerns:**

* **Wi-Fi Congestion Risk:** High-density areas may need additional APs.
* **Cabling Complexity:** Cat6 installation requires skilled labour.
* **Most Maintenance Needed:** Wireless APs (firmware updates, interference checks).

**Virtual Office Transition:**

* Core servers, VPN, and cloud services would remain.
* Physical switches/Wi-Fi could be downsized.

**6. Group working procedure/Group Collaboration & Remote Work Management**

**Communication Channels**

Since we worked remotely, we relied on:

**WhatsApp (Primary Communication)**

* + **Text Chats:** Used for quick updates, troubleshooting help, and file sharing.
  + **Voice Calls:** Held structured meetings (1–2 per week) to discuss progress, roadblocks, and next steps.

**GitHub (Collaboration & Version Control)**

* + Used to **share, edit, and track changes** to the Packet Tracer file.

**Advantages of Our Approach:**

**Flexibility:** Async communication allowed members in different time zones to contribute.  
**Transparency:** GitHub logs provided a clear history of changes.  
**Accountability:** Regular WhatsApp check-ins kept everyone on track.

**Challenges & Solutions:**

**Delayed Responses:** Some members were slower to reply.

* **Fix:** Set deadlines for feedback (e.g., "Review PR by EOD").
* **GitHub Learning Curve:** A few members were new to Git

**7.Work Ethic & Collaboration Methods**

**A. Task Delegation**

The **Group Leader (Tama)** assigned tasks based on roles.

**B. Progress Tracking**

* **Weekly WhatsApp Updates:** Each member summarised completed tasks.
* **GitHub Milestones:** Used to track major phases (e.g., "Phase 1: Subnetting Complete").

**C. Conflict Resolution**

**Technical Disagreements** (e.g., switch selection) were resolved via:

* 1. **Group Vote** (majority ruled).
  2. **Research Backup** (e.g., comparing specs/costs).

**Missed Deadlines:** Addressed privately first, then escalated to the leader if unresolved.

**8. Challenges & Lessons Learned:**

**A. Limited Router Ports**

**Problem:**

* Physical router ports were insufficient for all VLANs/departments.

**Solution:** **Router-on-a-Stick**

* Created **subinterfaces** on a single router port.
* Each subinterface handles a VLAN (e.g., Gi0/0.10 for VLAN 10, Gi0/0.20 for VLAN 20).

**Benefits:**

* + No extra hardware costs.
  + Better port utilisation.

**B. Access Point (AP) Management**

**Problem:**

* Devices auto-connected to all APs, cluttering the **Packet Tracer physical view**.

**Solution:**

1. **Disabled APs during setup** to avoid auto-connections.
2. **Staggered activation:**
   * Configured one AP at a time.
   * Assigned unique SSIDs per VLAN (e.g., Staff-WiFi, Guest-WiFi).

**C. Packet Tracer Performance Issues**

**Problem:**

* Lag when simulating **700+ devices** (PCs, phones, IoT).

**Solutions:**

1. **Simplified Simulations:**
   * Tested sections individually (e.g., only the open floor).
   * Used **"Fast Forward Time"** to speed up simulations.
2. **Device Grouping:**
   * Represented dense areas with **a few PCs + a note**

**D. Wireless Router Configuration Challenges**

**Problem:**

* Packet Tracer's **GUI interface** restricts default gateway IP addresses and overwrites CLI/Config tab settings if used afterward.

**Solution:**

1. **Followed a strict configuration order:**
   * **Step 1:** Complete all wireless settings (SSID, security) via the **GUI first**.
   * **Step 2:** Configured IP addresses/subnets via the **Config tab** afterwards.

**E. Security Implementation on a Budget**

**Problem:**

* No dedicated firewall due to budget constraints.
* Firewall devices and/or routers can handle security in the network. Due to the company's limited budget, security is dealt with via routers as they are already required within the network topology.
* Security is handled via ACLS, which requires secure connections within the company's network, limits access to wired devices, and ensures that all devices can communicate with the internet.

**Solution:** **Router-Based Security**

1. **Access Control Lists (ACLs):**
   * Blocked inter-VLAN traffic (e.g., guests can’t access HR VLAN).
   * Allowed only wired devices to access internal servers.
2. **NAT & PAT:**
   * Enabled on routers for internet access.
3. **Port Security:**
   * Restricted switch ports to specific MAC addresses.

**Conclusion**

The **hub-and-spoke topology** proved effective for scalability and fault isolation. Key takeaways:

1. **Router-on-a-stick** saved costs and simplified VLAN routing.
2. **AP management** requires staged activation to avoid chaos.
3. **Packet Tracer limitations** demand creative workarounds for large networks.
4. **GUI/Config tab order** is critical for wireless router setups.
5. **ACLs on routers** can replace firewalls in budget-constrained scenarios.

### **References:**

* Netgear (2024). GS724T Switch. Available at: [https://www.netgear.com](https://www.netgear.com/)
* Ubiquiti (2024). UniFi AP AC Pro. Available at: [https://www.ui.com](https://www.ui.com/)
* Takealot (2024). Cat6 Ethernet Cable (305m roll). Available at: <https://www.takealot.com/cat6-utp-network-cable-305m/PLID71783339>
* HP Online (2024). HP LaserJet Pro Printer. Available at: <https://www.hponline.co.za/collections/laserjet-printers>
* FirstShop (2024). Logitech Rally Plus System. Available at: <https://www.firstshop.co.za/products/logitech-rally-plus-group-video-conferencing-system>
* TechTribe IT Solutions (n.d.). Services and Rates. Available at: <https://www.techtribe.co.za/services/> [Accessed: 29 April 2025]