Project Report: Building a Secure Startup Network for Chege Innovations

Author: Samuel Chege

Date: September 20, 2025

1. Introduction: The Problem with Flat Networks

Every new business starts somewhere, and for "Chege Innovations," that meant a small office with a handful of employees. The immediate need was simple: get everyone online. The easiest solution is a flat network a single switch connecting everyone to the internet. While simple, this approach is riddled with security and performance issues. There's no separation between departments, meaning a malware infection in Sales could quickly spread to critical IT infrastructure. It's the digital equivalent of an open-plan office with no walls or locked doors.

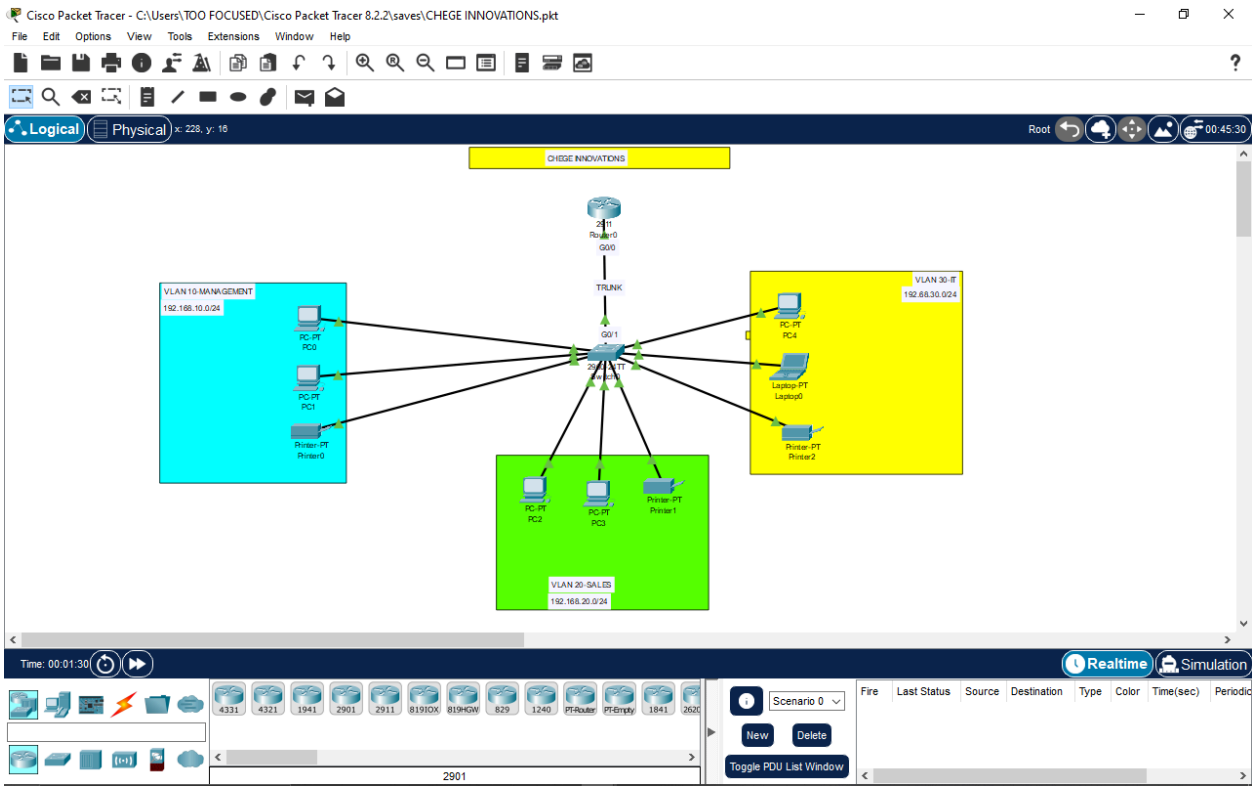
This project tackles that exact problem. The goal was to design and implement a secure, segmented, and scalable network foundation for this growing startup using Cisco Packet Tracer. We aimed to build a network that not only works but works *securely*, laying the groundwork for future growth and protecting company assets from day one.

2. Methodology: From a Blank Canvas to a Secure Network

This section details the step-by-step process of building the network, explaining the "why" behind each configuration choice.

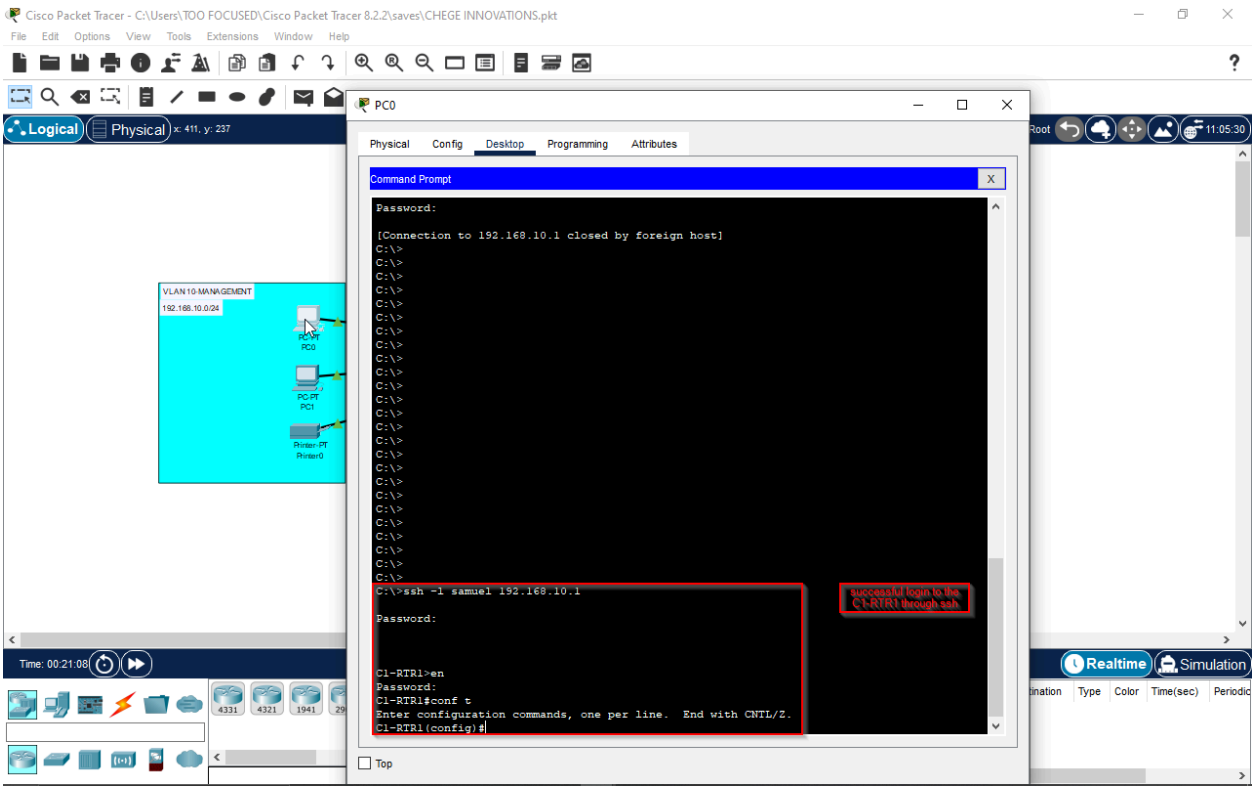
Phase 1: Topology and Foundational Security

Before any network traffic could flow, we had to lay the groundwork. The physical topology was designed for simplicity and function, consisting of a single router, a switch, and end devices representing three distinct departments.



With the devices in place, the first and most critical step was foundational hardening. Default settings are an open invitation for trouble. We applied a secure baseline to both the router and the switch, which included:

- **Setting unique hostnames (`CIRTR1` & `CI-SW1`).**
- **Securing privileged mode with an encrypted secret password.**
- **Securing console access with a password.**
- **Enabling SSH for secure, encrypted remote management** after creating a local user and generating RSA keys. This prevents eavesdropping on management sessions.

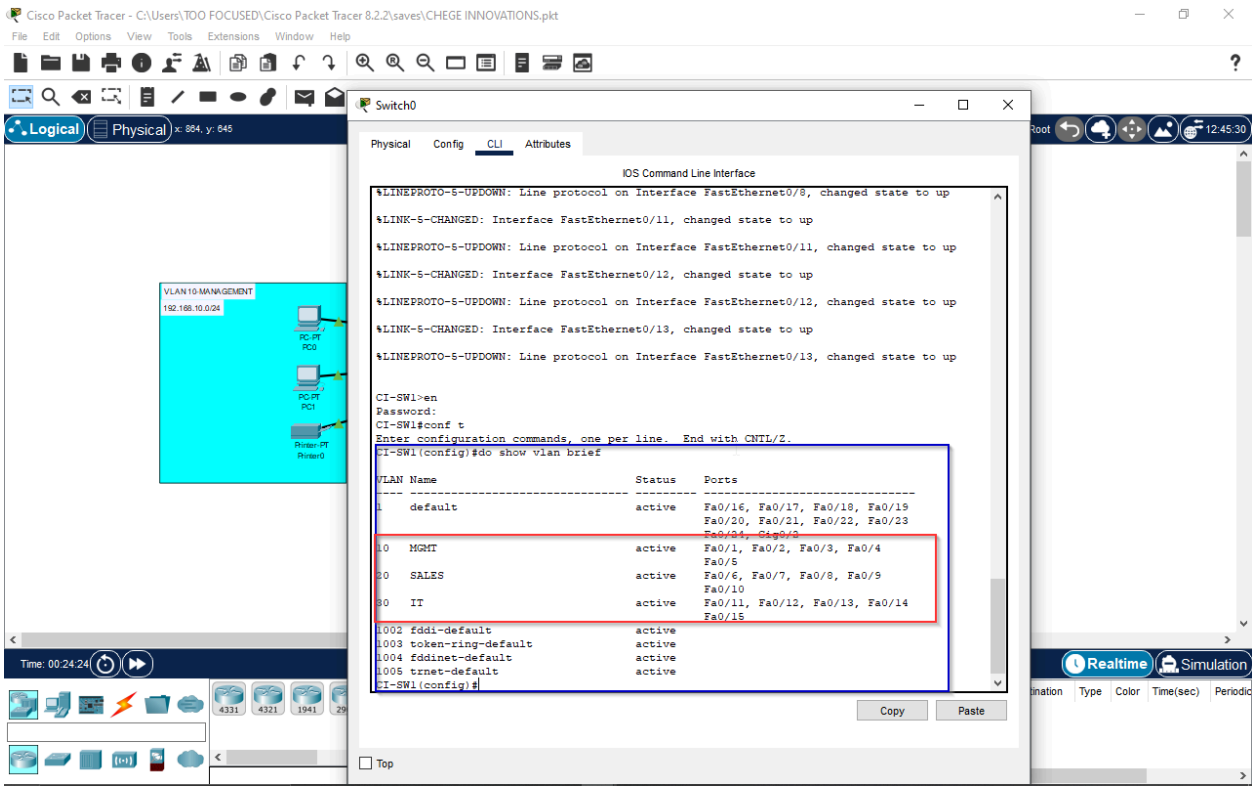
- 

Phase 2: Network Segmentation with VLANs

To solve the "flat network" problem, we implemented Virtual Local Area Networks (VLANs). VLANs act as virtual walls inside our switch, logically segmenting the network into isolated broadcast domains. We created three:

- **VLAN 10:** MANAGEMENT
- **VLAN 20:** SALES
- **VLAN 30:** IT

After creating the VLANs, we assigned switch ports to them, effectively placing each employee's computer into the correct virtual "room."



Phase 3: Enabling Communication with Inter-VLAN Routing

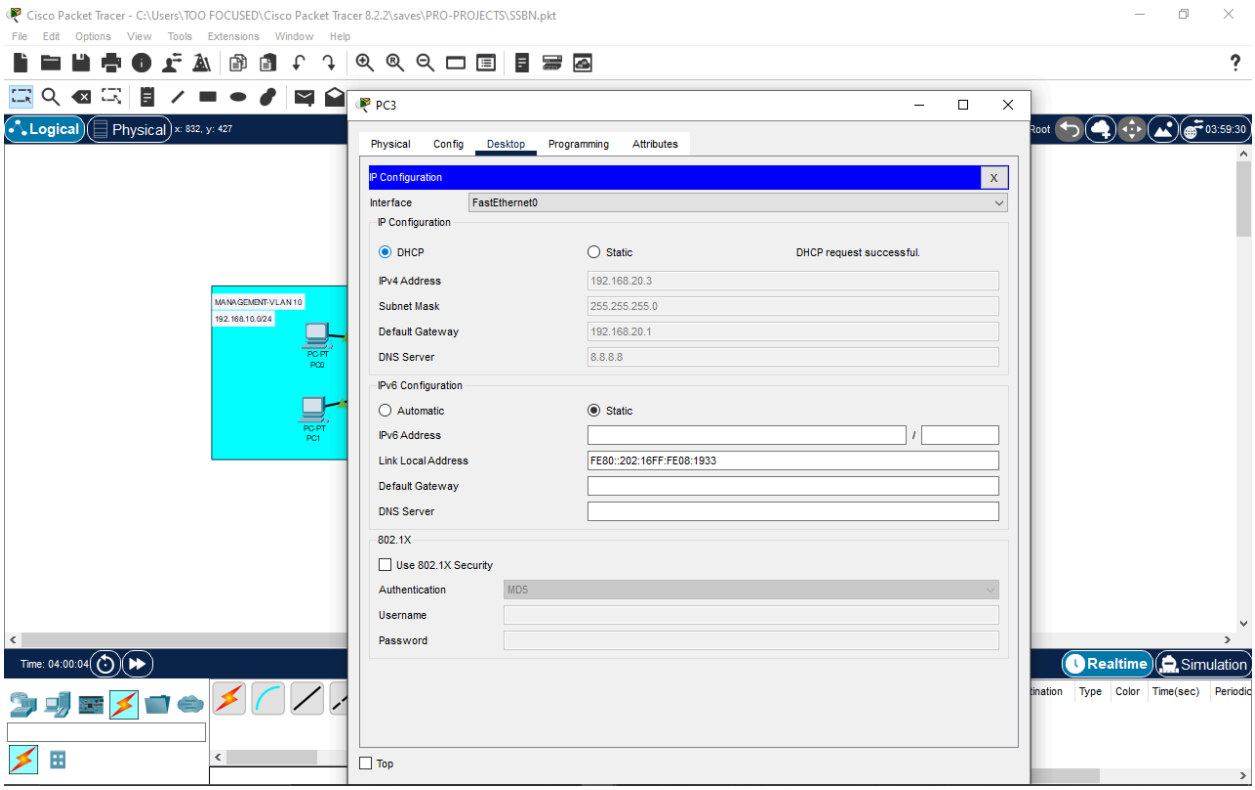
Segmentation is great for security, but departments still need to communicate in a controlled way. A Layer 2 switch can't handle this, so we enlisted our router. Using the **"Router-on-a-Stick" (ROAS)** method, we configured the single link between the switch and router as a trunk.

On the router, we created virtual subinterfaces for each VLAN, assigning each one an IP address to serve as the default gateway for its respective network. This configuration allows the router to receive tagged traffic from the switch, make a routing decision, and send the traffic back to the correct destination VLAN.

Phase 4: Automating IP Addressing with DHCP

Manually assigning IP addresses to every device is tedious and prone to human error, as we discovered during a troubleshooting session involving a duplicate IP. To automate this, we configured the router to act as a **DHCP server**.

We created a separate DHCP pool for each VLAN, ensuring that any device plugging into a specific department's port would automatically receive a correct IP address, subnet mask, and default gateway. We also excluded the gateway addresses from each pool to prevent conflicts.

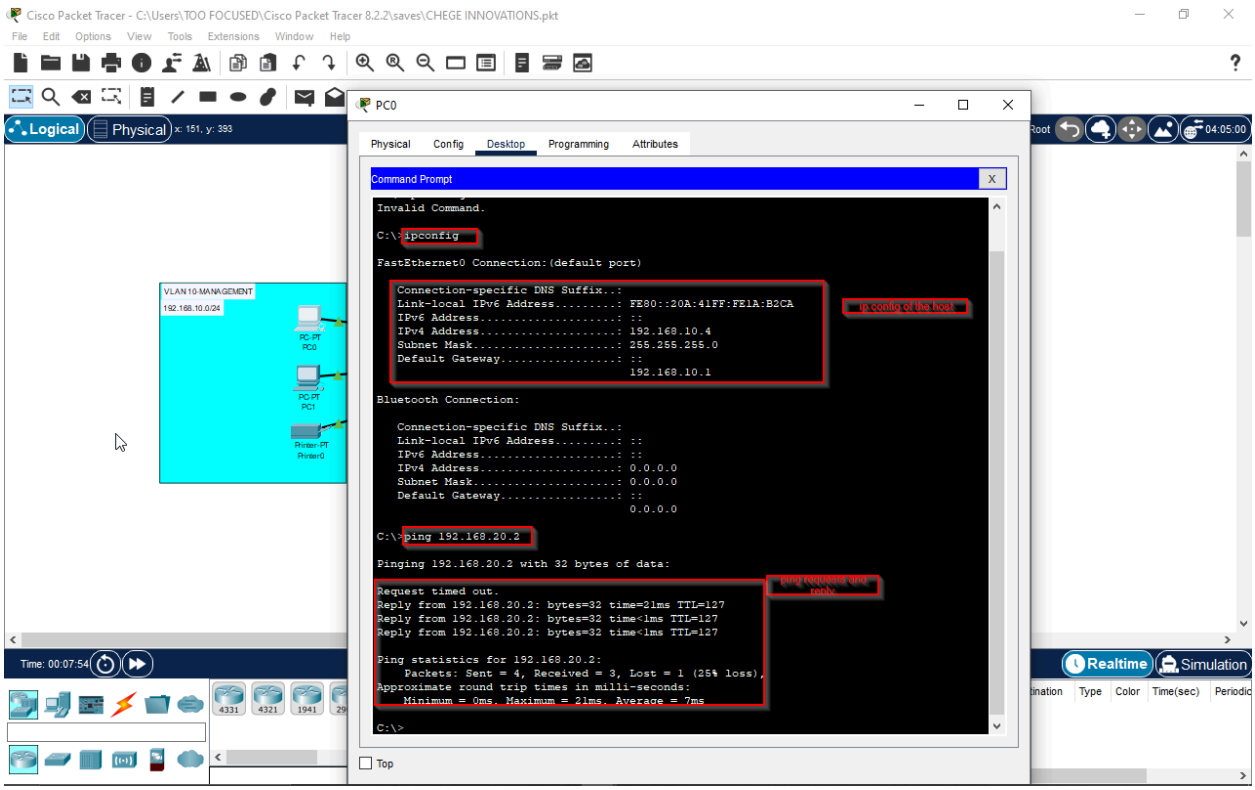


Phase 5: Locking Down the Ports

To prevent unauthorized users from simply plugging a laptop into an unused network jack, we enabled **Port Security** on all access ports. By configuring the ports to "stick" to the first MAC address they learn, we ensured that only the designated company devices could gain network access. If a violation occurs, the port automatically shuts down, alerting an administrator to a potential security breach.

3. Conclusion: A Foundation Built for Growth

The successful implementation of this network architecture transformed the insecure flat network of Chege Innovations into a secure, segmented, and efficiently managed environment. The final verification test—a successful ping between PCs in different VLANs—confirmed that all technologies were working in concert.



This project was a practical exercise in core networking principles that are directly applicable to my career goal in Cloud Security. The VLAN segmentation we implemented is the on-premise equivalent of creating VPCs and subnets in AWS or Azure. Understanding how to control traffic flow with routing and secure access at the port level are foundational skills for building secure cloud infrastructures. The troubleshooting we encountered, from Packet Tracer bugs to a duplicate IP address conflict, was an invaluable lesson in diagnostic methodology and the importance of meticulous verification.

This network isn't just a lab; it's a blueprint for a secure and scalable small business, ready for the challenges of the future.