Title: Secure Network Architecture Design Report

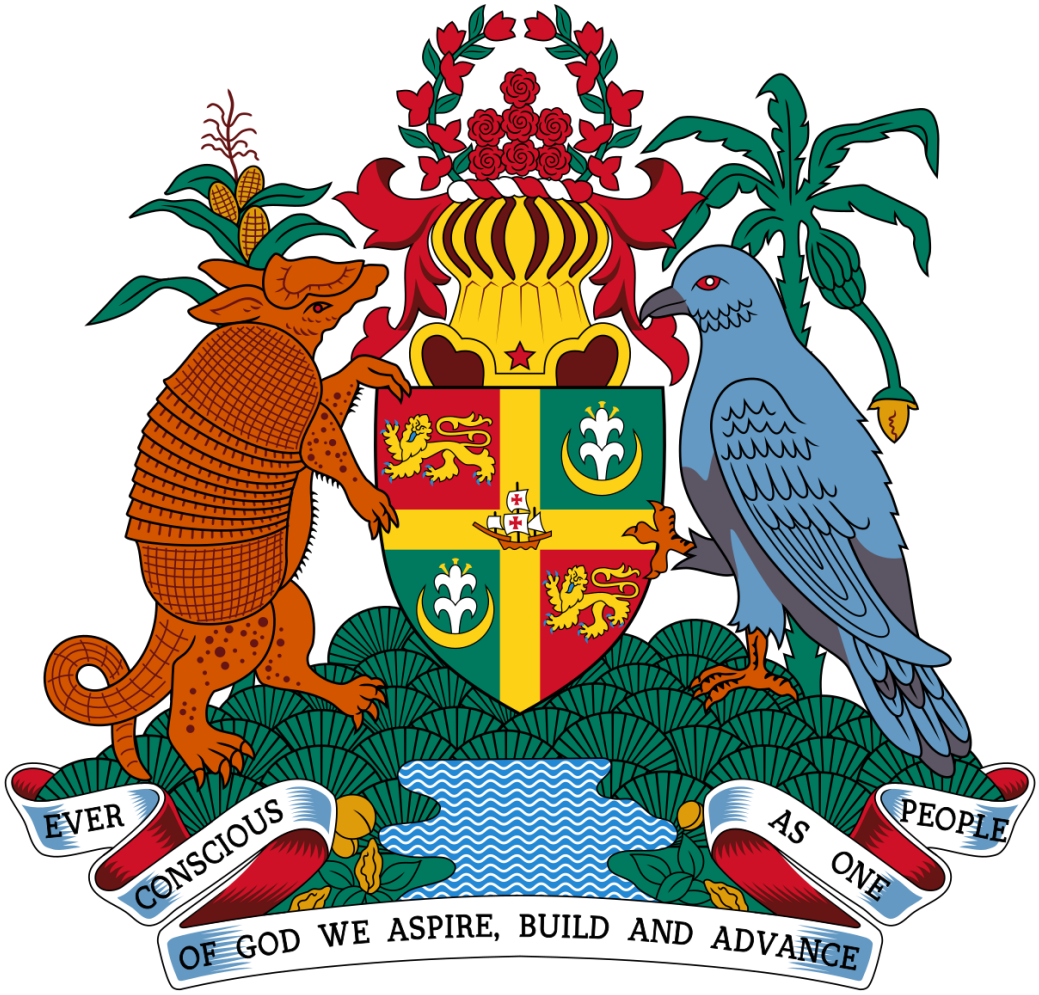
Subtitle: A Resilient and Scalable Infrastructure for the Ministry of Education, Youth, Sports & Culture

Student Name: Ahndre Walters

Cohort: Cyber Nations Grenada – Cohort 1

Ministry Designed: Ministry of Education, Youth, Sports & Culture

Submission Date: May 9, 2025



Declaration: I certify that this submission is my original work and complies with the guidelines for this assignment.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report outlines the proposed design for a secure, scalable, and resilient network infrastructure for the Ministry of Education, Youth, Sports & Culture. The solution is built with modern cybersecurity principles in mind, ensuring that ministry operations remain safe from cyber threats such as ransomware, while still allowing staff to work efficiently and collaboratively.

The network is structured to support key ministry services, including secure internal communications, departmental separation, guest wireless access, and centralized server management. The design incorporates redundancy and high availability to ensure continuous operation and scalability to accommodate future growth.

NETWORK TOPOLOGY OVERVIEW

The Ministry's network follows a **redundant star topology**, connecting various departments through **access switches** to **core switches**. This layout ensures each department operates independently but remains securely interconnected. The redundancy ensures that even if one connection fails, the system will continue to function without disruption. The **core switches** play a vital role in managing traffic between departments, and **VLANs** have been implemented to keep each department's network traffic separate for better performance and security.

Network Topology Overview:

Department	VLAN ID	Subnet	Purpose
Minister's Office	10	192.168.10.0/24	Executive staff access
Finance & Admin	20	192.168.20.0/24	Financial and administration services
IT Department	30	192.168.30.0/24	Network and Server Management
Public Relations	40	192.168.40.0/24	Media and communications
Internal Services	50	192.168.50.0/24	HR, logistics, and procurement
Guest Wi-Fi	60	192.168.60.0/24	Internet-only access for visitors
Servers	99	192.168.99.0/24	Critical servers and services

The network is segmented into multiple VLANs to ensure isolation, better manageability, and enhanced security. Each department has its own VLAN, and each VLAN is associated with a unique subnet.

KEY NETWORK DEVICES

To build a reliable and efficient network, we have selected a set of high-performance networking devices, including **routers**, **switches**, and **servers**, each serving specific roles in the overall infrastructure. These devices will be carefully configured to ensure seamless connectivity and security.

Key Network Devices:

Device Type	Model	Purpose
Router	Cisco 2911	Handles inter-VLAN routing and ACLs
Core Switches	Cisco 2960-24TT	Provides redundancy and distribution
Access Switches	Cisco2960-24TT	Connects departments to core switches
Servers	Server-PT	DHCP, DNS, Mail, and App services
End Devices (PCs, Laptops)	PC-PT, Laptop-PT	User endpoints in different departments
Wireless Router	Cisco WRT300N	Provides secure guest Wi-Fi access

These devices work together to ensure optimal network performance while providing scalability and flexibility for future expansions.

VLANs and Subnetting

The Ministry's network has been divided into different VLANs for each department, ensuring traffic separation and enhanced security. VLANs help to segment network traffic, thus limiting access to sensitive information and preventing congestion.

- Each department is assigned a specific **VLAN**, with its own dedicated **subnet**. This ensures smooth, secure, and isolated traffic between departments, as well as simplified management and troubleshooting.
- Additionally, **subnetting** provides efficient use of IP addresses, ensuring there is no wastage while also making it easier to manage the network.

CORE INFRASTRUCTURE SERVICES

For the Ministry's network to run efficiently and securely, several **core infrastructure services** have been put in place, such as **DHCP**, **DNS**, **Mail**, and **Application Servers**. These services are responsible for handling key tasks like IP address allocation, domain name resolution, and internal communications.

Core Infrastructure Services:

Service	Hostname	IP Address	Purpose
DHCP Server	DHCP-Server	192.168.99.10	Assigns IPs to departments
DNS Server	DNS-Server	192.168.99.13	Resolves internal and external names
Mail Server	Mail-Server	192.168.99.11	Manages ministry emails
App Server	App-Server	192.168.99.12	Runs internal applications

Each of these services is essential to the network's operation, ensuring that devices receive the appropriate IP addresses, can resolve domain names, and maintain secure email communication.

NETWORK SECURITY AND FIREWALL RULES

Security is paramount in this network design. Several **firewall rules** and **Access Control Lists (ACLs)** are enforced to control the flow of traffic and limit unauthorized access.

Firewall Rules:

The firewall will permit only necessary traffic, and any attempt to access critical resources outside of the allowed traffic will be blocked. This configuration ensures that only authorized users and devices can access sensitive resources.

Firewall and ACL Rules

Rule #	Protocol	Port(s)	Source	Destination	Action	Reason
1	UDP	53	VLANs 10-50	DNS Server	Allow	DNS lookups for all departments
2	UDP	67-68	VLANs 10-50	DHCP Server	Allow	Automatic IP assignment
3	TCP	25	Internal VLANs	Mail Server	Allow	Internal email traffic
4	TCP	8080	Internal VLANs	Application Server	Allow	Access to ministry web apps
5	ICMP	Any	VLAN 30 (IT only)	Any	Allow	Network testing (ping, traceroute)
6	ANY	Any	Guest VLAN	Internal VLANs	Deny	Ensures guest isolation

The default firewall policy is “deny all”, meaning only allowed traffic can pass. Inter-department traffic is limited unless explicitly needed.

REDUNDANCY AND HIGH AVAILABILITY

The Ministry's network architecture has been designed for **redundancy** and **high availability**. The use of **dual core switches** and **EtherChannel links** provides multiple paths for traffic in case of hardware failure. This ensures that the network remains operational even during failures.

Redundancy Features:

- **Dual Core Switches:** In case one core switch fails, the other one will continue to handle traffic without disruption.
- **EtherChannel Links:** These links provide increased bandwidth and ensure that if one link fails, the remaining links will continue to support traffic.

This redundancy guarantees the Ministry’s network remains available and reliable.

SCALABILITY

The network design is built with scalability in mind. The VLAN-based segmentation allows easy addition of new departments or devices without disturbing the current network structure. This flexibility means that as the Ministry grows or new departments are added, the network can scale to meet these needs.

Scalability Features:

- New **VLANs** can be added for additional departments.
- **Access switches** can be connected to the core switches, providing more ports for additional devices.
- The **IP address scheme** allows for easy allocation of new addresses as needed.

BALANCE BETWEEN SECURITY AND OPERATIONS

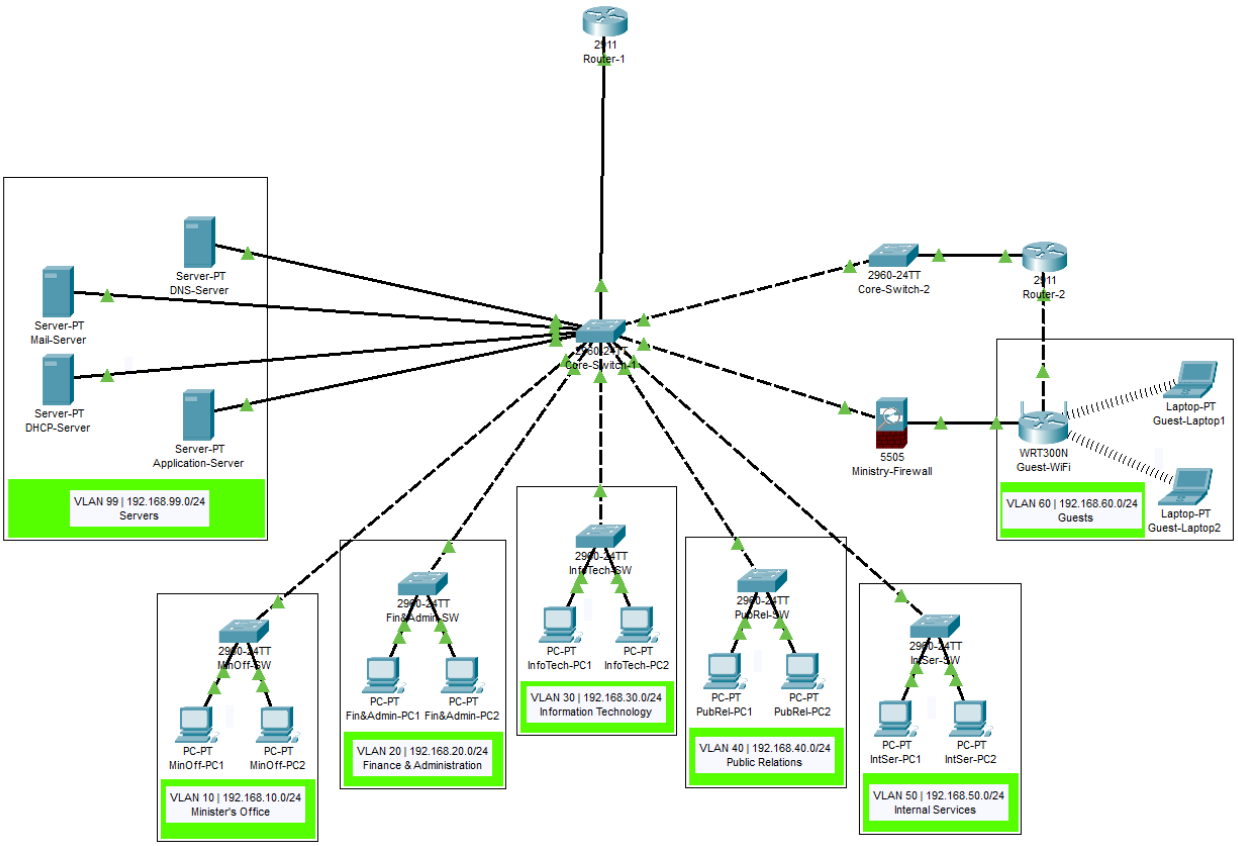
This design strikes a balance between maintaining **strong security** and ensuring **smooth operations**. While strict security measures are implemented, they do not hinder the usability or performance of the network. For example, the use of **guest VLANs** ensures that visitors can access the internet without compromising internal resources. At the same time, the **internal departments** are securely segmented through VLANs.

The design balances **strong security** with **smooth daily operations**:

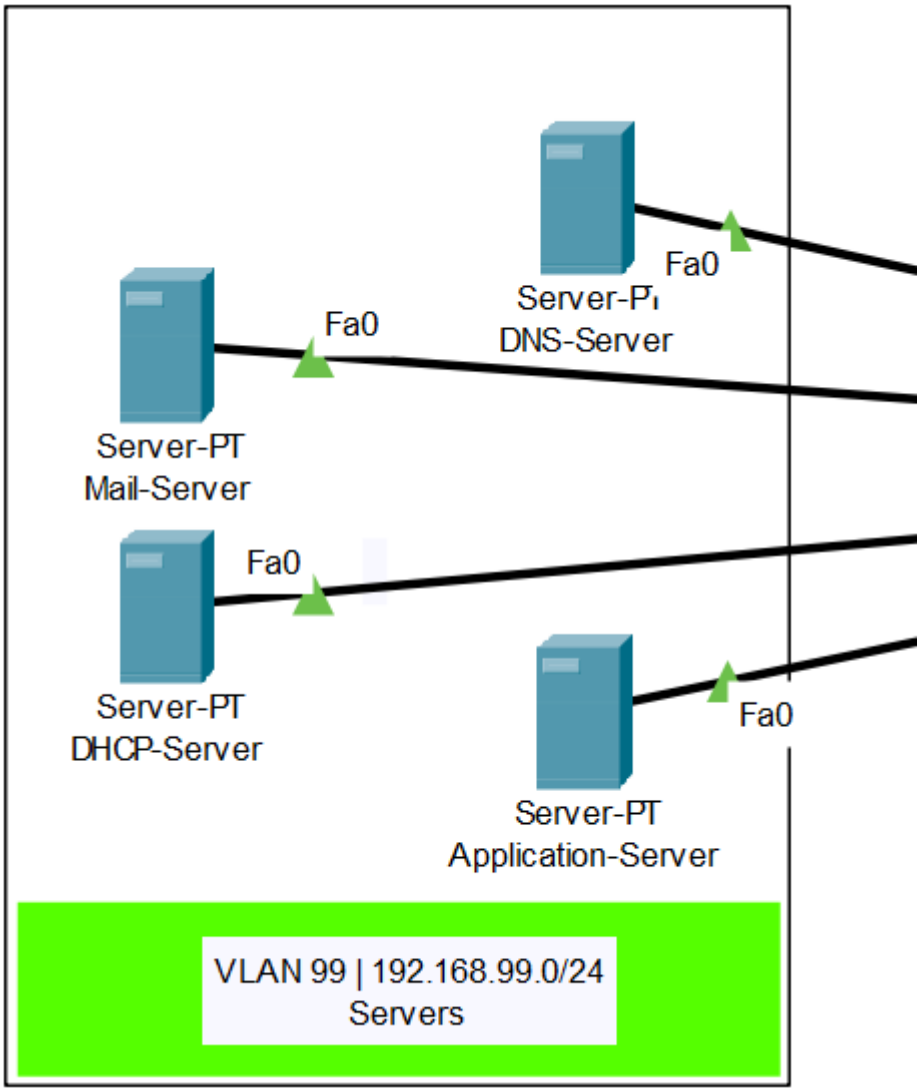
- VLAN separation keeps sensitive departments isolated
- Guest Wi-Fi is separate from internal systems
- IT can still troubleshoot using tools like ping and traceroute
- Access control ensures no one has more access than they need

VISUALS OF NETWORK DESIGN & CONFIGURATION

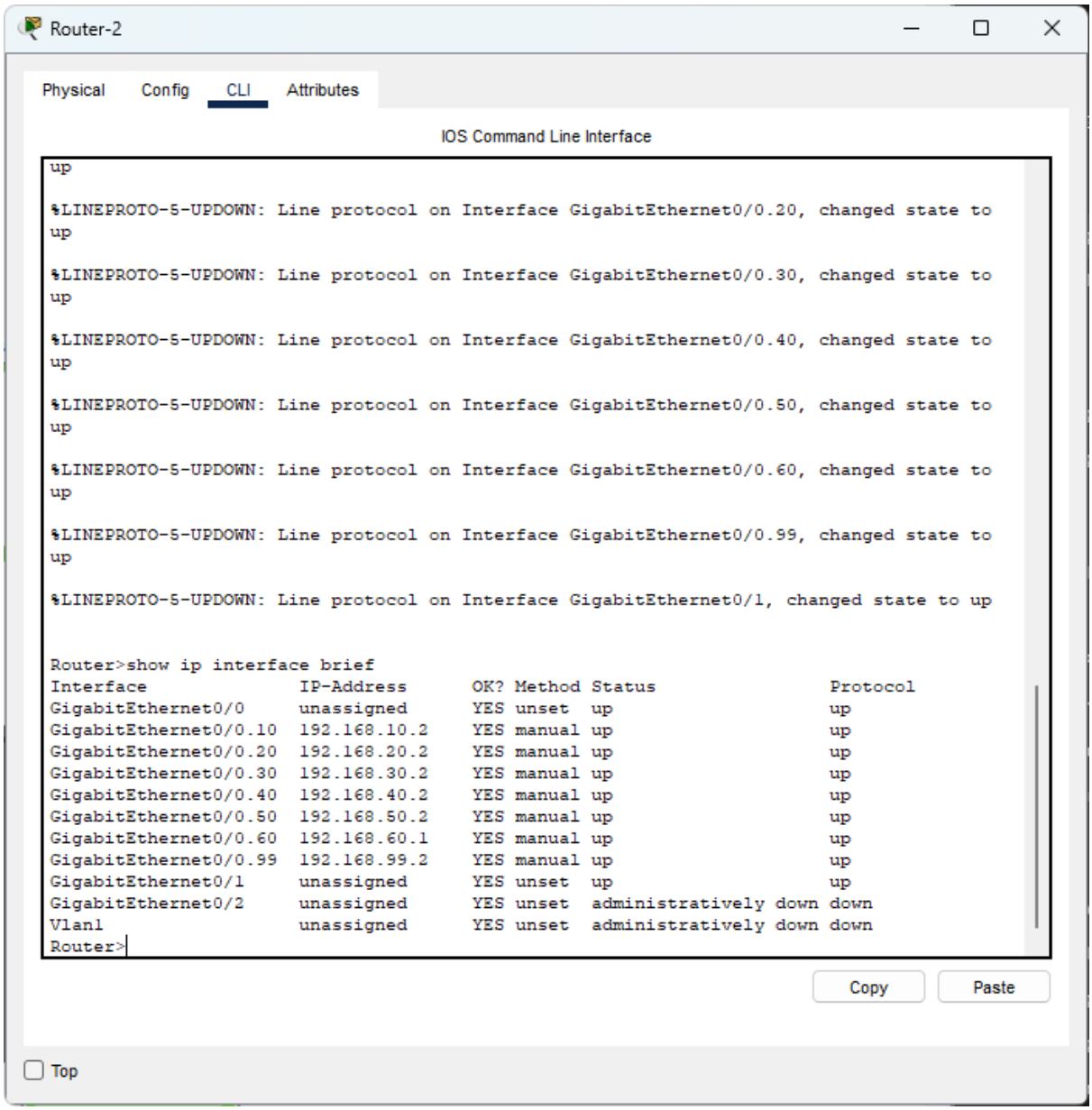
Complete Network Topology with Devices, IPs, and VLANs



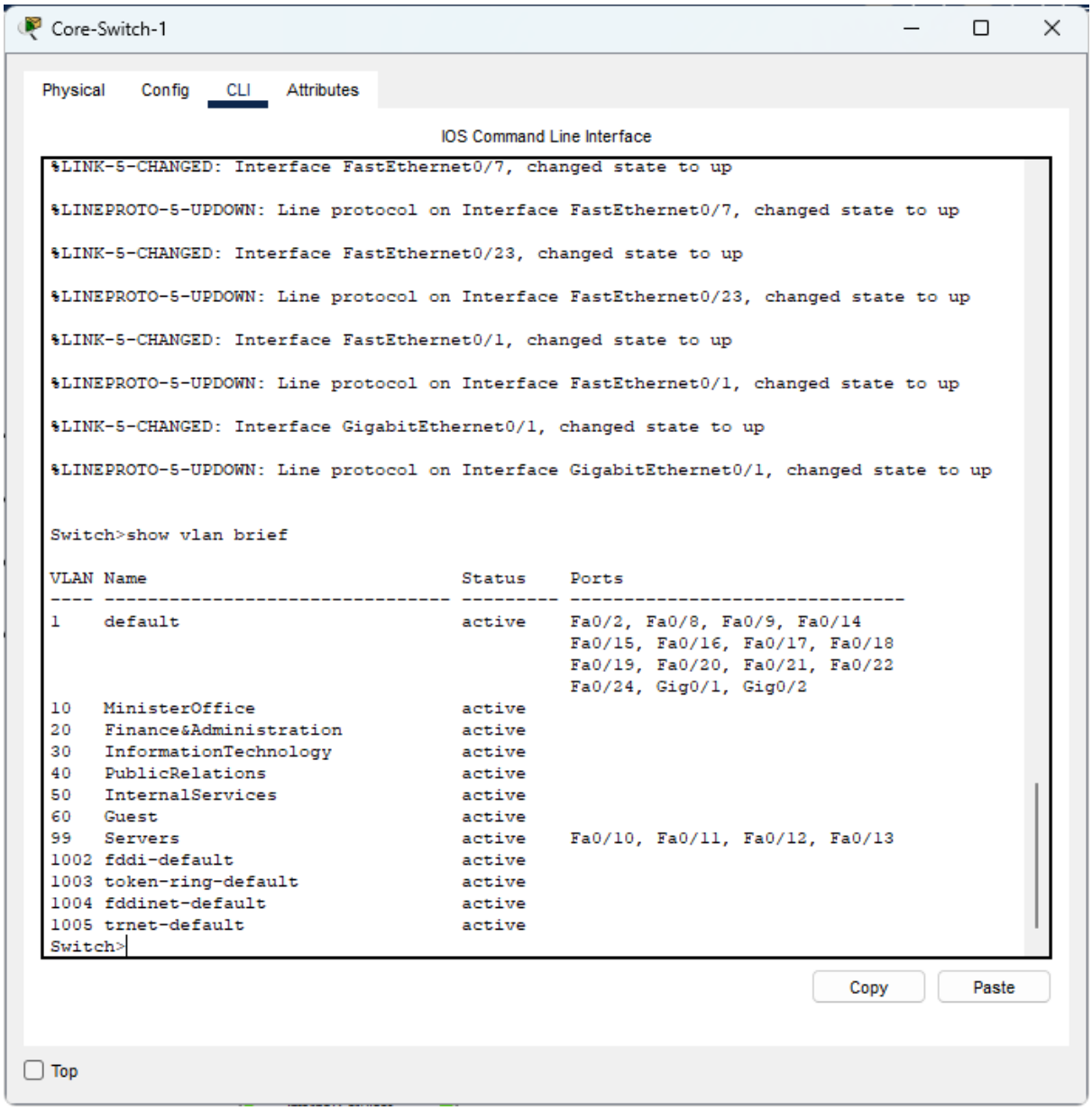
Core Infrastructure View – VLAN 99 Servers



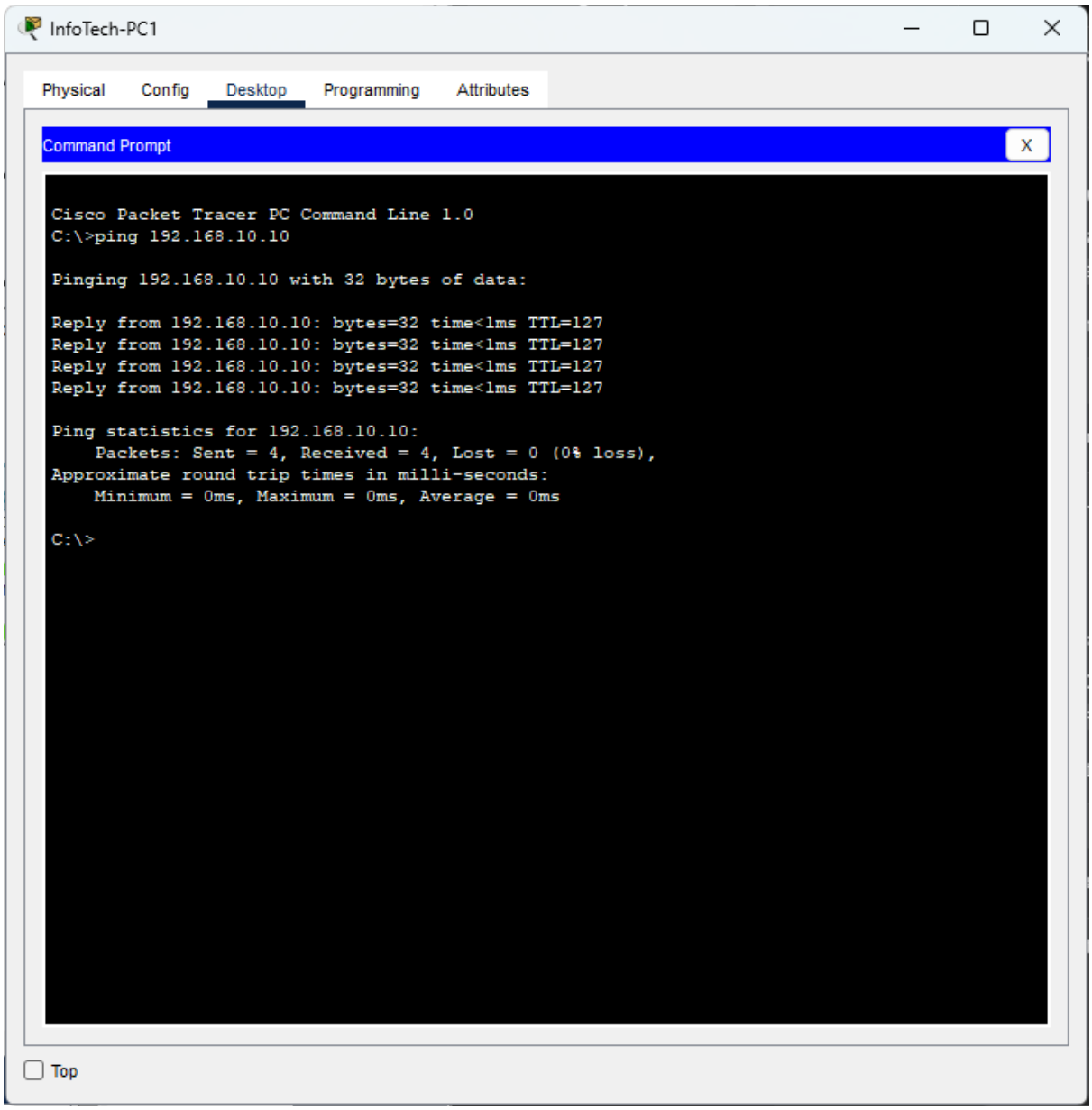
Router CLI Output – IP Interface Brief



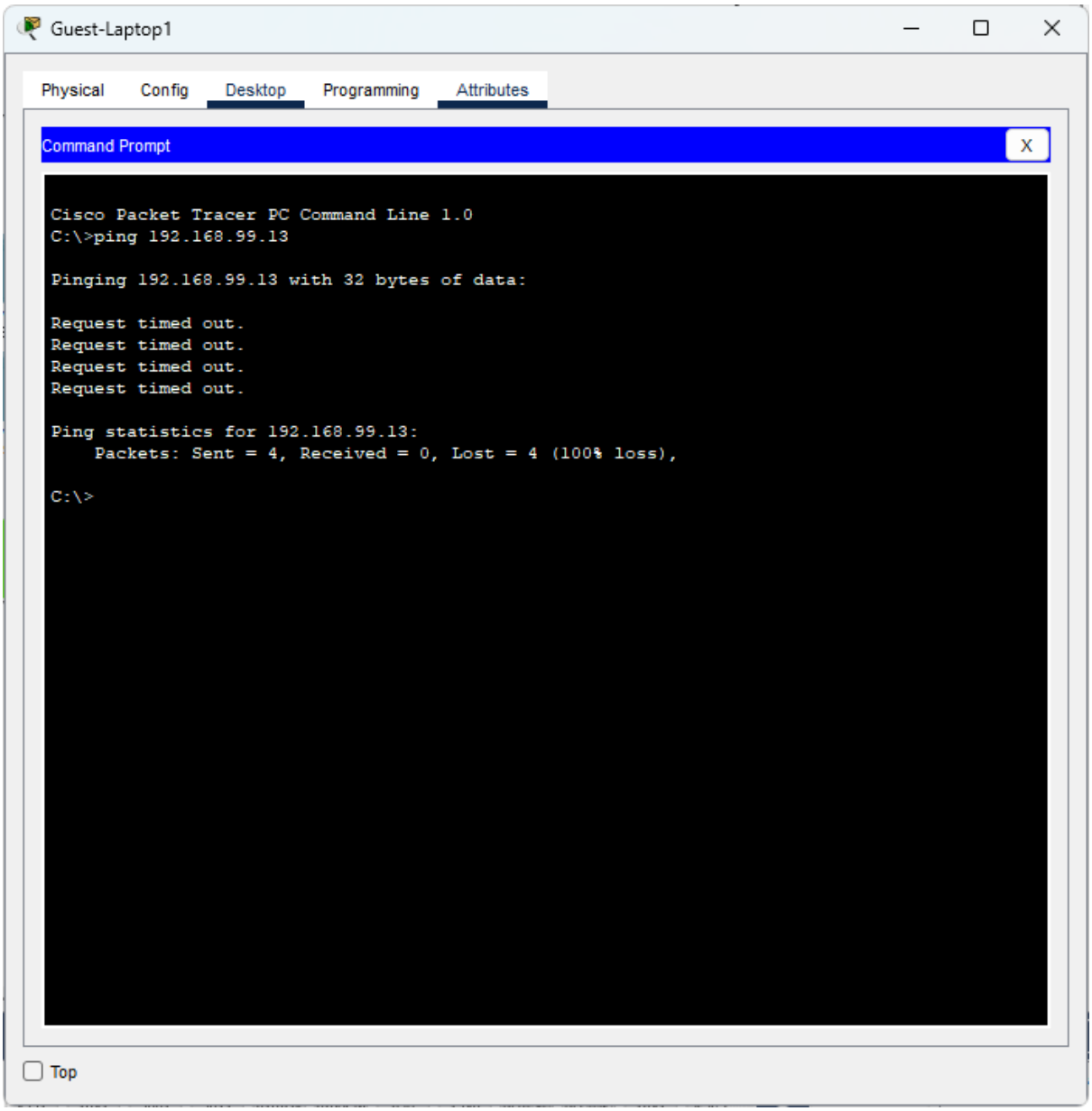
Core Switch CLI Output – VLAN Brief



Ping Test – PC-IT-1 Successfully Reaches Mail Server (192.168.99.10)



Ping Test – Laptop-Guest-1 Blocked from Reaching Application Server (192.168.99.13)



CONCLUSION

In conclusion, this network design offers a secure, scalable, and highly available solution for the Ministry of Education, Youth, Sports & Culture. It meets both current and future needs while ensuring that sensitive data and critical resources are well-protected. By implementing VLANs, subnetting, security protocols, and redundancy measures, the design provides a solid foundation for the Ministry's network operations. The architecture ensures secure, efficient, and reliable operations, supporting collaboration while adhering to modern cybersecurity standards. With these measures in place, the Ministry is better prepared to protect sensitive information, support day-to-day functions, and withstand cybersecurity threats such as ransomware and unauthorized access.