Juan Dominguez
Salissa Hernandez
Noah Nyabadza

Project 1: Secure Multi-Tier Network for a Small Educational Institution

Introduction

For our project, we designed and simulated a secure and scalable multi-tier network for a small school campus using Cisco Packet Tracer. The objective of the project was to build a realistic hierarchical network that supports multiple operational zones, including administrative offices, faculty departments, student labs, and guest Wi-Fi areas. A Core-Distribution-Access Architecture was implemented to provide high performance, efficient routing, and secure segmentation between network segments. This framework allows us to address scalability, performance, and layered security across different types of users and devices within the campus setup.

The network architecture was structured into three functional layers. For the Core Layer, a dual Cisco 2911 router and one Layer 3 switch were employed to facilitate inter-VLAN routing, external connectivity, and redundancy. The Distribution Layer consolidated department LANs and imposed ACL-based traffic control between VLANs. The Access Layer offers end device connectivity, wireless access points, server connectivity, and comprised endpoint security features such as port security and DHCP snooping. The three-layered configuration was simpler to manage, improved performance, and enabled particular security policies on each layer.

The completed network included two core routers, two Layer 3 distribution switches, and four Layer 2 access switches for administrative, faculty, student, and guest zones. Two wireless access points were added to implement student and guest Wi-Fi networks. Approximately twenty PCs and laptops were used as end hosts, and two servers were configured, one as a web and email, and the other as an authentication server. Firewall policies and ACLs were employed on routers and switches to segment internal networks and control perimeter traffic.

Motivation

The project was selected since educational institutions require robust and secure network infrastructures to support academic and administrative functions. Campuses have numerous user communities with various access needs; therefore, there is a need to provide solid connectivity as well as good network partitioning. By modeling an average school network, we were able to practice concepts addressed in class, including hierarchical network design, VLAN segmentation, access control, and redundancy, while meeting real-world performance and security demands.

Methodology

The methodology of the project incorporates the design, configuration, and testing of a secure and scalable multi-tier campus network on Cisco Packet Tracer. It was followed step by step to include VLAN and IP address configuration, routing configuration, DHCP and server

configuration, security configuration, and complete testing to ensure the network met all function and security needs.

To divide the network logically, separate VLANs were created for the server, admin, faculty, student, and guest networks. Each VLAN used a separate IP subnet to enable the correct addressing and inter-VLAN routing. For example, the admin VLAN used 10.0.10.0/24, the faculty VLAN used 10.0.20.0/24, the student VLAN used 10.0.30.0/24, the guest VLAN used 10.0.40.0/24, and the server VLAN used 10.0.50.0/24. Switched Virtual Interfaces (SVIs) were configured on the Layer 3 switches to enable inter-VLAN routing in the distribution layer. PCs and servers were allotted static IP addresses based on their own VLANs, administrative and server machines were allotted static addresses to maintain management uniformity, and faculty, student, and guest hosts were allotted their addresses dynamically through DHCP. This allowed logical partitioning between user groups as well as enabled controlled communication between them.

For routing, OSPF was employed on the distribution switches and the core routers to maintain dynamic routing and redundancy within the network. All subnets of VLAN were advertised into the OSPF routing process, and it would permit routes to automatically propagate and inter-VLAN communications efficiently. Redundancy was achieved by configuring the two core routers with the same-cost OSPF routes so that traffic would be forwarded through the other router if one of the routers became unavailable. A default route was configured on the core routers to facilitate connectivity to the outside cloud so that internal devices could access external networks while traffic was maintained on the network border.

To support network services, DHCP pools were installed on every VLAN router with the exclusion of the server VLAN, which used static IP addressing. This allowed faculty, student, and guest computers to automatically acquire their IP configurations. The web and email server was configured with limited HTTP and DNS services to provide internal available resources accessible for administrative and faculty networks, while the authentication server was deployed to provide device and wireless centralized authentication. All these services contributed to establishing a realistic campus environment with automated addressing, internal resource hosting, and central security management.

Security took center stage throughout the deployment. ACLs were used at the distribution and core layers to manage inter-VLAN traffic, disallowing student access to the administrative network while allowing faculty access to servers and restricting guest users to internet access. VLAN segmentation isolated different groups of users, and DHCP snooping was enabled for protection against unauthorized DHCP servers. Port security was implemented on administration and faculty access switches to limit the number of MAC addresses allowed per port. SSH and strong passwords were utilized to lock down all network devices to replace insecure administrative practices such as Telnet. Firewall-like ACLs were implemented on the edge routers to block incoming and outgoing traffic between the internal network and the external cloud, creating a secure perimeter and protecting valuable assets.

After the installation was completed, extensive testing was performed to verify that the network was performing as anticipated. Inter-VLAN communications were tested using ping and traceroute to verify that valid traffic traversed as anticipated and that ACLs would successfully block unauthorized access. DHCP functionality was also verified by ensuring that devices within faculty, student, and guest VLANs received valid IP addresses from their assigned pools. SSH was verified from admin hosts to provide secure device management, and server availability was verified to provide accessibility for faculty and administrative users to internal resources while limiting guest users appropriately. Redundancy was verified by powering down one of the core routers and verifying that OSPF dynamically routed traffic through the alternate path.

Through this systematic approach, a complete, finished, secure, and scalable school campus network simulation was established. Every stage of the process, from VLAN design and routing, down to service configuration, security hardening, and testing mapped onto real enterprise network design practices and kept the end network aligned with operational and security objectives.

Results & Testing

After deploying the network completely, extensive testing was carried out to ensure that all the equipment worked as required and met the design specifications. Ping and ACL tests were employed to ensure inter-VLAN communication and policing of traffic. Authorized messages, such as faculty PCs connecting to the server network, were successful, while unauthorized ones, such as student-to-admin traffic, were successfully denied by applied ACLs. DHCP operations were confirmed by observing that devices in faculty, student, and guest VLANs were automatically getting valid IP addresses from their corresponding DHCP pools, with dynamic and consistent addressing throughout the network. SSH remote connectivity was successfully established from admin PCs to switches and routers and thus confirming secure remote administration via secure protocols as opposed to insecure protocols like Telnet.

Server access testing validated that the administrator and faculty of user accounts were granted internal web and DNS services, while the guest account was appropriately restricted from internal services and only given external internet connectivity. Redundancy testing was also conducted by shutting down one of the primary routers, and OSPF redistributed the traffic to the other active router dynamically, giving complete network access without discernible packet loss. These results reaffirmed that the network attained its functional, security, and reliability goals, attesting to the success of the employed hierarchical and layered security paradigm.

Workload Distribution

Our team divided the workload equally and each of us contributed our own segment of the project. We each had an area that we were responsible for but collaborated with one another in each phase to make sure the network all fit well together.

Juan focused on creating the core layer of the network. He set up the two Cisco 2911 routers, created OSPF routing, gave redundancy to the core devices, and connected the network to the outside cloud. He also focused on including the routing with the distribution layer so that inter-VLAN communication was secure.

Salissa was responsible for the VLAN design and the access layer. She created and assigned VLANs for administrative, faculty, student, guest, and server networks, set up the Switched Virtual Interfaces (SVIs) on the Layer 3 switches, and applied the IP addressing plan across the network. She also set up the DHCP services to provide dynamic addresses and helped to set up the servers hosting web, DNS, and authentication services.

Noah focused on security and testing. He used the ACLs to control traffic between VLANs, port security, and DHCP snooping in access switches, and secured all the network devices through SSH and strong authentication. He also carried out the testing process, checking inter-VLAN communication, DHCP assignment, server availability, ACL filtering, and OSPF failover to ascertain that everything worked as required.

We worked together on the initial design of the topology, reviewed each other's setups, came up with the final report, and created the presentation video. Sharing tasks evenly allowed us to have valuable input and a clear understanding of the entire network.

Summary & Conclusion

The simulation and successful implementation of this secure multi-tier network validated the applicability of real-world networking principles to a systematic academic project. Using a hierarchical Core–Distribution–Access architecture allowed the team to create a scalable and efficient network that supported multiple groups of users with varying access requirements. Through VLAN partitioning, OSPF routing, DHCP configuration, and layer-level security policies, the network achieved reliable connectivity, logical separation, and access restriction between departments and user areas. Authentication, web, and DNS server provisioning added realism and utility to the test bed, simulating the services one would expect in a live campus environment.

Testing and verification confirmed that the network met all the design specifications. Inter-VLAN routing performed as expected, DHCP assigned addresses in multiple VLANs dynamically, and ACLs performed efficiently in enforcing access controls between users. SSH access ensured secure management of network devices, while OSPF provided redundancy and rapid failover. All the components were working in place, verifying the functionality of the team's design configurations and choices.

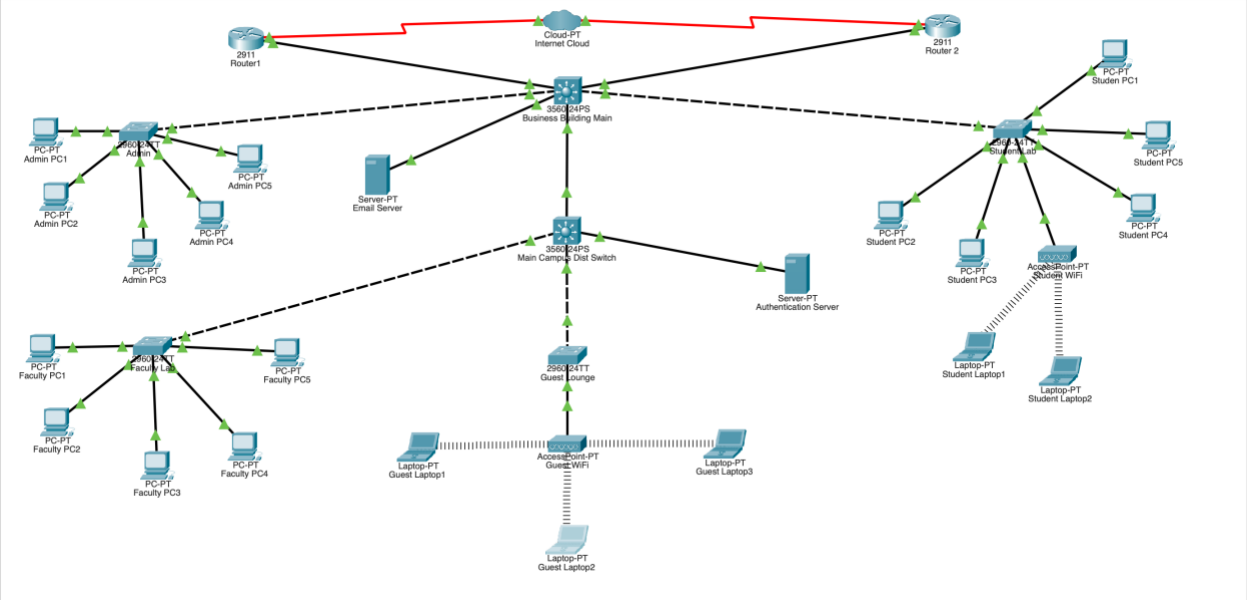
The project not only highlighted the importance of secure and scalable design but also involved practical experience applying enterprise networking concepts. The project enhanced our team's understanding of bringing performance, manageability, and security together into a single architecture. Overall, the project achieved its objectives by delivering a working, secure, and

stable school network simulation, a feat that demonstrated good technical implementation and effective collaboration from all members of our team.

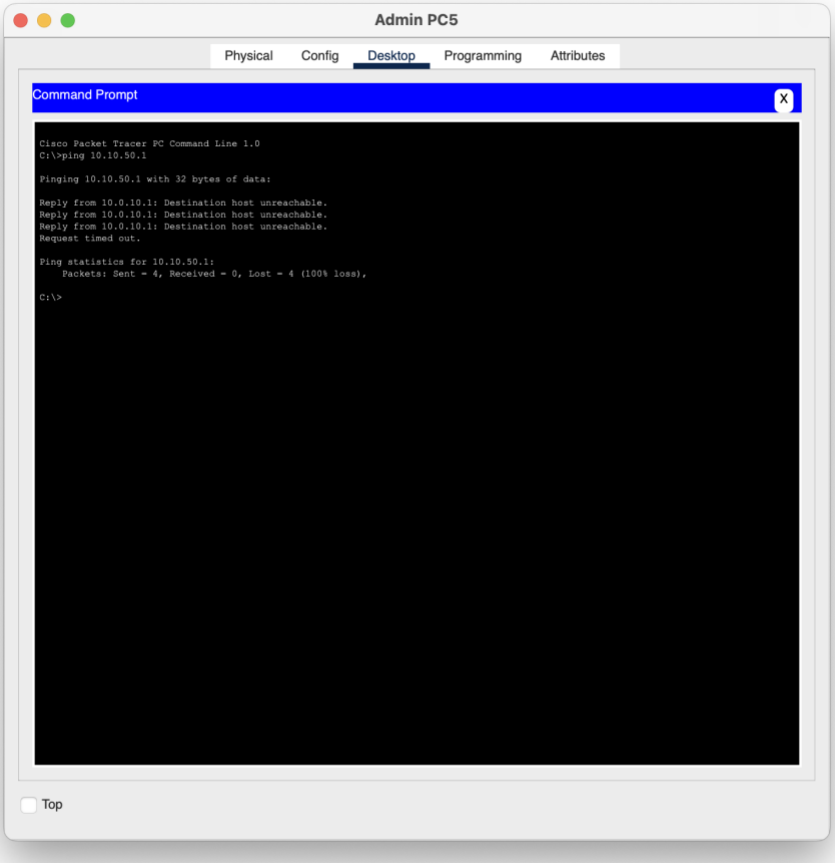
Video Link

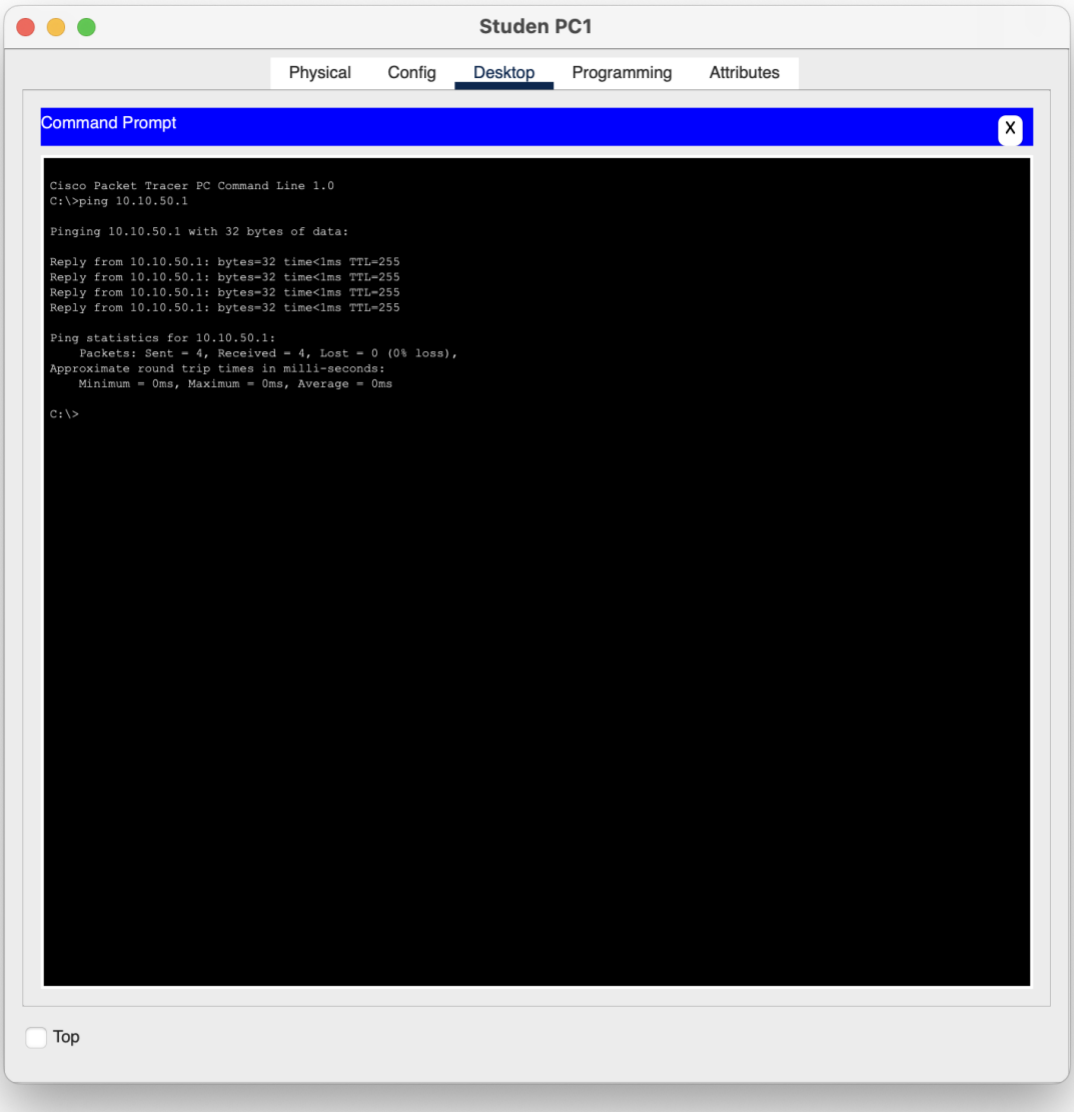
https://drive.google.com/file/d/1RI8Ubn_0HqnnA2eEHKvPqOBLweL-1JLV/view?usp=sharing

Topology Image



Testing Images


Admin PC5
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.50.1
Pinging 10.10.50.1 with 32 bytes of data:
Reply from 10.0.10.1: Destination host unreachable.
Reply from 10.0.10.1: Destination host unreachable.
Reply from 10.0.10.1: Destination host unreachable.
Request timed out.
Ping statistics for 10.10.50.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top


Studen PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.50.1
Pinging 10.10.50.1 with 32 bytes of data:
Reply from 10.10.50.1: bytes=32 time<1ms TTL=255
Reply from 10.10.50.1: bytes=32 time<1ms TTL=255
Reply from 10.10.50.1: bytes=32 time<1ms TTL=255
Reply from 10.10.50.1: bytes=32 time<1ms TTL=255
Ping statistics for 10.10.50.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top