ITNET03 Case Study

Phase 2

Alonzo IT Training Center (AITC) Documentation

Submitted by:

Abanes, Enzo Miguel N.

Bolima, Dave Aldwin L.

Go, Aldrich Matthew S.

Lim, Shaun Tristan Y.

Submitted to:

Ms. Katrina Ysabel Solomon

April 11, 2024

Table of Contents

1. Introduction

As the world becomes more connected, businesses require a more reliable and powerful network system. As such, this case study outlines the comprehensive expansion of Alonzo IT Training Center (AITC), a small IT school offering professional IT training courses. The school comprises a population of an Operations department, IT department, Services VLAN, Management department, Instructors department, Students, and Guests. This also includes the renting of an additional floor. The proposed network design aims to address critical requirements and challenges faced by the company, ensuring enhanced scalability, connectivity, security, support for wireless connectivity, and the ability to back up their configurations. This consists of better management capabilities for the network due to an increasing number of devices, a dedicated server for DHCP, a new server dedicated to network management tasks, the use of Gigabit Ethernet ports and EtherChannel for a more reliable and high-performance network, Hot Standby Router Protocol for increased redundancy and resilience, additional equipment to account for redundancy, wireless connectivity configured with AITC network access policies, monitoring, logging and management capabilities Orion through the use of Syslog, NTP, and SNMP, and the implementation of Access Control Lists or ACLs for added security.

The primary contents of this case study include a short introduction, physical layout, physical topology, logical topology, IP addressing scheme, security configuration, and device running configuration.

1. Physical Layout: The physical layout of the network infrastructure is pivotal for efficient operations, encompassing the arrangement of devices, cabling, and equipment within the premises. Careful considerations were given to factors such as cable routing, device placement, and physical resource utilization to ensure a secure and organized environment. The floor plans, which detail the physical layout of the network, can be found in the next section. Both the first floor's and second floor's floor plan can be found in this section.

2. Physical Topology: The physical topology defines the actual layout of the network components, including switches, layer 3 switches, routers, servers, wireless controller, light access point, printers, and host devices. Given the requirements of AITC, a three-layer hierarchical model consisting of the access layer, distribution layer, and core layer, can be found. A device interconnection table which provides a list of each network device's interfaces and the corresponding devices connected can also be found in this section.

3. Logical Topology: The logical topology focuses on the flow of data within the network, irrespective of its physical placement. It consists of proper user grouping implemented through VLANs with inter-VLAN routing enabled and managed through VTP. It also encompasses the configuration of WLAN support, correctly grouped according to the VLAN membership of their owners and following their same access policies as their wired counterparts. The logical topology represents all infrastructure devices (routers and switches), servers and network printers; and includes a representative PC for each department present

on a switch and indicates their host names and IP addresses. This topology also shows the use of high-speed links and aggregation where suitable for increased bandwidth and fine-tuning of STP where applicable for efficient data flow throughout the network to improve network performance. In addition, fault tolerance was implemented through EtherChannel and HSRP for redundancy. Support for wireless connectivity was also shown in the topology.

4. IP Addressing Scheme: A well designed IP addressing scheme is paramount to facilitate smooth communication between devices. Utilizing the IPv4 address space 192.168.0.0/20, a common subnet will be assigned to the departments within the organization. The departments on the first floor are the Operations department, IT department, Services VLAN, Management department, Instructors department, Students, and Guests. Meanwhile, the departments on the second floor consist of Operations, Services, Instructors, Students, and Guests. The subnet is sufficiently sized to accommodate the expected doubling of company size while ensuring a consistent address assignment scheme, with the consideration that each member will bring in at least 1 personal device that can connect to the organization wireless network. An IP Addressing Assignment Table that displays each device's hostname, IP address, subnet mask, default gateway, and the VLAN these are part of can be found in this section.

5. Security Configuration: In an era of increasing cyber threats, robust security measures are non-negotiable. Initial device settings -that is, housekeeping for routers and switches were configured following best practices to ensure manageability and security. Additionally, remote access to infrastructure devices were provided, as well as use of layer 2 security measures, such as adding a blackhole VLAN for unused ports, changing the default native VLAN, disabling DTP, enabling DHCP Snooping, DAI, and port-security commands, to protect switch operations, safeguarding against unauthorized access and data capture. A table showing the requirement and security measures implemented as well as the enable secret, console, VTY and VTP can be found in this section. BPDU Guard was also implemented to prevent spanning-tree loops in the topology. Finally, access to the WLANs are protected with a password and access to the WLC is protected with a password as well. CDP and LLDP were also disabled. ACLs were also implemented to prevent unauthorized access to certain VLANs.

Scope and Assumptions:

The scope of this network redesign focuses on what was built on the network made for ITNET02 (Xcite Interactive) for the various departments within the company, with WLANs and high-performance network logical addressing, scalability, intranet connectivity, basic security, and manageability. This case study assumes that the existing physical infrastructure can support the upgraded network design without the need for substantial structural modifications. and it assumes the affordability of necessary resources, including additional hardware for redundancy and network management.

Design Considerations:

- Scalability and Manageability: The design prioritizes scalability to accommodate the anticipated growth in manpower. Efficient cable routing, device selection, and installation ensure secure planning and optimal resource utilization. Finally, in order to improve manageability, the use of SNMP was implemented.

- Intranet Connectivity: Full connectivity among all network groups is paramount. Given this, the design emphasizes seamless communication between users and devices.

- Basic Security Measures: An organized IP addressing scheme, VLAN implementation, and naming conventions contribute to a secure network environment. Additionally, initial device settings and the use of strong passwords follow industry best practices for enhanced security. Finally, the use of ACLs was implemented to ensure added security.

- Network Redundancy: Implemented high-speed connections and link aggregation where needed to enhance the bandwidth capacity. Optimize network protocols as needed to facilitate the smooth transmission of data across the network. Integrated backup systems into the network architecture and utilize suitable protocols to enable automatic response to network errors. Optimize network protocols as needed to encourage swift adaptation to changes in network structure. Finally, all infrastructure devices will log all their events to the Orion sever.

Expectations:

Upon implementation of this upgraded network design, AITC can anticipate a robust, scalable, and secure infrastructure that aligns with their expansion plans. It expects to provide improved network management capabilities, enhanced performance, and fault-tolerance mechanisms to ensure uninterrupted operation of critical services. This includes the successful implementation of wireless connectivity for mobile devices, centralized network management, and updated security policies to mitigate potential risks. The project also anticipates thorough documentation and knowledge transfer to facilitate future maintenance and expansion of the network.

Deliverables:

This documentation will deliver comprehensive network documentation detailing the IP addressing scheme, physical and logical topology diagrams, device configurations, and a discussion of design choices. This also includes a packet tracer file of the proposed network to showcase its functionality as well as its adherence to company standards and requirements. The file will have all the devices pre-configured with the IP addressing scheme and the security measures included within this document. Each device is also connected according to the interconnection setup described. The simulated network aims to demonstrate that all devices can successfully communicate with each other and that all network devices follow the appropriate security measures to minimize vulnerabilities to external threats, with the design of the network being flexible, resilient, scalable, and manageable.

2. Physical Layout

The physical layout outlines the strategic placement of devices, L2 and L3 switches, routers, WLC, and LAPs to optimize communication flow across departments without cluttering the physical environment. Careful consideration has been given to the positioning of cabling, cable trays, and other essential components to maintain an organized and efficient environment. Safety is a paramount concern, and to mitigate potential workplace hazards, cables have been expertly routed along walls and ceilings, minimizing obstruction, and reducing the risk of accidents. Cables have been routed along walls and ceilings, to minimize obstruction and reduce the risk of accidents in the workplace. A legend has been provided in the physical layout to distinguish each VLAN from each other, with each VLAN being a different color. In addition to physical connections, the LAPs have been placed far enough away from each other to maximize their range and minimize the amount of overlap.

In addition to functionality, visual clarity and ease of maintenance were prioritized. Different colored cables serve as visual cues, symbolizing each department. Green cables denote the creative department, blue signifies the finance and marketing department, purple designates management, violet represents services, pink is allocated for the IT department, and red is reserved for the developer department.

This floor plan not only ensures efficient connectivity but also places a premium on safety and accessibility. The arrangement of devices and routing of cables has been optimized to create a robust and reliable network infrastructure that caters to the specific needs of each department. This meticulous planning is poised to contribute to a seamless and productive work environment, elevating operational efficiency across the organization.

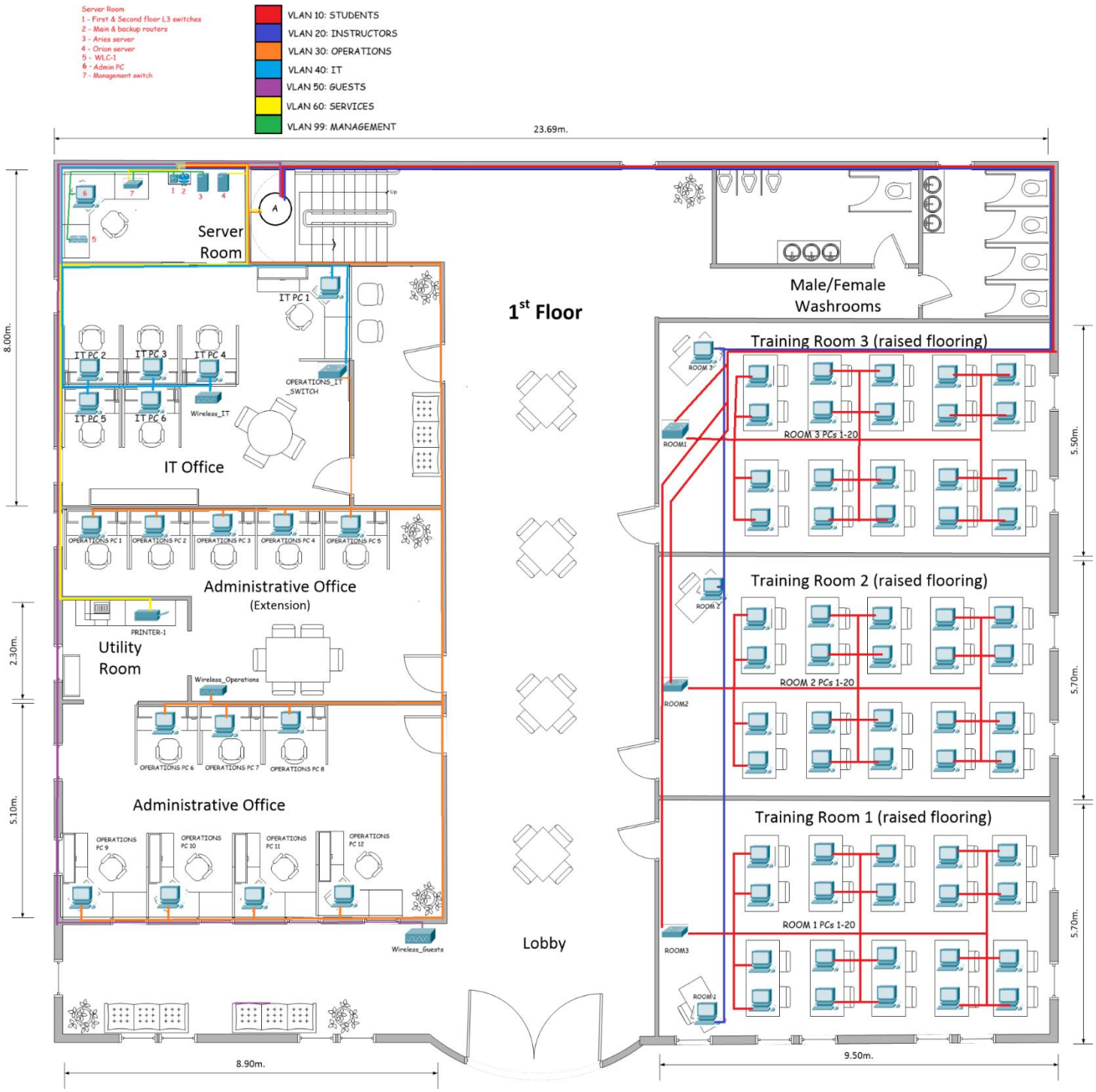

Figure 1. First Floor Physical Layout Device Names and Location

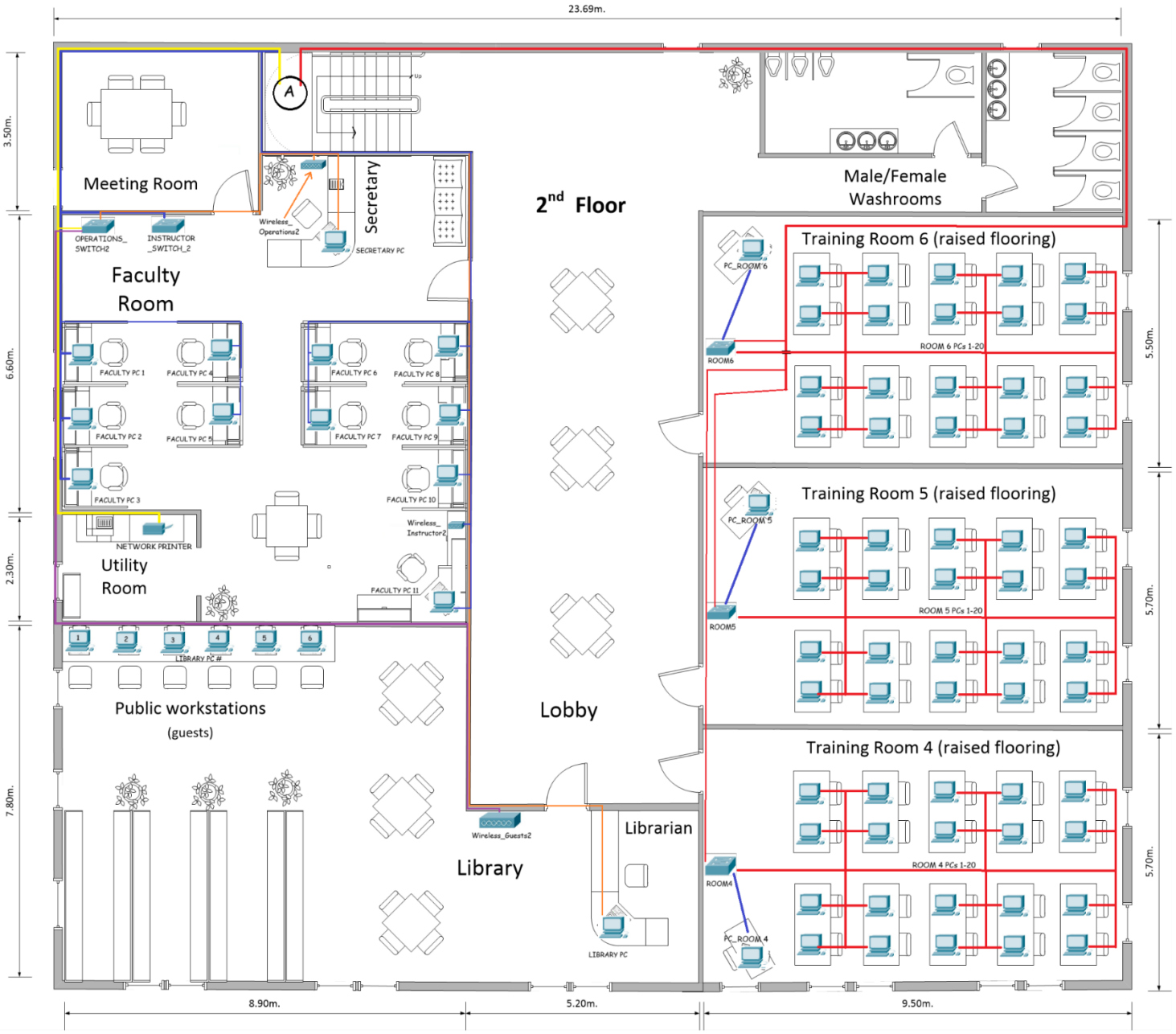

Figure 2. Second Floor Physical Layout Device Names and Location

3. Physical Topology

Prior to configuring the network, it is essential to determine the specific network devices that need to be acquired, as well as their respective placements and their interconnections. This section provides a comprehensive overview of the physical topology of the recommended network design as well as device interconnections table. The physical topology divides the device locations into their respective rooms, with additional consideration of the floor the rooms belong to. Access layer devices, distribution devices, core devices, servers, WLCs and LAPs are also placed in their corresponding racks and shelves. All network devices, except for certain L2 switches for easier management and LAPs for connectivity reasons, are placed in the server room to ensure security from unauthorized access. The rest of the end devices, certain L2 switches and LAPs are placed in their corresponding rooms depending on which department they belong to. The device interconnection tables list the source interface of a device, the VLAN it belongs to, what device it's connected to and the interface of the connected device. All switch to switch and switch to router connections used a fast Gigabit Ethernet port if available for faster speeds during high network usage. Both routers have 1 free gigabit ethernet port for internet connectivity.

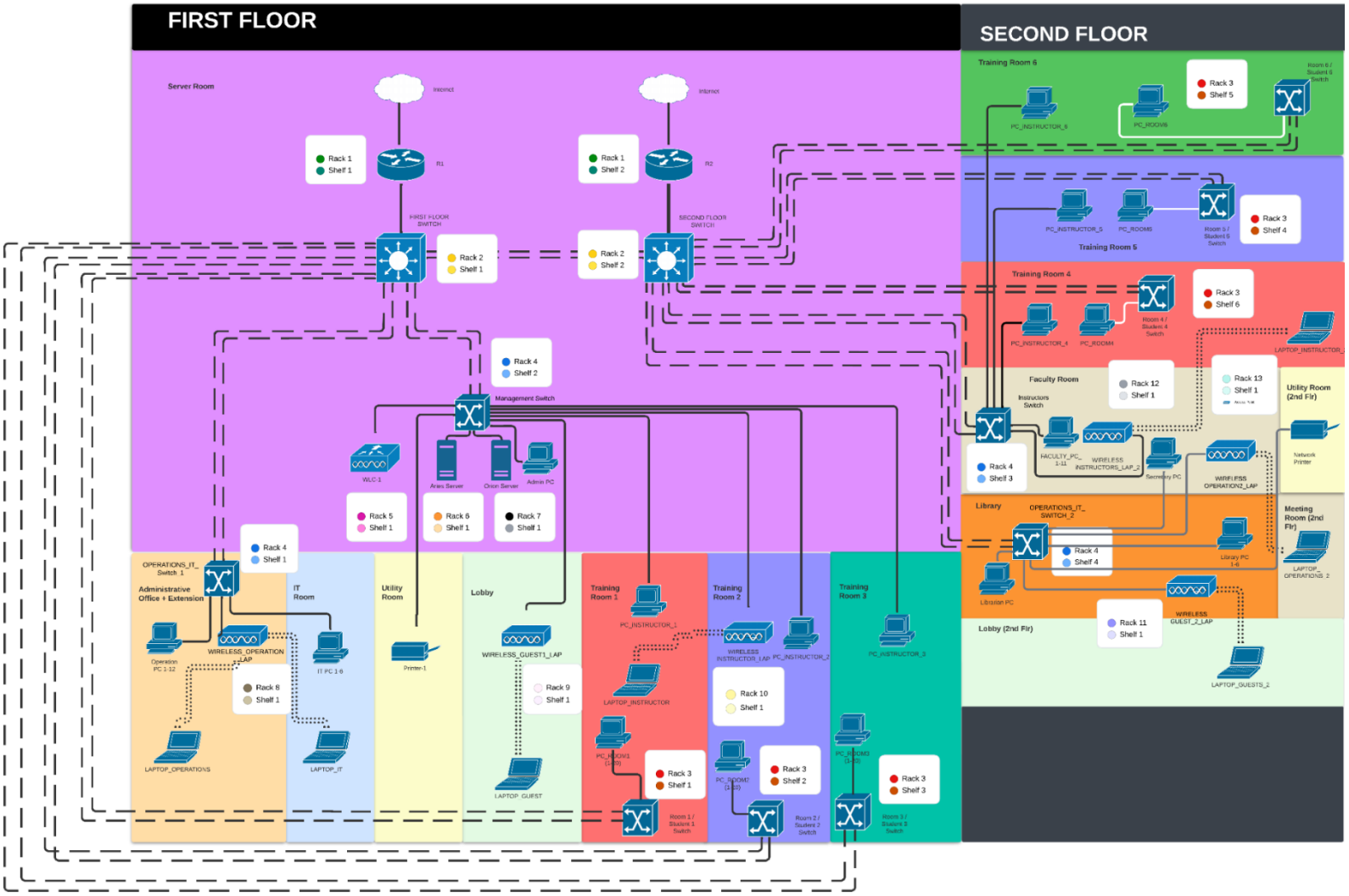

Figure 3. Physical Topology

Table 1. Device Interconnection Table for ROUTER_MAIN

ROUTER_MAIN			
Source Interface	VLAN	Connected To	Connected Interface
Gig0/0/0	N/A (trunk)	FIRST_FLOOR	Gig1/0/24

Table 2. Device Interconnection Table for ROUTER_BACKUP

ROUTER_BACKUP			
Source Interface	VLAN	Connected To	Connected Interface
Gig0/0/0	N/A (trunk)	SECOND_FLOOR	Gig1/0/24

Table 3. Device Interconnection Table for FIRST_FLOOR

FIRST_FLOOR			
Source Interface	VLAN	Connected To	Connected Interface
Gig1/0/1	N/A (trunk)	ROOM1	Gig0/1
Gig1/0/2	N/A (trunk)	ROOM1	Gig0/2

Gig1/0/3	N/A (trunk)	ROOM2	Gig0/1
Gig1/0/4	N/A (trunk)	ROOM2	Gig0/2
Gig1/0/5	N/A (trunk)	ROOM3	Gig0/1
Gig1/0/6	N/A(trunk)	ROOM3	Gig0/2
Gig1/0/7	N/A (trunk)	OPERATIONS_IT_SWITCH	Gig0/1
Gig1/0/8	N/A (trunk)	OPERATIONS_IT_SWITCH	Gig0/2
Gig1/0/9	N/A (trunk)	MANAGE_SWITCH	Gig0/1
Gig1/0/10	N/A (trunk)	MANAGE_SWITCH	Gig0/2
Gig1/0/21	N/A (trunk)	SECOND_FLOOR	Gig1/0/21
Gig1/0/22	N/A (trunk)	SECOND_FLOOR	Gig1/0/22

Table 4. Device Interconnection Table for SECOND_FLOOR

SECOND_FLOOR			
Source Interface	VLAN	Connected To	Connected Interface
Gig1/0/1	N/A (trunk)	ROOM4	Gig0/1
Gig1/0/2	N/A (trunk)	ROOM4	Gig0/2
Gig1/0/3	N/A (trunk)	ROOM5	Gig0/1
Gig1/0/4	N/A (trunk)	ROOM5	Gig0/2
Gig1/0/5	N/A (trunk)	ROOM6	Gig0/1
Gig1/0/6	N/A(trunk)	ROOM6	Gig0/2
Gig1/0/7	N/A (trunk)	OPERATIONS_IT_SWITCH_2	Gig0/1
Gig1/0/8	N/A (trunk)	OPERATIONS_IT_SWITCH_2	Gig0/2
Gig1/0/9	N/A (trunk)	INSTRUCTOR_SWITCH	Gig0/1
Gig1/0/10	N/A (trunk)	INSTRUCTOR_SWITCH	Gig0/2

Gig1/0/21	N/A (trunk)	FIRST_FLOOR	Gig1/0/21
Gig1/0/22	N/A (trunk)	FIRST_FLOOR	Gig1/0/22

Table 5. Device Interconnection Table for ROOM1

ROOM1			
Source Interface	VLAN	Connected To	Connected Interface
Fa0/1	10	ROOM 1 PC_1	Fa0
Fa0/2	10	ROOM 1 PC_2	Fa0
Fa0/3	10	ROOM 1 PC_3	Fa0
Fa0/4	10	ROOM 1 PC_4	Fa0
Fa0/5	10	ROOM 1 PC_5	Fa0
Fa0/6	10	ROOM 1 PC_6	Fa0
Fa0/7	10	ROOM 1 PC_7	Fa0

Fa0/8	10	ROOM 1 PC_8	Fa0
Fa0/9	10	ROOM 1 PC_9	Fa0
Fa0/10	10	ROOM 1 PC_10	Fa0
Fa0/11	10	ROOM 1 PC_11	Fa0
Fa0/12	10	ROOM 1 PC_12	Fa0
Fa0/13	10	ROOM 1 PC_13	Fa0
Fa0/14	10	ROOM 1 PC_14	Fa0
Fa0/15	10	ROOM 1 PC_15	Fa0
Fa0/16	10	ROOM 1 PC_16	Fa0
Fa0/17	10	ROOM 1 PC_17	Fa0
Fa0/18	10	ROOM 1 PC_18	Fa0
Fa0/19	10	ROOM 1 PC_19	Fa0

Fa0/20	10	ROOM 1 PC_20	Fa0
Gig0/1	N/A (trunk)	FIRST_FLOOR	Gig1/0/1
Gig0/2	N/A (trunk)	FIRST_FLOOR	Gig1/0/2

Table 6. Device Interconnection Table for ROOM2

ROOM2			
Source Interface	VLAN	Connected To	Connected Interface
Fa0/1	10	ROOM 2 PC_1	Fa0
Fa0/2	10	ROOM 2 PC_2	Fa0
Fa0/3	10	ROOM 2 PC_3	Fa0
Fa0/4	10	ROOM 2 PC_4	Fa0
Fa0/5	10	ROOM 2 PC_5	Fa0
Fa0/6	10	ROOM 2 PC_6	Fa0

Fa0/7	10	ROOM 2 PC_7	Fa0
Fa0/8	10	ROOM 2 PC_8	Fa0
Fa0/9	10	ROOM 2 PC_9	Fa0
Fa0/10	10	ROOM 2 PC_10	Fa0
Fa0/11	10	ROOM 2 PC_11	Fa0
Fa0/12	10	ROOM 2 PC_12	Fa0
Fa0/13	10	ROOM 2 PC_13	Fa0
Fa0/14	10	ROOM 2 PC_14	Fa0
Fa0/15	10	ROOM 2 PC_15	Fa0
Fa0/16	10	ROOM 2 PC_16	Fa0
Fa0/17	10	ROOM 2 PC_17	Fa0
Fa0/18	10	ROOM 2 PC_18	Fa0

Fa0/19	10	ROOM 2 PC_19	Fa0
Fa0/20	10	ROOM 2 PC_20	Fa0
Gig0/1	N/A (trunk)	FIRST_FLOOR	Gig1/0/3
Gig0/2	N/A (trunk)	FIRST_FLOOR	Gig1/0/4

Table 7. Device Interconnection Table for ROOM3

ROOM3			
Source Interface	VLAN	Connected To	Connected Interface
Fa0/1	10	ROOM 3 PC_1	Fa0
Fa0/2	10	ROOM 3 PC_2	Fa0
Fa0/3	10	ROOM 3 PC_3	Fa0
Fa0/4	10	ROOM 3 PC_4	Fa0
Fa0/5	10	ROOM 3 PC_5	Fa0

Fa0/6	10	ROOM 3 PC_6	Fa0
Fa0/7	10	ROOM 3 PC_7	Fa0
Fa0/8	10	ROOM 3 PC_8	Fa0
Fa0/9	10	ROOM 3 PC_9	Fa0
Fa0/10	10	ROOM 3 PC_10	Fa0
Fa0/11	10	ROOM 3 PC_11	Fa0
Fa0/12	10	ROOM 3 PC_12	Fa0
Fa0/13	10	ROOM 3 PC_13	Fa0
Fa0/14	10	ROOM 3 PC_14	Fa0
Fa0/15	10	ROOM 3 PC_15	Fa0
Fa0/16	10	ROOM 3 PC_16	Fa0
Fa0/17	10	ROOM 3 PC_17	Fa0

Fa0/18	10	ROOM 3 PC_18	Fa0
Fa0/19	10	ROOM 3 PC_19	Fa0
Fa0/20	10	ROOM 3 PC_20	Fa0
Gig0/1	N/A (trunk)	FIRST_FLOOR	Gig1/0/5
Gig0/2	N/A (trunk)	FIRST_FLOOR	Gig1/0/6

Table 8. Device Interconnection Table for OPERATIONS_IT_SWITCH

OPERATIONS_IT_SWITCH			
Source Interface	VLAN	Connected To	Connected Interface
Fa0/1	30	OPERATIONS PC1	Fa0
Fa0/2	30	OPERATIONS PC2	Fa0
Fa0/3	30	OPERATIONS PC3	Fa0
Fa0/4	30	OPERATIONS PC4	Fa0

Fa0/5	30	OPERATIONS PC5	Fa0
Fa0/6	30	OPERATIONS PC6	Fa0
Fa0/7	30	OPERATIONS PC7	Fa0
Fa0/8	30	OPERATIONS PC8	Fa0
Fa0/9	30	OPERATIONS PC9	Fa0
Fa0/10	30	OPERATIONS PC10	Fa0
Fa0/11	30	OPERATIONS PC11	Fa0
Fa0/12	30	OPERATIONS PC12	Fa0
Fa0/13	40	IT PC1	Fa0
Fa0/14	40	IT PC2	Fa0
Fa0/15	40	IT PC3	Fa0
Fa0/16	40	IT PC4	Fa0

Fa0/17	40	IT PC5	Fa0
Fa0/18	40	IT PC6	Fa0
Fa0/24	N/A (trunk)	WIRELESS_OPERATION_IT	Gig0
Gig0/1	N/A (trunk)	FIRST_FLOOR	Gig1/0/7
Gig0/2	N/A (trunk)	FIRST_FLOOR	Gig1/0/8

Table 9. Device Interconnection Table for Management Switch

Management Switch			
Source Interface	VLAN	Connected To	Connected Interface
Fa0/1	60	NETWORK PRINTER	Fa0
Fa0/2	60	ORION SERVER	Fa0
Fa0/4	99	ADMIN PC	Fa0
Fa0/5	99	ARIES SERVER	Fa0

Fa0/7	20	ROOM 1	Fa0
Fa0/8	20	ROOM 2	Fa0
Fa0/9	20	ROOM 3	Fa0
Fa0/22	N/A (trunk)	WLC-1	Gig1
Fa0/23	N/A (trunk)	WIRELESS_INSTRUCTOR	Gig0
Fa0/24	N/A (trunk)	WIRELESS_GUEST	Gig0
Gig0/1	N/A (trunk)	FIRST_FLOOR	Gig1/0/9
Gig0/2	N/A (trunk)	FIRST_FLOOR	Gig1/0/10

Table 10. Device Interconnection Table for ROOM4

ROOM4			
Source Interface	VLAN	Connected To	Connected Interface
Fa0/1	10	ROOM 4 PC_1	Fa0

Fa0/2	10	ROOM 4 PC_2	Fa0
Fa0/3	10	ROOM 4 PC_3	Fa0
Fa0/4	10	ROOM 4 PC_4	Fa0
Fa0/5	10	ROOM 4 PC_5	Fa0
Fa0/6	10	ROOM 4 PC_6	Fa0
Fa0/7	10	ROOM 4 PC_7	Fa0
Fa0/8	10	ROOM 4 PC_8	Fa0
Fa0/9	10	ROOM 4 PC_9	Fa0
Fa0/10	10	ROOM 4 PC_10	Fa0
Fa0/11	10	ROOM 4 PC_11	Fa0
Fa0/12	10	ROOM 4 PC_12	Fa0
Fa0/13	10	ROOM 4 PC_13	Fa0

Fa0/14	10	ROOM 4 PC_14	Fa0
Fa0/15	10	ROOM 4 PC_15	Fa0
Fa0/16	10	ROOM 4 PC_16	Fa0
Fa0/17	10	ROOM 4 PC_17	Fa0
Fa0/18	10	ROOM 4 PC_18	Fa0
Fa0/19	10	ROOM 4 PC_19	Fa0
Fa0/20	10	ROOM 4 PC_20	Fa0
Gig0/1	N/A (trunk)	SECOND_FLOOR	Gig1/0/1
Gig0/2	N/A (trunk)	SECOND_FLOOR	Gig1/0/2

Table 11. Device Interconnection Table for ROOM5

ROOM5			
Source Interface	VLAN	Connected To	Connected Interface
Fa0/1	10	ROOM 5 PC_1	Fa0
Fa0/2	10	ROOM 5 PC_2	Fa0
Fa0/3	10	ROOM 5 PC_3	Fa0
Fa0/4	10	ROOM 5 PC_4	Fa0
Fa0/5	10	ROOM 5 PC_5	Fa0
Fa0/6	10	ROOM 5 PC_6	Fa0
Fa0/7	10	ROOM 5 PC_7	Fa0
Fa0/8	10	ROOM 5 PC_8	Fa0
Fa0/9	10	ROOM 5 PC_9	Fa0

Fa0/10	10	ROOM 5 PC_10	Fa0
Fa0/11	10	ROOM 5 PC_11	Fa0
Fa0/12	10	ROOM 5 PC_12	Fa0
Fa0/13	10	ROOM 5 PC_13	Fa0
Fa0/14	10	ROOM 5 PC_14	Fa0
Fa0/15	10	ROOM 5 PC_15	Fa0
Fa0/16	10	ROOM 5 PC_16	Fa0
Fa0/17	10	ROOM 5 PC_17	Fa0
Fa0/18	10	ROOM 5 PC_18	Fa0
Fa0/19	10	ROOM 5 PC_19	Fa0

Fa0/20	10	ROOM 5 PC_20	Fa0
Gig0/1	N/A (trunk)	SECOND_FLOOR	Gig1/0/3
Gig0/2	N/A (trunk)	SECOND_FLOOR	Gig1/0/4

Table 12. Device Interconnection Table for ROOM6

ROOM6			
Source Interface	VLAN	Connected To	Connected Interface
Fa0/1	10	ROOM 6 PC_1	Fa0
Fa0/2	10	ROOM 6 PC_2	Fa0
Fa0/3	10	ROOM 6 PC_3	Fa0
Fa0/4	10	ROOM 6 PC_4	Fa0
Fa0/5	10	ROOM 6 PC_5	Fa0

Fa0/6	10	ROOM 6 PC_6	Fa0
Fa0/7	10	ROOM 6 PC_7	Fa0
Fa0/8	10	ROOM 6 PC_8	Fa0
Fa0/9	10	ROOM 6 PC_9	Fa0
Fa0/10	10	ROOM 6 PC_10	Fa0
Fa0/11	10	ROOM 6 PC_11	Fa0
Fa0/12	10	ROOM 6 PC_12	Fa0
Fa0/13	10	ROOM 6 PC_13	Fa0
Fa0/14	10	ROOM 6 PC_14	Fa0
Fa0/15	10	ROOM 6 PC_15	Fa0

Fa0/16	10	ROOM 6 PC_16	Fa0
Fa0/17	10	ROOM 6 PC_17	Fa0
Fa0/18	10	ROOM 6 PC_18	Fa0
Fa0/19	10	ROOM 6 PC_19	Fa0
Fa0/20	10	ROOM 6 PC_20	Fa0
Gig0/1	N/A (trunk)	SECOND_FLOOR	Gig1/0/5
Gig0/2	N/A (trunk)	SECOND_FLOOR	Gig1/0/6

Table 13. Device Interconnection Table for OPERATIONS_IT_SWITCH_2

OPERATIONS_IT_SWITCH_2			
Source Interface	VLAN	Connected To	Connected Interface
Fa0/1	30	SECRETARY PC	Fa0

Fa0/2	30	LIBRARY PC	Fa0
Fa0/3	50	LIBRARY PC 1	Fa0
Fa0/4	50	LIBRARY PC 2	Fa0
Fa0/5	50	LIBRARY PC 3	Fa0
Fa0/6	50	LIBRARY PC 4	Fa0
Fa0/7	50	LIBRARY PC 5	Fa0
Fa0/8	50	LIBRARY PC 6	Fa0
Fa0/9	60	NETWORK PRINTER	Fa0
Fa0/23	N/A (trunk)	WIRELESS_OPERATION 2	Gig0
Fa0/24	N/A (trunk)	WIRELESS_GUESTS_2	Gig0

Gig0/1	N/A (trunk)	SECOND_FLOOR	Gig1/0/7
Gig0/2	N/A (trunk)	SECOND_FLOOR	Gig1/0/8

Table 14. Device Interconnection Table for INSTRUCTORS SWITCH

INSTRUCTORS SWITCH			
Source Interface	VLAN	Connected To	Connected Interface
Fa0/1	20	FACULTY PC 1	Fa0
Fa0/2	20	FACULTY PC 2	Fa0
Fa0/3	20	FACULTY PC 3	Fa0
Fa0/4	20	FACULTY PC 4	Fa0
Fa0/5	20	FACULTY PC 5	Fa0
Fa0/6	20	FACULTY PC 6	Fa0

Fa0/7	20	FACULTY PC 7	Fa0
Fa0/8	20	FACULTY PC 8	Fa0
Fa0/9	20	FACULTY PC 9	Fa0
Fa0/10	20	FACULTY PC 10	Fa0
Fa0/11	20	FACULTY PC 11	Fa0
Fa0/12	20	ROOM 4	Fa0
Fa0/13	20	ROOM 5	Fa0
Fa0/14	20	ROOM 6	Fa0
Fa0/24	N/A (trunk)	WIRLESS_INSTRUCTOR_2	Gig0
Gig0/1	N/A (trunk)	SECOND_FLOOR	Gig1/0/9

Gig0/2	N/A (trunk)	SECOND_FLOOR	Gig1/0/10

4. Logical Topology

The logical topology diagram of the network illustrates a well-structured and resilient architecture designed for efficiency, scalability, and reliability. The network is organized according to VLAN assignments, facilitating efficient communication and management across the different departments. The inclusion of one representative PC per department for the physical connection and one representative PC for departments with wireless connections allows for comprehensive testing of intra-VLAN connectivity, ensuring robust communication within each segment. This approach reflects a thorough consideration for network reliability. Redundancy is another cornerstone of this design, with two routers in the core layer and two layer 3 switches in the distribution layer. Furthermore, EtherChannel and HSRP has also been configured to help improve redundancy within the network. This setup guarantees continuous available connectivity even in the event of a cable or device failure. This redundancy strategy aligns with best practices for network resilience. The architecture also adheres to the three-layer hierarchical model consisting of the access layer, distribution layer, and core layer, allowing the visualization of the role of switches depending on where they are in the hierarchy and ensures consistent configuration across switches per layer. In addition, this topology follows a replicable pattern where if the department contains enough users, it can have its own corresponding layer 2 switch. This allows for seamless network expansion and integrated services without heavy impact on network performance. This logical topology provides a hierarchical visualization to easily distinguish the core layer, distribution layer and access layer from each other. Lastly, high traffic areas use Gigabit ethernet ports instead of fast ethernet ports to enhance network performance and prevent bottlenecks. It also has EtherChannels built in to enhance network performance.

The network is divided into six distinct subnets, each corresponding to a specific department or function. These include the Students (VLAN 10), Instructors (VLAN 20), Operations (VLAN 30), IT Department (VLAN 40), Guests (VLAN 50), Services (VLAN 60), and Management (VLAN 99). There is also a blackhole VLAN (VLAN 100) reserved for unused ports. This segmentation enhances security, manageability, and performance optimization. The operations and IT department share one switch for the first floor. Meanwhile, each room for the students on the first floor is equipped with 1

layer 2 switch, accommodating its higher user density. Finally, the management, instructor, services, and LAP for the guests share a single layer 2 switch for the first floor. However, on the second floor, the instructors have a dedicated layer 2 switch for the second floor. In addition, similar to the first floor, each room for the students on the second floor is equipped with 1 layer 2 switch, accommodating its higher user density. Lastly, the operations, guests and services share a single layer 2 switch for the second floor, demonstrating an efficient allocation of resources.

In the diagram, each port is meticulously labeled, and devices are clearly designated, providing a visual reference for easy identification. Devices belonging to the same VLAN are grouped together, with VLAN names, network addresses, subnet masks, and default gateways clearly indicated. Each VLAN is also color coded. This enhances the diagram's clarity and aids in understanding the assignment of devices to specific VLANs. Overall, this network design exemplifies a balanced approach to resilience, modularity, and manageability. Its scalability and redundancy measures position it as a robust foundation for future growth and integrated services, while its logical organization and comprehensive labeling make it a valuable tool for administrators and technicians alike.

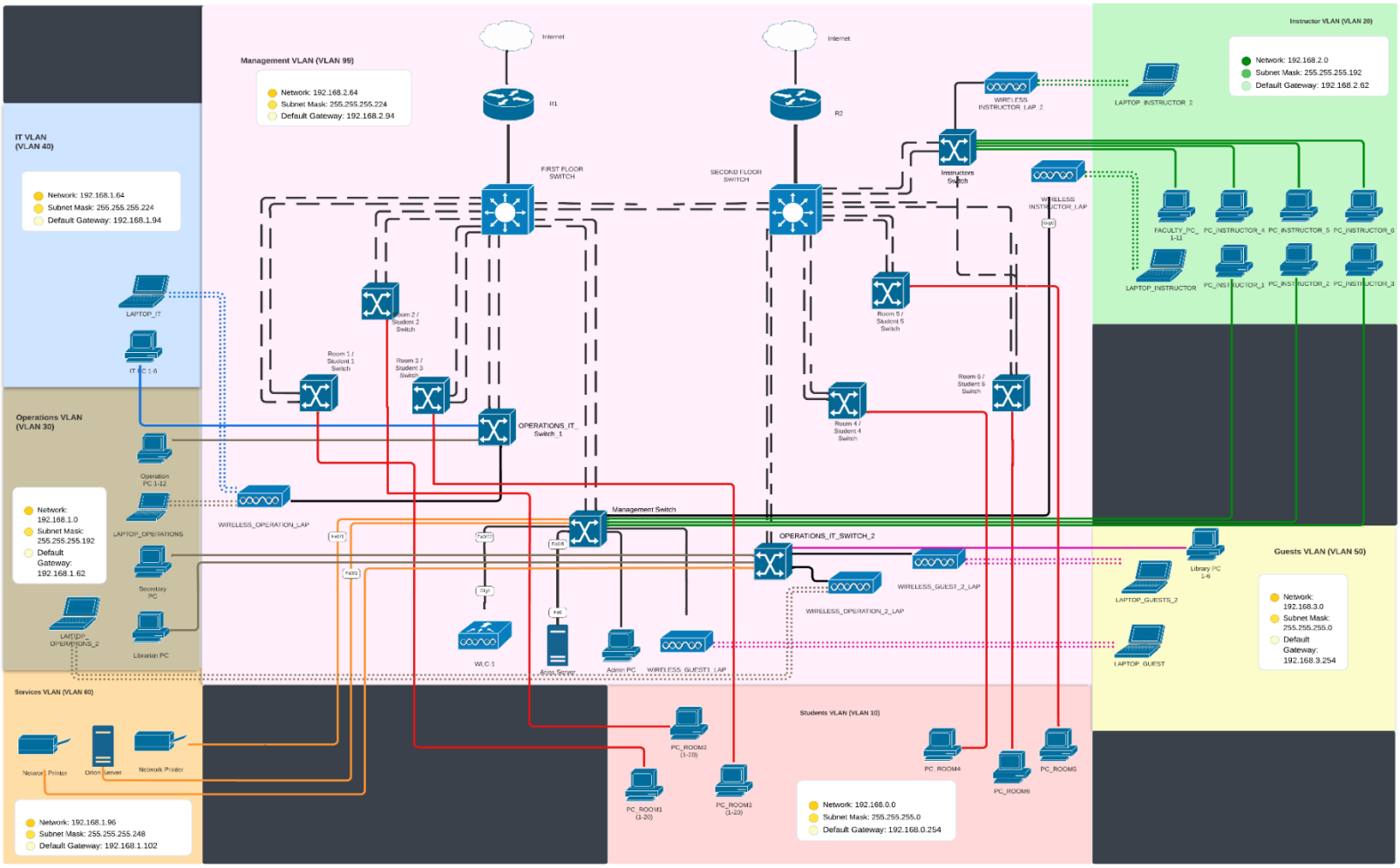

Figure 4. Logical Topology (Overall view)

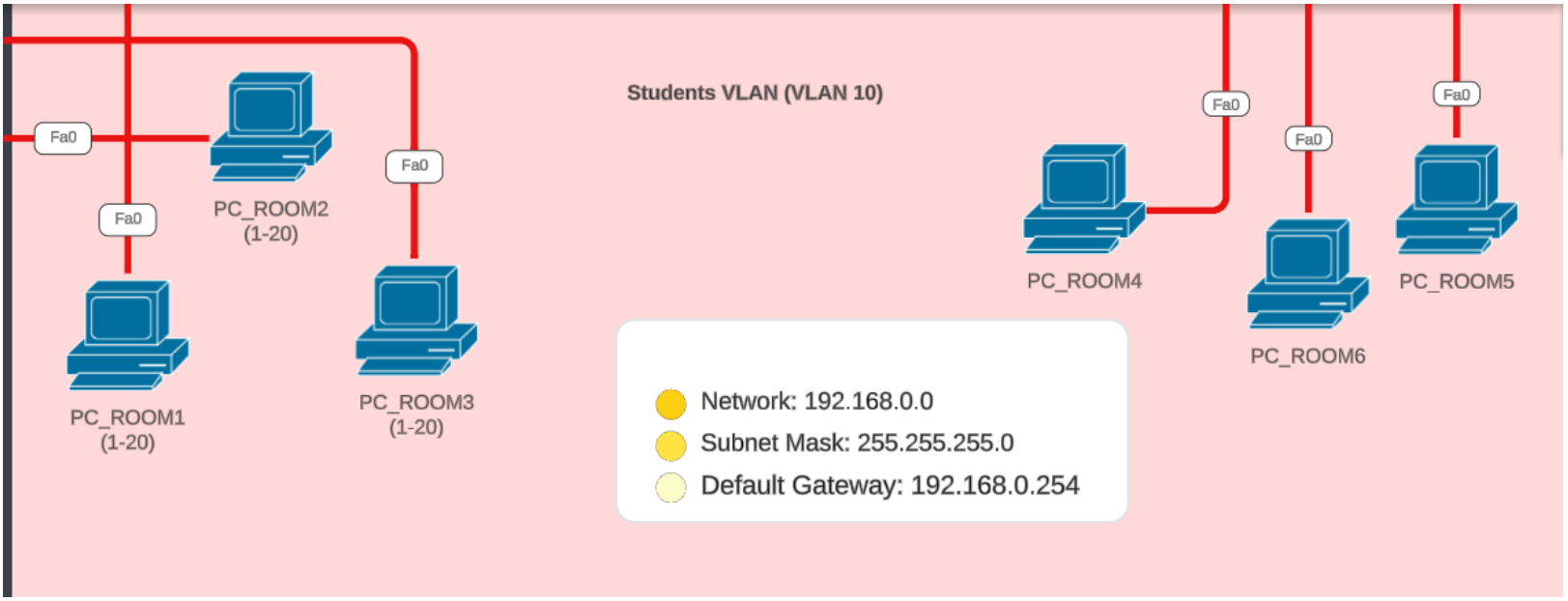

Figure 5. Zoomed in Logical Topology of VLAN 10

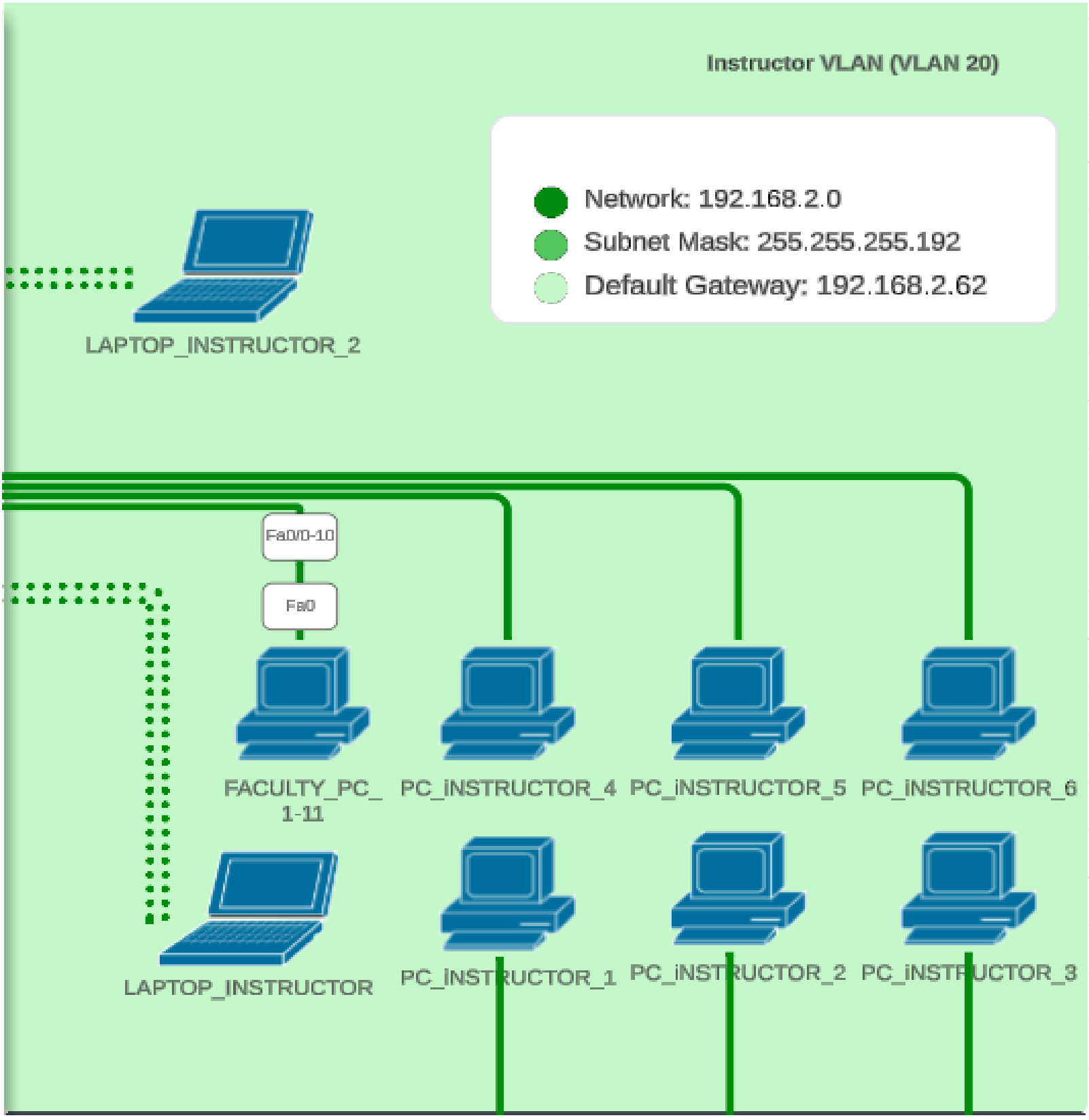

Figure 6. Zoomed in Logical Topology of VLAN 20

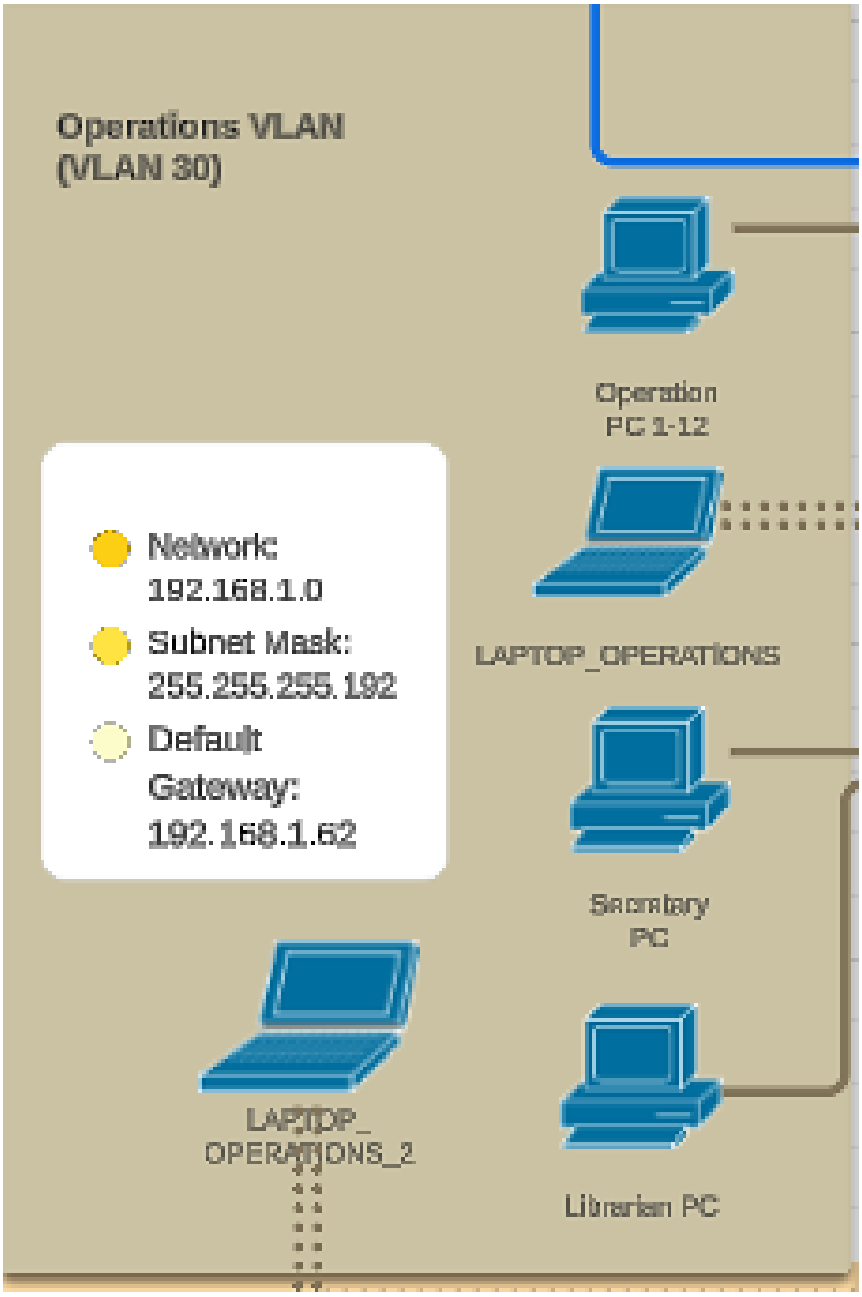

Figure 7. Zoomed in Logical Topology of VLAN 30

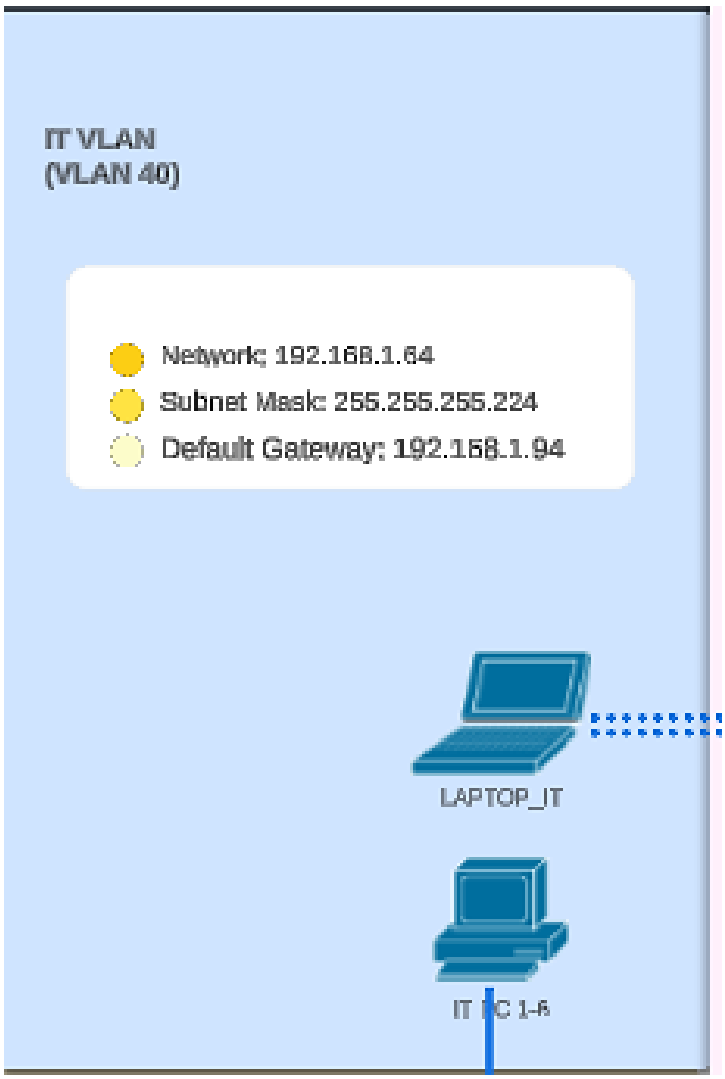

Figure 8. Zoomed in Logical Topology of VLAN 40

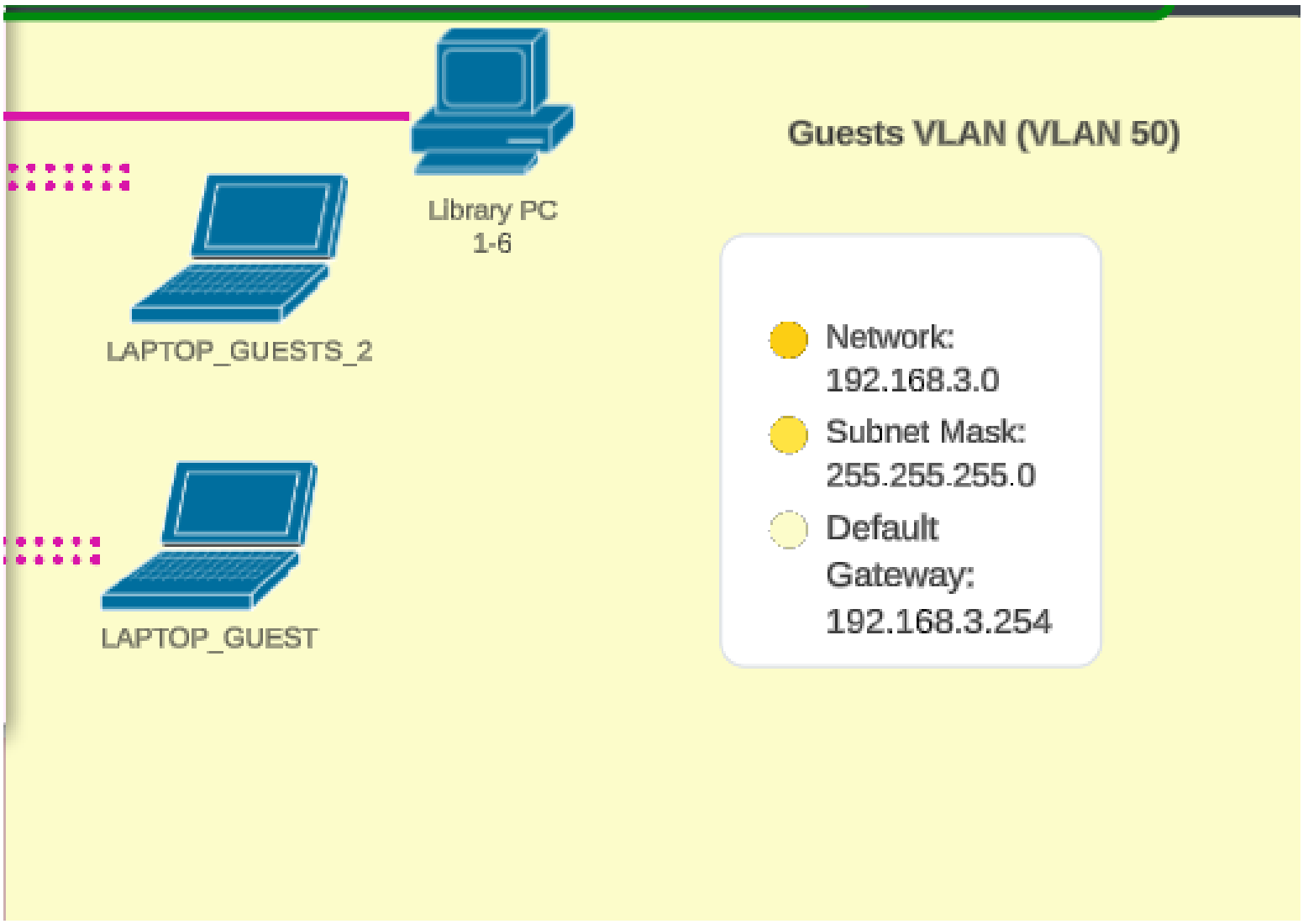

Figure 8. Zoomed in Logical Topology of VLAN 50

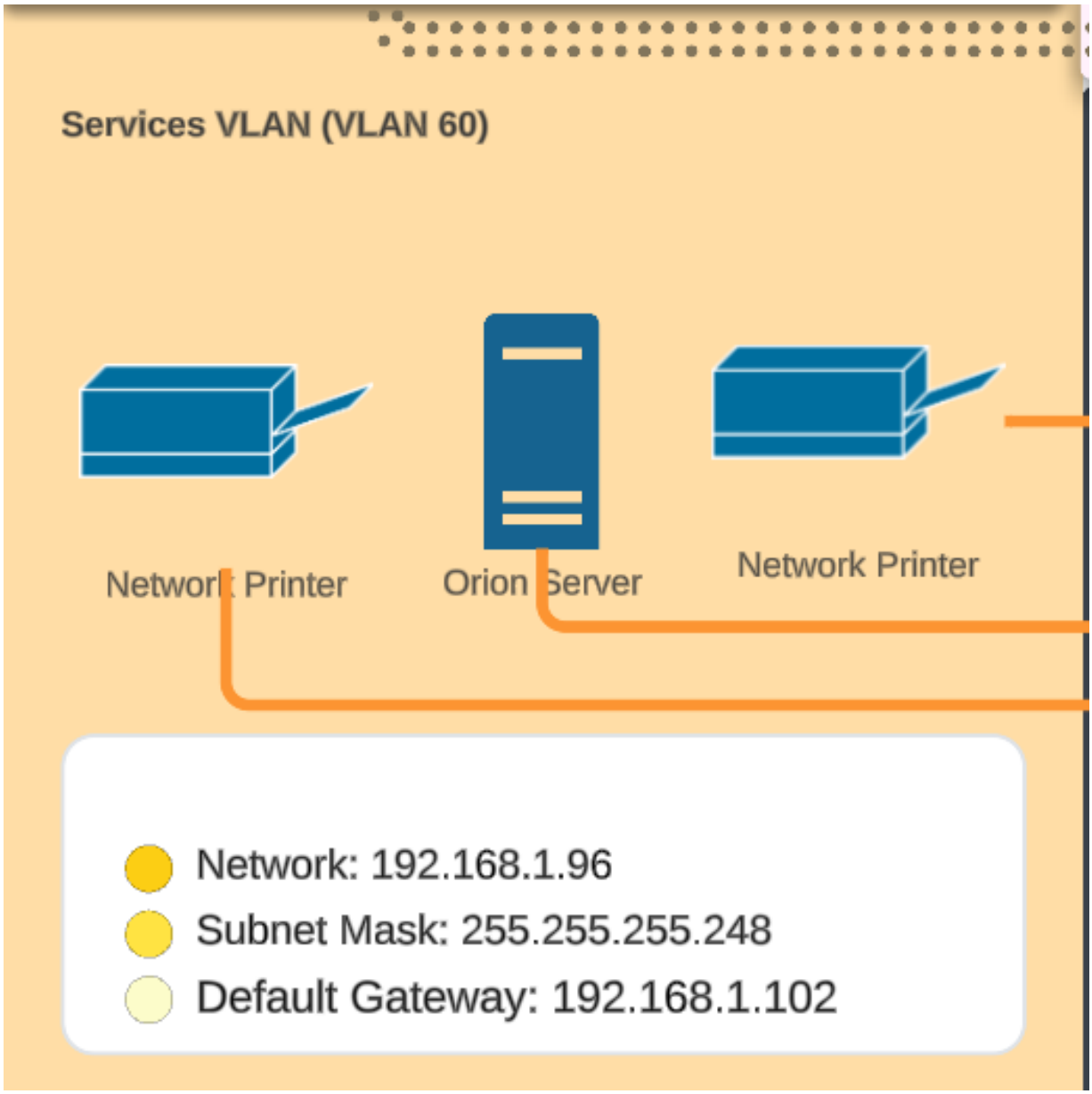

Figure 9. Zoomed in Logical Topology of VLAN 60

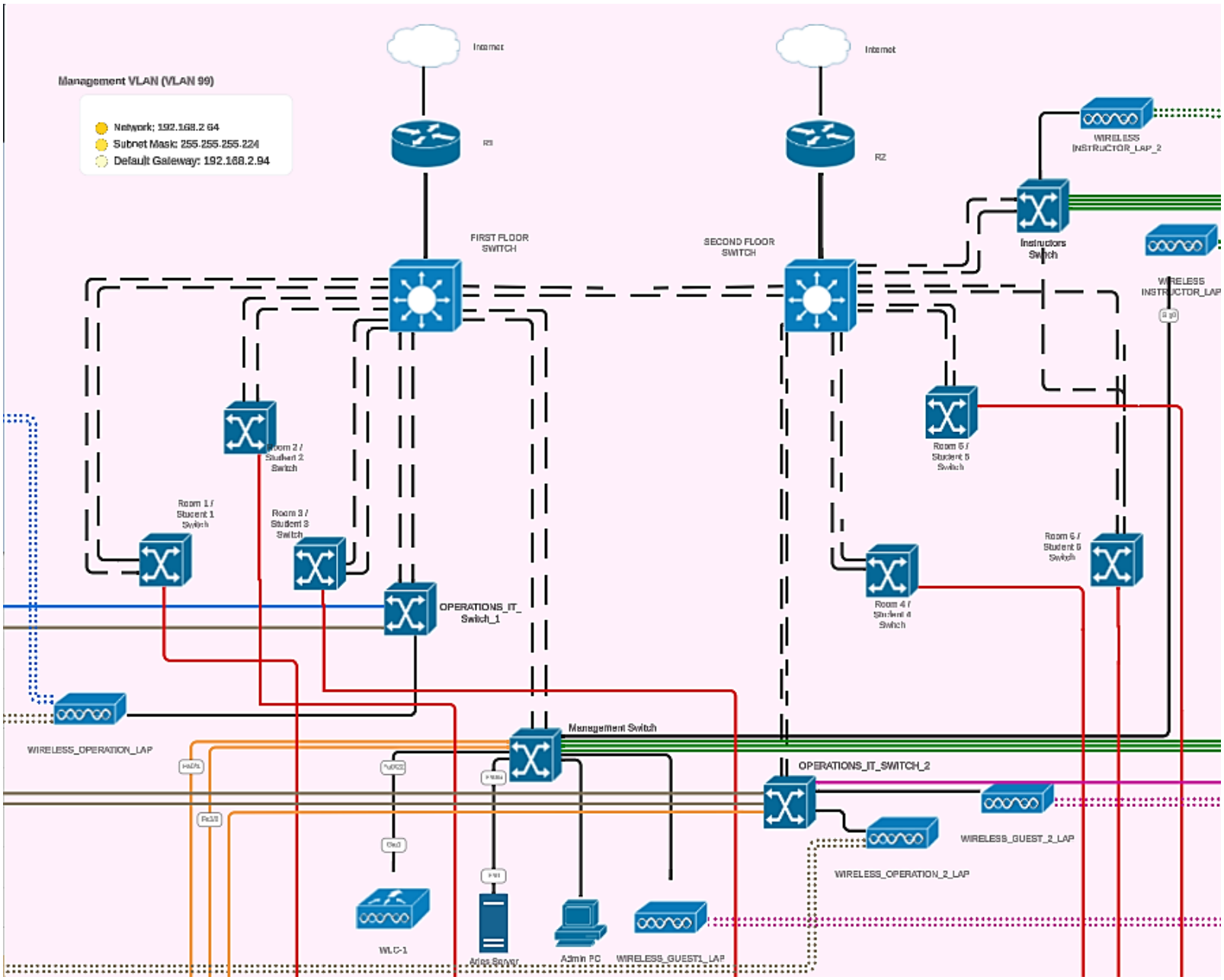

Figure 10. Zoomed in Logical Topology of VLAN 99

Table 15. IP Addressing Table

Network Name	Network Address	Subnet Mask	Host Range	VLAN ID
Students (6 x 20 hosts)	192.168.0.0	255.255.255.0	192.168.0.1-192.168.0.254	10
Instructors (3 + 11 + 3 + 11 hosts)	192.168.2.0	255.255.255.192	192.168.2.1-192.168.2.62	20
Operations (12 + 2 + 14 hosts)	192.168.1.0	255.255.255.192	192.168.1.1-192.168.1.62	30
IT (6 + 6 hosts)	192.168.1.64	255.255.255.224	192.168.1.65-192.168.1.94	40
Guests (50 + 6 hosts)	192.168.3.0	255.255.255.0	192.168.3.1-192.168.3.254	50
Services (2 + 1 hosts)	192.168.1.96	255.255.255.248	192.168.1.97-192.168.1.102	60
Management (21 hosts)	192.168.2.64	255.255.255.224	192.168.2.65-192.168.2.94	99

5. IP Addressing Scheme

This section provides comprehensive details about the IP Addresses of each network, including information such as device names within the network, connected interface/s as well as assigned IP addresses, subnet masks and default gateways. Following the allocation of the IPv4 address space 192.168.0.0/20 and employing Variable Length Subnet Masking (VLSM), there will be multiple subnet masks which includes 255.255.255.0 for VLANs 10 and 50, 255.255.255.192 for VLANs 20 and 30, 255.255.255.224 for VLANs 40 and 99, and 255.255.255.248 for VLAN 60. This approach allows for an easily scalable network which will be advantageous to an expanding organization such as the Alonzo IT Training Center (AITC). It enhances the security of the network as the different user types are separated which reduces the damage caused by potential data breaches. This affects the implementation of access control units to be more effective by specifically restricting access of each department to relevant resources to the respective department. The default gateway for each VLAN is set to the last usable address in the network. This practice adheres to Cisco standards and promotes a clear understanding of the network's capacity in terms of device accommodation.

Table 16. IP Addressing Assignment Table for Management VLAN

Device Name	Interface	IP Address	Subnet Mask	Default Gateway
MANAGEMENT (VLAN 99)				
ROUTER_MAIN	G0/0.10	192.168.0.253	255.255.255.0	N/A
	G0/0.20	192.168.2.61	255.255.255.192	
	G0/0.30	192.168.1.61	255.255.255.192	
	G0/0.40	192.168.1.93	255.255.255.224	
	G0/0.50	192.168.3.253	255.255.255.0	
	G0/0.60	192.168.1.101	255.255.255.248	
	G0/0.99	192.168.2.93	255.255.255.224	
ROUTER_BACKUP	G0/0.10	192.168.0.252	255.255.255.0	
	G0/0.20	192.168.2.60	255.255.255.192	
	G0/0.30	192.168.1.60	255.255.255.192	

	G0/0.40	192.168.1.92	255.255.255.224	N/A
	G0/0.50	192.168.3.252	255.255.255.0	
	G0/0.60	192.168.1.100	255.255.255.248	
	G0/0.99	192.168.2.92	255.255.255.224	
ARIES_SERVER	F0	192.168.2.65	255.255.255.224	192.168.2.94
ADMIN PC	F0	192.168.2.66	255.255.255.224	192.168.2.94
FIRST_FLOOR	VLAN 10	192.168.0.250	255.255.255.0	N/A
	VLAN 20	192.168.2.58	255.255.255.192	
	VLAN 30	192.168.1.58	255.255.255.192	
	VLAN 40	192.168.1.90	255.255.255.224	
	VLAN 50	192.168.3.250	255.255.255.0	
	VLAN 60	192.168.1.98	255.255.255.248	

	VLAN 99	192.168.2.90	255.255.255.224	
ROOM1	VLAN 99	192.168.2.68	255.255.255.224	192.168.2.94
ROOM2		192.168.2.69	255.255.255.224	
ROOM3		192.168.2.70	255.255.255.224	
OPERATIONS_IT_SWITCH		192.168.2.71	255.255.255.224	
MANAGE_SWITCH		192.168.2.72	255.255.255.224	
SECOND_FLOOR	VLAN 10	192.168.0.249	255.255.255.0	N/A
	VLAN 20	192.168.2.57	255.255.255.192	
	VLAN 30	192.168.1.57	255.255.255.192	
	VLAN 40	192.168.1.89	255.255.255.224	
	VLAN 50	192.168.3.249	255.255.255.0	
	VLAN 60	192.168.1.97	255.255.255.248	

	VLAN 99	192.168.2.89	255.255.255.224	
ROOM4	VLAN 99	192.168.2.74	255.255.255.224	192.168.2.94
ROOM5		192.168.2.75	255.255.255.224	
ROOM6		192.168.2.76	255.255.255.224	
OPERATIONS_IT_SWITCH_2		192.168.2.77	255.255.255.224	
INSTRUCTOR_SWITCH		192.168.2.78	255.255.255.224	
WLC-1	Management	192.168.2.79	255.255.255.224	
WIRELESS_OPERATION_IT	Gig0	192.168.2.80	255.255.255.224	
WIRELESS_INSTRUCTOR	Gig0	192.168.2.81	255.255.255.224	
WIRELESS_GUEST1	Gig0	192.168.2.82	255.255.255.224	
WIRELESS_OPERATION_2	Gig0	192.168.2.83	255.255.255.224	
WIRELESS_GUESTS_2	Gig0	192.168.2.84	255.255.255.224	

WIRELESS_INSTRUCTOR_2	Gig0	192.168.2.85	255.255.255.224	

Table 17. IP Addressing Assignment Table for Students VLAN

Device Name	Interface	IP Address	Subnet Mask	Default Gateway
STUDENTS (VLAN 10)				
ROOM 1 PC_1	F0	192.168.0.1	255.255.255.0	192.168.0.254
ROOM 1 PC_2	F0	192.168.0.2	255.255.255.0	192.168.0.254
ROOM 1 PC_3	F0	192.168.0.3	255.255.255.0	192.168.0.254
ROOM 1 PC_4	F0	192.168.0.4	255.255.255.0	192.168.0.254
ROOM 1 PC_5	F0	192.168.0.5	255.255.255.0	192.168.0.254
ROOM 1 PC_6	F0	192.168.0.6	255.255.255.0	192.168.0.254
ROOM 1 PC_7	F0	192.168.0.7	255.255.255.0	192.168.0.254
ROOM 1 PC_8	F0	192.168.0.8	255.255.255.0	192.168.0.254

ROOM 1 PC_9	F0	192.168.0.9	255.255.255.0	192.168.0.254
ROOM 1 PC_10	F0	192.168.0.10	255.255.255.0	192.168.0.254
ROOM 1 PC_11	F0	192.168.0.11	255.255.255.0	192.168.0.254
ROOM 1 PC_12	F0	192.168.0.12	255.255.255.0	192.168.0.254
ROOM 1 PC_13	F0	192.168.0.13	255.255.255.0	192.168.0.254
ROOM 1 PC_14	F0	192.168.0.14	255.255.255.0	192.168.0.254
ROOM 1 PC_15	F0	192.168.0.15	255.255.255.0	192.168.0.254
ROOM 1 PC_16	F0	192.168.0.16	255.255.255.0	192.168.0.254
ROOM 1 PC_17	F0	192.168.0.17	255.255.255.0	192.168.0.254
ROOM 1 PC_18	F0	192.168.0.18	255.255.255.0	192.168.0.254
ROOM 1 PC_19	F0	192.168.0.19	255.255.255.0	192.168.0.254
ROOM 1 PC_20	F0	192.168.0.20	255.255.255.0	192.168.0.254

ROOM 2 PC_1	F0	192.168.0.21	255.255.255.0	192.168.0.254
ROOM 2 PC_2	F0	192.168.0.22	255.255.255.0	192.168.0.254
ROOM 2 PC_3	F0	192.168.0.23	255.255.255.0	192.168.0.254
ROOM 2 PC_4	F0	192.168.0.24	255.255.255.0	192.168.0.254
ROOM 2 PC_5	F0	192.168.0.25	255.255.255.0	192.168.0.254
ROOM 2 PC_6	F0	192.168.0.26	255.255.255.0	192.168.0.254
ROOM 2 PC_7	F0	192.168.0.27	255.255.255.0	192.168.0.254
ROOM 2 PC_8	F0	192.168.0.28	255.255.255.0	192.168.0.254
ROOM 2 PC_9	F0	192.168.0.29	255.255.255.0	192.168.0.254
ROOM 2 PC_10	F0	192.168.0.30	255.255.255.0	192.168.0.254
ROOM 2 PC_11	F0	192.168.0.31	255.255.255.0	192.168.0.254
ROOM 2 PC_12	F0	192.168.0.32	255.255.255.0	192.168.0.254

ROOM 2 PC_13	F0	192.168.0.33	255.255.255.0	192.168.0.254
ROOM 2 PC_14	F0	192.168.0.34	255.255.255.0	192.168.0.254
ROOM 2 PC_15	F0	192.168.0.35	255.255.255.0	192.168.0.254
ROOM 2 PC_16	F0	192.168.0.36	255.255.255.0	192.168.0.254
ROOM 2 PC_17	F0	192.168.0.37	255.255.255.0	192.168.0.254
ROOM 2 PC_18	F0	192.168.0.38	255.255.255.0	192.168.0.254
ROOM 2 PC_19	F0	192.168.0.39	255.255.255.0	192.168.0.254
ROOM 2 PC_20	F0	192.168.0.40	255.255.255.0	192.168.0.254
ROOM 3 PC_1	F0	192.168.0.41	255.255.255.0	192.168.0.254
ROOM 3 PC_2	F0	192.168.0.42	255.255.255.0	192.168.0.254
ROOM 3 PC_3	F0	192.168.0.43	255.255.255.0	192.168.0.254
ROOM 3 PC_4	F0	192.168.0.44	255.255.255.0	192.168.0.254

ROOM 3 PC_5	F0	192.168.0.45	255.255.255.0	192.168.0.254
ROOM 3 PC_6	F0	192.168.0.46	255.255.255.0	192.168.0.254
ROOM 3 PC_7	F0	192.168.0.47	255.255.255.0	192.168.0.254
ROOM 3 PC_8	F0	192.168.0.48	255.255.255.0	192.168.0.254
ROOM 3 PC_9	F0	192.168.0.49	255.255.255.0	192.168.0.254
ROOM 3 PC_10	F0	192.168.0.50	255.255.255.0	192.168.0.254
ROOM 3 PC_11	F0	192.168.0.51	255.255.255.0	192.168.0.254
ROOM 3 PC_12	F0	192.168.0.52	255.255.255.0	192.168.0.254
ROOM 3 PC_13	F0	192.168.0.53	255.255.255.0	192.168.0.254
ROOM 3 PC_14	F0	192.168.0.54	255.255.255.0	192.168.0.254
ROOM 3 PC_15	F0	192.168.0.55	255.255.255.0	192.168.0.254
ROOM 3 PC_16	F0	192.168.0.56	255.255.255.0	192.168.0.254

ROOM 3 PC_17	F0	192.168.0.57	255.255.255.0	192.168.0.254
ROOM 3 PC_18	F0	192.168.0.58	255.255.255.0	192.168.0.254
ROOM 3 PC_19	F0	192.168.0.59	255.255.255.0	192.168.0.254
ROOM 3 PC_20	F0	192.168.0.60	255.255.255.0	192.168.0.254
ROOM 4 PC_1	F0	192.168.0.61	255.255.255.0	192.168.0.254
ROOM 4 PC_2	F0	192.168.0.62	255.255.255.0	192.168.0.254
ROOM 4 PC_3	F0	192.168.0.63	255.255.255.0	192.168.0.254
ROOM 4 PC_4	F0	192.168.0.64	255.255.255.0	192.168.0.254
ROOM 4 PC_5	F0	192.168.0.65	255.255.255.0	192.168.0.254
ROOM 4 PC_6	F0	192.168.0.66	255.255.255.0	192.168.0.254
ROOM 4 PC_7	F0	192.168.0.67	255.255.255.0	192.168.0.254
ROOM 4 PC_8	F0	192.168.0.68	255.255.255.0	192.168.0.254

ROOM 4 PC_9	F0	192.168.0.69	255.255.255.0	192.168.0.254
ROOM 4 PC_10	F0	192.168.0.70	255.255.255.0	192.168.0.254
ROOM 4 PC_11	F0	192.168.0.71	255.255.255.0	192.168.0.254
ROOM 4 PC_12	F0	192.168.0.72	255.255.255.0	192.168.0.254
ROOM 4 PC_13	F0	192.168.0.73	255.255.255.0	192.168.0.254
ROOM 4 PC_14	F0	192.168.0.74	255.255.255.0	192.168.0.254
ROOM 4 PC_15	F0	192.168.0.75	255.255.255.0	192.168.0.254
ROOM 4 PC_16	F0	192.168.0.76	255.255.255.0	192.168.0.254
ROOM 4 PC_17	F0	192.168.0.77	255.255.255.0	192.168.0.254
ROOM 4 PC_18	F0	192.168.0.78	255.255.255.0	192.168.0.254
ROOM 4 PC_19	F0	192.168.0.79	255.255.255.0	192.168.0.254
ROOM 4 PC_20	F0	192.168.0.80	255.255.255.0	192.168.0.254

ROOM 5 PC_1	F0	192.168.0.81	255.255.255.0	192.168.0.254
ROOM 5 PC_2	F0	192.168.0.82	255.255.255.0	192.168.0.254
ROOM 5 PC_3	F0	192.168.0.83	255.255.255.0	192.168.0.254
ROOM 5 PC_4	F0	192.168.0.84	255.255.255.0	192.168.0.254
ROOM 5 PC_5	F0	192.168.0.85	255.255.255.0	192.168.0.254
ROOM 5 PC_6	F0	192.168.0.86	255.255.255.0	192.168.0.254
ROOM 5 PC_7	F0	192.168.0.87	255.255.255.0	192.168.0.254
ROOM 5 PC_8	F0	192.168.0.88	255.255.255.0	192.168.0.254
ROOM 5 PC_9	F0	192.168.0.89	255.255.255.0	192.168.0.254
ROOM 5 PC_10	F0	192.168.0.90	255.255.255.0	192.168.0.254
ROOM 5 PC_11	F0	192.168.0.91	255.255.255.0	192.168.0.254
ROOM 5 PC_12	F0	192.168.0.92	255.255.255.0	192.168.0.254

ROOM 5 PC_13	F0	192.168.0.93	255.255.255.0	192.168.0.254
ROOM 5 PC_14	F0	192.168.0.94	255.255.255.0	192.168.0.254
ROOM 5 PC_15	F0	192.168.0.95	255.255.255.0	192.168.0.254
ROOM 5 PC_16	F0	192.168.0.96	255.255.255.0	192.168.0.254
ROOM 5 PC_17	F0	192.168.0.97	255.255.255.0	192.168.0.254
ROOM 5 PC_18	F0	192.168.0.98	255.255.255.0	192.168.0.254
ROOM 5 PC_19	F0	192.168.0.99	255.255.255.0	192.168.0.254
ROOM 5 PC_20	F0	192.168.0.100	255.255.255.0	192.168.0.254
ROOM 6 PC_1	F0	192.168.0.101	255.255.255.0	192.168.0.254
ROOM 6 PC_2	F0	192.168.0.102	255.255.255.0	192.168.0.254
ROOM 6 PC_3	F0	192.168.0.103	255.255.255.0	192.168.0.254
ROOM 6 PC_4	F0	192.168.0.104	255.255.255.0	192.168.0.254

ROOM 6 PC_5	F0	192.168.0.105	255.255.255.0	192.168.0.254
ROOM 6 PC_6	F0	192.168.0.106	255.255.255.0	192.168.0.254
ROOM 6 PC_7	F0	192.168.0.107	255.255.255.0	192.168.0.254
ROOM 6 PC_8	F0	192.168.0.108	255.255.255.0	192.168.0.254
ROOM 6 PC_9	F0	192.168.0.109	255.255.255.0	192.168.0.254
ROOM 6 PC_10	F0	192.168.0.110	255.255.255.0	192.168.0.254
ROOM 6 PC_11	F0	192.168.0.111	255.255.255.0	192.168.0.254
ROOM 6 PC_12	F0	192.168.0.112	255.255.255.0	192.168.0.254
ROOM 6 PC_13	F0	192.168.0.113	255.255.255.0	192.168.0.254
ROOM 6 PC_14	F0	192.168.0.114	255.255.255.0	192.168.0.254
ROOM 6 PC_15	F0	192.168.0.115	255.255.255.0	192.168.0.254
ROOM 6 PC_16	F0	192.168.0.116	255.255.255.0	192.168.0.254

ROOM 6 PC_17	F0	192.168.0.117	255.255.255.0	192.168.0.254
ROOM 6 PC_18	F0	192.168.0.118	255.255.255.0	192.168.0.254
ROOM 6 PC_19	F0	192.168.0.119	255.255.255.0	192.168.0.254
ROOM 6 PC_20	F0	192.168.0.120	255.255.255.0	192.168.0.254

Table 18. IP Addressing Assignment Table for Instructors VLAN

Device Name	Interface	IP Address	Subnet Mask	Default Gateway
INSTRUCTORS (VLAN 20)				
ROOM 1	F0	192.168.2.1	255.255.255.192	192.168.2.62
ROOM 2	F0	192.168.2.2	255.255.255.192	192.168.2.62
ROOM 3	F0	192.168.2.3	255.255.255.192	192.168.2.62
FACULTY PC 1	F0	192.168.2.4	255.255.255.192	192.168.2.62
FACULTY PC 2	F0	192.168.2.5	255.255.255.192	192.168.2.62

FACULTY PC 3	F0	192.168.2.6	255.255.255.192	192.168.2.62
FACULTY PC 4	F0	192.168.2.7	255.255.255.192	192.168.2.62
FACULTY PC 5	F0	192.168.2.8	255.255.255.192	192.168.2.62
FACULTY PC 6	F0	192.168.2.9	255.255.255.192	192.168.2.62
FACULTY PC 7	F0	192.168.2.10	255.255.255.192	192.168.2.62
FACULTY PC 8	F0	192.168.2.11	255.255.255.192	192.168.2.62
FACULTY PC 9	F0	192.168.2.12	255.255.255.192	192.168.2.62
FACULTY PC 10	F0	192.168.2.13	255.255.255.192	192.168.2.62
FACULTY PC 11	F0	192.168.2.14	255.255.255.192	192.168.2.62
ROOM 4	F0	192.168.2.15	255.255.255.192	192.168.2.62
ROOM 5	F0	192.168.2.16	255.255.255.192	192.168.2.62
ROOM 6	F0	192.168.2.17	255.255.255.192	192.168.2.62

MOBILE 1	F0	192.168.2.18	255.255.255.192	192.168.2.62
MOBILE 2	F0	192.168.2.19	255.255.255.192	192.168.2.62
MOBILE 3	F0	192.168.2.20	255.255.255.192	192.168.2.62
MOBILE 4	F0	192.168.2.21	255.255.255.192	192.168.2.62
MOBILE 5	F0	192.168.2.22	255.255.255.192	192.168.2.62
MOBILE 6	F0	192.168.2.23	255.255.255.192	192.168.2.62
MOBILE 7	F0	192.168.2.24	255.255.255.192	192.168.2.62
MOBILE 8	F0	192.168.2.25	255.255.255.192	192.168.2.62
MOBILE 9	F0	192.168.2.26	255.255.255.192	192.168.2.62
MOBILE 10	F0	192.168.2.27	255.255.255.192	192.168.2.62
MOBILE 11	F0	192.168.2.28	255.255.255.192	192.168.2.62

Table 19. IP Addressing Assignment Table for Operations VLAN

Device Name	Interface	IP Address	Subnet Mask	Default Gateway
OPERATIONS (VLAN 30)				
OPERATIONS PC1	F0	192.168.1.1	255.255.255.192	192.168.1.62
OPERATIONS PC2	F0	192.168.1.2	255.255.255.192	192.168.1.62
OPERATIONS PC3	F0	192.168.1.3	255.255.255.192	192.168.1.62
OPERATIONS PC4	F0	192.168.1.4	255.255.255.192	192.168.1.62
OPERATIONS PC5	F0	192.168.1.5	255.255.255.192	192.168.1.62
OPERATIONS PC6	F0	192.168.1.6	255.255.255.192	192.168.1.62
OPERATIONS PC7	F0	192.168.1.7	255.255.255.192	192.168.1.62
OPERATIONS PC8	F0	192.168.1.8	255.255.255.192	192.168.1.62
OPERATIONS PC9	F0	192.168.1.9	255.255.255.192	192.168.1.62
OPERATIONS PC10	F0	192.168.1.10	255.255.255.192	192.168.1.62

OPERATIONS PC11	F0	192.168.1.11	255.255.255.192	192.168.1.62
OPERATIONS PC12	F0	192.168.1.12	255.255.255.192	192.168.1.62
SECRETARY PC	F0	192.168.1.13	255.255.255.192	192.168.1.62
LIBRARY PC	F0	192.168.1.14	255.255.255.192	192.168.1.62
MOBILE 1	F0	192.168.1.15	255.255.255.192	192.168.1.62
MOBILE 2	F0	192.168.1.16	255.255.255.192	192.168.1.62
MOBILE 3	F0	192.168.1.17	255.255.255.192	192.168.1.62
MOBILE 4	F0	192.168.1.18	255.255.255.192	192.168.1.62
MOBILE 5	F0	192.168.1.19	255.255.255.192	192.168.1.62
MOBILE 6	F0	192.168.1.20	255.255.255.192	192.168.1.62
MOBILE 7	F0	192.168.1.21	255.255.255.192	192.168.1.62
MOBILE 8	F0	192.168.1.22	255.255.255.192	192.168.1.62

MOBILE 9	F0	192.168.1.23	255.255.255.192	192.168.1.62
MOBILE 10	F0	192.168.1.24	255.255.255.192	192.168.1.62
MOBILE 11	F0	192.168.1.25	255.255.255.192	192.168.1.62
MOBILE 12	F0	192.168.1.26	255.255.255.192	192.168.1.62
MOBILE 13	F0	192.168.1.27	255.255.255.192	192.168.1.62
MOBILE 14	F0	192.168.1.28	255.255.255.192	192.168.1.62

Table 20. IP Addressing Assignment Table for IT Department

Device Name	Interface	IP Address	Subnet Mask	Default Gateway
IT DEPARTMENT (VLAN 40)				
IT PC1	F0	192.168.1.65	255.255.255.224	192.168.1.94
IT PC2	F0	192.168.1.66	255.255.255.224	192.168.1.94
IT PC3	F0	192.168.1.67	255.255.255.224	192.168.1.94

IT PC4	F0	192.168.1.68	255.255.255.224	192.168.1.94
IT PC5	F0	192.168.1.69	255.255.255.224	192.168.1.94
IT PC6	F0	192.168.1.70	255.255.255.224	192.168.1.94
IT MOBILE_1	F0	192.168.1.71	255.255.255.224	192.168.1.94
IT MOBILE_2	F0	192.168.1.72	255.255.255.224	192.168.1.94
IT MOBILE_3	F0	192.168.1.73	255.255.255.224	192.168.1.94
IT MOBILE_4	F0	192.168.1.74	255.255.255.224	192.168.1.94
IT MOBILE_5	F0	192.168.1.75	255.255.255.224	192.168.1.94
IT MOBILE_6	F0	192.168.1.76	255.255.255.224	192.168.1.94

Table 21. IP Addressing Assignment Table for Guests VLAN

Device Name	Interface	IP Address	Subnet Mask	Default Gateway
GUESTS (VLAN 50)				
DEVICE 1	N/A	192.168.3.7	255.255.255.0	192.168.3.254
DEVICE 2	N/A	192.168.3.8	255.255.255.0	192.168.3.254
DEVICE 3	N/A	192.168.3.9	255.255.255.0	192.168.3.254
DEVICE 4	N/A	192.168.3.10	255.255.255.0	192.168.3.254
DEVICE 5	N/A	192.168.3.11	255.255.255.0	192.168.3.254
DEVICE 6	N/A	192.168.3.12	255.255.255.0	192.168.3.254
DEVICE 7	N/A	192.168.3.13	255.255.255.0	192.168.3.254
DEVICE 8	N/A	192.168.3.14	255.255.255.0	192.168.3.254
DEVICE 9	N/A	192.168.3.15	255.255.255.0	192.168.3.254
DEVICE 10	N/A	192.168.3.16	255.255.255.0	192.168.3.254

DEVICE 11	N/A	192.168.3.17	255.255.255.0	192.168.3.254
DEVICE 12	N/A	192.168.3.18	255.255.255.0	192.168.3.254
DEVICE 13	N/A	192.168.3.19	255.255.255.0	192.168.3.254
DEVICE 14	N/A	192.168.3.20	255.255.255.0	192.168.3.254
DEVICE 15	N/A	192.168.3.21	255.255.255.0	192.168.3.254
DEVICE 16	N/A	192.168.3.22	255.255.255.0	192.168.3.254
DEVICE 17	N/A	192.168.3.23	255.255.255.0	192.168.3.254
DEVICE 18	N/A	192.168.3.24	255.255.255.0	192.168.3.254
DEVICE 19	N/A	192.168.3.25	255.255.255.0	192.168.3.254
DEVICE 20	N/A	192.168.3.26	255.255.255.0	192.168.3.254
DEVICE 21	N/A	192.168.3.27	255.255.255.0	192.168.3.254
DEVICE 22	N/A	192.168.3.28	255.255.255.0	192.168.3.254

DEVICE 23	N/A	192.168.3.29	255.255.255.0	192.168.3.254
DEVICE 24	N/A	192.168.3.30	255.255.255.0	192.168.3.254
DEVICE 25	N/A	192.168.3.31	255.255.255.0	192.168.3.254
DEVICE 26	N/A	192.168.3.32	255.255.255.0	192.168.3.254
DEVICE 27	N/A	192.168.3.33	255.255.255.0	192.168.3.254
DEVICE 28	N/A	192.168.3.34	255.255.255.0	192.168.3.254
DEVICE 29	N/A	192.168.3.35	255.255.255.0	192.168.3.254
DEVICE 30	N/A	192.168.3.36	255.255.255.0	192.168.3.254
DEVICE 31	N/A	192.168.3.37	255.255.255.0	192.168.3.254
DEVICE 32	N/A	192.168.3.38	255.255.255.0	192.168.3.254
DEVICE 33	N/A	192.168.3.39	255.255.255.0	192.168.3.254
DEVICE 34	N/A	192.168.3.40	255.255.255.0	192.168.3.254

DEVICE 35	N/A	192.168.3.41	255.255.255.0	192.168.3.254
DEVICE 36	N/A	192.168.3.42	255.255.255.0	192.168.3.254
DEVICE 37	N/A	192.168.3.43	255.255.255.0	192.168.3.254
DEVICE 38	N/A	192.168.3.44	255.255.255.0	192.168.3.254
DEVICE 39	N/A	192.168.3.45	255.255.255.0	192.168.3.254
DEVICE 40	N/A	192.168.3.46	255.255.255.0	192.168.3.254
DEVICE 41	N/A	192.168.3.47	255.255.255.0	192.168.3.254
DEVICE 42	N/A	192.168.3.48	255.255.255.0	192.168.3.254
DEVICE 43	N/A	192.168.3.49	255.255.255.0	192.168.3.254
DEVICE 44	N/A	192.168.3.50	255.255.255.0	192.168.3.254
DEVICE 45	N/A	192.168.3.51	255.255.255.0	192.168.3.254
DEVICE 46	N/A	192.168.3.52	255.255.255.0	192.168.3.254

DEVICE 47	N/A	192.168.3.53	255.255.255.0	192.168.3.254
DEVICE 48	N/A	192.168.3.54	255.255.255.0	192.168.3.254
DEVICE 49	N/A	192.168.3.55	255.255.255.0	192.168.3.254
DEVICE 50	N/A	192.168.3.56	255.255.255.0	192.168.3.254
LIBRARY PC 1	N/A	192.168.3.1	255.255.255.0	192.168.3.254
LIBRARY PC 2	N/A	192.168.3.2	255.255.255.0	192.168.3.254
LIBRARY PC 3	N/A	192.168.3.3	255.255.255.0	192.168.3.254
LIBRARY PC 4	N/A	192.168.3.4	255.255.255.0	192.168.3.254
LIBRARY PC 5	N/A	192.168.3.5	255.255.255.0	192.168.3.254
LIBRARY PC 6	N/A	192.168.3.6	255.255.255.0	192.168.3.254

Table 22. IP Addressing Assignment Table for Services Department

Device Name	Interface	IP Address	Subnet Mask	Default Gateway
SERVICES DEPARTMENT (VLAN 50)				
ORION SERVER	N/A	192.168.1.97	255.255.255.248	192.168.1.102
NETWORK PRINTER	N/A	192.168.1.98	255.255.255.248	192.168.1.102
NETWORK PRINTER	N/A	192.168.1.99	255.255.255.248	192.168.1.102

6. Security Configuration

Network security is a critical aspect of any network infrastructure. Without proper safeguards, networks are vulnerable to numerous threats, including DHCP snooping, DHCP starvation attacks, ARP poisoning attacks and many more. Furthermore, unauthorized infiltrators can illicitly retrieve vital network data, potentially leading to financial losses and reputational damage. Given these potential vulnerabilities, prioritizing network security is of utmost importance.

In response to these challenges, we have implemented a comprehensive suite of security measures. The first line of defense is the configuration of all routers and switches with initial device settings, adhering to best practices for manageability and security. For secure remote access, all routers and switches are configured to allow SSH instead of Telnet. Additionally, all switches are configured with VLAN Trunk Protocol (VTP) to ensure consistency and accuracy of VLAN configuration across the network. This also optimizes the use of trunk links by pruning unnecessary broadcast traffic from VLANs not present on downstream switches.

To streamline network administration, there is now a dedicated DHCP server unlike in the previous setup where the routers function as the DHCP server. This facilitates easier monitoring and management of network addresses. Syslog, NTP and SNMP with its respective read and write passwords were also implemented for monitoring, time synchronization, and increased management capabilities. ACLs were also implemented to only allow certain departments to communicate with each other, following security best practices. Trunk ports are also configured to disable DTP negotiation, preventing the sending of DTP frames when the neighboring device does not support DTP. Moreover, access ports in a switch are secured from unauthorized access by observing incoming source MAC addresses on a configured port, dynamically learning them, and adding them to the running configuration. Portfast was also enabled for access ports for faster connectivity in order to not wait for STP convergence. All unused ports are also assigned to a blackhole VLAN. Furthermore, to enhance security, IP DHCP snooping is enabled to prevent breaches and attacks such as DHCP Starvation and DHCP spoofing. ARP inspection is also enabled to validate ARP packets in the network, thereby

preventing data theft, unauthorized monitoring, ARP spoofing attacks, and other threats that exploit ARP weaknesses. Next, to prevent spanning tree loops and block BPDUs sent from unauthorized devices, BPDU Guard was implemented. CDP and LLDP were also disabled for security purposes. Lastly, the default native VLAN was also changed from VLAN 1 to VLAN 2 to prevent attackers from sending untagged traffic to gain unauthorized access.

Coupled with secure password practices and basic housekeeping, these measures ensure the robustness of our network security. This comprehensive approach to network security ensures that AITC's network remains secure, efficient, and resilient in the face of potential threats. By prioritizing security, we can protect the network and the valuable data it carries, ensuring the continued success of AITC's operations.

Table 19. Security Measures Implemented

Requirement	Security Measure Implemented
All routers and switches must be configured with initial device settings as a primary line of defense against unauthorized access to a network and its sensitive data following best practices for manageability and security.	§ Set up a banner message warning users of unauthorized access § Set privileged exec, console and line VTY passwords § All network devices have their own unique passwords § Implement password encryption § Used passwords with the following characteristics: 1. Minimum length of 8 characters with all passwords having a length of 16 characters for additional security. 2. Included lowercase and uppercase letters. 3. Always begins with a letter. 4. Included a mix of symbols except the '?' 5. No similar, duplicate, or sequential characters § Shutdown unused ports
All routers and switches must be configured to allow for SSH instead of Telnet to remotely access the devices securely.	§ Had all network devices' IP domain set to xcite.com § Generated an RSA Key with 2048 bits § Set the SSH version to 2 to gain full access to all the features § Set a unique username and password for each network device § Used unique passwords with the following characteristics: 1. Minimum length of 8 characters with all passwords having a length of 16 characters for additional security. 2. Included lowercase and uppercase letters. 3. Always begins with a letter. 4. Included a mix of symbols except the '?' 5. No similar, duplicate or sequential characters § Configure the virtual terminal lines (VTY) on a Cisco device to accept incoming SSH connections only

	§ Configure the VTY lines to enable the SSH protocol on the VTY lines and require local authentication using the local username database. § Set the maximum idle time of the connection for 3 minutes § (Router only) Set the VTY lines' blocking duration to 300 seconds for 5 incorrect login attempts within 120 seconds.
All switches must be configured with VTP to maintain consistency and accuracy of VLAN configuration by propagating any changes made on one switch to all other switches in the domain. This also allows for efficient use of trunk links by pruning unnecessary broadcast traffic from VLANs that are not present on the downstream switches.	§ Set S1 and S2 as the VTP server since they are the common switches that all the departments are connected to. § All other department switches are the VTP clients § Set the VTP domain name as xcite.com § Used a common VTP password with the following characteristics: 1. Minimum length of 8 characters with all passwords having a length of 16 characters for additional security. 2. Included lowercase and uppercase letters. 3. Always begins with a letter. 4. Included a mix of symbols except the '?' 5. No similar, duplicate or sequential characters § Set the VTP version to 2, since version 2 can perform additional consistency checks and support Token Ring networks.
Assigned Aries Server as the dedicated DHCP server to simplify the process of assigning and managing IP addresses within a network. This simplifies network administration by centralizing the control of IP address distribution, making it easier to monitor and manage network configurations.	§ Create a DHCP pool for each VLAN with its corresponding department name § Specify the corresponding network for each VLAN § Specify the corresponding default gateway assigned for each VLAN § Assigned helper addresses to the L3 switches to allow them to connect to the DHCP server.
Configure the trunk ports to disable DTP negotiation to stop it from sending DTP frames when the neighboring device does not support DTP.	§ Issued the switchport trunk nonegotiate command

Secure all the access ports in a switch from unauthorized access by observing the incoming source MAC addresses on a configured port, dynamically learning it and adding them to the running configuration. Assign all unused ports to a blackhole VLAN to prevent VLAN hopping attacks, isolate traffic in the data flow, and restrict user access within the network. Implement BPDU Guard to prevent spanning tree loops and block BPDUs sent from unauthorized devices. Changed default native VLAN from VLAN 1 to VLAN 2. Enabled portfast for access ports.	§ Enable port security § Set the maximum number of MAC addresses allowed on each port to 2 § Set the maximum number of MAC addresses allowed on the admin port to 1 § Enable the sticky learning of MAC addresses § Set the action to take when a violation occurs to restrict to drop the packets but not shutdown the port. § Set the action to take when a violation occurs to shutdown for the admin port for increased security. § Assign the unused ports to VLAN 100 or the blackhole VLAN § Implement BPDU Guard § Issued the command "switchport trunk native VLAN 2" § Enabled portfast for access ports
Enable IP DHCP snooping to prevent security breaches and attacks such as DHCP Starvation attack and DHCP spoofing attack.	§ Enable DHCP snooping globally on the switch § Enable DHCP snooping on the specified VLANs that will pass through the switch. § Configure the selected interfaces that are connected to switches or routers as trusted interfaces § Set a rate limit for DHCP packets on the selected interfaces that are access ports to 2. If the number of DHCP packets received per second exceeds this limit, the extra packets will be dropped.
Enable ARP inspection to check the validity of ARP packets in a network. This stops data theft, unauthorized monitoring, ARP spoofing attacks, and other threats that use ARP weaknesses.	§ Enable Dynamic ARP Inspection (DAI) on the specified VLANs that will pass through the switch. § Configure the selected interfaces that are connected to switches or routers as trusted interfaces so the switch does not check ARP packets that it receives on the trusted interface.
Enable wireless connectivity and implement a secured password to access the WLAN. This	§ End devices are required to input a password to access their corresponding WLANs. § A password is needed to access a WLAN.

allows flexibility for a BYOD setup within the office network, while securing the network from unauthorized access.	§ The passwords followed these characteristics: 1. Minimum length of 8 characters with all passwords having a length of 16 characters for additional security. 2. Included lowercase and uppercase letters. 3. Always begins with a letter. 4. Included a mix of symbols except the '?' 5. No similar, duplicate or sequential characters
Require a username and password to access the WLC and modify the configurations for wireless connectivity. This prevents unauthorized access from hacking the network.	§ A corresponding username and password is needed to access the WLC. § The passwords followed these characteristics: 1. Minimum length of 8 characters with all passwords having a length of 16 characters for additional security. 2. Included lowercase and uppercase letters. 3. Always begins with a letter. 4. Included a mix of symbols except the '?' 5. No similar, duplicate or sequential characters
Enable syslog to log events to the Orion server and enable NTP to sync all the times of all the infrastructure devices. Disable Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) for added security.	§ Configure no cdp run and no lldp run on all infrastructure devices § Enable NTP and sync all devices' clock to the Orion Server § Configure the devices to timestamp logging messages including the date and time to the Orion Server
Enable SNMP on devices. However, only the administrator PC must have read/write access to devices, while members of the IT office will have read only access to device configurations.	§ Configure read-only access to members of the IT office § Configure read-write access to the administrator PC § The passwords followed these characteristics: 1. Minimum length of 8 characters with all passwords having a length of 16 characters for additional security. 2. Included lowercase and uppercase letters. 3. Always begins with a letter. 4. Included a mix of symbols except the '?' 5. No similar, duplicate or sequential characters
Implement Access Control Lists (ACLs) to prevent unauthorized access to certain VLANs	§ Add a remark to know the function of the ACL and which VLANs are restricted.

and organize traffic to improve network efficiency.	§ Number the ACL according to the VLAN number § Configure the allowed VLANs in the corresponding ACL § Configure a deny statement to block all traffic that doesn't match the permitted IP addresses § Assign the ACL to the corresponding sub interface § Apply the ACL to outbound traffic on the selected interface

Table 20. Access Control Matrix

Department	Students	Instructors	Operations	IT	Guests	Services	Management
Students	✓						
Instructors		✓	✓	✓		✓	
Operations		✓	✓	✓		✓	
IT		✓	✓	✓	✓	✓	
Guests				✓	✓		
Services		✓	✓	✓		✓	
Management							✓

Table 21. Usernames and Password

Device	Enable Secret	Console	SSH	VTP
ROUTER_MAIN	D-C*P[V<(;u=3&_#	Y.{H/dyew6A)#$t}	Username: AdminR1 Password: L]+'gb)5Y/&V?%#A	N/A
ROUTER_BACKUP	BX%TdAeFWx7/s{G`	J!yb_t<(nTg=7;"C	Username: AdminR2 Password: rW_3GA>&(;yF^dT=	N/A
FIRST_FLOOR	a3@h+4Tzk/rFVBvC	VZ$"[4{,muph5eLc	Username: Admin_FirstFloorSwitch Password: TtX5{u73V6-G^4Lb	Server Password: Mz$NruW2,7f~[:'Y
SECOND_FLOOR	U[W_X.JfF{B5gK'P	tFR*c-=wn7,5f<P]	Username: Admin_SecondFloorSwitch Password: TjJEX/zsAC>G)_6x	Server Password: Mz$NruW2,7f~[:'Y

ROOM1	W}r<m5>3vGB$!24'	r>)D"+v2YjWu@R4Q	Username: Student_Switch1 Password: ZT%39cr;_B#)4A$j	Client Password: Mz$NruW2,7f~[:'Y
ROOM2	xnqAR}"W$8vS4,-D	A'%@8v7;kq-sTp*R	Username: Student_Switch2 Password: e}qU3;@LwH$_<aPh	Client Password: Mz$NruW2,7f~[:'Y
ROOM3	Xr-3WxQ[b+p2;Fqw	q,95}`hfNAHa=!:v	Username: Student_Switch3 Password: dX4#[;J]r,f@De'!	Client Password: Mz$NruW2,7f~[:'Y
OPERATIONS_IT_SWITCH	LU'9n@(u4;E5-TF<	B.s(D&hUF_5YHT^R	Username: Operations_IT_Switch Password: PmEK6j79h+Xd*=qx	Client Password: Mz$NruW2,7f~[:'Y
MANAGE_SWITCH	K(_G`Hs}kX~5nhQJ	hTP*)E&#7q-A,X94	Username: Manage_Switch Password: WC#q~}"wb3fR{Lp2	Client Password: Mz$NruW2,7f~[:'Y
ROOM4	VCM3~*YUcR8kLx;=	x@j}*-^)h2Mb3y%z	Username:	Client

			Student_Switch4 Password: ZT%39cr;_B#)4A$j	Password: Mz$NruW2,7f~[:'Y
ROOM5	g8W+;dk}x)u63A*y	zB.V4]KU:>%q*FMS	Username: Student_Switch5 Password: p[W-254_c3Am{J`;	Client Password: Mz$NruW2,7f~[:'Y
ROOM6	yEj~ZaL4BV635`zv	f.m~CM4Ehg28G-B/	Username: Student_Switch6 Password: WK4pNEH(}c5/n9M*	Client Password: Mz$NruW2,7f~[:'Y
OPERATIONS_IT_SWITCH_2	L;)8HGU*DtrnzX^J	U2mr6[#xcbJ-E95n	Username: Other2_Switch Password: Qsd#2w'}Y[{;>&C_	Client Password: Mz$NruW2,7f~[:'Y
INSTRUCTOR_SWITCH	vKT[jY`ka3'^y9p=	Xw)(v7zQ~Lx>TFhA	Username: Instructor_Switch Password:	Client Password: Mz$NruW2,7f~[:'Y

			HY2BE<rT5w#Qyf*W	

Table 22. Wireless Usernames and Passwords

Username	Password
Admin_WLC	t$_[u"Ub*5!vQ@9,
Instructors	g5VN.By;%L,wD(Zh
Operations	Mxw=)TE>gC4es7dH
IT	L4k+HPCR,p{9?qKz
Guests	AVmP)[nf9KeL8>7{

Table 23. SNMP passwords

Department	Password
IT (read only)	khgp8{6#nW93sJ$B[DP>w!
Management (read and write)	Suf~Gs94wNW{2xX<JA>,Ph

7. Design Discussion

This design discussion will focus on explaining the group's choices regarding the physical layout and topology, logical topology, IP addressing scheme, and the various configurations made for network functionality and security.

The network design of the physical layout emphasizes both functionality and safety, optimizing the layout of devices, switches, routers, and cabling to ensure efficient communication flow while minimizing workplace hazards. This was done by the use of raised flooring as well as routing of cables across walls and

ceilings when raised flooring was not available. The use of different coloured cables for departmental distinctions, aids visual clarity and ease of maintenance.

For the physical topology, all network devices, except for certain L2 switches for easier management and LAPs for connectivity reasons, were placed in the server room to ensure security from unauthorized access. The rest of the end devices, certain L2 switches and LAPs are placed in their corresponding rooms depending on which department they belong to. All switch to switch and switch to router connections used a fast Gigabit Ethernet port if available for faster speeds in the case of high network usage. Both routers have 1 free gigabit ethernet port for internet connectivity. Regarding switch and LAP placement, the operations and IT department share one switch for the first floor. Meanwhile, each room for the students on the first floor is equipped with 1 layer 2 switch, accommodating its higher user density. Finally, the management, instructor, services, and LAP for the guests share a single layer 2 switch for the first floor. However, on the second floor, the instructors have a dedicated layer 2 switch for the second floor. In addition, similar to the first floor, each room for the students on the second floor is equipped with 1 layer 2 switch, accommodating its higher user density. Lastly, the operations, guests and services share a single layer 2 switch for the second floor, demonstrating an efficient allocation of resources.

The logical topology reflects a resilient architecture, employing redundancy strategies like EtherChannel and HSRP, and adhering to a hierarchical model for consistent configuration and scalability. The architecture also adheres to the three-layer hierarchical model consisting of the access layer, distribution layer, and core layer, allowing the visualization of the role of switches depending on where they are in the hierarchy and ensures consistent configuration across switches per layer. In addition, this topology follows a replicable pattern where if the department contains enough users, it can have its own corresponding layer 2 switch. This allows for seamless network expansion and integrated services without heavy impact on network performance. Tuning STP, using etherchannels in high traffic areas and changing the active router for several VLANs was done for load balancing of the network. Portfast was also enabled for access ports for faster connectivity. The design also consists of proper user grouping implemented through VLANs with inter-VLAN routing enabled and managed through VTP. It also encompasses the configuration of WLAN support, correctly grouped according to the VLAN membership of their owners and following their same access policies as their wired counterparts. All in all, this setup guarantees continuous available connectivity even in the event of a cable or device failure. This redundancy strategy aligns with best practices for network resilience. For network administration, syslog, NTP and SNMP with its respective read and write passwords were implemented to allow for robust monitoring, time synchronization, and management capabilities for AITC.

For the IP addressing scheme, the group allocated the IPv4 address space 192.168.0.0/20 and employing Variable Length Subnet Masking (VLSM), made use of multiple subnet masks including 255.255.255.0 for VLANs 10 and 50, 255.255.255.192 for VLANs 20 and 30, 255.255.255.224 for VLANs 40 and 99, and 255.255.255.248 for VLAN 60. Some additional VLANs are VLAN 100 for the Blackhole VLAN for unused ports, and VLAN 2 for the native VLAN, with these VLANS being more geared towards security purposes. Regardless, this implementation made for an easily scalable network, advantageous to Alonzo IT Training Center (AITC). Moreover, this enhances the security of the network as the different user types are separated which reduces the damage caused by potential data breaches. This also makes the implementation of access control units more effective via the restricting access of each department to relevant resources to the respective department. The default gateway for each VLAN is set to the last usable address in the

network adhering to Cisco standards and promoting a clear understanding of the network's capacity in terms of device accommodation. In the instructions for the case study, while the table for the expected number of guests only considered mobile devices in some departments, the first set of instructions for the logical topology noted that it is expected that each person in each user group will carry an extra device to be connected to a wireless network, so for departments that never mentioned that it would be carrying mobile devices (eg. the student VLAN), additional leeway was considered for the ip addressing scheme to accommodate this earlier instruction, such as making the subnet mask /24 for the student VLAN instead of /25 since including a personal device for each student would mean there needing to be 240 available addresses instead of 120.

Prioritizing network security, the design implements a suite of measures to safeguard against DHCP snooping, ARP poisoning, and unauthorized access. Industry practices were made use of such as basic housekeeping, generation of strong passwords following secure password best practice, making use of SSH and disabling Telnet, as well as a dedicated DHCP server to streamline network administration and enhance manageability. Furthermore, trunk ports and access ports were secured. Unused ports were assigned to a blackhole VLAN, and additional measures such as disabling DTP, enabling DHCP snooping, ARP inspection, BPDU Guard, and changing the default native VLAN were employed to prevent breaches and attacks. CDP and LLDP were disabled for security purposes and to prevent reconnaissance of AITC's network devices. ACLs were also implemented to only allow certain departments to communicate with each other. Doing all of these ensures the resilience and efficiency of AITC's operations, safeguarding valuable data and maintaining network integrity.