ITNET03 Case Study
Alonzo IT Training Center Network Documentation

PHASE 2

Submitted by:

Bañez, Laiven Carleen

Bueno, Jonathan Angelo

Conde, Dominique Ann

Lee, Cayra Maxine

Salvador, Merylle Shayne

Submitted to:

Gregory Cu

Date:

Aug 4, 2023

I. IP ADDRESSING SCHEME

Listed below is the IP Addressing Scheme Table which includes all the subnets, the number of hosts needed per subnet, network addresses, subnet masks, prefix lengths, and usable host address ranges, as well as the IP addresses assigned to each device, WLAN, and DHCP pools in the network.

SUBNETS						
Subnet	No. of Host	Prefix	Network Address	First Host	Last Host	Broadcast Address
Management/ VLAN 99	32	/27	192.168.99.0	192.168.99.1	192.168.99.30	192.168.99.31
IT / VLAN 10	16	/28	192.168.10.0	192.168.10.1	192.168.10.14	192.168.10.15
Services / VLAN 20	8	/29	192.168.20.0	192.168.20.1	192.168.20.6	192.168.20.7
Operations / VLAN 30	32	/27	192.168.30.0	192.168.30.1	192.168.30.30	192.168.30.31
Instructors / VLAN 40	32	/27	192.168.40.0	192.168.40.1	192.168.40.30	192.168.40.31
Students / VLAN 50	128	/25	192.168.50.0	192.168.50.1	192.168.50.126	192.168.50.127
Guests / VLAN 60	64	/26	192.168.60.0	192.168.60.1	192.168.60.62	192.168.60.63

Device	Interface	IP Address	Subnet Mask	Default Gateway
MANAGEMENT				
ALPHA_R1	S0/1/0	10.1.1.1	255.255.255.0	
	S0/1/1	10.2.2.1	255.255.255.0	
BETA_R2	S0/1/0	10.1.1.2	255.255.255.0	
	G0/0/0.99	192.168.99.1	255.255.255.224	
	G0/0/0.10	192.168.10.1	255.255.255.240	
	G0/0/0.20	192.168.20.1	255.255.255.248	
	G0/0/0.30	192.168.30.1	255.255.255.224	
	G0/0/0.40	192.168.40.1	255.255.255.224	
	G0/0/0.50	192.168.50.1	255.255.255.128	
	G0/0/0.60	192.168.60.1	255.255.255.192	
CHARLIE_R3	S0/1/0	10.2.2.2	255.255.255.0	
	G0/0/0.99	192.168.99.2	255.255.255.224	
	G0/0/0.10	192.168.10.2	255.255.255.240	
	G0/0/0.20	192.168.20.2	255.255.255.248	
	G0/0/0.30	192.168.30.2	255.255.255.224	
	G0/0/0.40	192.168.40.2	255.255.255.224	

	G0/0/0.50	192.168.50.2	255.255.255.128	
	G0/0/0.60	192.168.60.2	255.255.255.192	
ADMINPC	Fa0/1	192.168.99.29	255.255.255.224	192.168.99.30
ADMIN_AP	G0	192.168.99.19	255.255.255.224	192.168.99.30
ARIES_Server	Fa0	192.168.99.28	255.255.255.224	192.168.99.30
WLC	Management	192.168.99.27	255.255.255.224	192.168.99.30
ADMIN_SW	VLAN 99	192.168.99.6	255.255.255.224	192.168.99.30
SW_FLOOR1	VLAN 99	192.168.99.4	255.255.255.224	192.168.99.30
Port Channel 7	G0/23			
	G0/24			
SW_FLOOR2	VLAN 99	192.168.99.5	255.255.255.224	192.168.99.30
Port Channel 7	G0/23			
	G0/24			
IT				
ITPC1-6	Fa0/1	DHCP		
SERVICES				
PrinterF1	Fa0/1	192.168.20.3	255.255.255.248	192.168.20.6
PrinterF2	Fa0/1	192.168.20.4	255.255.255.248	192.168.20.6
ORION_Server	F0	192.168.99.25	255.255.255.248	192.168.20.6
OPERATIONS				
OD_SWF1	VLAN 99	192.168.99.7	255.255.255.224	192.168.99.30
OD_SWF2	VLAN 99	192.168.99.8	255.255.255.224	192.168.99.30
OD_PC1F1-12	Fa0/1	DHCP		
OD_PC1F2-2	Fa0/1	DHCP		
OD_SPF1	Wi-Fi	DHCP		
OD_SPF2	Wi-Fi	DHCP		
OD_AP1	G0	192.168.99.27	255.255.255.224	192.168.90.30
OD_AP2	G0	192.168.30.27	255.255.255.224	192.168.30.30
INSTRUCTORS				
ID_SW1F1	VLAN 99	192.168.99.9	255.255.255.224	192.168.99.30
ID_SW1F2	VLAN 99	192.168.99.10	255.255.255.224	192.168.99.30
ID_PC1F1-3	Fa0/1	DHCP		
ID_PC1F2-14	Fa0/1	DHCP		
ID_SPF1	Wi-Fi	DHCP		
ID_SPF2	Wi-Fi	DHCP		
ID_AP1	G0	192.168.99.20	255.255.255.224	192.168.99.30
ID_AP2	G0	192.168.99.21	255.255.255.224	192.168.99.30
STUDENTS				
STUDENTS_SW1F1	VLAN 99	192.168.99.11	255.255.255.224	192.168.99.30
STUDENTS_SW2F1	VLAN 99	192.168.99.12	255.255.255.224	192.168.99.30
STUDENTS_SW3F1	VLAN 99	192.168.99.13	255.255.255.224	192.168.99.30

STUDENTS_SW1F2	VLAN 99	192.168.99.14	255.255.255.224	192.168.99.30
STUDENTS_SW2F2	VLAN 99	192.168.99.15	255.255.255.224	192.168.99.30
STUDENTS_SW3F2	VLAN 99	192.168.99.16	255.255.255.224	192.168.99.30
STUDENTS_PC1F1-20	Fa0/1	DHCP		
STUDENTS_PC1F2-20	Fa0/1	DHCP		
STUDENTS_SP1F1	Wi-Fi	DHCP		
STUDENTS_SP1F2	Wi-Fi	DHCP		
STUDENTS_AP1	G0	192.168.99.22	255.255.255.224	192.168.90.30
STUDENTS_AP2	G0	192.168.99.23	255.255.255.224	192.168.90.30
GUESTS				
GUEST_SW1F1	VLAN 99	192.168.99.17	255.255.255.224	192.168.99.30
GUEST_SW1F2	VLAN 99	192.168.99.18	255.255.255.224	192.168.99.30
GUEST_PC1F2-6	Fa0/1	DHCP		
GUEST_SPF1	Wi-Fi	DHCP		
GUEST_SPF2	Wi-Fi	DHCP		
GUESTS_AP1	G0	192.168.99.24	255.255.255.224	192.168.90.30
GUESTS_AP2	G0	192.168.99.26	255.255.255.224	192.168.90.30

SW_FLOOR1 DHCP POOL			
Name	Network Address	Subnet Mask	Default-Router
Management	192.168.99.0	255.255.255.224	192.168.99.30
IT	192.168.10.0	255.255.255.240	192.168.10.14
Services	192.168.20.0	255.255.255.248	192.168.20.6
Operations	192.168.30.0	255.255.255.224	192.168.30.30
Instructors	192.168.40.0	255.255.255.224	192.168.40.30
Students	192.168.50.0	255.255.255.128	192.168.50.126
Guests	192.168.60.0	255.255.255.192	192.168.60.62

SW_FLOOR2 DHCP POOL			
Name	Network Address	Subnet Mask	Default-Router
Management	192.168.99.0	255.255.255.224	192.168.99.30
IT	192.168.10.0	255.255.255.240	192.168.10.14
Services	192.168.20.0	255.255.255.248	192.168.20.6
Operations	192.168.30.0	255.255.255.224	192.168.30.30
Instructors	192.168.40.0	255.255.255.224	192.168.40.30
Students	192.168.50.0	255.255.255.128	192.168.50.126
Guests	192.168.60.0	255.255.255.192	192.168.60.62

WLC Interface Configurations

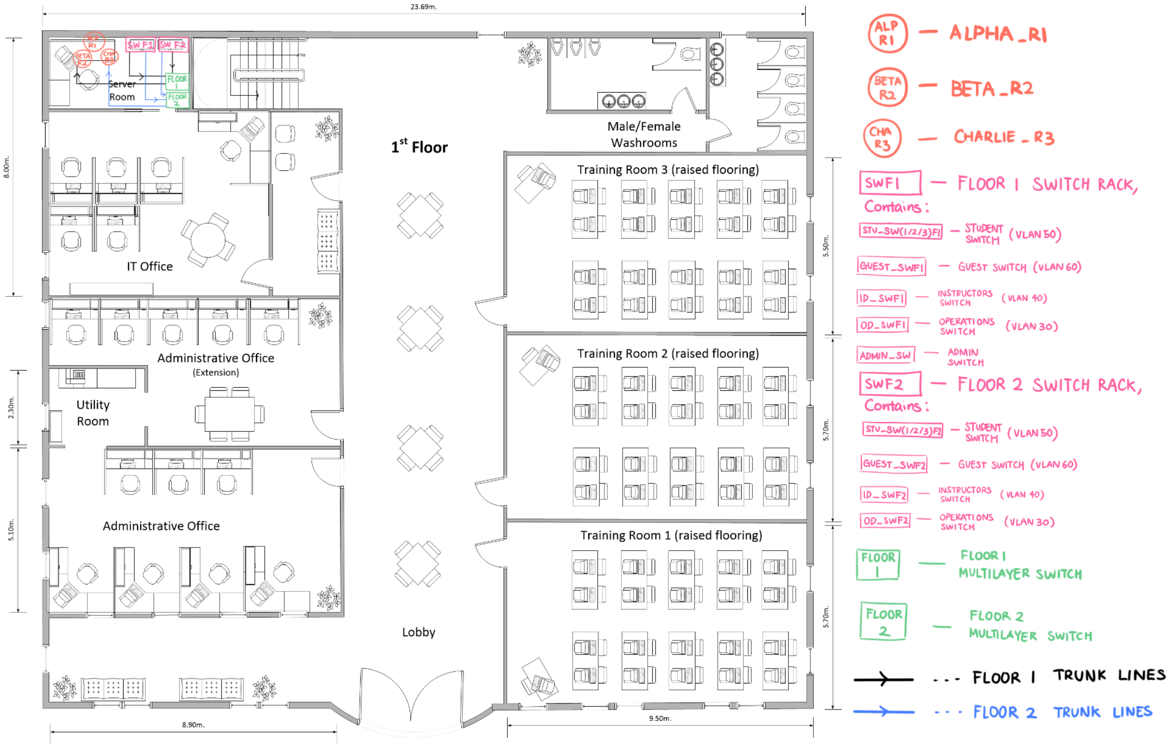
Interface	ID	IP Address	Subnet Mask	Gateway	DHCP Server
IT	10	192.168.10.13	255.255.255.240	192.168.10.14	192.168.99.28
Services	20	192.168.20.5	255.255.255.248	192.168.20.6	192.168.99.28
Operations	30	192.168.30.29	255.255.255.224	192.168.30.30	192.168.99.28
Instructors	40	192.168.40.29	255.255.255.224	192.168.40.30	192.168.99.28
Students	50	192.168.50.125	255.255.255.128	192.168.50.126	192.168.99.28
Guests	60	192.168.60.61	255.255.255.192	192.168.60.62	192.168.99.28
Management	99	192.168.99.27	255.255.255.224	192.168.99.30	

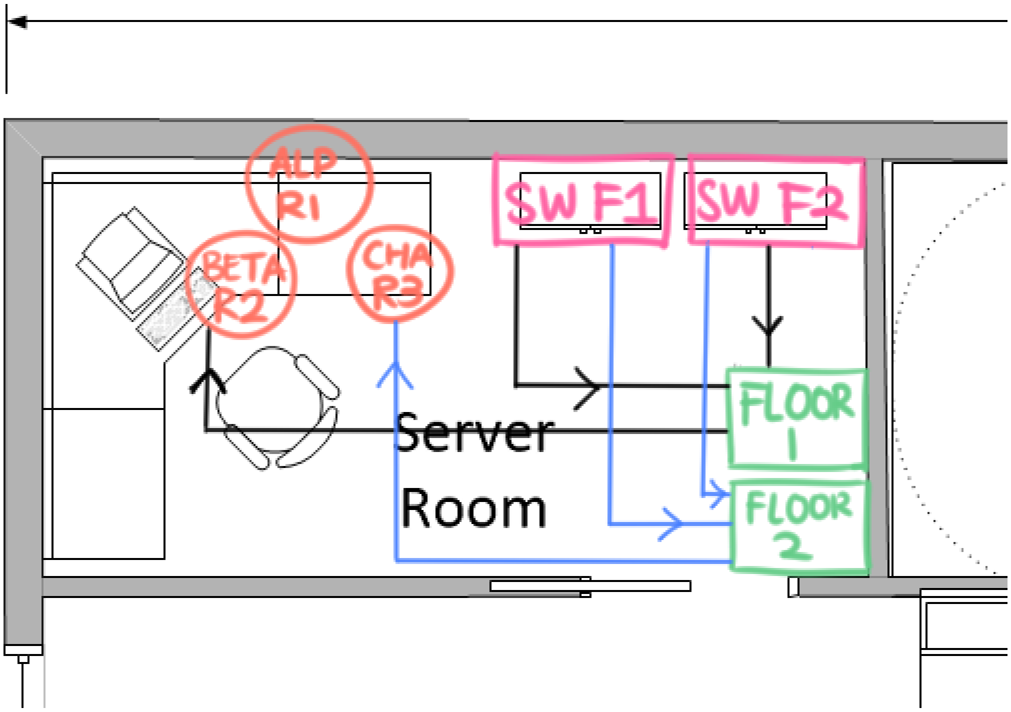
II. PHYSICAL TOPOLOGY

This section illustrates the cable layout of the network devices. The server room located on floor 1 is the central management area where the network infrastructure devices and switch racks are found. This setup provides convenience to the administrators and security for the network.

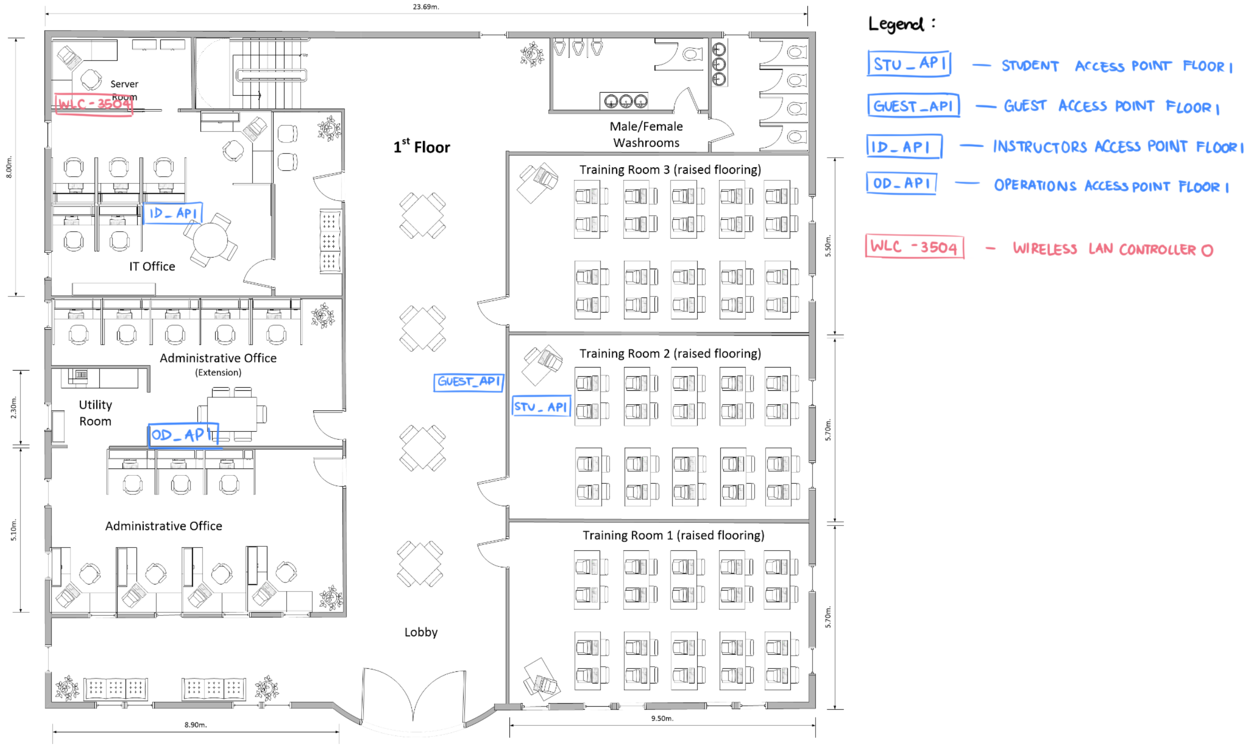
A. First Floor

First Floor - Routers, Multilayer Switches, Access Switches and Trunk Lines


23.69m.
ALP R1
BETA R2
CHA R3
SW F1
SW F2
FLOOR 1
FLOOR 2
Server Room
1st Floor
Male/Female Washrooms
Training Room 3 (raised flooring)
IT Office
Administrative Office (Extension)
Training Room 2 (raised flooring)
Utility Room
Administrative Office
Training Room 1 (raised flooring)
Lobby
8.00m.
2.30m.
5.10m.
5.50m.
5.70m.
5.70m.
8.90m.
9.50m.
ALP R1 — ALPHA_R1
BETA R2 — BETA_R2
CHA R3 — CHARLIE_R3
SWF1 — FLOOR 1 SWITCH RACK, Contains:
STU_SW(1/2/3)F1 — STUDENT SWITCH (VLAN 50)
GUEST_SWF1 — GUEST SWITCH (VLAN 60)
ID_SWF1 — INSTRUCTORS SWITCH (VLAN 40)
OD_SWF1 — OPERATIONS SWITCH (VLAN 30)
ADMIN_SW — ADMIN SWITCH
SWF2 — FLOOR 2 SWITCH RACK, Contains:
STU_SW(1/2/3)F2 — STUDENT SWITCH (VLAN 50)
GUEST_SWF2 — GUEST SWITCH (VLAN 60)
ID_SWF2 — INSTRUCTORS SWITCH (VLAN 40)
OD_SWF2 — OPERATIONS SWITCH (VLAN 30)
FLOOR 1 — FLOOR 1 MULTILAYER SWITCH
FLOOR 2 — FLOOR 2 MULTILAYER SWITCH
... FLOOR 1 TRUNK LINES
... FLOOR 2 TRUNK LINES

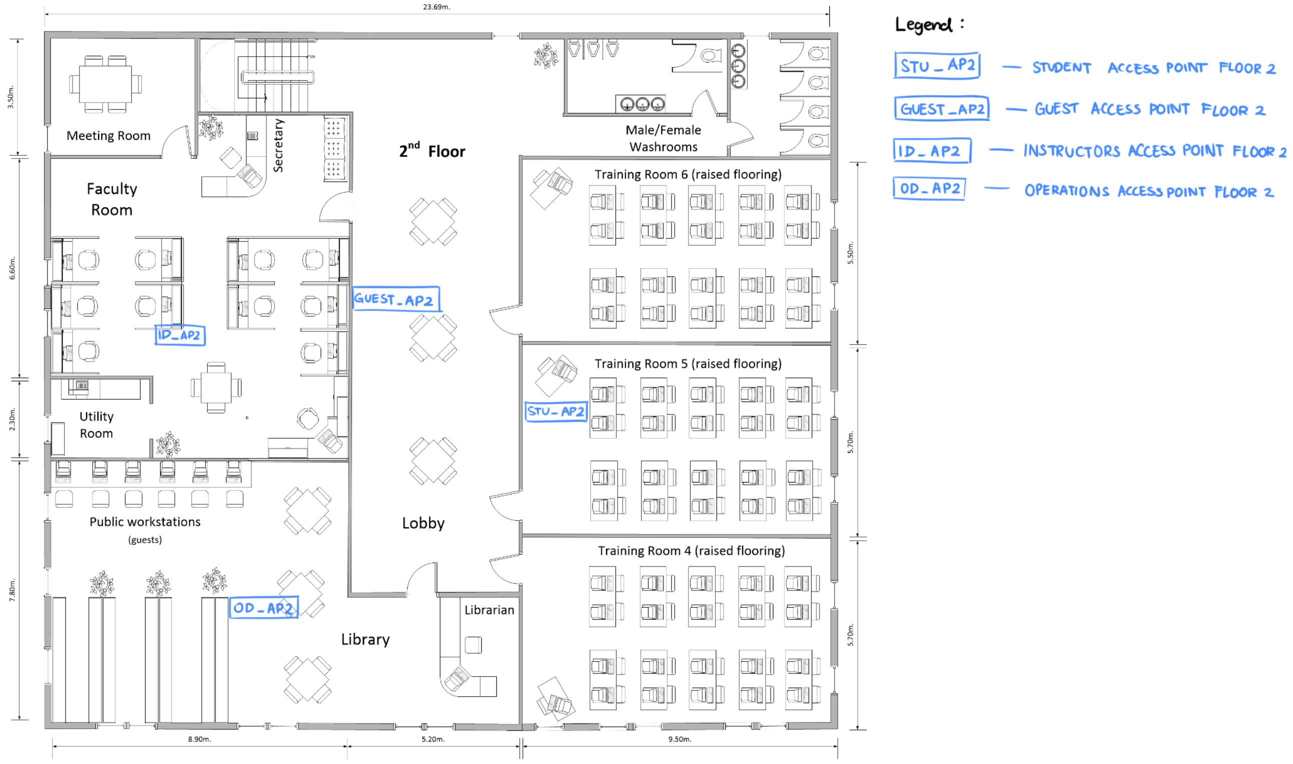


First Floor - Access Points and WLC


23.69m.
Server Room
WLC - 3504
1st Floor
Male/Female Washrooms
Training Room 3 (raised flooring)
ID_AP1
IT Office
Administrative Office (Extension)
GUEST_AP1
STU_AP1
Training Room 2 (raised flooring)
Utility Room
OD_AP1
Administrative Office
Training Room 1 (raised flooring)
Lobby
8.00m.
2.30m.
5.10m.
5.50m.
5.70m.
5.70m.
8.90m.
9.50m.
Legend :
STU_AP1 — STUDENT ACCESS POINT FLOOR 1
GUEST_AP1 — GUEST ACCESS POINT FLOOR 1
ID_AP1 — INSTRUCTORS ACCESS POINT FLOOR 1
OD_AP1 — OPERATIONS ACCESS POINT FLOOR 1
WLC - 3504 - WIRELESS LAN CONTROLLER 0

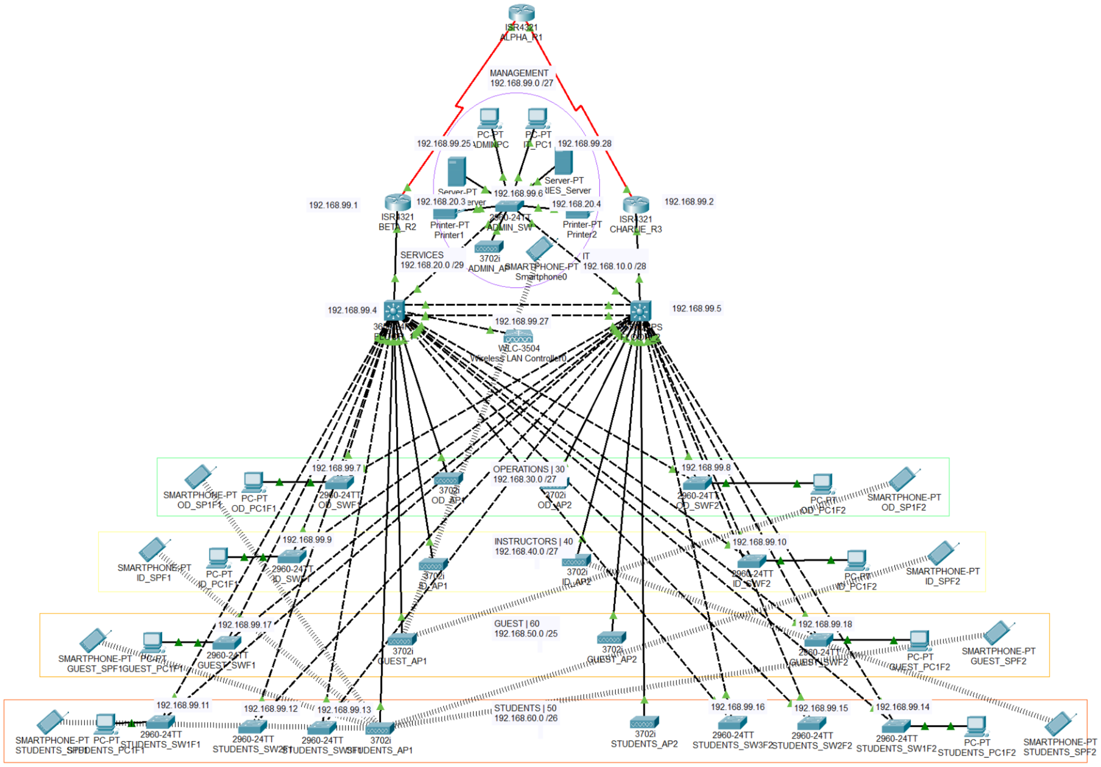
B. Second Floor

Second Floor - Access Points


23.69m.
3.50m.
6.60m.
2.30m.
7.80m.
Meeting Room
Up
Secretary
2nd Floor
Faculty Room
ID_AP2
GUEST_AP2
Utility Room
Public workstations
(guests)
Lobby
OD_AP2
Library
Librarian
Male/Female Washrooms
Training Room 6 (raised flooring)
5.50m.
Training Room 5 (raised flooring)
STU_AP2
5.70m.
Training Room 4 (raised flooring)
5.70m.
8.90m.
5.20m.
9.50m.
Legend :
STU_AP2 — STUDENT ACCESS POINT FLOOR 2
GUEST_AP2 — GUEST ACCESS POINT FLOOR 2
ID_AP2 — INSTRUCTORS ACCESS POINT FLOOR 2
OD_AP2 — OPERATIONS ACCESS POINT FLOOR 2

III. LOGICAL TOPOLOGY

The Logical Topology follows a typical hierarchical model. Using infrastructure devices such as routers, switches, and layer 3 switches that have been configured accordingly, core, distribution, and access layers are formed. To have fault tolerance, the topology utilizes HSRP and STP protocols. It is evident in the number of switches in contrast to the number of users and VLANs. These provide redundancy that prevents complete network failure after one device fails. Additionally, with 3 routers, redundancy in terms of routing will increase network reliability. Additionally, for BYOD, WLANs were implemented in the network using CAPWAP with a central WLC communicating to the APs. These let users connect their devices wirelessly ensuring a seamless connection to the network.



IV. DEVICE PASSWORDS AND CONFIGURATIONS

Devices in the network must be protected from unauthorized users, which is why passwords were configured in all switches and routers. The password is composed of special characters as well, which will make it more difficult to guess. The tables below contain all the passwords as well as what is enabled on each device, as well as the STP Configurations.

VTP Configurations	
Domain Name	Password
ITNET.com	ITN3vtpPass!

Password Configurations		
Device	Console	Privileged Exec Mode
ALPHA_R1	A_R1con!	A_R1en!
BETA_R2	B_R2con!	B_R2en!
CHARLIE_R3	C_R3con!	C_R3en!
ADMIN_SW	A_SW1con!	A_SW1en!
FLOOR_1	F_1con!	F_1en!
FLOOR_2	F_2con!	F_2en!
OD_SWF1	O_SWF1con!	O_SWF1en!
OD_SWF2	O_SWF2con!	O_SWF2en!
ID_SWF1	I_SWF1con!	I_SWF1en!
ID_SWF2	I_SWF2con!	I_SWF2en!
GUEST_SWF1	G_SWF1con!	G_SWF1en!
GUEST_SWF2	G_SWF2con!	G_SWF2en!
STUDENTS_SW1F1	S_SW1F1con!	S_SW1F1en!
STUDENTS_SW2F1	S_SW2F1con!	S_SW2F1en!
STUDENTS_SW3F1	S_SW3F1con!	S_SW3F1en!
STUDENTS_SW1F2	S_SW1F2con!	S_SW1F2en!
STUDENTS_SW2F2	S_SW2F2con!	S_SW2F2en!
STUDENTS_SW3F2	S_SW3F2con!	S_SW3F2en!

STP Configurations			
VLAN	Name	Primary Root	Secondary Root
10	IT	FLOOR_1	ADMIN_SW
20	Services	FLOOR_1	ADMIN_SW
30	Operations	FLOOR_1	ADMIN_SW
40	Instructors	FLOOR_2	ADMIN_SW
50	Students	FLOOR_2	ADMIN_SW
60	Guests	FLOOR_2	ADMIN_SW

SSH Configurations				
Device	Domain Name	SSH Version	Username	Password
ALPHA_R1	ITNET.com	Version 2	Alonzo_Alpha	ITN3SSHAlphaPass!

BETA_R2	ITNET.com	Version 2	Alonzo_Beta	ITN3SSHBetaPass!
CHARLIE_R3	ITNET.com	Version 2	Alonzo_Charlie	ITN3SSHCharliePass!
ADMIN_SW	ITNET.com	Version 2	Alonzo_Admin	ITN3SSHAdminPass!
FLOOR_1	ITNET.com	Version 2	AlonzoF1	ITN3SSHF1Pass!
FLOOR_2	ITNET.com	Version 2	AlonzoF2	ITN3SSHF2Pass!
OD_SWF1	ITNET.com	Version 2	Alonzo_OSWF1	ITN3SSHOSWF1Pass!
OD_SWF2	ITNET.com	Version 2	Alonzo_OSWF2	ITN3SSHOSWF2Pass!
ID_SWF1	ITNET.com	Version 2	Alonzo_ISWF1	ITN3SSHISWF1Pass!
ID_SWF2	ITNET.com	Version 2	Alonzo_ISWF2	ITN3SSHISWF2Pass!
GUEST_SWF1	ITNET.com	Version 2	Alonzo_GSWF1	ITN3SSHGSWF1Pass!
GUEST_SWF2	ITNET.com	Version 2	Alonzo_GSWF2	ITN3SSHGSWF2Pass!
STUDENTS_SW1F1	ITNET.com	Version 2	Alonzo_SSW1F1	ITN3SSHGSW1F1Pass!
STUDENTS_SW2F1	ITNET.com	Version 2	Alonzo_SSW2F1	ITN3SSHGSW2F1Pass!
STUDENTS_SW3F1	ITNET.com	Version 2	Alonzo_SSW3F1	ITN3SSHGSW3F1Pass!
STUDENTS_SW1F2	ITNET.com	Version 2	Alonzo_SSW1F2	ITN3SSHGSW1F2Pass!
STUDENTS_SW2F2	ITNET.com	Version 2	Alonzo_SSW2F2	ITN3SSHGSW2F2Pass!
STUDENTS_SW3F2	ITNET.com	Version 2	Alonzo_SSW3F2	ITN3SSHGSW3F2Pass!

WLC Admin Accounts		
Device	Username	Password
WLC	admin	adminWLC1!

RADIUS Client Configurations		
Client Name	Client IP	Secret
WLC	192.168.99.27	passSecrets19!

SNMP Configurations	
Read-only	Read-write
BeaString	AlonzoString

WLAN Configurations	
Profile Name	WLAN SSID
Alonzo_IT	IT
Alonzo_Services	Services
Alonzo_Operations	Operations

Alonzo Instructors	Instructors
Alonzo_Students	Students
Alonzo Guests	Guests

ACL Matrix								
■	Mgmt	IT	Services	Oprts	Instructs	Students	Guests	Admin PC
Mgmt	■	■	■	■	■	■	■	🟦
IT	■	■	🟦	🟦	🟦	■	🟦	🟦
Services	■	🟦	■	🟦	🟦	■	■	🟦
Oprts	■	🟦	🟦	■	🟦	■	■	🟦
Instructs	■	🟦	🟦	🟦	■	■	■	🟦
Students	■	■	■	■	■	■	■	🟦
Guests	■	🟦	■	■	■	■	■	🟦
Admin PC	🟦	🟦	🟦	🟦	🟦	🟦	🟦	■

V. DISCUSSION OF DESIGN

1. What technology / design was implemented to address the requirement?

Multiple network architecture concepts were implemented in this case study to meet the design specifications. First, the group designed the network such that it follows a standard hierarchical network complete with the core, distribution, and access layers. Second, to achieve redundancy, the network is equipped with abundant network infrastructure devices to create a sufficient Spanning Tree Protocol (STP) and Hot Standby Router Protocol (HSRP). Third, for load balancing and network convergence, Rapid PVST+ and PortFast were used in all switches and Link Aggregation was applied to links that require more bandwidth and redundancy due to the nature of its traffic. Fourth, to provide users access to the network and preserve unused IP addresses, the group utilized VLSM to lease the appropriate number of IP addresses to subnets based on the target number of users. Fifth, for network security, unused ports were shut down, unique passwords were implemented on all network infrastructure devices' VTY lines, console, and Privileged Exec Mode, port security was configured, WPA2 Enterprise Mode was used for WLANs, and BPDU Guard was enabled for access ports. Sixth, for a dynamic network, DHCP was added with appropriate DHCP pools and assigned VLANs to the system. Seventh, for network management, VTP, NTP, Syslog, and SNMP were used. Eighth, a Router-on-a-stick network topology was used to minimize the cost of buying multiple routers. Ninth, to support BYOD, Wireless LANs are implemented using WLCs and controller-based Wireless Access Points (WAPs) or CAPWAP. Lastly, for access control, ACL configurations were placed on the routers in the network.

I. Hierarchical Network Design

II. Network Redundancy

  A. Spanning Tree Protocol (STP)

  B. Hot Standby Router Protocol (HSRP)

  C. Link Aggregation

III. Load Balancing

  A. Rapid PVST+

  B. Spanning Tree Protocol (STP)

  C. Link Aggregation

IV. Network Convergence

  A. Rapid PVST+

  B. PortFast

V. User Access

  A. Variable Length Subnet Mask (VLSM)

  B. Dynamic Host Configuration Protocol (DHCP)

VI. Network Security

  A. Shutdown unused ports

B. Unique Console, VTY Lines, and Privileged Exec Mode passwords
C. Port Security
D. WPA2 Enterprise Mode
E. BPDU Guard
F. All network infrastructure devices are secured in the server room

VII. Dynamic Network
A. Dynamic Host Configuration Protocol (DHCP)

VIII. Network Management
A. VLAN Trunking Protocol (VTP)
B. Network Time Protocol (NTP)
C. Syslog
D. Simple Network Management Protocol (SNMP)

IX. Cost
A. Router-on-a-stick network topology

X. Logical Topology
A. Router-on-a-stick network topology

XI. Bring your own device (BYOD)
A. Wireless Local Area Network (WLAN)
B. Dynamic Host Configuration Protocol (DHCP)
C. Control And Provisioning of Wireless Access Points (CAPWAP)

XII. Access Control
A. Access Control List (ACL)

2. How was the technology / protocol / design implemented (i.e. configuration options and parameters)?

All technology, protocol, and design decisions were made deliberately to cater to the project specifications. To create a Hierarchical Network Design, the group utilized network infrastructure devices to simulate the core, distribution, and access layers. The core and access layers are divided by the two multilayer switches which serve as the distribution layer. Everything above the distribution layer is the core layer wherein most of the computations and operations happen. Below, the access layer can be seen with its multiple switches which aim to provide users access to the network. For the Spanning Tree Protocol (STP), all switches are configured with Rapid PVST+ with both multilayer switches being designated root bridges for specific VLANs (see Device Passwords and Configurations). To utilize the Hot Standby Router Protocol (HSRP), the group decided to use Beta_R2 as its primary source of virtual ip address to use as a default gateway in the network. Charlie_R3 on the other hand is configured as the backup default gateway in case Beta_R2 malfunctions. Link Aggregation was used on the connection between both multilayer switches' GigabitEthernet0/23 and GigabitEthernet0/24. Together, they are called Port Channel 7, which uses the EtherChannel Management Protocol, Port Aggregation Protocol (PAgP). PortFast was configured on all designated access ports (see IP Addressing Scheme) of all switches in the access layer. Variable Length Subnet Mask (VLSM) was appropriately used to provide the correct amount of IP addresses to the VLANs (see IP Addressing Scheme). The subnet masks of the VLANs were decided to be the way it is based on the foreseen number of users on the project specifications. Dynamic Host Configuration Protocol (DHCP) was used on the network by configuring the ARIES Server to be the primary DHCP server. Specific DHCP pool configurations can be found in the section, IP Addressing Scheme. It provides IP addresses to all users trying to connect to the network, wired or wireless, based on their assigned VLAN. To shut down unused ports, they are assigned to a VLAN, then the VLAN is shut down to collectively disable the ports assigned to it. For added security, unique passwords (and usernames, if applicable) for the Consoles, VTY Lines, and Privileged Exec Modes of all network infrastructure devices and the security interface of the WLC were configured (see Device Device Passwords and Configurations). Additionally, Port Security is also configured on all designated access ports with a maximum MAC address of 1 which is dynamically learned (sticky). For WLAN security, a WPA2 Enterprise Mode level of authentication is required. To do this, the ARIES Server acts as the RADIUS Server of the network which authenticates users based on a shared-key system. BPDU Guard is also enabled on all designated access points for added security. Then, all infrastructure devices are secured in the server room where they are unlikely to be accessed remotely preventing threats. VLAN Trunking Protocol (VTP) is configured by providing an appropriate domain name and tight password on all switches for VLAN synchronization. The VTP Servers are ADMIN_SW, SW_FLOOR1, and SW_FLOOR2. The rest of the switches are configured as Clients. For Network Management, Network Time Protocol (NTP) was used by assigning the ORION Server as an NTP Server, SysLog sends system messages and debug output to a centralized server, ORION Server, and Simple Network Management Protocol (SNMP) was utilized by configuring read-only and read-write community strings on all routers (see Device Passwords and Configurations). A Router-on-a-stick logical topology was followed by making subinterfaces and proper encapsulation methods in the routers, BETA_R2 and CHARLIE_R3, to simulate VLAN-tagging in the network. The network also supports Wireless Local Area Networks (WLANs) by employing Control And Provisioning of Wireless Access Points (CAPWAP) on the WLC and APs. This was done by interfacing with the WLC using the Admin PC and creating WLANs assigned to their proper VLANs. Lastly, ACL configurations were placed on the router, CHARLIE_R3, by configuring the main routers following the requirements stated from the given specification (see ACL Matrix).

3. Why was the technology / protocol /design selected and why did you implement it in the way that you did?

The network will incorporate redundancy in its design to enhance fault tolerance and ensure high availability. Applicable protocols, such as Rapid Spanning Tree Protocol were used to enable automatic response to network faults and topology changes, ensuring rapid recovery in case of link or device failures. STP was configured with Rapid PVST+ to ensure a loop-free topology and rapid convergence in case of network changes. Link Aggregation was employed between the two multilayer switches to increase available bandwidth and provide network fault tolerance, and PortFast was enabled on designated access ports to accelerate user access. Port Security was enabled on designated access ports to restrict unauthorized devices from connecting to the network. Additionally, shutting down unused ports, enabling BPDU Guard on designated access ports of all switches, network infrastructure devices being secured in the server room (for convenience and to prevent unwanted remote access), and configuring unique passwords for the consoles, VTY lines, and privileged exec modes of all network infrastructure devices are measures that the group took to enhance network security. Network management provides system administrators with more control over the web. That's why protocols/technologies such as VLAN Trunking Protocol (VTP) which synchronizes VLANs across all switches, Network Time Protocol (NTP) which creates proper timing for networking devices, Syslog captures device messages/notifications from all machines and collects them into one centralized server, and Simple Network Management Protocol (SNMP) whose job is to remotely alter network devices' configurations on a consolidated administrative PC are essential to the network. To reduce costs, the group utilized a Router-on-a-stick network topology by dividing a router's interface into subinterfaces eliminating the need to buy multiple routers to accommodate different VLANs. The group decided to implement a wireless network following an enterprise design. Choosing an enterprise design enables the network to have adaptability, reliability, and convenience. Wireless Controller is implemented to prevent tedious tasks from the network administrators especially as it serves a large company. The following APs are spread out within each floor to ensure full access to the network allowing the users to continue their work even when they are in motion. Radius Server is also implemented as it serves as the authenticator and partitioner to guarantee VLAN division. Each individual that connects has a subnet that acts as a barrier for security not only for the network but also for the individuals' privacy, therefore maintaining WPA2 Enterprise Mode as authentication is our best solution to maintain control by adding unique identifiers to each user as it doubles as security. Overall, the implementation of these technologies and protocols was aimed to provide a scalable, high-performance, and secure network infrastructure that meets the requirements of Alonzo IT Training Center's growing user base and supports its operations effectively.

Appendices

Device Configuratios

```
en
conf t
vtp domain ITNET.com
vtp version 2
vtp mode client
vtp password ITN3vtpPass!

vlan 999
name Native
exit

int range g1/0/3-6, g1/0/16-19, g1/0/7-10
en
conf t
vtp domain ITNET.com
vtp version 2
vtp mode client
vtp password ITN3vtpPass!
int range g0/1-2
switchport mode trunk
switchport trunk native vlan 999

ip domain-name ITNET.com
crypto key generate rsa
ip ssh version 2
username Alonzo secret ITN3SSHPass!
line vty 0 15
transport input ssh
login local
exec-timeout 2
login block-for 600 attempts 3 within 120

en
conf t
enable secret C1$co
line con 0
password cL4$$
login
end
Exit

conf t
```

```
banner motd $Unauthorized access is not allowed!$
enable secret

line con 0
password

login
end
Exit

exit
service password-encryption
```