ITNET02 Case Project

Phase 2
Xcite Network Documentation

Members:
Alfonso, Lorenzo Morris Hidalgo
Bueno, Jonathan Angelo Cagampang
Soemadipradja, Sadira Mareeze
Young, Matthew Mitchell Kha

April 11, 2023

Section 1. IP Addressing Scheme

Displayed below are the tables for the List of Subnets and the Statically Configured Addresses.

The devices that belong to the subnets follow those that are indicated in the Case Study Specifications. All-in-all, the network has 6 subnets. The allotted hosts for each are based on the number of devices in the group doubled. This is to ensure that the network is scalable because Xcite will increase its manpower eventually. The subnets are also designed in such a way that, if hosts were to exceed the allotted number, the network administrator can simply change the subnet mask to compensate.

Device naming conventions may also be observed throughout the network for manageability. For the naming of PCs and Printers, the device's location followed by the PC number is the generic format. For example, a PC located in the Finance and Marketing Department would have the name, FM-PC4, and a Printer located in the Utility Room would have the name, UR-Printer1. On the other hand, similar to PCs, the format for switch names is as follows: the department that it's generally associated with then the switch number. However, some devices don't adhere to this system because either they are not PCs, printers, or switches or they are significant devices in the network. These include the Central Switch, Central Router, Alpha Server, and Bravo Server.

For IP addressing, the network utilizes DHCP for manageability. Most hosts get their IP address, DNS server (Alpha Server), Domain name (Xcite.com), and Default Gateway based on the DHCP Pool configured in the router. All VLANs are assigned their own DHCP Pool. Table 1.2 shows the devices in the network that have to be configured statically. All switches, since they don't have DHCP capabilities, aside from being a DHCP server, are part of the list. The Alpha Server is static because this device serves as the network's DNS Server. Because IT-Admin has to be specifically permitted in ACL configurations, its details are static. Lastly, with the Central Router Subinterfaces' IP Addresses being the default gateway of all hosts, they have to be configured manually.

Table No. 1.1 List of Subnets

Subnet	Assigned VLAN	Subnet Mask	Network Address	First Host	Last Host
Developer Dept.	VLAN 10	255.255.255.192	172.16.10.0	172.16.10.1	172.16.10.62
Marketing / Finance Dept.	VLAN 20	255.255.255.128	172.16.20.0	172.16.20.1	172.16.20.30
Creative Dept.	VLAN 30	255.255.255.128	172.16.30.0	172.16.30.1	172.16.30.30
IT Dept.	VLAN 40	255.255.255.0	172.16.40.0	172.16.40.1	172.16.40.14
Services	VLAN 50	255.255.254.0	172.16.50.0	172.16.50.1	172.16.50.6
Management	VLAN 60	255.255.255.128	172.16.60.0	172.16.60.1	172.16.60.30

Table No. 1.2 Statically Configured Addresses

Device	Interface	Subnet Mask	IP Address	Default Gateway
DD-Switch1	VLAN 60	255.255.255.128	172.16.60.1	172.16.60.30
DD-Switch3	VLAN 60	255.255.255.128	172.16.60.2	172.16.60.30
FM-Switch	VLAN 60	255.255.255.128	172.16.60.4	172.16.60.30
IT-Switch	VLAN 60	255.255.255.128	172.16.60.5	172.16.60.30
CD-Switch	VLAN 60	255.255.255.128	172.16.60.6	172.16.60.30
UR-Switch	VLAN 60	255.255.255.128	172.16.60.7	172.16.60.30
IT-Admin	F0/0	255.255.255.128	172.16.60.8	172.16.60.30
Alpha Server	F0/0	255.255.255.128	172.16.60.9	172.16.60.30
DD-Switch2	VLAN 60	255.255.255.128	172.16.60.10	172.16.60.30
Central Switch	VLAN 60	255.255.255.128	172.16.60.11	172.16.60.30
Central Router	G0/0/0.10	255.255.255.192	172.16.10.62	N/A
	G0/0/0.20	255.255.255.128	172.16.20.30	N/A
	G0/0/0.30	255.255.255.128	172.16.30.30	N/A
	G0/0/0.40	255.255.255.0	172.16.40.14	N/A
	G0/0/0.50	255.255.254.0	172.16.50.6	N/A
	G0/0/0.60	255.255.255.128	172.16.60.30	N/A

Section 2. Physical Topology

The physical topology generally followed the floor plan of Xcite. All PCs and Printers are placed where they appear in the document. A few important details to note however are the cable management and the location of all infrastructure devices.

For the cabling of the topology, all wires, as much as possible, run through the walls to prevent them from being damaged or altered by people or other external factors. This feature also provides the manageability of wires throughout the network. Lastly, all infrastructure devices are located in the server room. This is to enhance the security and control of the network.

Table No. 2.1 Legends

Legends	Meaning
	Cable Management
	PC
	Switch
	Printer
	Server
	Router
	Raceway

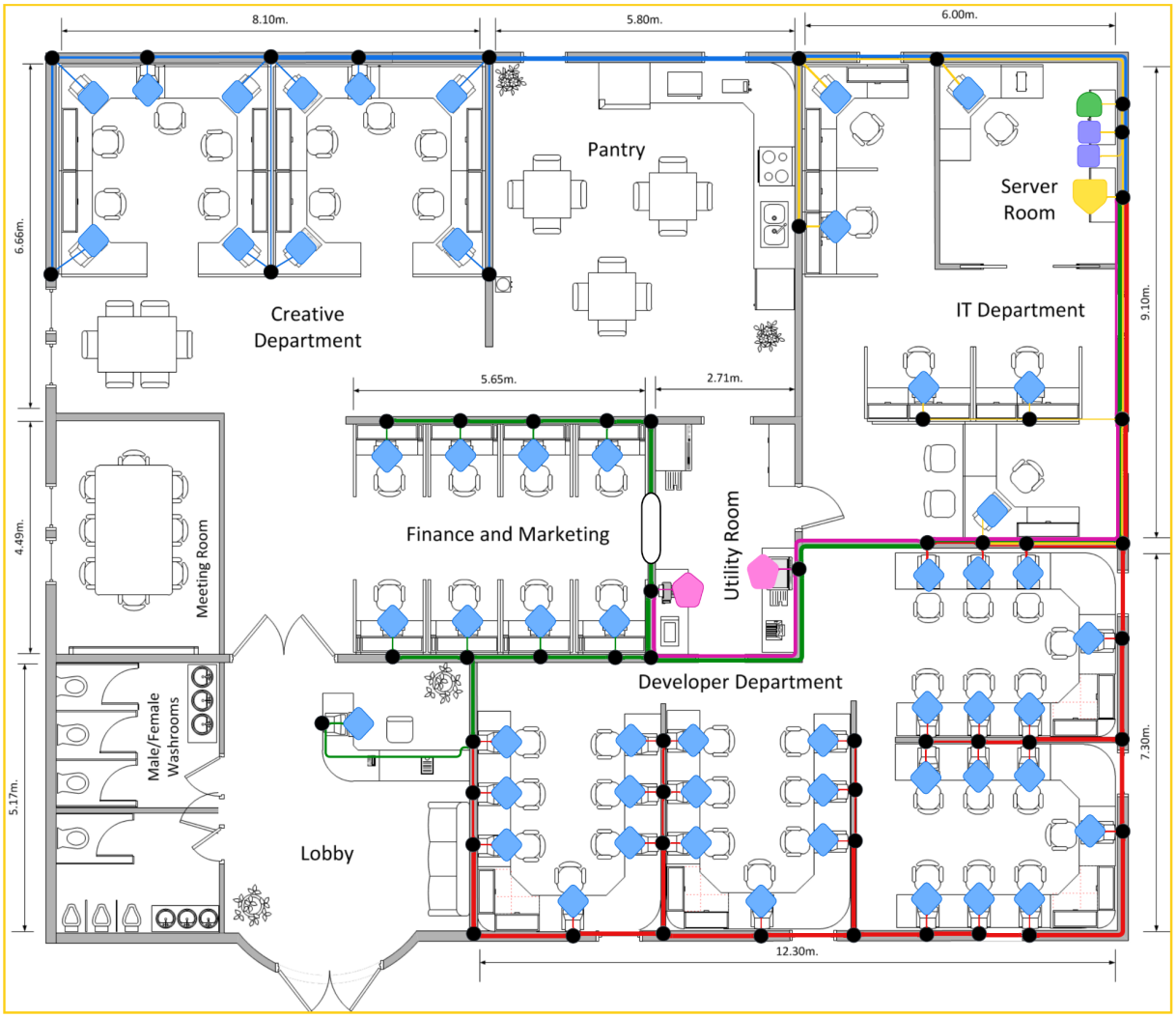

Image No. 2.1 Floor Plan (Arranged)

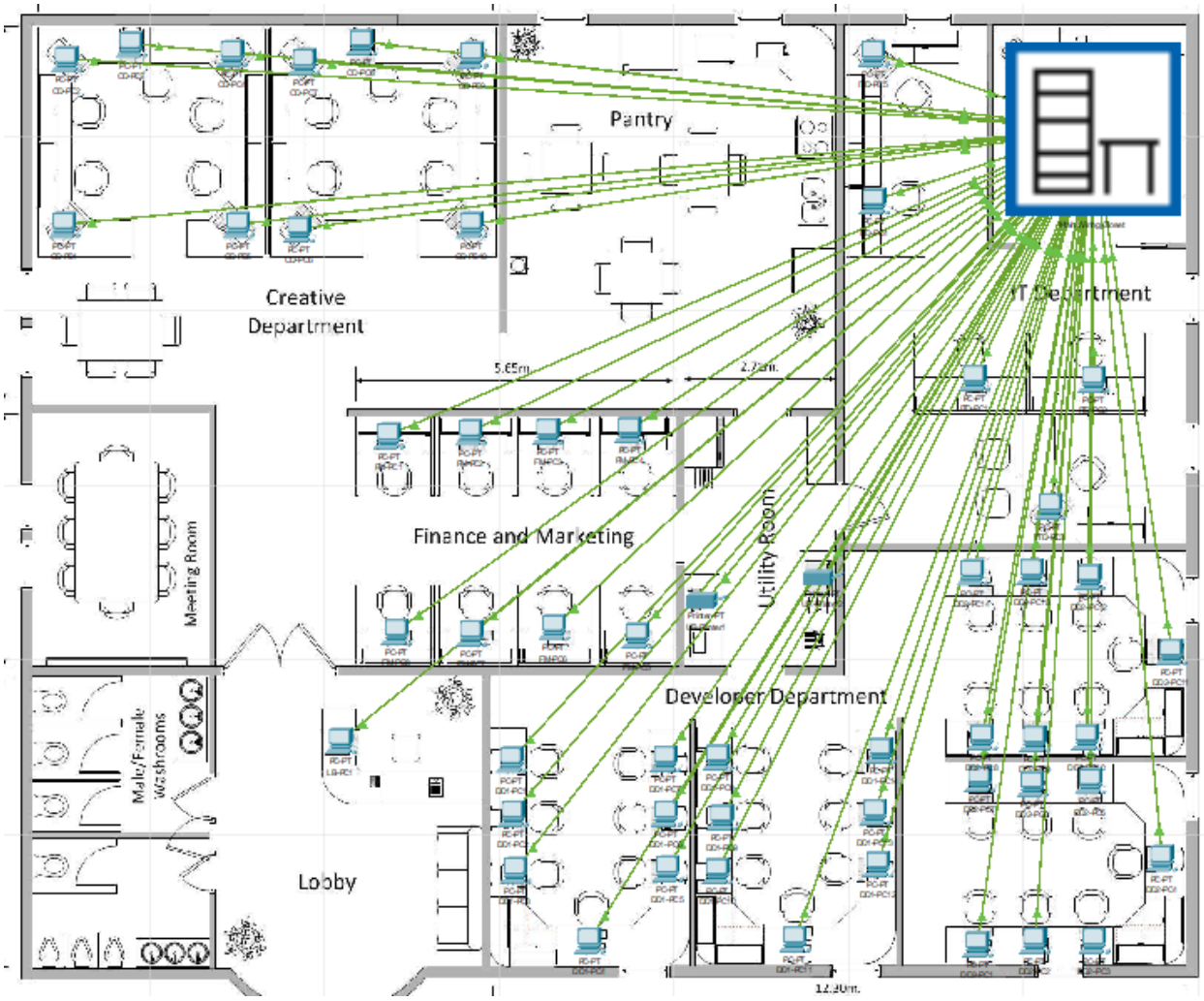

Image No. 2.2 Floor Plan (Packet Tracer)

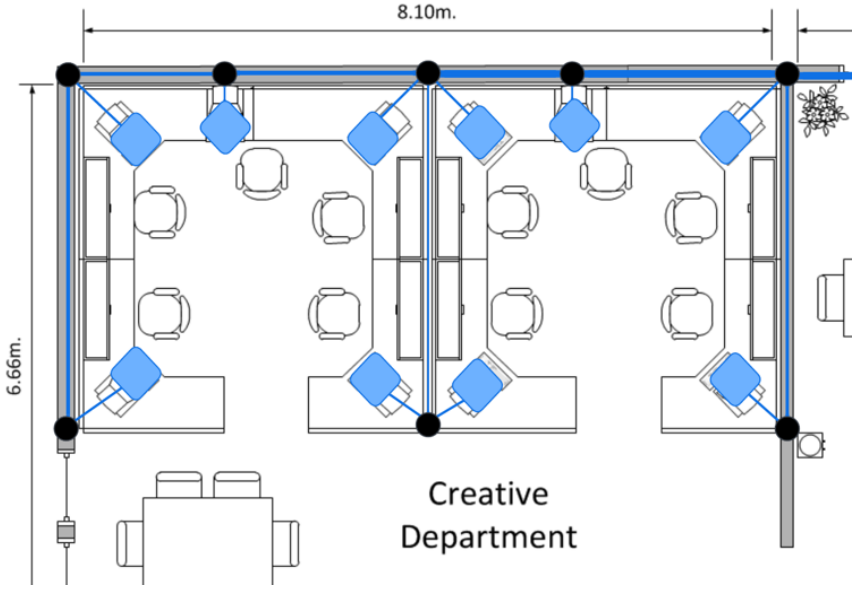

Image No. 2.3 Creative Department

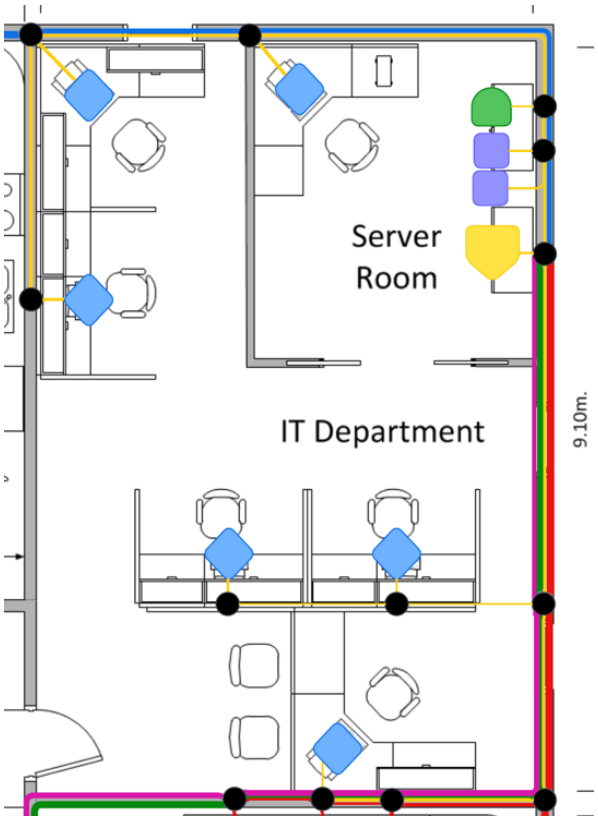

Image No. 2.4 IT Department/Server Room

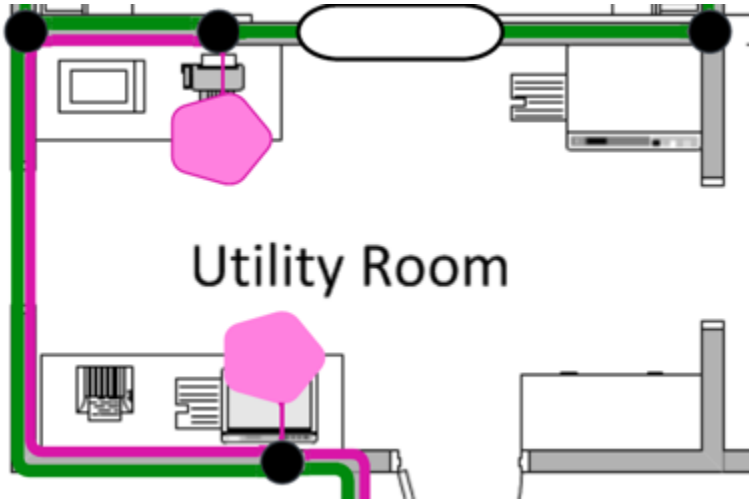

Image No. 2.5 Utility Room

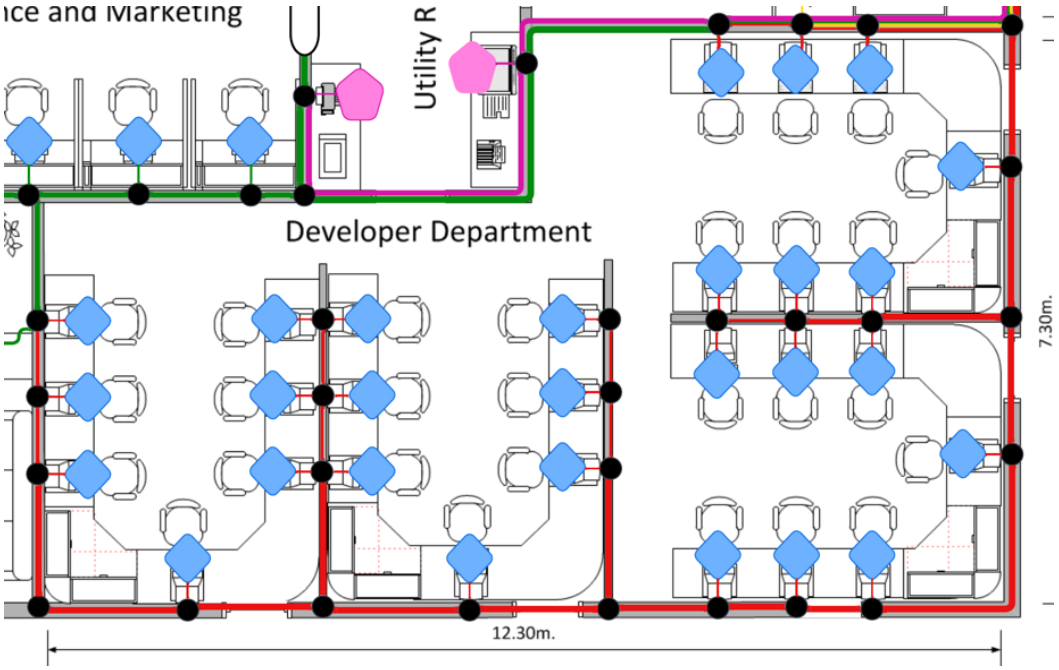

Image No. 2.6 Developer Department

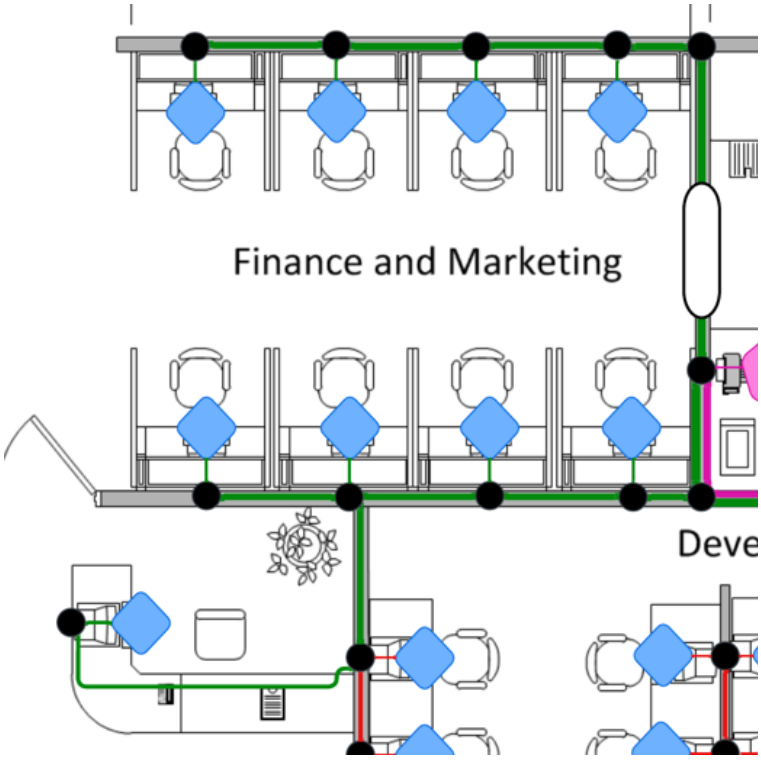

Image No. 2.7 Finance and Marketing/Lobby

Image No. 2.8 Server Room Racks and Table

Table No. 2.2 Device Connection and VLAN Assignment

Source	Interface	Connected to	Assigned VLAN
Central Router	GigabitEthernet0/0/0	Central Switch	N/A
Central Switch	GigabitEthernet0/2	Central Router	N/A
	GigabitEthernet0/1	FM-Switch	VLAN 60
	FastEthernet0/1	DD-Switch2	
	FastEthernet0/2	CD-Switch	
	FastEthernet0/3	IT-Switch	
	FastEthernet0/4	UR-Switch	
DD-Switch2	GigabitEthernet0/1	DD-Switch1	VLAN 60
	GigabitEthernet0/2	DD-Switch2	
DD-Switch1	FastEthernet0/1	DD1-PC1	VLAN10
	FastEthernet0/2	DD1-PC2	
	FastEthernet0/3	DD1-PC3	
	FastEthernet0/4	DD1-PC4	
	FastEthernet0/5	DD1-PC5	
	FastEthernet0/6	DD1-PC6	
	FastEthernet0/7	DD1-PC7	

	FastEthernet0/8	DD1-PC8	
	FastEthernet0/9	DD1-PC9	
	FastEthernet0/10	DD1-PC10	
	FastEthernet0/11	DD1-PC11	
	FastEthernet0/12	DD1-PC12	
	FastEthernet0/13	DD1-PC13	
	FastEthernet0/14	DD1-PC14	
DD-Switch3	FastEthernet0/1	DD2-PC1	VLAN 10
	FastEthernet0/2	DD2-PC2	
	FastEthernet0/3	DD2-PC3	
	FastEthernet0/4	DD2-PC4	
	FastEthernet0/5	DD2-PC5	
	FastEthernet0/6	DD2-PC6	
	FastEthernet0/7	DD2-PC7	
	FastEthernet0/8	DD2-PC8	
	FastEthernet0/9	DD2-PC9	
	FastEthernet0/10	DD2-PC10	
	FastEthernet0/11	DD2-PC11	
	FastEthernet0/12	DD2-PC12	
	FastEthernet0/13	DD2-PC13	
	FastEthernet0/14	DD2-PC14	
FM-Switch	FastEthernet0/1	FM-PC1	VLAN 20
	FastEthernet0/2	FM-PC2	
	FastEthernet0/3	FM-PC3	
	FastEthernet0/4	FM-PC4	
	FastEthernet0/5	FM-PC5	
	FastEthernet0/6	FM-PC6	

	FastEthernet0/7	FM-PC7	
	FastEthernet0/8	FM-PC8	
	FastEthernet0/9	LB-PC1	
CD-Switch	FastEthernet0/1	CD-PC1	VLAN 30
	FastEthernet0/2	CD-PC2	
	FastEthernet0/3	CD-PC3	
	FastEthernet0/4	CD-PC4	
	FastEthernet0/5	CD-PC5	
	FastEthernet0/6	CD-PC6	
	FastEthernet0/7	CD-PC7	
	FastEthernet0/8	CD-PC8	
	FastEthernet0/9	CD-PC9	
	FastEthernet0/10	CD-PC10	
IT-Switch	FastEthernet0/1	IT-PC1	VLAN 40
	FastEthernet0/2	IT-PC2	
	FastEthernet0/3	IT-PC3	
	FastEthernet0/4	IT-PC4	
	FastEthernet0/5	IT-PC5	
	FastEthernet0/6	IT-Admin	VLAN 60
	FastEthernet0/7	Alpha Server	
	FastEthernet0/8	Bravo Server	VLAN 50
UR-Switch	FastEthernet0/1	UR-Printer1	VLAN 50
	FastEthernet0/2	UR-Printer2	

Section 3. Logical topology

All devices are grouped in subnets as specified in the case study. Each subnet is generally associated with one or two switches that are connected to a central switch. This device is then connected, via a trunk link, to the Central Router which will handle Inter-VLAN communication (router configurations are indicated in Table 1.8). Additionally, the Xcite network follows a Router-on-a-Stick Inter-VLAN model for scalability and manageability for a cheap price. For expansion, if the network administrator wants to add a new subnet, they can connect a new switch to the Central Router, follow the VTP and IP configurations, and add a subinterface to the Central Router with ease.

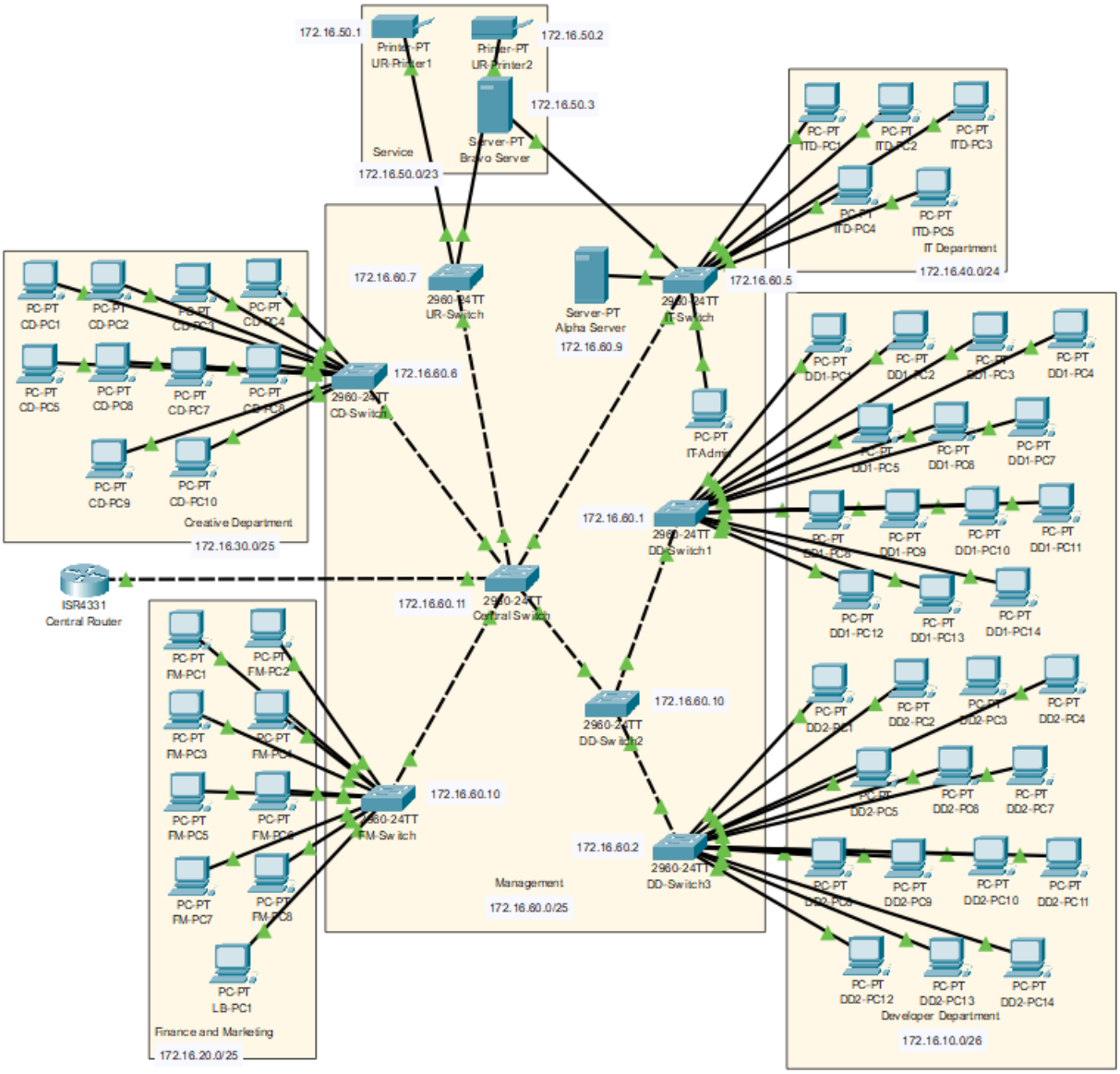

Image 3.1 Logical Topology

Section 4. Security Implementation

Network security is one of the most critical aspects of our network planning. This is because we do not want unauthorized people to access and/or modify our configurations. Some of the security requirements that we have applied are as follows.

1. Strong password combinations

   Having a strong password combination could help us in preventing any unwanted hacks or password breaches, especially via brute forcing. We implemented this by having passwords with a combination of uppercase and lowercase letters, numbers, and special characters on all of our console, privileged exec, VTP, and SSH passwords.

2. Limiting the number of attempts

   With the previous point, the brute force method to gain passwords is quite common and the easiest way to gain access to the system. So, to avoid that, we decided to limit the number of tries in inputting the passwords. This was done by issuing the command:

   login block-for 120 attempts 3 within 60

3. Secure unused ports

   Another way to gain access to networking devices is to connect to the ports. If a port is left unsecured and open to the public, it might be taken advantage of by hackers. This is why we shut down the unused ports in all of our networking devices. This brings us to our next security measure.

4. Storing routers and switches in a secure place

   As said before, if a networking device were left out in the open, unauthorized people/hackers who want to take control of the networking device might take advantage of this since they have free access to the actual networking device.

5. Enabling SSH/Telnet

   We decided to enable the Security Shell(SSH) to keep the communication between the router, switches, and other devices in the network secure by encrypting the data sent between the computers in the network.

6. Port Security

   To secure our ports and in order to prevent attacks, we did the following;

   a. VLAN Hopping Attacks and Mitigation:
      - Disabling auto trunking on trunk links, and on ports that will not be used as trunks
      - Native VLAN is used for trunk links only
      - Placing unused ports in an unused VLAN (Vlan 99)
      - Implementing the ***switchport nonegotiate*** command to prevent DTP (negotiation) packets from being sent out the interface

b. MAC Address Table Attack and Mitigation:
    - Shutdown unused ports
    - Enable static access mode and use the switchport port-security command
    - Setting the maximum number of MAC addresses allowed on a port to one only
    - Set to learn about MAC addresses on a secure port to sticky
    - Set the port security violation mode to restrict
    - Set the port security aging time to automatically delete existing secure MAC addresses after a certain amount of time (20 minutes)

7. DHCP Snooping

    To prevent DHCP starvation and DHCP spoofing attacks, we enabled DHCP snooping by designating devices as trusted or untrusted. On untrusted interfaces, we set the rate limit for DHCP Discover messages to 5 packets-per-seconds, then applied DHCP snooping on the trusted VLANs of the network.

8. Dynamic ARP Inspection (DAI)

    To prevent ARP spoofing starvation and ARP poisoning attacks, we enabled DAI on the assigned VLANs of the network, and configured trusted interfaces for DHCP snooping and ARP inspection. This was done by implementing the commands ***ip arp inspection vlan [vlan number]*** and ***ip arp inspection trust*** on the trusted interfaces and vlans respectively.

9. Access Control List

    The Access Control Lists are a powerful tool for network administrators. This provides different benefits and uses for a network. Which are:
    - Security: Used to restrict access to a network or specific resources within a network.
    - Traffic Filtering: Used to filter traffic in a network. This helps with network efficiency through the prioritization of network traffic, and the management of network congestion.
    - Quality of Service: Used to prioritize certain types of network traffic over others.
    - Network Monitoring: Used to capture and log network traffic for analysis and troubleshooting purposes.

Table No. 4.1 Access Control Matrix

	DD	CD	MF	IT	Services	Admin PC	Management
DD		✓	✗	✓	✓	✗	✗
CD	✓		✗	✓	✓	✗	✗
MF	✗	✗		✓	✓	✗	✗
IT	✓	✓	✓		✓	✗	✗
Services	✓	✓	✓	✓		✗	✗
Admin PC	✗	✗	✗	✗	✗		✓
Management	✗	✗	✗	✗	✗	✓	

Table No. 4.2 Passwords

Interface	Password
Console	cL4$$
Privileged Exec Mode	C1$co

Table No. 4.3 VTP Configurations

VTP Field	Value
Mode	1
Domain Name	ITNET02.com
Password	vtp1TNPass!

Table No. 4.4 SSH/Telnet Configurations

SSH/Telnet Field	Value
Domain Name	www.ITNET02.com
Username	admin
Password	c1sCo