**Design and Implementation of a Simple Networking Project #1**

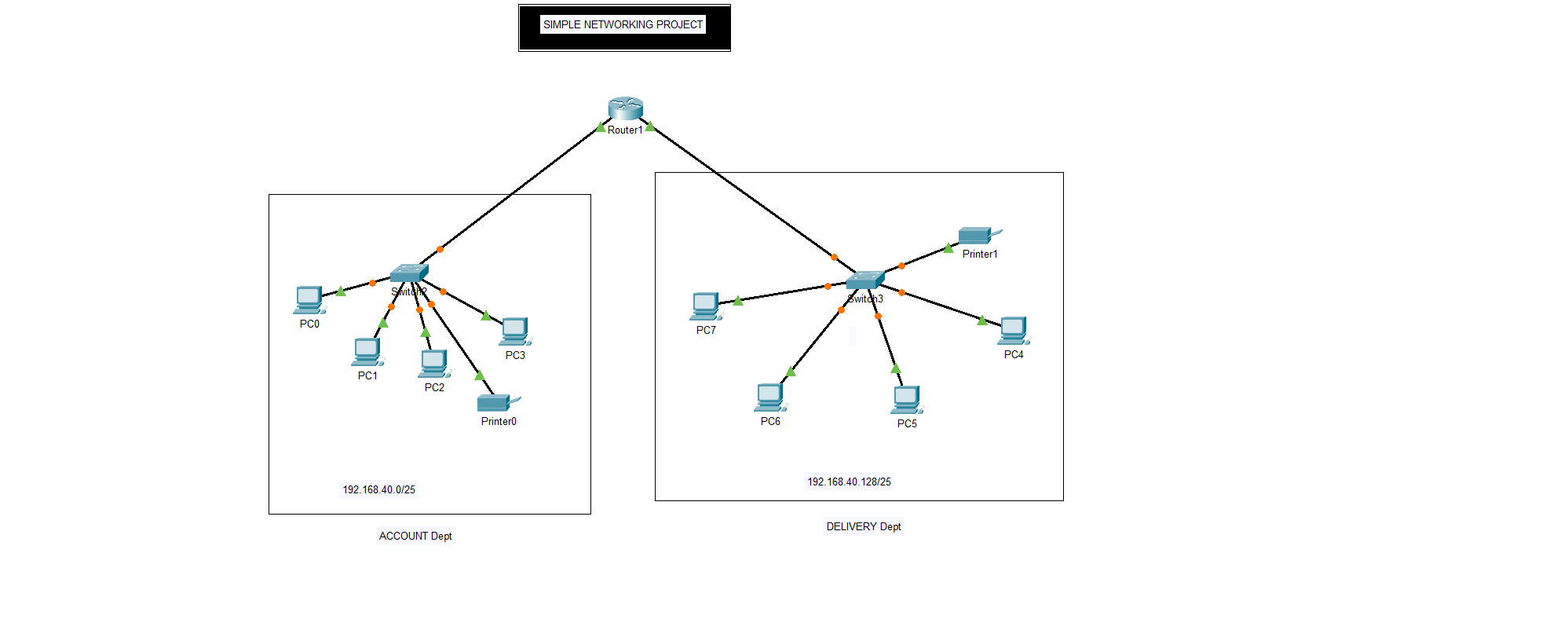
**Project #1 Case Study and Requirements**

Design a network in Cisco Packet Tracer to connects ACCOUNTS and DELIVERY departments through the following:

* Each department should contain at least two PCs.
* Appropriate number of switches and routers should be used in the network.
* Using the given network 192.168.40.0, all interfaces should be configured with correct IP addresses, subnet mask and gateways.
* All devices in the network should be connected using appropriate cables.
* Test communication between devices in both ACCOUNTS and DELIVERY departments.

**Technologies Implemented**

1. Creating a Simple Network using a Router and Access Layer Switch.
2. Connecting Networking devices with Correct cabling.
3. Connecting two Networks using a Router.
4. Subnetting and IP Addressing.
5. Assigning IP Addresses to Router's interfaces.
6. Static IP Address allocation to Host Devices.
7. Test and Verifying Network Communication.



**Design and Implementation of a Small Office Home Office Network -SOHO Project#2**

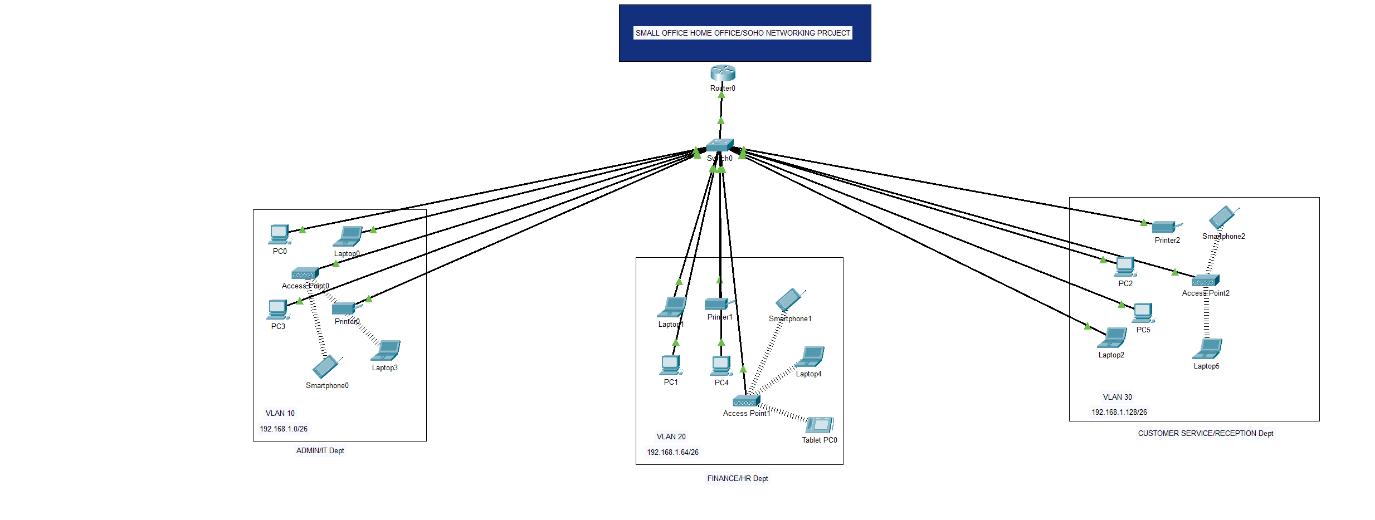
**Project #2 Case Study and Requirements**

XYZ company is a fast-growing company in Eastern Australia with more than 2 million customers globally. The company deals with selling and buying of food items, which are basically operated from the headquarters. The company is intending to open a branch near the local village Bonalbo. Thus, the company requires young IT graduates to design the network for the branch. The network is intended to operate separately from the HQ network. Being a small network, the company has the following requirements during implementation.

* One router and one switch to be used (all CISCO products).
* 3 departments (Admin/IT, Finance/HR and Customer service/Reception).
* Each department is required to be in different VLANS.
* Each department is required to have a wireless network for the users.
* Host devices in the network are required to obtain IPv4 address automatically.
* Devices in all the departments are required to communicate with each other.

Assume the ISP gave out a base network of 192.168.1.0, you as the young network engineer who has been hired, design and implement a network considering the above requirements.   
  
**Technologies Implemented**

1. Creating a Simple Network using a Router and Access Layer Switch.
2. Connecting Networking devices with Correct cabling.
3. Creating VLANs and assigning ports VLAN numbers.
4. Subnetting and IP Addressing.
5. Configuring Inter-VLAN Routing (Router on a stick).
6. Configuring DHCP Server (Router as the DHCP Server).
7. Configuring WLAN or wireless network (Cisco Access Point).
8. Host Device Configurations.
9. Test and Verifying Network Communication.



**Design and Implementation of an Hotel System Network Design Project #3**

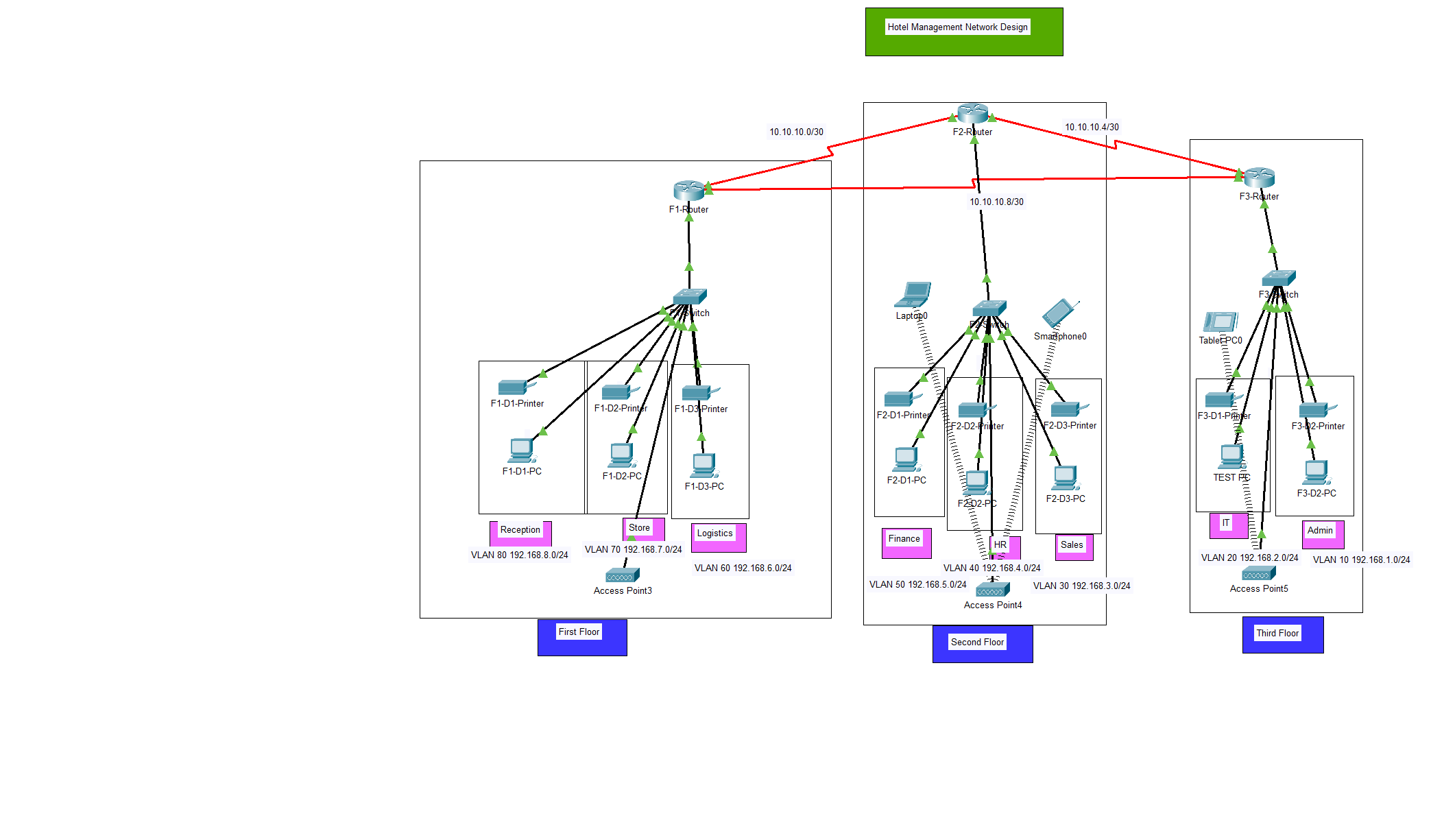
**Project #3 Case Study and Requirements**

As a part of your end year networking project, you are required to design and implement Vic Modern Hotel network. The hotel has three floors; on the first floor there three departments (Reception, store and Logistics), in the second floor there are three departments (Finance, HR and Sales/Marketing), while the third floor hosts the IT and Admin. Therefore, the following are part of the considerations during the design and implementation.

* There should be three routers connecting each floor (all placed in the server room in IT department).
* All routers should be connected to each other using serial DCE cable.
* The network between the routers should be 10.10.10.0/30,10.10.10.4/30 and 10.10.10.8/30.
* Each floor is expected to have one switch (placed in the respective floor).
* Each floor is expected to have WIFI networks connected to laptops and phones.
* Each department is expected to have a printer.
* Each department is expected to be in different VLAN with the following details;   
  **1st Floor;**   
  - Reception- VLAN 80, Network of 192.168.8.0/24   
  - Store- VLAN 70, Network of 192.168.7.0/24   
  - Logistics- VLAN 60, Network of 192.168.6.0/24   
  **2nd Floor;**   
  - Finance- VLAN 50, Network of 192.168.5.0/24   
  - HR- VLAN 40, Network of 192.168.4.0/24   
  - Sales- VLAN 30, Network of 192.168.3.0/24   
  **3rd Floor;**   
  - Admin- VLAN 20, Network of 192.168.2.0/24   
  - IT- VLAN 10, Network of 192.168.1.0/24
* Use OSPF as the routing protocol to advertise routes.
* All devices in the network are expected to obtain IP address dynamically with their respective router configured as the DHCP server.
* All the devices in the network are expected to communicate with each other.
* Configure SSH in all the routers for remote login.
* In IT department, add PC called Test-PC to port fa0/1 and use it to test remote login.
* Configure port security to IT-dept switch to allow only Test-PC to access port fa0/1 (use sticky method to obtain mac-address with violation mode of shutdown.)

**Technologies Implemented**

1. Creating a network topology using Cisco Packet Tracer.
2. Hierarchical Network Design.
3. Connecting Networking devices with Correct cabling.
4. Creating VLANs and assigning ports VLAN numbers.
5. Subnetting and IP Addressing.
6. Configuring Inter-VLAN Routing (Router on a stick).
7. Configuring DHCP Server (Router as the DHCP Server).
8. Configuring SSH for secure Remote access.
9. Configuring switchport security or Port-Security on the switches.
10. Configuring WLAN or wireless network (Cisco Access Point).
11. Host Device Configurations.
12. Test and Verifying Network Communication.



**Design and Implementation of a Campus/University System Network Design (Project #4)**

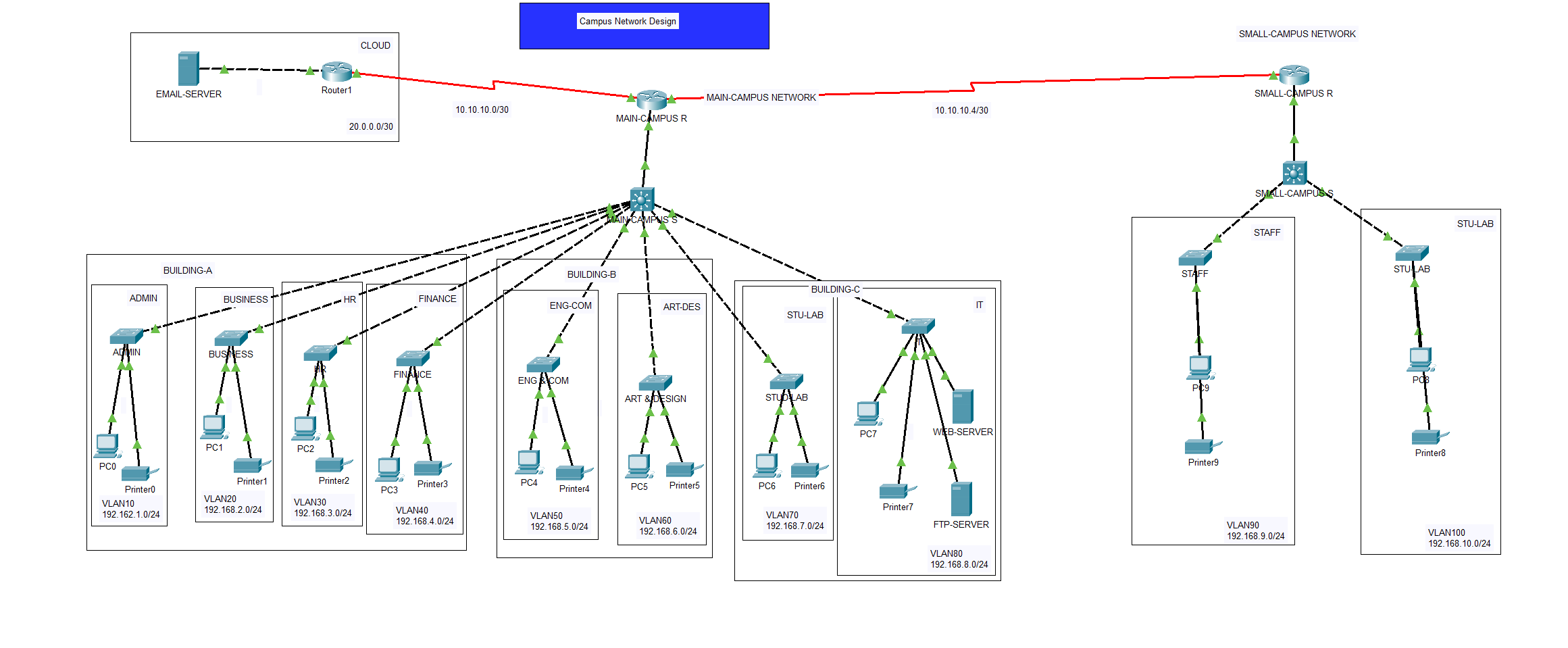
**Project #4 Case Study and Requirements**

Albion University is a large university which has two campuses situated 20 miles apart. The university’s students and staff are distributed in 4 faculties; these include the faculties of Health and Sciences; Business; Engineering/Computing and Art/Design. Each member of staff has a PC, and students have access to PCs in the labs. Create a network topology with the main components to support the following:

* University location.   
  **Main Campus**  
  - Building A: Administrative staff in the departments of management, HR and finance. The admin staff PCs are distributed in the building offices, and it is expected that they will share some networking equipment (Hint: use of VLANs is expected here). The Faculty of Business is also situated in this building   
  - Building B: Faculty of Engineering and Computing and Faculty of Art and Design.   
  - Building C: Students’ labs and IT department. The IT department hosts the University Web server and other servers - There is also an email server hosted externally on the cloud.   
  **Smaller campus:**  
  Faculty of Health and Sciences (staff and students’ labs are situated on separate floors)
* Each department/faculty is expected to be on its own separate IP network.
* The switches should be configured with appropriate VLANs and security settings.
* RIPv2 will be used to provide routing for the routers in the internal network and static routing for the external server.
* The devices in building A will be expected to acquire dynamic IP addresses from a router-based DHCP server.

Configure in Packet Tracer the network with appropriate settings to achieve the connectivity and functionalities specified in the requirements.   
  
**Technologies Implemented**

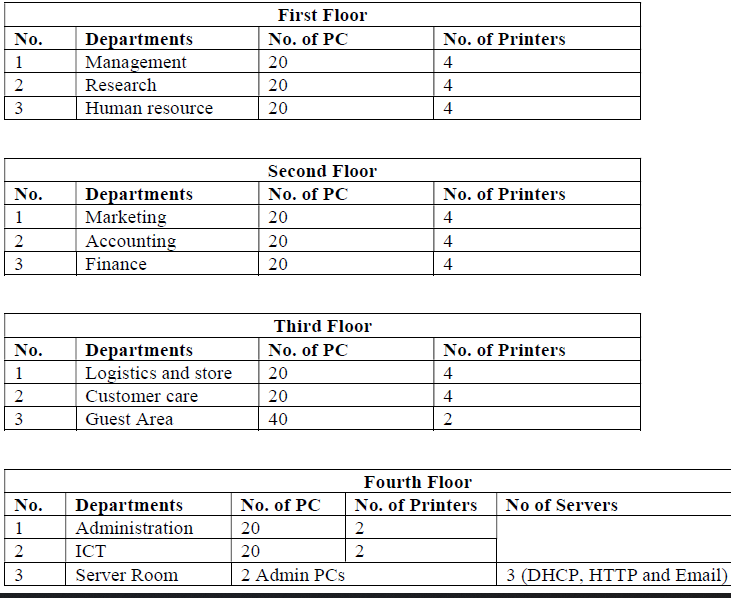
1. Creating a network topology using Cisco Packet Tracer.
2. Hierarchical Network Design.
3. Connecting Networking devices with Correct cabling.
4. Creating VLANs and assigning ports VLAN numbers.
5. Subnetting and IP Addressing.
6. Configuring Inter-VLAN Routing (Router on a stick).
7. Configuring DHCP Server (Router as the DHCP Server).
8. Configuring RIPv2 as the routing protocol.
9. Configuring switchport security or Port-Security on the switches.
10. Host Device Configurations.
11. Test and Verifying Network Communication.



**Design and Implementation of a Bank System Network Design (Project #5)**

**Project #5 Case Study and Requirements**

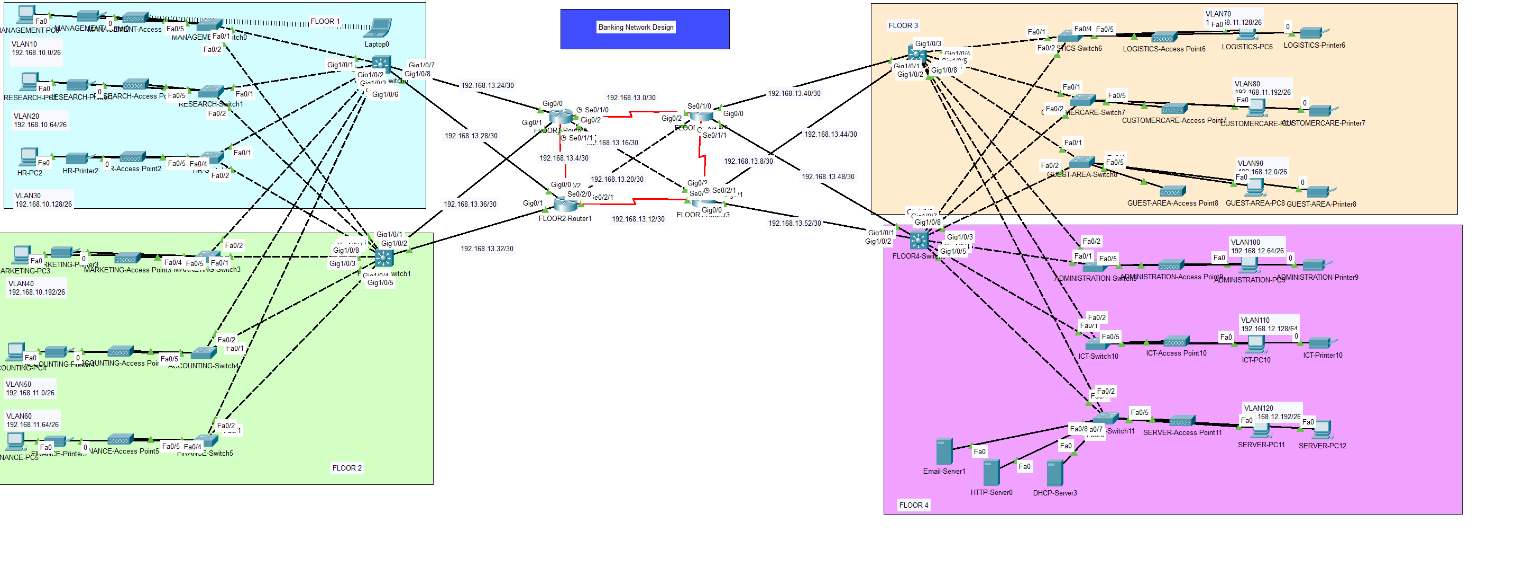
Radeon Company Ltd. is a US-owned company that deals with Banking and Insurance. The company is intending to expand its services across the African continent having the first branch to be in Nairobi, Kenya. The company has secured a four-story building to operate within the Kenyan capital city. Therefore, the company would like to allow sourcing the knowledge from a group of final-year students from the local university to design and implement their company network. Assume you are among the students to take over this role, carefully read down the requirements then model the design and implement the network based on the company's needs. Each floor has departments as provided in the table below.;



* Use a software modelling tool to visualize the network topology (Use Hierarchical Network Design   
  - Software Modelling Tools: MS Visio, Visual Paradigm, or Draw.io for modeling network design.
* Use any of the following network simulation software to implement the above topology.   
  - Simulation software: Cisco Packet tracer or GNS3 for design and implementation.
* Use OSPF as the routing protocol to advertise routes.
* Each department is required to have a wireless network for the users.
* Each department except the server room will be anticipated to have around 60 users both wired and wireless users.
* Host devices in the network are required to obtain IPv4 addresses automatically.
* Devices in all the departments are required to communicate with each other.
* Create HTTP, and E-mail servers.
* All devices in the network are expected to obtain an IP address dynamically from the dedicated DHCP servers located at the server room.
* Configure SSH in all the routers for remote login.
* Configure the basic configuration of the devices: Hostnames, Line Console and Enable passwords, Banner messages Disable domain IP lookup, encrypt all configured passwords.
* Each department should be in a different VLAN and subnetwork; VLANs you will use in your case, e.g. 10, 20, 30… etc.
* Planning of IP Addresses: You have been given 192.168.10.0 as the base address for this network. Do subnetting based on the number of hosts in every department as provided above. Identify subnet mask, useable IP address range, and broadcast address for each subnet.
* End Device Configurations: Configure all the end devices in the network with the appropriate IP address based on the calculations above.
* Configure port-security: Use sticky command to obtain MAC Address and Violation mode of the shutdown.
* Test and Verifying Network Communication.

**Technologies Implemented**

1. Creating a network topology using Cisco Packet Tracer.
2. Hierarchical Network Design.
3. Connecting Networking devices with Correct cabling.
4. Configuring Basic device settings.
5. Creating VLANs and assigning ports VLAN numbers.
6. Subnetting and IP Addressing.
7. Configuring Inter-VLAN Routing on the Multilayer switches (Switch Virtual Interface).
8. Configuring Dedicated DHCP Server device to provide dynamic IP allocation.
9. Configuring SSH for secure Remote access.
10. Configuring OSPF as the routing protocol.
11. Configuring switchport security or Port-Security on the switches.
12. Configuring WLAN or wireless network (Cisco Access Point).
13. Host Device Configurations.
14. Test and Verifying Network Communication.



**Design and Implementation of a Company/Business System Network Design (Project #6)**

**Project #6 Case Study and Requirements**

A trading floor Support centre employs 600 staff. They have recently expanded and as a result, need to move to a new building. A building has been identified but has no network. This means that before they can make to move out, new network service needs to be designed and implemented in the new building. Existing Network comprises of the following elements: The new building is expected to have three floors with two departments in each for example;

1. **First floor-** (Sales and Marketing Department-120 users expected, Human Resource and Logistics Department-120 users expected).
2. **Second floor-** (Finance and Accounts Department-120 users expected, Administrator and Public Relations Department-120 users expected).
3. **Third floor-** (ICT-120 users expected, Server Room-12 devices expected).

Therefore, as a key member of the Networks Team, you have been tasked to design a network for the new building. At this stage, logical design is required, which shows the measures that you would put in place to ensure that the new network meets the current business need and is future-proofed:

* Use Cisco Packet Tracer to design and implement the network solution.
* Use hieratical model providing redundancy at every layer i.e. two routers and two multilayer switches are expected to be used to provide redundancy.
* The network is also expected to connect to at least two ISPs to provide redundancy and each router to the connected to the two ISPs.
* Each department is required to have a wireless network for the users.
* Each department should be in a different VLAN and in different subnetwork.
* Provided a base network of 172.16.1.0, carry out subnetting to allocate the correct number of IP addresses to each department.
* The company network is connected to the static, public IP addresses (Internet Protocol) 195.136.17.0/30, 195.136.17.4/30, 195.136.17.8/30 and 195.136.17.12/30 connected to the two Internet providers.
* Configure basic device settings such as hostnames, console password, enable password, banner messages, disable IP domain lookup.
* Devices in all the departments are required to communicate with each other with the respective multilayer switch configured for inter-VLAN routing.
* The Multilayer switches are expected to carry out both routing and switching functionalities thus will be assigned IP addresses.
* All devices in the network are expected to obtain an IP address dynamically from the dedicated DHCP servers located at the server room.
* Devices in the server room are to be allocated IP address statically.
* Use OSPF as the routing protocol to advertise routes both on the routers and multilayer switches.
* Configure SSH in all the routers and layer three switches for remote login.
* Configure port-security for the Finance and Accounts department to allow only one device to connect to a switchport, use sticky method to obtain mac-address and violation mode shutdown.
* Configure PAT to use the respective outbound router interface IPv4 address, implement the necessary ACL rule.
* Test Communication, ensure everything configured is working as expected.

**Technologies Implemented**

1. Creating a network topology using Cisco Packet Tracer.
2. Hierarchical Network Design.
3. Connecting Networking devices with Correct cabling.
4. Configuring Basic device settings.
5. Creating VLANs and assigning ports VLAN numbers.
6. Subnetting and IP Addressing.
7. Configuring Inter-VLAN Routing on the Multilayer switches (Switch Virtual Interface).
8. Configuring Dedicated DHCP Server device to provide dynamic IP allocation.
9. Configuring SSH for secure Remote access.
10. Configuring OSPF as the routing protocol.
11. Configuring NAT Overload(Port Address Translation PAT).
12. Configuring standard and extended Access Control Lists ACL.
13. Configuring switchport security or Port-Security on the switches.
14. Configuring WLAN or wireless network (Cisco Access Point).
15. Host Device Configurations.
16. Configuring ISP routers.
17. Test and Verifying Network Communication.

**Design and Implementation of a Hospital System Network Design (Project #7)**

**Project #7 Case Study and Requirements**

Melbourne Health Services is a well-established health provider in Australia, which offers health solutions and services to its clients. The institution operates in two locations within the same city, having the hospital headquarters 20km away from the branch hospital. Therefore, it has the following departments within its main headquarters Medical Lead Operation & Consultancy Services (MLOCS), Medical Emergency and Reporting (MER), Medical Records Management (MRM), Information Technology (IT), and Customer Service (CS). The branch hospital was designed to share the workloads with the headquarters hence it contains the following departments; Nurses & Surgery Operations (NSO), Hospital Labs (HL), Human resource (HR), Marketing (MK), and Finance (FIN). Each location is also expected to have a Guest/Waiting area (GWA) for patients or visitors.   
So far the network was using third-party services to maintain its IT services. The senior management has decided to own their network infrastructure including Local Area Network (LAN), Wide Area Network (WAN), and a Server-Side site that is expected to be located separately at the headquarters and is connected to the HQ Router with an access switch. The server-side site will host the DHCP server, DNS Server, Web Server, and Email Server. The network is expected to be cost-effective and observes the information security rule of the CIA (Confidentiality, Integrity, and Availability).   
The network is expected to have a hierarchical model with two already purchased Core routers (one at HQ and one Branch) each connecting to two subscribed ISPs. Due to security requirements, it has been decided that all the departments will be on a separate network segment within the same local area network.   
You have been hired as a network security engineer to design the network according to the requirements set by the senior management. You will consult an appropriate robust network design model to meet the design requirements. You will also implement Access Control Lists and Virtual Private Network (VPN) to enable secure communication considering security and network performance factors paramount to safeguarding Confidentiality, Integrity, and Availability of data and communication. The network security policy will comprehensively dictate the user's access to each site using Access Control List (ACL).

* Use Cisco Packet Tracer to design and implement the network solution.
* Use a hierarchical model providing redundancy in the network.
* Both HQ and Branch routers are expected to be connected using a serial connection.
* As mentioned earlier, for network cost-effectiveness, each site is expected to have one core router, two multilayer switches, and several access switches connecting each department.
* Each department is required to have a wireless network for the users.
* Every department in HQ is estimated to have around 60 users while in Branch is estimated to be 30 users.
* Each department should be in a different VLAN and a different subnetwork.
* Provided a base network of 192.168.100.0, and carry out subnetting to allocate the correct number of IP addresses to each department.
* The company network is connected to the static, public IP addresses (Internet Protocol) 195.136.17.0/30, 195.136.17.4/30, 195.136.17.8/30, and 195.136.17.12/30 connected to the two Internet providers.
* Configure basic device settings such as hostnames, console password, enable password, banner messages, and disable IP domain lookup.
* Devices in all the departments are required to communicate with each other with the respective multilayer switch configured for inter-VLAN routing.
* The Multilayer switches are expected to carry out both routing and switching functionalities and thus will be assigned IP addresses.
* All devices in the network are expected to obtain an IP address dynamically from the dedicated DHCP servers located in the server room.
* Devices in the server room are to be allocated IP addresses statically.
* Use OSPF as the routing protocol to advertise routes both on the routers and multilayer switches.
* Configure default static routing to enable routers and multilayer switches to forward any traffic that does not match routing table entries. Use next-hop IP addresses.
* Configure SSH in all the routers and layer three switches for remote login.
* Configure port-security for the server site department switch to allow only one device to connect to a switch port, use sticky method to obtain mac-address and violation mode shutdown.
* Configure the extended ACL rule together with site-to-site VPN (IPSec VPN) to create a tunnel and encrypt communication between HQ and the Branch network.
* Configure PAT to use the respective outbound router interface IPv4 address, and implement the necessary ACL rule.
* Test Communication, ensure everything configured is working as expected.

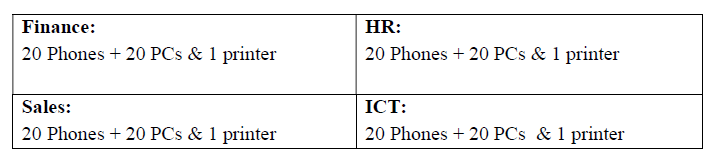
**Technologies Implemented**

1. Creating a network topology using Cisco Packet Tracer.
2. Hierarchical Network Design.
3. Connecting Networking devices with Correct cabling.
4. Configuring Basic device settings.
5. Creating VLANs and assigning ports VLAN numbers.
6. Subnetting and IP Addressing.
7. Configuring Inter-VLAN Routing on the Multilayer switches (Switch Virtual Interface).
8. Configuring Dedicated DHCP Server device to provide dynamic IP allocation.
9. Configuring SSH for secure Remote access.
10. Configuring OSPF as the routing protocol.
11. Configuring NAT Overload(Port Address Translation PAT).
12. Configuring Site-to-Site IPsec VPN.
13. Configuring standard and extended Access Control Lists ACL.
14. Configuring switchport security or Port-Security on the switches.
15. Configuring WLAN or wireless network (Cisco Access Point).
16. Host Device Configurations.
17. Configuring ISP routers.
18. Test and Verifying Network Communication.

**Design and Implementation of a VoIP- IP Telephony System Network Design (Project #8)**

**Project #8 Case Study and Requirements**

Turtle Consultancy Limited specialised in delivering IT infrastructure solutions to mediumsized organizations worldwide. With the expansion of the company, a newly acquired branch needs a network. Your manager is faced with the demands of business and a plethora of technology challenges.   
You have been recently hired as a Network Engineer and assigned the task of designing and implementing a VoIP network that is based on the requirements and specifications outlined by your manager.   
All desktops have an associated telephone set (each PC is connecting directly to a Phone, not a switch). The network consists of four servers (DHCP, EMAIL, DNS,HTTP) located at the server side site and is fully configured for the operations, and all servers are shared between all users.   
Each group has been assigned the task of designing, and implementing a network infrastructure for Turtle Consultancy Limited by internetworking three departments which are as follows:;



The IT Manager emphasized scalability and availability, and hence you are required to provide a complete network infrastructure design and implementation. Turtle Consultancy Limited will be using the following IP address: 192.168.100.0/24 for Data, 172.16.100.0/24 for Voice, and 10.10.10.0/24 between the routers.

* Design a networked system to meet the given specifications. Use packet tracer software to design your network.
* Routers- Each department is to have VoIP enabled router with server-side LAN attached to the ICT department router. Note: use Cisco 2811 router.
* Switches- Each department has an access layer switch. Note: use Cisco 2960 switch.
* Connections- Use serial connections between a router and a router, then a straightthrough cable between the router to switch, switch to hosts, phones to PCs.
* Subnets- Each department will be accessing two subnetworks, for example, data and voice subnets. Note: carry out appropriate subnetting.
* Basic settings- Configure basic device settings such as hostnames, console passwords, enable passwords, banner messages, encrypt all passwords, and disable IP domain lookup.
* DHCP Server- For voice (VoIP), use the respective router as the DHCP server while for Data use the DHCP server device at the server-side site.
* VLANs- Each department will be in two VLANS. One for data and another for voice. Note: All IP phones in the network should be in VLAN 100.
* Inter-VLAN Routing- Use router-on-a-stick to enable inter-VLAN routing on the network. Note: create subinterfaces for both data and voice VLANs.
* IP Addressing- All devices in the network are expected to obtain an IP address dynamically from the respective DHCP servers while the devices in the server room are to be allocated IP addresses statically.
* Routing protocol- Use OSPF as the routing protocol to advertise routes on the routers.
* Remote Access- Configure SSH in all the routers for remote login.
* Telephony service- Configure VoIP on the routers and allocate dial numbers in this format for the departments, Finance(1..), HR (2..), Sales (3..), and ICT (4..), (where 1.. can be 101 to 199) and so on.
* Routing for VoIP- Configure dial-peering on the routers to allow IP phones from different routers to communicate.
* Finalize- Test Communication, ensure everything configured is working as expected.

**Technologies Implemented**

1. Creating a network topology using Cisco Packet Tracer.
2. Hierarchical Network Design.
3. Connecting Networking devices with Correct cabling.
4. Configuring Basic device settings.
5. Creating VLANs and assigning ports VLAN numbers.
6. Creating both data and voice VLANs and assigning ports VLAN numbers.
7. Subnetting and IP Addressing.
8. Configuring Inter-VLAN Routing on the Routers (router-on-a-stick).
9. Configuring Dedicated DHCP Server device for Data to provide dynamic IP allocation.
10. Configuring Routers as DHCP server for Voice to provide IP Phones dynamic IP allocation.
11. Configuring SSH for secure Remote access.
12. Configuring OSPF as the routing protocol.
13. Configuring VoIP or Telephony service configuration in all routers.
14. Configuring Routing for VoIP or Dial peering configuration in all routers.
15. Host Device Configurations.
16. Test and Verifying Network Communication.

**Design and Implementation of a Financial Institution System Networking Project (Project #9)**

**Project #9 Case Study and Requirements**

Jubilee Financial Services Ltd (JFSL) is a well-established finance service provider in Kenya, which offers online finance solutions and services to its clients. The company operates in the country’s capital city, Nairobi, and is hosted within an eleven-story building. The company primarily operates from the seventh to the eighth floors where on each floor there are at least two departments. The company has the following five departments within its main headquarter Human resource (HR), Customer Service (CS), Marketing (MK), Legal Management (LM), and Information Technology (IT). The number of users and other devices per department include;

1. Seventh Floor- HR, CS and MK; each department has at least 40 user devices plus 40 IP phones, and one WIFI-AP.
2. Eighth Floor- LM and IT; each department has at least 20 user devices plus 20 IP phones, and one WIFI-AP. N/B- each user can have an associated VoIP phone (but not a must).

The network infrastructure is currently run and managed by a third-party firm called Infinitive IT Systems Kenya. The senior management has decided to own its network infrastructure including Local Area Network (LAN), Wide Area Network (WAN), and an external Server-Side location connected via appropriate WAN technology with prioritizing secure communication between the HQ network and the external site. The server-side site will host DHCP, DNS, WEB, and EMAIL servers. The Company is intending to subscribe to two ISPs (Safaricom and JTL ISPs) to provide redundancy and load-balancing in terms of internet provisions. The company has also purchased two Cisco Catalyst 2911 routers (one for HQ and other for serverside) plus one gateway router Catalyst 2811 router(for HQ VoIP), two multilayer switches(both for HQ), and six access switches for the departments.   
Due to security requirements, it has been decided that all five departments will be on a separate network segment within the same local area network. None of the servers is located within the local area network but will be hosted from an external site accessible via a WAN connection. The network security policy will comprehensively dictate the user access to the external site using Access Control LIST (ACL).   
You have been hired as a network security engineer to design the network for Jubilee Financial Services Ltd (JFSL) according to the requirements set by the senior management. You will consult an appropriate robust network design model to meet the design requirements. You will also implement Access Control Lists and Virtual Private Networks to enable secure communication considering security and network performance factors paramount to safeguard the Confidentiality, Integrity, and Availability of data and communication.   
The company has emphasized high performance, redundancy, scalability, and availability, and hence you are required to provide a complete JFSL network infrastructure design and implementation. The company will be using the following IP address: 192.168.20.0/24 for Data, 10.10.10.0/24 for Voice, and 190.200.100.0 for public addresses.

* Design Tool- Use Cisco Packet Tracer to design and implement the network solution.
* Hierarchical Design- Use a hierarchical model providing redundancy at every layer.
* ISPs- The network is also expected to connect to at least two ISPs to provide redundancy and each router is connected to the two ISPs.
* WIFI- Each department is required to have a wireless network for the users.
* VoIP- Each department should have IP phones and users in the department should be able to call each other.
* VLAN- Each department should be in a different VLAN and a different subnetwork. The voice VLAN ID number will remain at VID 120 for the entire network.
* Subnetting- Provided the networks above, carry out subnetting to allocate the correct number of IP addresses to each department.
* Basic settings- Configure basic device settings such as hostnames, and console passwords, enable passwords, and banner messages, encrypt all passwords and disable IP domain lookup.
* Inter-VLAN Routing- Devices in all the departments are required to communicate with each other with the respective multilayer switch configured for inter-VLAN routing.
* Core Switches- The Multilayer switches are expected to carry out both routing and switching functionalities and thus will be assigned IP addresses.
* DHCP Server- All devices in the network (except IP phones) are expected to obtain an IP address dynamically from the dedicated DHCP servers located at the server-side site.
* Cisco 2811 Router- Ensure to have a router that can support telephony service i.e Cisco Catalyst 2811(the VoIP router should be connected to any of the l3-switches at HQ).
* Static Addressing- Devices in the server room are to be allocated IP addresses statically.
* Telephony Service- Configure VoIP on the voice gateway router and allocate dial numbers in format (4..).
* Routing Protocol- Use OSPF as the routing protocol to advertise routes both on the routers and multilayer switches.
* Switchport security- Configure port security for the server site department switch to allow only one device to connect to a switch port, and use the sticky method to obtain mac-address and violation mode shutdown.
* SSH- Configure SSH in all the routers and layer three switches for remote login.
* Standard ACL for SSH- configure a simple standard ACL on the line VTY to allow only the ICT department to carry out all remote administrative tasks using SSH.
* NAT + ACL- Configure PAT to use the respective outbound router interface IPv4 address, and implement the necessary ACL rule.
* IPsec VPN + ACL- Configure site-to-site IPsec VPN between the HQ router and the Server-side router, and implement the necessary ACL rule.
* Final- Test Communication, ensure everything configured is working as expected.

**Technologies Implemented**

1. Creating a network topology using Cisco Packet Tracer.
2. Hierarchical Network Design.
3. Connecting Networking devices with Correct cabling.
4. Configuring Basic device settings.
5. Creating VLANs and assigning ports VLAN numbers.
6. Creating both data and voice VLANs and assigning ports VLAN numbers.
7. Subnetting and IP Addressing.
8. Configuring Inter-VLAN Routing both on the Switches (SVI) and Routers (router-on-a-stick).
9. Configuring Dedicated DHCP Server device for Data to provide dynamic IP allocation.
10. Configuring Routers as DHCP server for Voice to provide IP Phones dynamic IP allocation.
11. Configuring SSH for secure Remote access.
12. Configuring OSPF as the routing protocol.
13. Configuring Standard ACL for VTY interfaces to restrict remote Access using SSH.
14. Configuring Port Address Traslations or PAT for NAT.
15. Configuring Standard ACL for PAT.
16. Configuring VoIP or Telephony service configuration in all routers.
17. Configuring site-to-site IPsec VPN on the gateway routers.
18. Configuring Standard ACL for site-to-site IPsec VPN.
19. Host Device Configurations.
20. Test and Verifying Network Communication.

**Design and Implementation of a Secure Telecommunication Company Network System (Project #10)**

**Project #10 Case Study and Requirements**

Cairo Telco is a fast-growing telecommunication company in Egypt, which offers IT solutions and services to its clients. The company is located in the Egyptian capital city, Cairo, and has occupied the fourth and fifth floors of Pharaoh’s Mega Plaza. The company has its fourth floor hosting HR and Finance(40), Product Brand and Marketing(45), and finally, Admin and Corporate departments(35). The fifth floor is designed for IT Network & Support(45), Software Engineering(36), and Cloud Engineering departments(32).   
  
As part of ICT infrastructure, the company has subscribed to Seacom ISP for internet services and also has purchased one 5525-X Cisco ASA Firewall, one Catalyst 3850 48-Port Switch, 3 Catalyst 2960 48-Port Switches, 2 Catalyst 2960 24-Port Switches, 1 Cisco Voice Gateway, 1 Cisco WLC, and 6 LAPs. The company uses Windows Server 2022 to manage the Active Directory and Radius Server, the server is responsible for DNS services and for allocating IPv4 addresses to the DHCP hosts in the network. The company has an internally hosted ERP system, Email server, and File server. The company has settled on using Cisco Voice Gateways to provide VoIP or telephony services in the network and Cisco WLC to provide central management for Aps.   
  
Cairo Telco leverages using Microsoft Azure cloud platform to facilitate service delivery thus this is one of the core business functions of the firm. The developers and cloud engineers use several MS Azure resources like VM, blob storage, networking, and security among others to ensure seamless business continuity. The proposed network should allow the team access to these resources.  
  
Due to security requirements, it has been decided that all LAN, WLAN, and VoIP users will be on a separate network segment within the same local area network. The firewall will be used to set security zones and filter traffic that moves in and out of the zones based on the configured inspection policies. You have been hired as a network security engineer to design the network for Cairo Telco according to the requirements set by the senior management. You will consult an appropriate robust network design model to meet the design requirements. You are required to design and implement a secured, reliable, scalable, and robust network system that is paramount to safeguarding the Confidentiality, Integrity, and Availability of data and communication.  
  
The company has emphasized high performance, redundancy, scalability, and availability, and hence you are required to provide a complete Cairo Telco network infrastructure design and implementation. The company will be using the following IP address: 10.20.0.0/16 for WLAN, 192.168.10.0/24 for LAN, 172.16.10.0/24 for Voice, 10.10.10.0/28 for DMZ and 197.200.100.0 for public addresses.

* Design Tool- Use Cisco Packet Tracer to design and implement the network solution.
* Hierarchical Design- Use a hierarchical model providing redundancy at every layer.
* ISPs- The network is also expected to connect to a Seacom ISP Router.
* WLC- Each department is required to have a WAP providing both employees and guest WIFI managed by WLC.
* VoIP- Each department should have IP phones.
* VLAN- The LAN, WLAN, and VoIP VLANs remain at 50, 60 & 101 respectively for the entire network.
* EtherChannel- Use standard LACP as a method of link aggregation.
* STP PortFast and BPDUguard- configure the two protocols to enable faster port transition from blocking to forwarding.
* Subnetting- Provided the networks above, carry out subnetting to allocate the correct number of IP addresses to each department.
* Basic settings- Configure basic device settings such as hostnames, and console passwords, enable passwords, and banner messages, encrypt all passwords, and disable IP domain lookup.
* Inter-VLAN Routing- Devices in all the departments are required to communicate with each other with the respective multilayer switch configured for inter-VLAN routing.
* Core Switch- The Multilayer switches are expected to carry out both routing and switching functionalities and thus will be assigned IP addresses.
* DHCP Server- All devices in the network (except IP phones) are expected to obtain an IP address dynamically from the AD servers located at the server farm site.
* Cisco 2811 Router- Ensure to have a router that can support telephony service i.e Cisco Catalyst 2811(the VoIP router should be connected to the l3-switch).
* Static Addressing- Devices in the server room are to be allocated IP addresses statically.
* Telephony Service- Configure VoIP on the voice gateway router and allocate dial numbers in format (1...).
* Routing Protocol- Use OSPF as the routing protocol to advertise routes both on the routers and multilayer switches.
* Standard ACL for SSH- configure a simple standard ACL on the line VTY to allow only the Senior Network Security Engineer to carry out all remote administrative tasks using SSH.
* Cisco ASA Firewall- Configure security levels, zones, and policies to define how resources are accessed in the network
* Final- Test Communication, ensure everything configured is working as expected.

**Technologies Implemented**

1. Creating a network topology using Cisco Packet Tracer.
2. Hierarchical Network Design.
3. Connecting Networking devices with Correct cabling.
4. Configuring Basic device settings.
5. Creating VLANs and assigning ports VLAN numbers.
6. Creating both data and voice VLANs and assigning ports VLAN numbers.
7. Subnetting and IP Addressing.
8. Configuring Inter-VLAN Routing both on the Switches (SVI) and Routers (router-on-a-stick).
9. Configuring Dedicated DHCP Server device for Data to provide dynamic IP allocation.
10. Configuring Routers as DHCP server for Voice to provide IP Phones dynamic IP allocation.
11. Configuring Spanning-Tree Protocol - STP PortFast and BPDUGuard.
12. Configuring Active Directory as DHCP Server.
13. Configuring SSH for secure Remote access.
14. Configuring OSPF as the routing protocol.
15. Configuring Standard ACL for VTY interfaces to restrict remote Access using SSH.
16. Configuring VoIP or Telephony service configuration in all routers.
17. Configuring WLAN network- Wireless LAN Controller + Wireless Lighweight Access Points .
18. Configuring Cisco ASA Firewall Interface descriptions, zones and security levels.
19. Configuring Cisco ASA Firewall Object Network + Network Address Translation (NAT).
20. Configuring Cisco ASA Firewall OSPF + Default Static Routes.
21. Configuring Cisco ASA Firewall Inspection Policiesto filter traffic based on predetermined ACLs .
22. Host Device Configurations.
23. Test and Verifying Network Communication.