

Enterprise Networking Project Bank System Network

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 located 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.

First Floor			
No.	Departments	No. of PC	No. of Printers
1	Management	20	4
2	Research	20	4
3	Human resource	20	4

Second Floor			
No.	Departments	No. of PC	No. of Printers
1	Marketing	20	4
2	Accounting	20	4
3	Finance	20	4

Third Floor			
No.	Departments	No. of PC	No. of Printers
1	Logistics and store	20	4
2	Customer care	20	4
3	Guest Area	40	2

Fourth Floor				
No.	Departments	No. of PC	No. of Printers	No of Servers
1	Administration	20	2	
2	ICT	20	2	
3	Server Room	2 Admin PCs		3 (DHCP, HTTP and Email)

Requirements:

1. Use a software modeling tool to visualize the network topology (consider requirement 3)
 - Software Modelling Tools: MS Visio, Visual Paradigm, or Draw.io for modeling network design.
2. Use any of the following network simulation software to implement the above topology:
 - Simulation software: Cisco Packet tracer or GNS3 for design and implementation.
 - There should be one router on each floor. The router should be connecting switches on that floor.
 - 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.
 - All devices in the network are expected to obtain an IP address dynamically from the dedicated DHCP servers located at the server room.
 - Create HTTP, and E-mail servers
 - Configure SSH in all the routers for remote login.
3. Use hierarchical network design with redundancy included:
 - Having core, distribution, and access layers.
4. Configure the basic configuration of the devices:
 - Hostnames
 - Line Console and VTY passwords
 - Banner messages
 - Disable domain IP lookup
5. Each department should be in a different VLAN
 - Create VLANs in every department
 - VLANs you will use in your case, including VLAN1 also e.g. 10, 20, 30... etc.
 - Each VLAN should be a different subnetwork.
6. 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.
7. End Device Configurations:
 - Configure all the end devices in the network with the appropriate IP address based on the calculations above.
8. Configure port-security:
 - Use sticky command to obtain MAC Address.
 - Violation mode of the shutdown.
9. Test Communication:
 - Do devices in the same VLAN communicate?
 - Do the devices in different VLANs communicate?
10. Document the project design and implementation

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.