



Key Components of the Diagram:

1. Core Network (Central Area - Yellow Box)

- This section contains OSPF (Open Shortest Path First) Routing.
- Multiple routers and switches are interconnected.
- The routers and switches facilitate communication between different VLANs.

2. Departmental VLANs (Left and Right Sections)

- The left side includes:
 - Management
 - Research
 - HR
 - Marketing
 - Accounts
 - Finance
- The right side includes:
 - Logistics
 - Customer
 - Guest
 - Admin
 - ICT
 - Servers Room

3. Network Device

- 12 Access Points (APs) for wireless connectivity
- 12 PCs for employees.
- 12 Printers for document processing.
- 12 IP Phone
- 12 Switch
- 4 Multilayer Switch
- 4 Router

4. Connections Between Core and VLANs

- The core network is linked to the VLANs using Gigabit Ethernet (Gig) connections.
- The dotted and solid lines indicate physical and logical connections.

Naming:

EX. FF_M_A

FF: Floor Number

M: Department Or Section

A: Device Name

Next Table Contains All the abbreviations

| Floor | |
|------------|--------------|
| FF | First Floor |
| SF | Second Floor |
| TF | Third Floor |
| FourF | Fourth Floor |
| Department | |
| M | Managment |
| R | Research |
| HR. | HR. |
| Mar | Marketing |
| A | Accounts |
| F | Finance |
| L | Logistics |
| C | Customer |
| G | Guest |
| Admin | Admin |
| ICT | ICT |
| Servers | Servers |
| Devices | |
| PC | PC |
| A | AccessPoint |
| IPP | IP Phone |
| S | Switch |
| Pr | Printer |

Code Explain:

Switches Config.

enable ! Enter privileged EXEC mode

configure terminal ! Enter global configuration mode

hostname Router4 ! Set the router's hostname to "Router4"

! Configure console access

line console 0 ! Enter console line configuration mode

password cisco ! Set the console password to "cisco"

login ! Require login authentication for console access

exit ! Exit console line configuration mode

! Configure VTY (Telnet/SSH) access

line vty 0 4 ! Enter virtual terminal (VTY) configuration mode for remote access

password cisco ! Set the VTY password to "cisco"

login ! Require login authentication for remote access

exit ! Exit VTY line configuration mode

! Configure Message of the Day (MOTD) Banner

banner motd #

* WARNING: Unauthorized access is prohibited! *

* This system is for authorized users only. *

* All activities are logged and monitored. *

! End of banner message

no ip domain-lookup ! Disable DNS lookup to prevent delays from mistyped commands

service password-encryption ! Encrypt all plaintext passwords for security

do wr ! Save the running configuration to NVRAM (make changes permanent)

Switch Vlan Config.:

enable ! Enter privileged EXEC mode

cisco ! Enter the password (assuming it's set to "cisco")

conf terminal ! Enter global configuration mode

! Configure interfaces FastEthernet 0/1 and 0/2 as trunk ports

int range fa0/1-2 ! Select interface range Fa0/1 to Fa0/2

switchport mode trunk ! Set the interfaces to trunk mode for VLAN tagging

exit ! Exit interface configuration mode

! Create VLAN 40 and assign a name

vlan 40 ! Create VLAN 40

name Fourth_Floor ! Assign the name "Fourth_Floor" to VLAN 40

exit ! Exit VLAN configuration mode

! Configure interfaces FastEthernet 0/3 to 0/24

int range fa0/3-24 ! Select interface range Fa0/3 to Fa0/24

switchport mode trunk ! Set these ports as trunk ports

switchport access vlan 40 ! Assign VLAN 40 as the access VLAN (should be 'switchport mode access' instead)

switchport port-security ! Enable port security

switchport port-security maximum 2 ! Allow a maximum of 2 MAC addresses per port

switchport port-security mac-address sticky ! Enable sticky MAC addresses (learned and saved dynamically)

switchport port-security violation shutdown ! Shut down the port if a security violation occurs

exit ! Exit interface configuration mode

do wr ! Save the running configuration to NVRAM (make changes permanent)

exit ! Exit global configuration mode

Multi Level Switch Config:

enable ! Enter privileged EXEC mode

configure terminal ! Enter global configuration mode

! Configure console access

line console 0 ! Enter console line configuration mode

password cisco ! Set console password to "cisco"

login ! Require password authentication for console access

exit ! Exit console configuration mode

! Configure SSH settings

ip domain-name cisco.net ! Set the domain name (required for SSH key generation)

username cisco password cisco ! Create a local user "cisco" with password "cisco"

crypto key generate rsa ! Generate RSA encryption keys for SSH

1024 ! Set the key size to 1024 bits for security

! Configure VTY (Telnet/SSH) access

line vty 0 15 ! Enter configuration mode for virtual terminal (remote access)

login local ! Use the locally configured username and password for authentication

transport input ssh ! Allow only SSH for remote access (disables Telnet)

exit ! Exit VTY configuration mode

! Additional security configurations

no ip domain-lookup ! Disable automatic DNS lookup to prevent delays from mistyped commands

enable password cisco ! Set privileged EXEC mode password to "cisco"

service password-encryption ! Encrypt all plaintext passwords in the configuration

do wr ! Save the running configuration to NVRAM (make changes permanent)

! Configure access ports for VLAN 10

configure terminal ! Enter global configuration mode

interface range fa0/1 - 24 ! Select interface range Fa0/1 to Fa0/24

switchport mode access ! Set interfaces to access mode (not trunk)

switchport access vlan 10 ! Assign VLAN 10 to these ports

exit ! Exit interface configuration mode