COMPUTER NETWORKS

DOCUMENTATION ON HOTEL MANAGEMENT SYSTEM DESIGN USING PACKET TRACER

COURSE COORDINATOR:PROFESSOR KHONDEKAR LUTFUL HASAN

DEPT. OF CSE, ALIAH UNIVERSITY

SUBJECT CODE: CSEUGPC23

SEMESTER: 6TH YEAR: 3RD

PROGRAM: B. TECH DEPARTMENT: COMPUTER SCIENCE AND ENGINEERING

GROUP MEMBERS:

NAME	ROLL NO
RAJASREE LAHA	CSE214002
MOUBANI SHEE	CSE214019

Acknowledgment

We would like to express our sincere gratitude to Mr. KhondekarLutful Hasan for his invaluable guidance and support throughout this project. Their expertise and insights have been instrumental in successfully completing the Vic Modern Hotel network design and implementation.

This comprehensive documentation provides a detailed overview of the design, implementation, and testing of the Vic Modern Hotel network, serving as a valuable resource for understanding the intricacies of the project.

CONTENTS

Introduction to the Project:

The entire design of the network proposed for a university is constructedusing a Cisco packet tracer which could be used and implemented inreal life for better connectivity across a university.

The various devices that are being used in designing the network of**HOTEL MANAGEMENT SYSTEM:**

1) ROUTER: A router is a device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect and are the critical device that keeps data flowing between networks and keeping the networks connected to the internet. When data is sent between locations on one network or from one network to a second network the data is always seen and directed to the correct location by the router. The router accomplishes this by using headers and forwarding tables to determine the best path for forwarding the data packets, and they also use protocols such as ICMP to communicate with each other and configure the best route

between any two hosts.

Dual WAN 4-Port Gigabit Wireless VPN Router A Linksys Wireless RouterDSR-500N.

2) SWITCH: A switch is an electrical component that can break an electrical circuit, interrupting the current or diverting it from one conductor to another. The most familiar form of switch is a manually operated electromechanical device with one or more sets of electric contacts. Each set of contacts can be in one of two states: either 'closed' meaning the contacts are touching and electricity can flow between them, or 'open', meaning the contacts are separated and non conducting. A switch may be directly manipulated by a human as a control signal to a system, such as a computer keyboard button, or to control power flowin a circuit, such as a light switch. Automatically-operated switches can be used to control the motions of machines, for example, to indicate that a garage door has reached its full open position or that a machine tool is in a position to accept another work piece. Switches may be operated by process variables such as pressure, temperature, flow, current, voltage, and force, acting as sensors in a process and used to automatically control a system. For example, a thermostat is an automatically-operated switch used to control a heating process. A switch that is operated by another electrical circuit is called a relay. Large switches may be remotely operated by amotor drive mechanism.

Network Switches

3) MULTILAYER SWITCH: MLS provides high-performance Layer 3

switching for Cisco routers and switches. MLS switches IP data packets between subnets using advanced application-specific integrated circuit (ASIC) switching hardware. Standard routing protocols, such as Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (Enhanced IGRP), Routing Information Protocol (RIP), and Intermediate System-to-Intermediate System (IS-IS), are used for route determination. MLS enables hardware-based Layer 3 switching to offload routers from forwarding unicast IP data packets over shared media networking technologies such as Ethernet. The packet forwarding function is moved onto Layer 3 Cisco series switches whenever a partial or complete switched path exists between two hosts. Packets that do not have a partial or

complete switched path to reach their destinations still use routers for forwarding packets. MLS also provides traffic statistics as part of its switching function. These statistics are used for identifying traffic characteristics for administration, planning, and troubleshooting. MLS uses NetFlow Data Export (NDE) to export the flow statistics.
Cisco MDS 9396S 16G Multilayer Fabric Switch

e ROLE OF SWITCHES IN NETWORK - Switches may operate at one or more layers of the OSI model, including data link and network. A device that operates simultaneously at more than one of these layers is known as a multilayer switch. In switches intended for commercial use, built-in or modular interfaces make it possible to connect different types of networks, including Ethernet, Fibre Channel, ATM, ITU-TG.hn and 802.11.This connectivity can be at any of the layers mentioned. While layer-2 functionality is adequate for bandwidth-shifting within one technology, interconnecting technologies such as Ethernet and token ring is easier at layer 3. Devices that interconnect at layer 3 are traditionally called routers, so layer-3 switches can also be regarded as (relatively primitive) routers. In some service provider and other environments where there is a need for a great deal of analysis of network performance and security, switches may be connected between WAN routers as places for analytic modules. Some vendors provide firewall, network intrusion detection, and performance analysis modules that can plug into switch ports. Some of these functions may be on combined modules. In other cases, the switch is used to create a mirror image of data that can go to an external device. Since most switch port mirroring provides only one mirrored stream, network hubs can be useful for fanning out data to several read-only analyzers, such as intrusion detection systems and packet sniffers.

4)SERVER :

1) In information technology, a server is a computer program that provides services to other computer programs (and their users) in thesame or other computers.

2) The computer that a server. program runs in is also frequently referred to as a server.

Theory

Computer networking is the practice of interfacing two or more computing devices with each other to share data. Computer networks are built with a combination of hardwareand software.

Note: This page focuses on wireless networking and computer networks, which is related, but quite different, from social networking.

◍Computer Network Classification and Area Networks:

Computer networks can be categorized in several different ways. Oneapproach defines the type of network according to the geographicarea it spans. Local area networks (LANs), for example, typicallyspan a single home, school, or small office building, whereas widearea networks (WANs), reach across cities, states, or even across theworld. The Internet is the world's largest public WAN.

◍Network Design:

Computer networks also differ in their design approach. The two basicforms of network design are called client/server and peer-to-peer.

Client-server networks feature centralized server computers that

store email, Web pages, files and or applications accessed by clientcomputers and other client devices. On a peer-to-peer network,

conversely, all devices tend to support the same functions.

Client-server networks are much common in business and

peer-to-peer networks more common in homes.

A network topology defines its layout or structure from the point ofview of data flow. In so-called bus networkscomputers share and communicate across one common conduit,

whereas in a star network, all data flows through one centralized

device. Common types of network topologies include bus, star, ringnetworks and mesh networks.

Computer Network Hardware and Software

Special purpose communication devices including network routers,

access points, and network cables physically glue a network together.

Network operating systems and other software applications generatenetwork traffic and enable users to do useful things.

Home Computer Networking

While other types of networks are built and maintained by

engineers, home networks belong to ordinary homeowners, peopleoften with little or no technical background. Various manufacturersproduce broadband router hardware designed to simplify homenetwork setup. A home router enables devices in different rooms toefficiently share a broadband Internet connection, helps people tomore easily share their files and printers within the network, andimproves overall network security.

Home networks have increased in capability with each generation ofnew technology. Years ago, people commonly set up their homenetwork just to connect a few PCs, share some documents andperhaps a printer. Now it's common for households to also networkgame consoles, digital video recorders, and smartphones forstreaming sound and video. Home automation systems have alsoexisted for many years, but these too have grown in popularity morerecently with practical systems for controlling lights, digitalthermostats, and appliances.

Business Computer Networks

Small and home office (SOHO) environments use similar technologyas found in home networks. Businesses often have additionalcommunication, data storage, and security requirements that requireexpanding their networks in different ways, particularly as thebusiness gets larger.

Whereas a home network generally functions as one LAN, a businessnetwork tends to contain multiple LANs. Companies with buildings inmultiple locations utilize wide-area networking to connect thesebranch offices together. Though also available and used by somehouseholds, voice over IP communication and network storage andbackup technologies are prevalent in businesses. Larger companiesalso maintain their own internal Web sites, called intranets to helpwith employee business communication.

◍Project Scope:

The scope of the project encompasses the design and implementation of network topology, VLAN configuration, DHCP setup, SSH configuration, and port security measures for the Vic Modern Hotel.

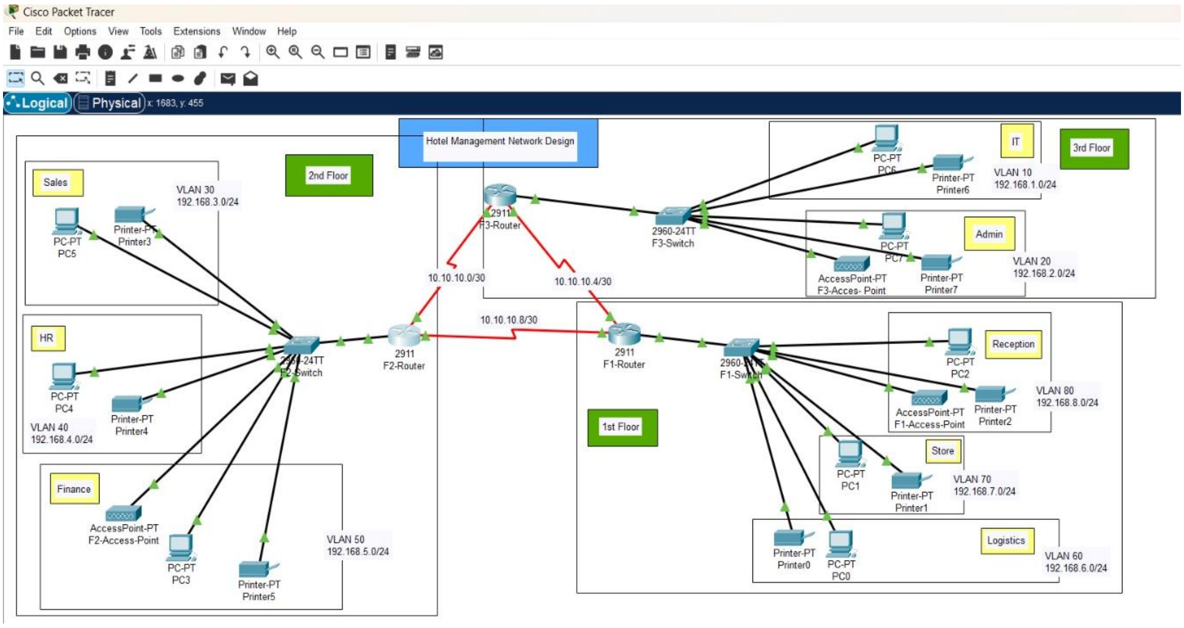
Additionally, the project includes testing and verification procedures to ensure the reliability and functionality of the deployed network infrastructure.

◍Network Topology:

Physical Layout: The server room is centrally located within the IT department on the third floor to facilitate easy access and maintenance of network equipment.

Logical Layout: A hierarchical network design is adopted, with routers connecting each floor and switches deployed on each floor to connect departmental devices.

Device Specifications: Cisco routers and switches are utilized, with specific models chosen based on performance, scalability, and feature requirements.



◍Technologies Implemented:

Hierarchical Network Design: The hierarchical design provides scalability and facilitates efficient traffic management by segregating network functions into distinct layers.

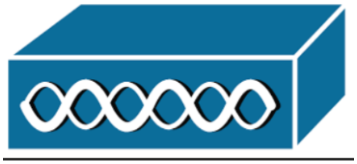
Subnetting and IP Addressing: Subnets are meticulously planned and allocated to accommodate each department's network requirements while minimizing IP address wastage.

Port Security: Port security features are configured on switches to mitigate security risks associated with unauthorized access to network resources.

WLAN Configuration: Wireless networks are configured using Cisco Access Points to provide seamless connectivity for laptops and mobile devices throughout the hotel premises.

◍Hardware and Software Requirements:

The hardware requirements include Cisco routers, switches, and access points, pc, printers, while the software requirements comprise the Cisco Packet Tracer for network simulation and configuration.



◍Physical Setup:

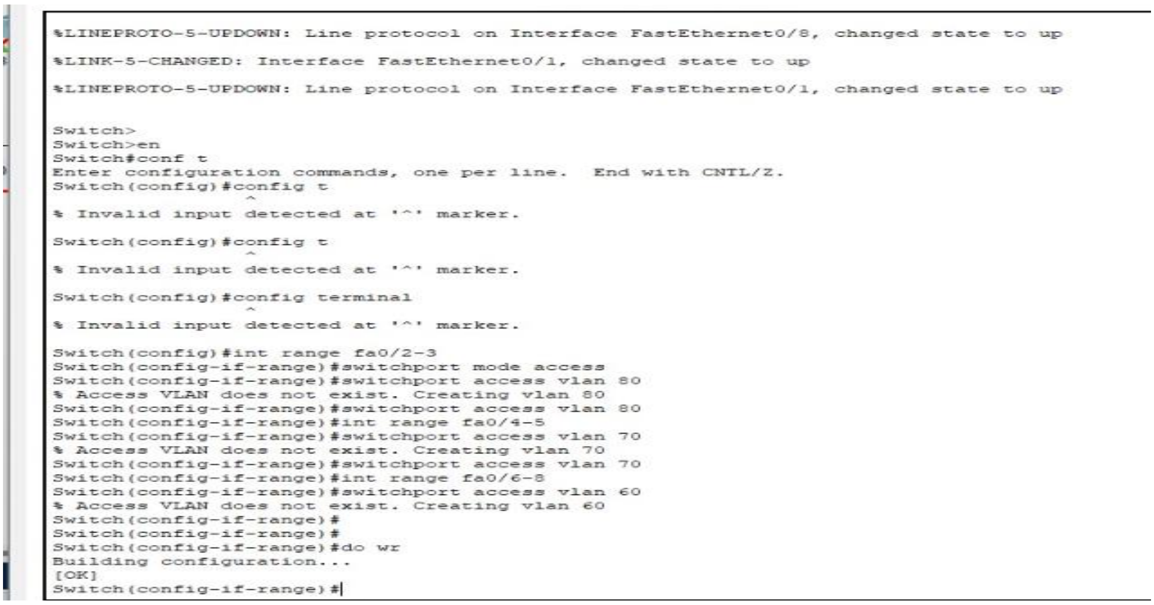
Here is the detailed documentation of the physical setup, including the placement of routers, switches, and access points within the hotel premises.

Description of cabling infrastructure used to interconnect network devices and ensure reliable data transmission.

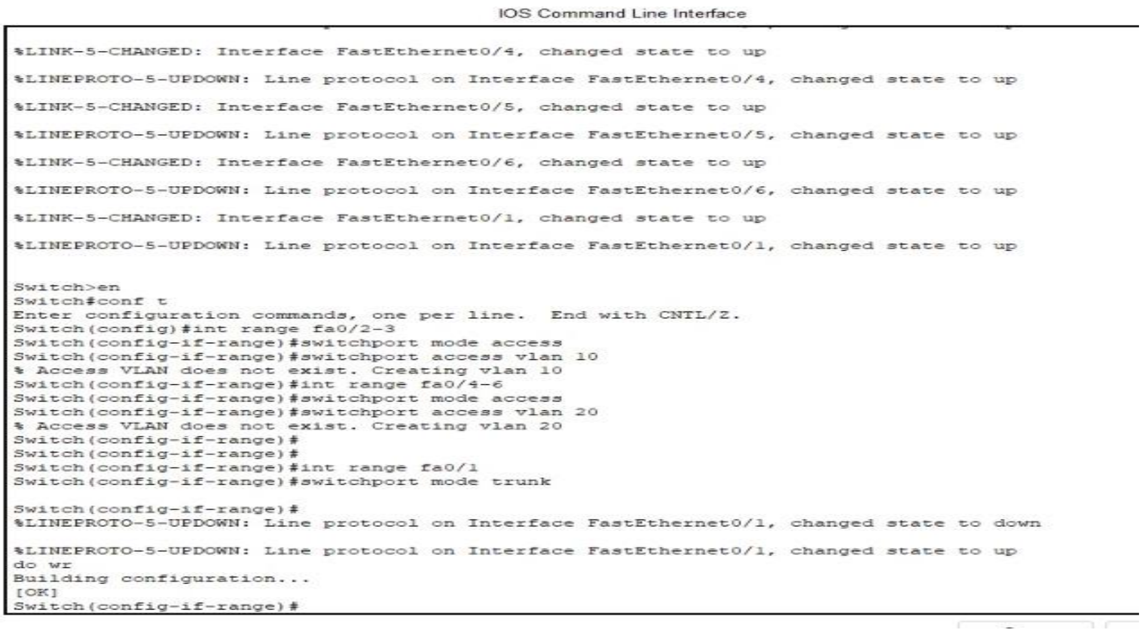
◍VLAN Configuration:

VLAN Design Considerations: The rationale behind VLAN assignment for each department is explained, emphasizing security, performance, and manageability.

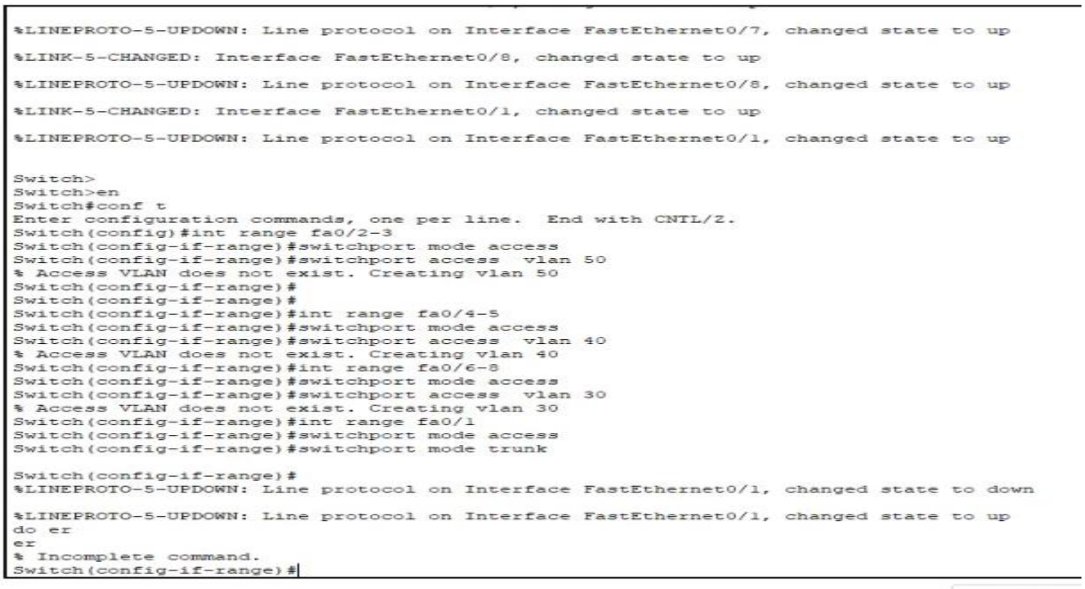
VLAN Implementation: Step-by-step instructions on VLAN configuration, including VLAN creation, port assignment, and VLAN interface configuration.



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up


Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#config t
               ^
% Invalid input detected at '^' marker.

Switch(config)#config t
               ^
% Invalid input detected at '^' marker.

Switch(config)#config terminal
               ^
% Invalid input detected at '^' marker.

Switch(config)#int range fa0/2-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 80
% Access VLAN does not exist. Creating vlan 80
Switch(config-if-range)#switchport access vlan 80
Switch(config-if-range)#int range fa0/4-5
Switch(config-if-range)#switchport access vlan 70
% Access VLAN does not exist. Creating vlan 70
Switch(config-if-range)#switchport access vlan 70
Switch(config-if-range)#int range fa0/6-8
Switch(config-if-range)#switchport access vlan 60
% Access VLAN does not exist. Creating vlan 60
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#do wr
Building configuration...
[OK]
Switch(config-if-range)#
```



```
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up


Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range fa0/2-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
Switch(config-if-range)#int range fa0/4-6
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#int range fa0/1
Switch(config-if-range)#switchport mode trunk

Switch(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
do wr
Building configuration...
[OK]
Switch(config-if-range)#
```



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up


Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range fa0/2-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access  vlan 50
% Access VLAN does not exist. Creating vlan 50
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#int range fa0/4-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access  vlan 40
% Access VLAN does not exist. Creating vlan 40
Switch(config-if-range)#int range fa0/6-8
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access  vlan 30
% Access VLAN does not exist. Creating vlan 30
Switch(config-if-range)#int range fa0/1
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport mode trunk

Switch(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
do er
er
% Incomplete command.
Switch(config-if-range)#
```

Inter-VLAN Routing: Explanation of router-on-a-stick configuration for inter-VLAN communication, along with configuration steps and verification procedures.

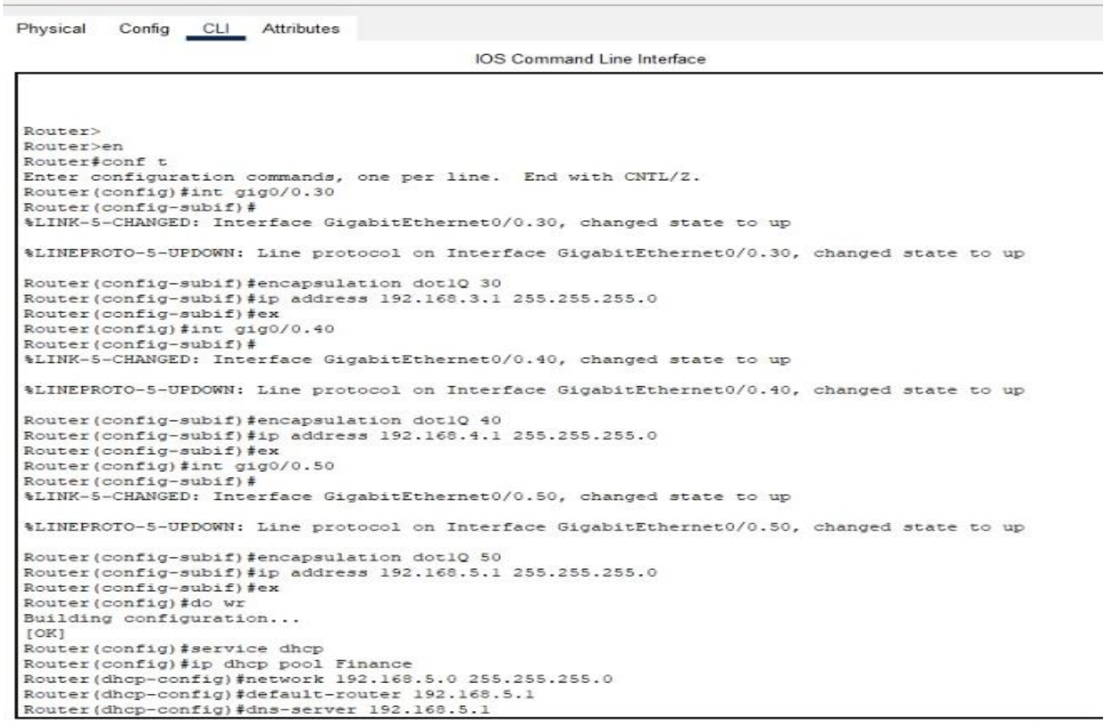
◍Inter-VLAN Routing:

A detailed explanation of how inter-VLAN communication is facilitated using router sub-interfaces, VLAN tagging, and routing protocols such as OSPF.

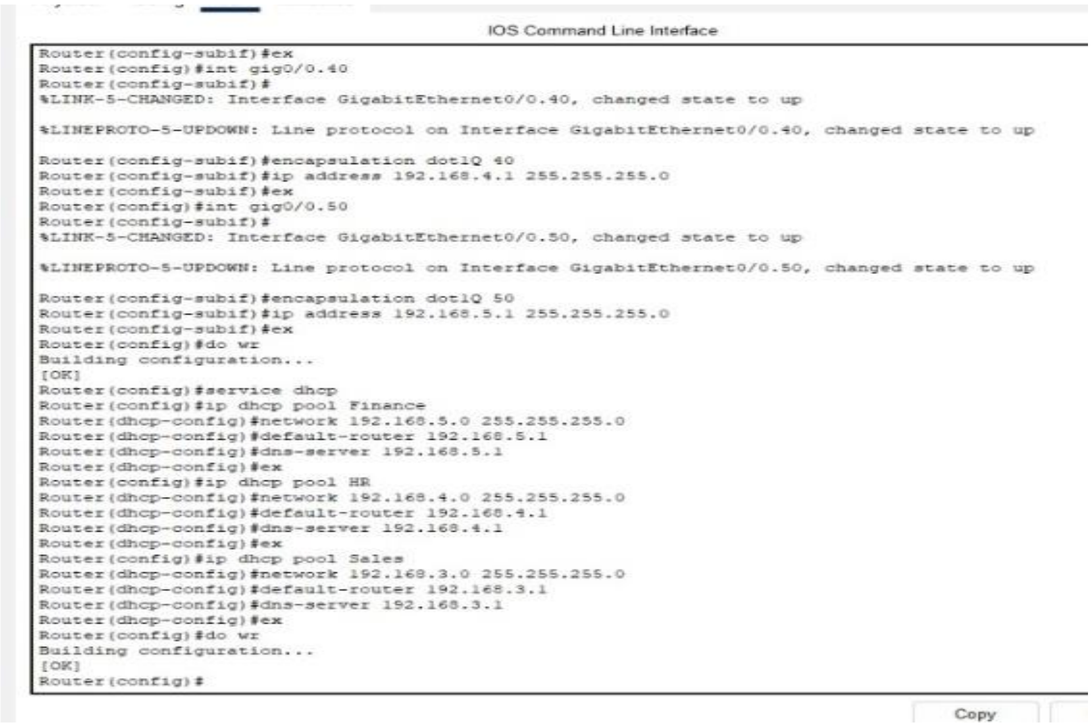
◍DHCP Setup:

Configuration of DHCP pools on routers to dynamically allocate IP addresses to devices within each VLAN.

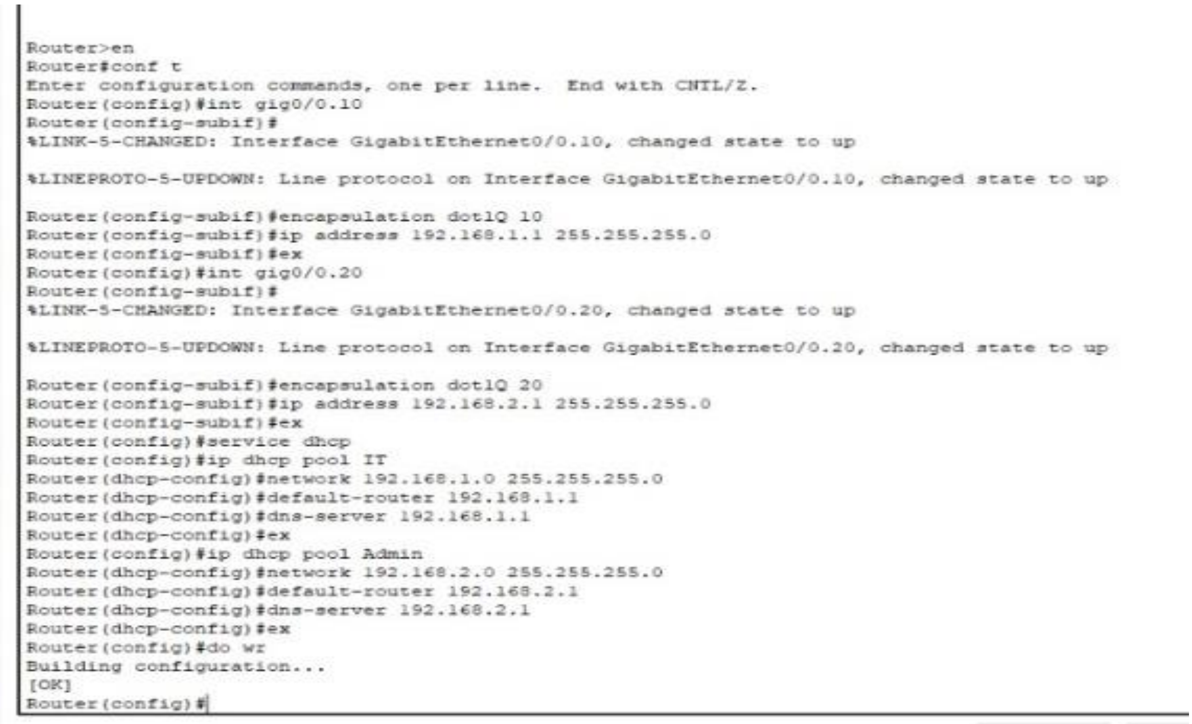
Explanation of DHCP server role on routers and configuration steps for DHCP pool setup.



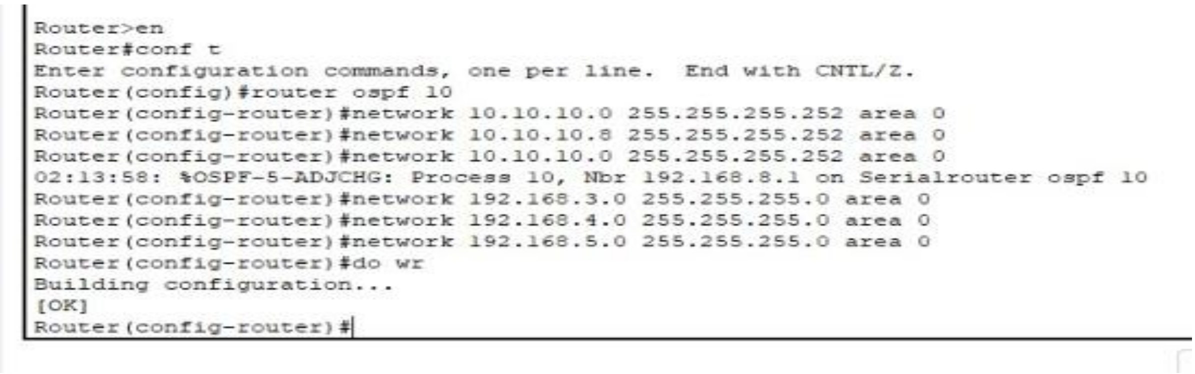
```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/0.30
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to up

Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#ex
Router(config)#int gig0/0.40
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.40, changed state to up

Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.4.1 255.255.255.0
Router(config-subif)#ex
Router(config)#int gig0/0.50
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.50, changed state to up

Router(config-subif)#encapsulation dot1Q 50
Router(config-subif)#ip address 192.168.5.1 255.255.255.0
Router(config-subif)#ex
Router(config)#do wr
Building configuration...
[OK]
Router(config)#service dhcp
Router(config)#ip dhcp pool Finance
Router(dhcp-config)#network 192.168.5.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.5.1
Router(dhcp-config)#dns-server 192.168.5.1
```



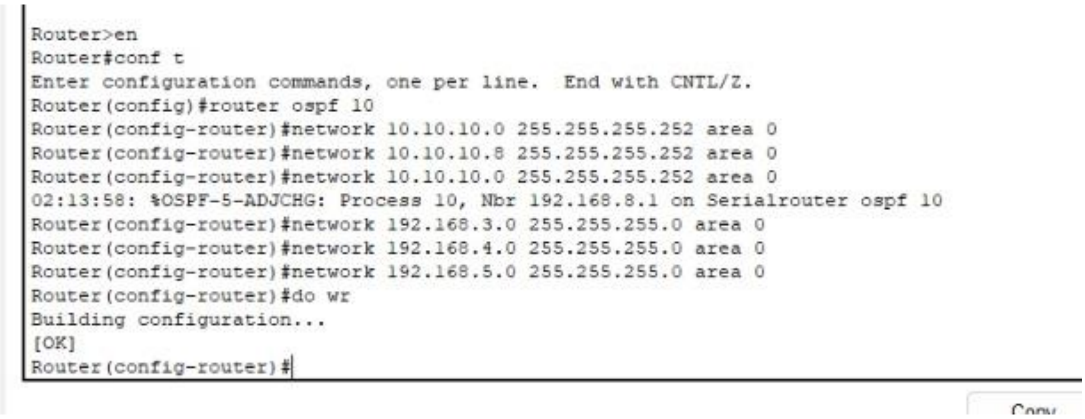
```
Router(config-subif)#ex
Router(config)#int gig0/0.40
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.40, changed state to up

Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.4.1 255.255.255.0
Router(config-subif)#ex
Router(config)#int gig0/0.50
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.50, changed state to up

Router(config-subif)#encapsulation dot1Q 50
Router(config-subif)#ip address 192.168.5.1 255.255.255.0
Router(config-subif)#ex
Router(config)#do wr
Building configuration...
[OK]
Router(config)#service dhcp
Router(config)#ip dhcp pool Finance
Router(dhcp-config)#network 192.168.5.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.5.1
Router(dhcp-config)#dns-server 192.168.5.1
Router(dhcp-config)#ex
Router(config)#ip dhcp pool HR
Router(dhcp-config)#network 192.168.4.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.4.1
Router(dhcp-config)#dns-server 192.168.4.1
Router(dhcp-config)#ex
Router(config)#ip dhcp pool Sales
Router(dhcp-config)#network 192.168.3.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.3.1
Router(dhcp-config)#dns-server 192.168.3.1
Router(dhcp-config)#ex
Router(config)#do wr
Building configuration...
[OK]
Router(config)#
```



```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/0.10
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10, changed state to up

Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#ex
Router(config)#int gig0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up

Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#ex
Router(config)#service dhcp
Router(config)#ip dhcp pool IT
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 192.168.1.1
Router(dhcp-config)#ex
Router(config)#ip dhcp pool Admin
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#dns-server 192.168.2.1
Router(dhcp-config)#ex
Router(config)#do wr
Building configuration...
[OK]
Router(config)#
```



```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 10
Router(config-router)#network 10.10.10.0 255.255.255.252 area 0
Router(config-router)#network 10.10.10.8 255.255.255.252 area 0
Router(config-router)#network 10.10.10.0 255.255.255.252 area 0
02:13:58: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.8.1 on Serialrouter ospf 10
Router(config-router)#network 192.168.3.0 255.255.255.0 area 0
Router(config-router)#network 192.168.4.0 255.255.255.0 area 0
Router(config-router)#network 192.168.5.0 255.255.255.0 area 0
Router(config-router)#do wr
Building configuration...
[OK]
Router(config-router)#
```



```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 10
Router(config-router)#network 10.10.10.0 255.255.255.252 area 0
Router(config-router)#network 10.10.10.8 255.255.255.252 area 0
Router(config-router)#network 10.10.10.0 255.255.255.252 area 0
02:13:58: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.8.1 on Serialrouter ospf 10
Router(config-router)#network 192.168.3.0 255.255.255.0 area 0
Router(config-router)#network 192.168.4.0 255.255.255.0 area 0
Router(config-router)#network 192.168.5.0 255.255.255.0 area 0
Router(config-router)#do wr
Building configuration...
[OK]
Router(config-router)#
```

◍SSH Configuration:

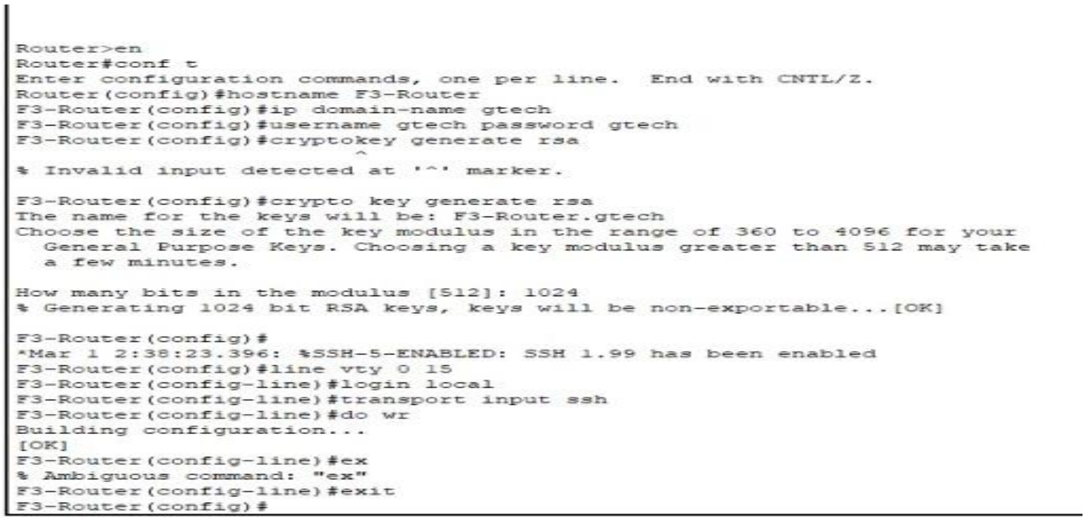
Secure Access Management: The importance of SSH for secure remote access to network devices is emphasized, highlighting its superiority over less secure protocols like Telnet.

SSH Configuration Steps: Detailed instructions on SSH configuration for routers, including key generation, user account creation, and access control settings.

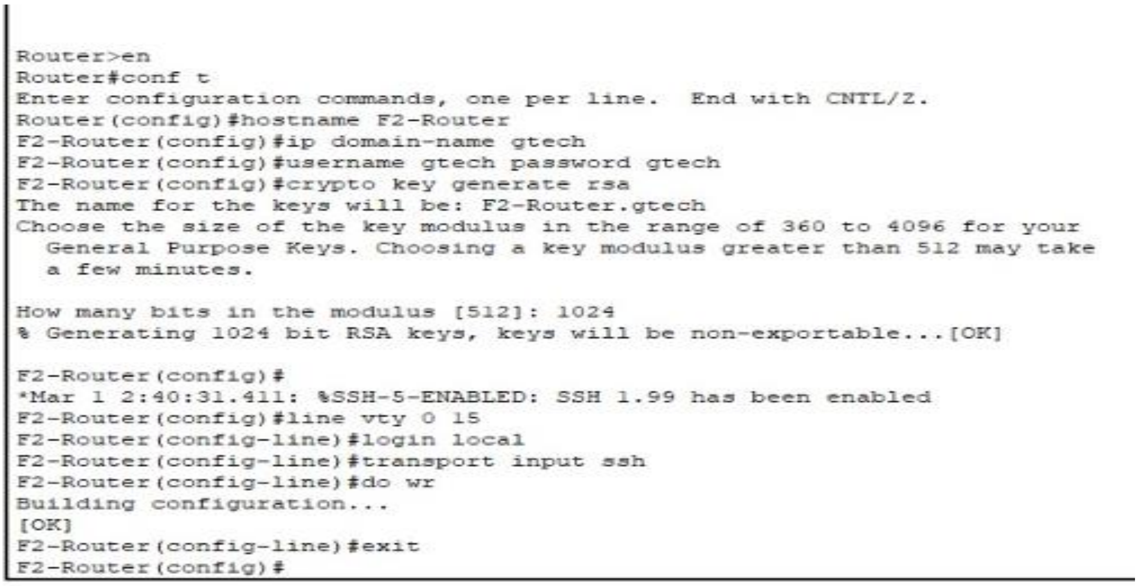
Best Practices: Recommendations for implementing SSH security best practices to safeguard against unauthorized access and ensure secure remote management.

◍Port Security Configuration:

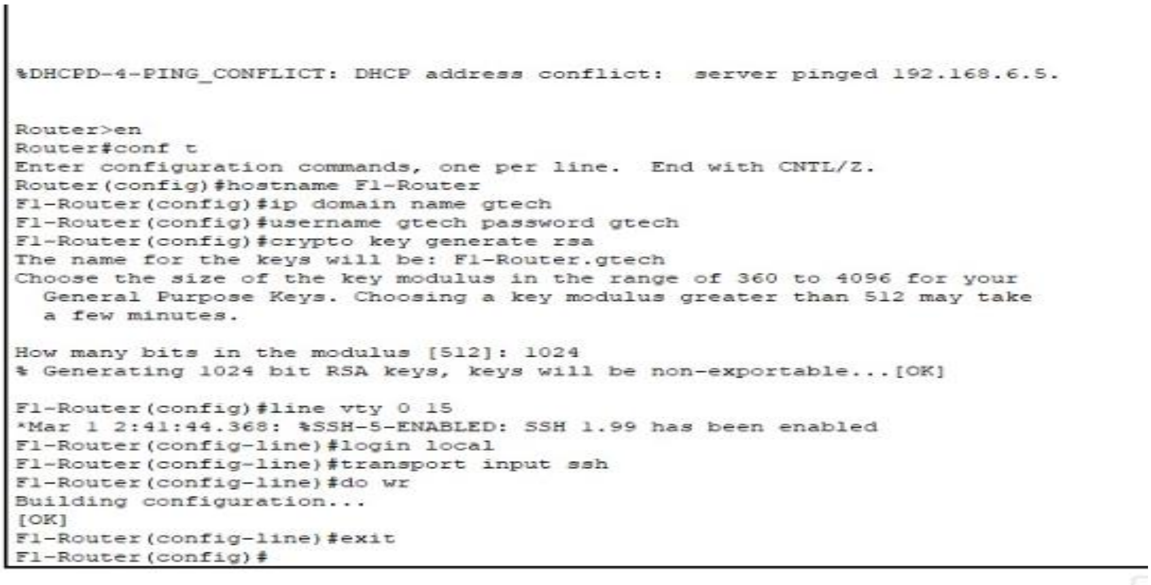
Configuration of port security features on switches to prevent unauthorized access to network resources.



```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname F3-Router
F3-Router(config)#ip domain-name gtech
F3-Router(config)#username gtech password gtech
F3-Router(config)#cryptokey generate rsa
                         ^
% Invalid input detected at '^' marker.

F3-Router(config)#crypto key generate rsa
The name for the keys will be: F3-Router.gtech
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

F3-Router(config)#
*Mar 1 2:38:23.396: %SSH-5-ENABLED: SSH 1.99 has been enabled
F3-Router(config)#line vty 0 15
F3-Router(config-line)#login local
F3-Router(config-line)#transport input ssh
F3-Router(config-line)#do wr
Building configuration...
[OK]
F3-Router(config-line)#ex
% Ambiguous command: "ex"
F3-Router(config-line)#exit
F3-Router(config)#
```



```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname F2-Router
F2-Router(config)#ip domain-name gtech
F2-Router(config)#username gtech password gtech
F2-Router(config)#crypto key generate rsa
The name for the keys will be: F2-Router.gtech
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

F2-Router(config)#
*Mar 1 2:40:31.411: %SSH-5-ENABLED: SSH 1.99 has been enabled
F2-Router(config)#line vty 0 15
F2-Router(config-line)#login local
F2-Router(config-line)#transport input ssh
F2-Router(config-line)#do wr
Building configuration...
[OK]
F2-Router(config-line)#exit
F2-Router(config)#
```



```
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 192.168.6.5.

Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname F1-Router
F1-Router(config)#ip domain name gtech
F1-Router(config)#username gtech password gtech
F1-Router(config)#crypto key generate rsa
The name for the keys will be: F1-Router.gtech
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

F1-Router(config)#line vty 0 15
*Mar 1 2:41:44.368: %SSH-5-ENABLED: SSH 1.99 has been enabled
F1-Router(config-line)#login local
F1-Router(config-line)#transport input ssh
F1-Router(config-line)#do wr
Building configuration...
[OK]
F1-Router(config-line)#exit
F1-Router(config)#
```

Description of sticky MAC address learning method and its implementation to enhance port security.

◍Total Configuration:

```
en

F2-Router#sh start

Using 1789 bytes

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname F2-Router

!

!

!

!

!
```

```
ipdhcp pool Finance
 network 192.168.5.0 255.255.255.0
 default-router 192.168.5.1
dns-server 192.168.5.1
ipdhcp pool HR
 network 192.168.4.0 255.255.255.0
 default-router 192.168.4.1
dns-server 192.168.4.1
ipdhcp pool Sales
 network 192.168.3.0 255.255.255.0
 default-router 192.168.3.1
dns-server 192.168.3.1
!
!
!
no ipcef
no ipv6 cef
!
!
!
username gtech password 0 gtech
!
!
license udipid CISCO2911/K9 sn FTX1524W341-
!
!
!
!
!
```

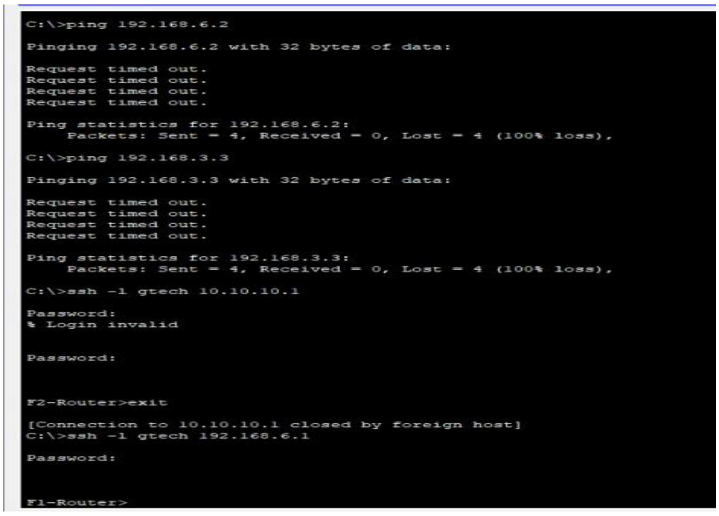
```
!
!
!
!
ip domain-name gtech
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
ip address 192.168.3.1 255.255.255.0
!
interface GigabitEthernet0/0.40
 encapsulation dot1Q 40
ip address 192.168.4.1 255.255.255.0
!
interface GigabitEthernet0/0.50
 encapsulation dot1Q 50
```

```
ip address 192.168.5.1 255.255.255.0
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/2/0
ip address 10.10.10.1 255.255.255.252
!
interface Serial0/2/1
ip address 10.10.10.10 255.255.255.252
 clock rate 64000
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 10
 log-adjacency-changes
 network 10.10.10.0 0.0.0.3 area 0
 network 10.10.10.8 0.0.0.3 area 0
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.4.0 0.0.0.255 area 0
 network 192.168.5.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
end
```

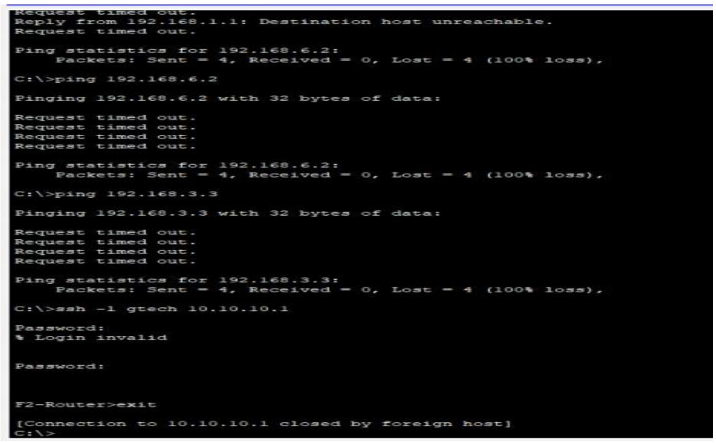
r ataholo total ki ki configured acha seta

◍Testing and Verification:

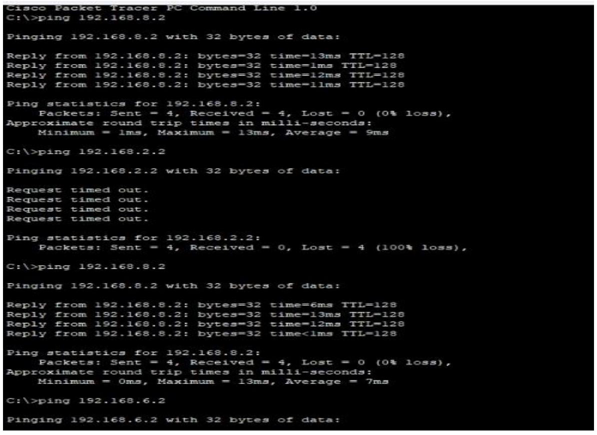
Test Plan: Outline of the test plan used to validate network functionality, including connectivity tests, DHCP lease verification, and inter-department communication tests.



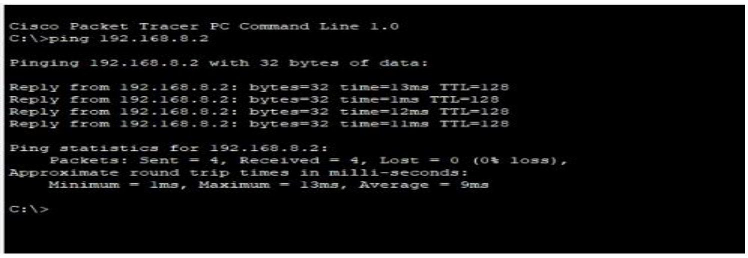
```
C:\>ping 192.168.6.2

Pinging 192.168.6.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.6.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ssh -l gtech 10.10.10.1

Password:
% Login invalid


Password:



F2-Router>exit

[Connection to 10.10.10.1 closed by foreign host]
C:\>ssh -l gtech 192.168.6.1

Password:



F1-Router>
```



```
Request timed out.
Reply from 192.168.1.1: Destination host unreachable.
Request timed out.

Ping statistics for 192.168.6.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.6.2

Pinging 192.168.6.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.6.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ssh -l gtech 10.10.10.1

Password:
% Login invalid


Password:



F2-Router>exit

[Connection to 10.10.10.1 closed by foreign host]
C:\>
```

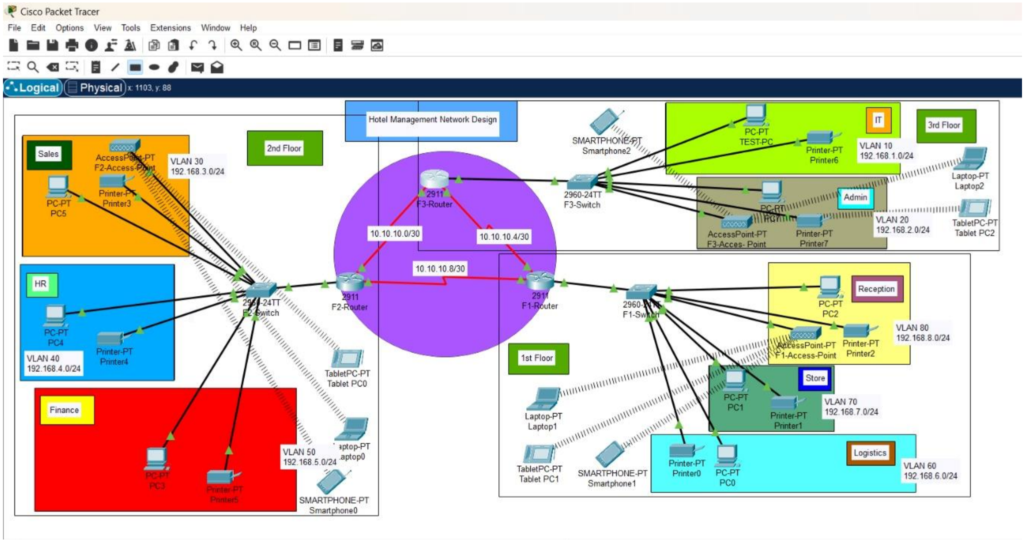


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.8.2

Pinging 192.168.8.2 with 32 bytes of data:

Reply from 192.168.8.2: bytes=32 time=13ms TTL=128
Reply from 192.168.8.2: bytes=32 time=1ms TTL=128
Reply from 192.168.8.2: bytes=32 time=12ms TTL=128
Reply from 192.168.8.2: bytes=32 time=11ms TTL=128

Ping statistics for 192.168.8.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 13ms, Average = 9ms

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.8.2

Pinging 192.168.8.2 with 32 bytes of data:

Reply from 192.168.8.2: bytes=32 time=6ms TTL=128
Reply from 192.168.8.2: bytes=32 time=13ms TTL=128
Reply from 192.168.8.2: bytes=32 time=12ms TTL=128
Reply from 192.168.8.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.8.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 7ms

C:\>ping 192.168.6.2

Pinging 192.168.6.2 with 32 bytes of data:
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.8.2

Pinging 192.168.8.2 with 32 bytes of data:

Reply from 192.168.8.2: bytes=32 time=13ms TTL=128
Reply from 192.168.8.2: bytes=32 time=1ms TTL=128
Reply from 192.168.8.2: bytes=32 time=12ms TTL=128
Reply from 192.168.8.2: bytes=32 time=11ms TTL=128

Ping statistics for 192.168.8.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 13ms, Average = 9ms

C:\>
```

Results Analysis: Analysis of test results, identification of issues encountered, and steps taken to troubleshoot and resolve them.



Performance Metrics: Measurement of network performance metrics such as latency, throughput, and packet loss to ensure optimal operation.

Troubleshooting:

During implementation, issues like IP conflicts, faulty cables, and misconfigured routers were encountered. Troubleshooting steps included verifying physical connections, using diagnostic tools to ping and trace routes, and resetting network devices. Common network troubleshooting techniques involve checking for IP address conflicts, ensuring correct DNS settings, and examining firewall configurations. Best practices include documenting network changes, keeping firmware updated, and using reliable network monitoring tools. Regularly backing up configurations and implementing robust security measures also help prevent and quickly resolve connectivity issues.

Future Recommendations:

Next-Generation Technologies:

- **SDN and NFV:** Centralize control and virtualize network services for flexibility and cost reduction.
- **5G and Wi-Fi 6:** Prepare for higher bandwidth and lower latency to support more devices and better performance.

Security Improvements:

- **Zero Trust Architecture:** Trust no device by default, enhancing internal and external threat protection.
- **AI-based Threat Detection:** Use AI for proactive threat identification and response.
- **SASE:** Combine network security with WAN capabilities for simplified management and secure access.

Performance Enhancements:

- **Network Optimization:** Deploy advanced tools to identify and mitigate bottlenecks.
- **QoS Policies:** Prioritize critical applications to reduce latency.

- **Edge Computing:** Process data closer to its source, reducing latency and bandwidth use.

Scalability:

- **Modular Design:** Use modular components for easy expansion.
- **Cloud Integration:** Leverage cloud services for elastic scalability and cost efficiency.
- **Automation:** Implement automation tools for streamlined management and rapid scaling.

Lessons Learned:

- **Documentation:** Develop comprehensive network documentation.
- **Continuous Monitoring:** Regularly audit and monitor the network for proactive issue resolution.
- **Training:** Provide ongoing training on new technologies.
- **Feedback Loop:** Integrate user feedback for continuous improvement.

IMPORTANCE OF THIS PROJECT

Wide Area Networks are spread over a (very) wide area so that companies and institutes that are located far from each other are directly connected via the network. Wide Area Networks have mostly on more than one location external connections with other big networks. Internet Service

Providers (ISPs) and multinationals with many offices frequently own a WAN themselves. Regional education networks and company networks between several establishments are also examples of Wide Area Networks. Two great advantages of WAN are allowing secure and fast data transmission between the different nodes in the network. The data transmission is also reliable and inexpensive. The characteristics of the transmission facilities lead to an emphasis on efficiency of communications techniques in the design of WANs. Controlling the volume of traffic and avoiding excessive delays is important. Since the topologies of WANs are likely to be more complex than those of LANs, routing algorithms also receive more emphasis. Many WANs also implement sophisticated monitoring procedures to account for which users consume the network resources.

Conclusion:

Project Summary

Key Achievements

The Vic Modern Hotel network project has been a significant success, delivering a robust and high-performance network infrastructure across all hotel locations. Key achievements include:

Comprehensive Coverage: Seamless wireless connectivity was established throughout all hotel properties, ensuring guests and staff experience uninterrupted service.

High-Speed Internet: Implementation of fiber-optic connections has resulted in exceptionally high-speed internet access, significantly enhancing the guest experience.

Advanced Security Measures: Deployment of state-of-the-art security protocols and systems to safeguard sensitive data and maintain guest privacy.

Lessons Learned

Challenges Faced

Coordination Among Stakeholders: Ensuring seamless communication and coordination among diverse stakeholders was a significant challenge, requiring robust project management and frequent updates.

Technical Complexities: Encountered technical difficulties related to integrating new technologies with existing systems, which necessitated detailed planning and expert troubleshooting.

Budget Constraints: Managing budget constraints while striving for high-quality outcomes required innovative cost-saving measures and continuous financial monitoring.

Future Outlook

Potential Future Directions

Further Optimization: Continuous monitoring and assessment to identify areas for optimization, such as enhancing bandwidth management and improving latency.

Expansion: Expanding the network to new hotel locations or adding additional services, such as IoT-based room controls, to further enhance the guest experience.

The successful completion of the Vic Modern Hotel network project not only demonstrates our capability to deliver high-quality network solutions but also sets a strong foundation for future advancements and improvements. By reflecting on our experiences and planning for future enhancements, we ensure that the network remains a key asset in delivering exceptional guest experiences and supporting hotel operations.

References:

1. "Computer Networks." Pearson.Forouzan, B. A. (2012).

2. "Data Communications and Networking." McGraw-Hill Education.Cisco. (2021).

3. "OSPF Configuration Guide." Retrieved from Cisco OSPF Configuration Guide.Stallings, W. (2013).

4. "NetworK Security Essentials." Pearson.Cisco. (2019).

Teacher's Signature

THE END.