”Voice Over IP Network (VoIP)”

Submitted By

Student Name	Student ID
Tanvir Ahmed Bipul	221-15-4925
Jahidul Islam Rakib	221-15-4814
MD Samsul Arefin	221-15-5279
Fariha Rahman Aisharjo	221-15-5604
Jahid Hasan Tutul	221-15-4901

MINI LAB PROJECT REPORT

This Report Presented in Partial Fulfillment of the course **CSE313: COMPUTER NETWORK in the Computer Science and Engineering Department**

DAFFODIL INTERNATIONAL UNIVERSITY
Dhaka, Bangladesh

December 14, 2024

DECLARATION

We hereby declare that this lab project has been done by us under the supervision of **Taslima Akhter**, **Lecturer**, Department of Computer Science and Engineering, Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere as lab projects.

Submitted To:

Taslima Akhter
Lecturer
Department of Computer Science and Engineering
Daffodil International University

Submitted by

TANVIR AHAMMED BIPUL Student ID:221-15-4925 Dept. of CSE, DIU	
MD. JAHIDUL ISLAM RAKIB Student ID:221-15-4814 Dept. of CSE, DIU	**MD SAMSUL AREFIN** Student ID:221-15-5279 Dept. of CSE, DIU
FARIA RAHMAN AISHORJO Student ID:221-15-5604 Dept. of CSE, DIU	**JAHID HASAN TUTUL** Student ID:221-15-4901 Dept. of CSE, DIU

COURSE & PROGRAM OUTCOME

The following course have course outcomes as following:.

Table 1: Course Outcome Statements

CO's	Statements
CO1	**Define** and **Relate** core concepts of VoIP, including protocols (SIP, RTP) and network components used in communication.
CO2	**Formulate** a working VoIP network topology and configure key routing protocols to establish connectivity.
CO3	**Analyze** the performance of VoIP networks by testing call quality (QoS) and bandwidth utilization.
CO4	**Develop** and Implement a fully functional VoIP system, applying VLANs, DHCP helper, and routing techniques to optimize communication.

Table 2: Mapping of CO, PO, Blooms, KP and CEP

CO	PO	Blooms	KP	CEP
CO1	PO1	C1, C2	KP3	EP1,EP3
CO2	PO2	C2,A2	KP3	EP1,EP3
CO3	PO3	C4, A3	KP3	EP1,EP2
CO4	PO4	C5, C6,P3	KP4	EP1,EP3

The mapping justification of this table is provided in section **4.3.1**, **4.3.2** and **4.3.3**.

Table of Contents

Chapter 1

Introduction

chapter introduces the concept of Voice over IP (VoIP) networks, which enable voice communication over the internet by converting voice signals into data packets. It explores the evolution of communication technologies, highlighting the benefits of cost efficiency, flexibility, and integration with modern digital services.

1.1 Introduction

This chapter outlines the background and problem statement addressed by the project. The project aims to design and implement a Voice over IP (VoIP) telephony service network using Cisco Packet Tracer, integrating key network technologies for efficient and secure communication.

1.2 Motivation

The growing reliance on IP-based communication in organizations has motivated this project. Implementing VoIP provides a cost-effective solution, enhances technological skills, and prepares for real-world challenges in telecommunications.

1.3 Objectives

- To design a hierarchical network supporting VoIP services.
- To implement VLAN segmentation and Inter-VLAN Routing.
- To configure DHCP for dynamic IP assignment.
- To enable SSH for secure remote management.
- To set up and configure VoIP services and dial-peering.
- To test and analyze network performance.

1.4 Feasibility Study

Research indicates VoIP's growing adoption due to cost-effectiveness and flexibility. Tools like Cisco Packet Tracer allow simulation and analysis of VoIP networks without requiring physical infrastructure.[1].

1.5 Gap Analysis

Existing studies focus on advanced VoIP configurations but often neglect simulations limited to educational tools. This project addresses this gap by creating a scalable, secure VoIP network in Cisco Packet Tracer.

1.6 Project Outcome

- A simulated VoIP-enabled telephony network.
- Improved understanding of hierarchical network design.
- Documentation of methodologies and results.
- Understand the fundamental concepts of VoIP technology, including key protocols like SIP, RTP, and their applications.
- Design and configure a VoIP network using VLANs, IP addressing, and inter-VLAN routing for communication between different segments.
- Implement inter-VLAN routing and integrate DHCP helper addresses to enable dynamic IP address allocation.
- Analyze the performance of the VoIP network by monitoring Quality of Service (QoS), latency, and bandwidth utilization.
- Test and evaluate the overall VoIP system to ensure it meets performance requirements and industry standards.

Chapter 2

Proposed Methodology/Architecture

This chapter outlines the steps and processes used to study, design, and analyze VoIP networks. It includes data collection techniques, simulation tools, and evaluation metrics. A detailed explanation of the conversion of analog voice signals into digital packets and their transmission over IP networks is provided to showcase the technological workflow.

2.1 Requirement Analysis & Design Specification

This section focuses on identifying and specifying the network requirements for the project, ensuring they align with the goals of scalability, security, and efficiency.

2.1.1 Overview

The proposed network architecture integrates hierarchical network design principles to ensure scalability and efficiency. VLANs are implemented for segmentation and security, and the VoIP services are configured to simulate real-world telephony systems. These core features ensure that the network meets performance and operational expectations.

2.1.2 Proposed Methodology/ System Design

Phase 1: Research and Network Design
• Task 1: Review hierarchical network models and VoIP requirements to understand best practices for network segmentation and VoIP implementation.
• Task 2: Design a network topology using Cisco Packet Tracer, incorporating:
o Routers: For gateway and inter-VLAN communication.
o Switches: For network segmentation and VLAN management.
o IP Phones: To simulate VoIP devices.
o VLANs: To segregate traffic logically.
Phase 2: VLAN and DHCP Configuration
• Task 1: Create VLANs on switches to segment the network by department or purpose (e.g., Voice, Data, Management).
• Task 2: Configure DHCP on routers or switches to dynamically allocate IP addresses for each VLAN.
Phase 3: Inter-VLAN Routing and SSH Configuration

• Task 1: Set up Router-on-a-Stick configuration by:
o Creating subinterfaces for each VLAN on the router.
o Assigning IP addresses to the subinterfaces as gateways for respective VLANs.
• Task 2: Configure SSH on network devices to:
o Enhance security for remote management.
o Test connectivity using SSH clients.
Phase 4: VoIP and Dial-Peering Setup
• Task 1: Configure VoIP settings:
o Assign IP addresses to IP phones manually or via DHCP.
o Set up a VoIP server (e.g., CUCM simulation) if required.
• Task 2: Configure dial-peering on gateway routers to enable communication across different networks.
Phase 5: Testing and Optimization
• Task 1: Test network functionality:
o Verify VLAN segmentation using ping tests.
o Check inter-VLAN routing by testing connectivity between devices in different VLANs.
o Confirm VoIP service functionality using test calls between IP phones.
• Task 2: Evaluate network performance:
o Measure call quality, latency, jitter, and packet loss.
o Optimize configurations to improve performance and resolve identified issues.
Phase 6: Documentation
• Task 1: Document the entire network setup:
o Provide a detailed summary of the design and configurations for VLANs, DHCP, routing, and VoIP.
o Include test results and optimization changes.
• Task 2: Create a diagram summarizing the final network topology with all elements from the phases.

2.2 Overall Project Plan

The project follows a structured and phased approach to ensure all objectives are met efficiently. The plan is divided into six phases:
1. Research and Network Design: Analyze VoIP requirements and design the network topology.
2. Configuration of VLANs and DHCP: Segment the network into VLANs and automate IP allocation using DHCP.
3. Inter-VLAN Routing and SSH Configuration: Enable communication across VLANs and secure remote access with SSH.
4. Implementation of VoIP Services: Configure IP phones, dial-peering, and test call functionality.
5. Testing and Optimization: Evaluate the network for functionality, performance, and reliability, making adjustments as needed.
6. Documentation: Compile detailed records of design choices, configurations, and testing results for future reference.

2.3 UI Design

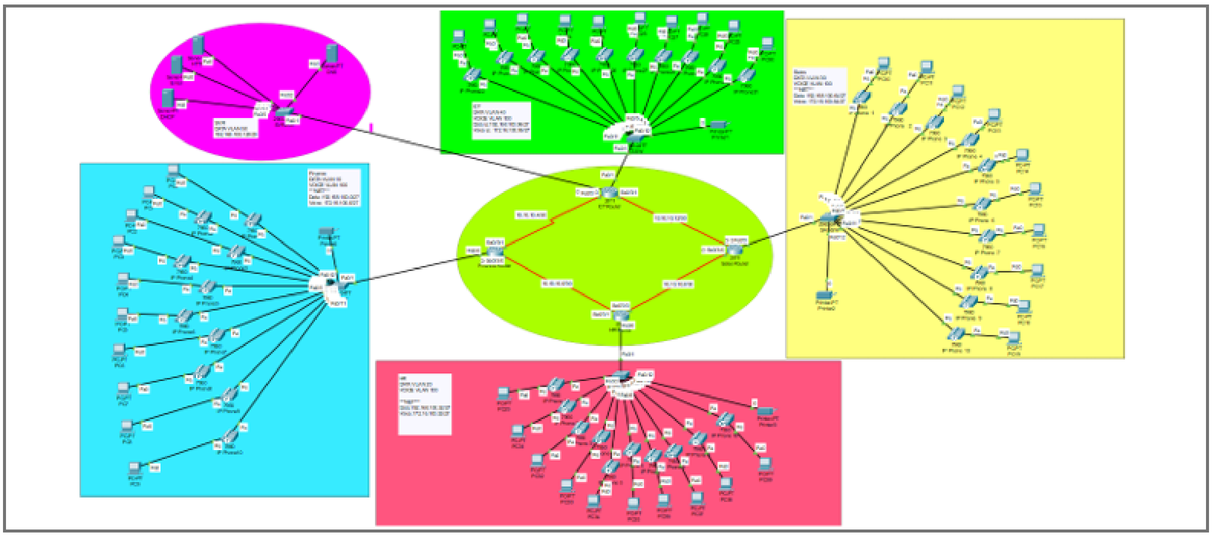


Figure 2.1: UI diagram

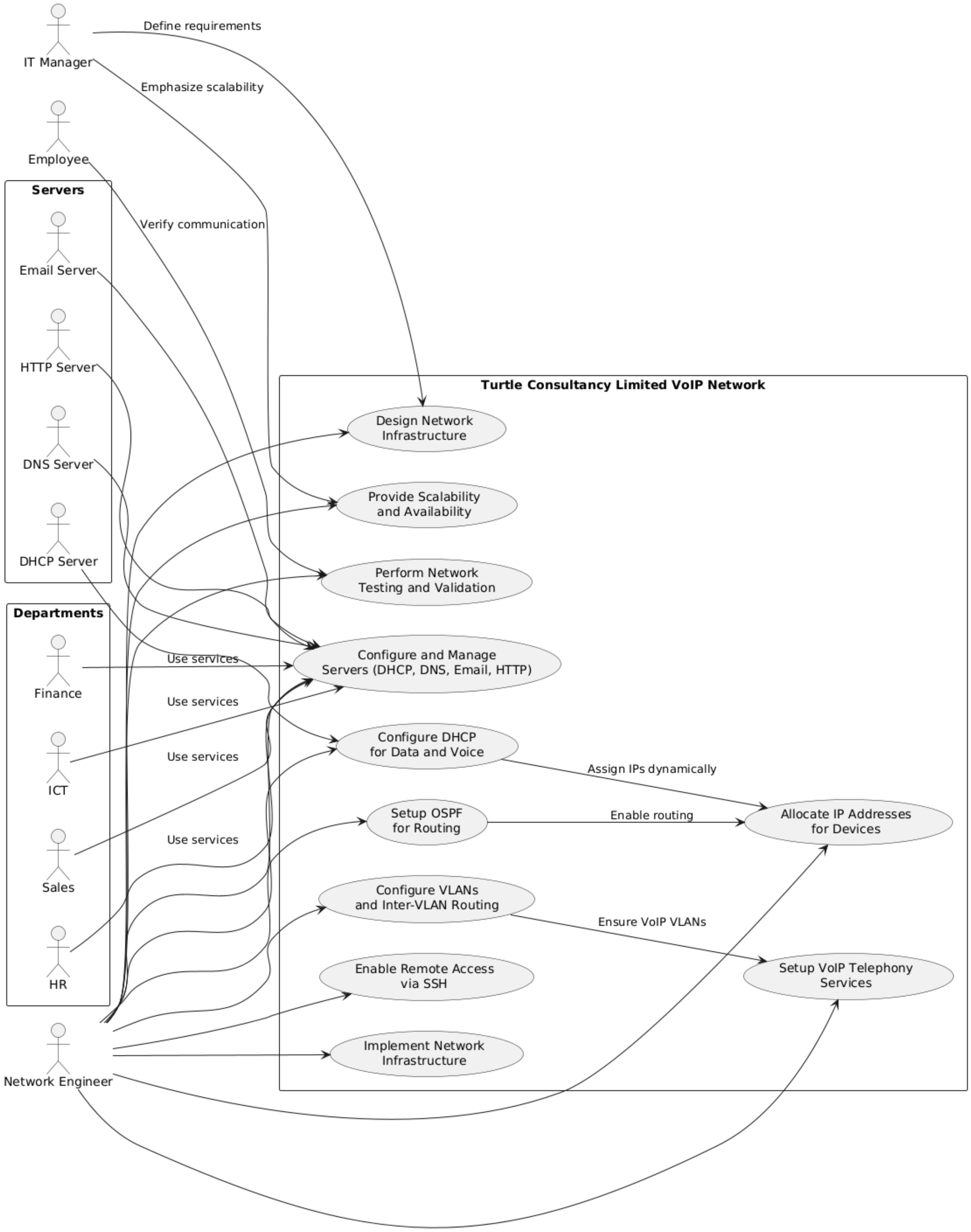

IT Manager
Define requirements
Emphasize scalability
Employee
Verify communication
Servers
Email Server
HTTP Server
DNS Server
DHCP Server
Departments
Finance
ICT
Sales
HR
Use services
Use services
Use services
Use services
Network Engineer
Turtle Consultancy Limited VoIP Network
Design Network Infrastructure
Provide Scalability and Availability
Perform Network Testing and Validation
Configure and Manage Servers (DHCP, DNS, Email, HTTP)
Configure DHCP for Data and Voice
Assign IPs dynamically
Setup OSPF for Routing
Enable routing
Allocate IP Addresses for Devices
Configure VLANs and Inter-VLAN Routing
Ensure VoIP VLANs
Setup VoIP Telephony Services
Enable Remote Access via SSH
Implement Network Infrastructure

Figure 2.2: UI diagram backend part

Chapter 3

Implementation and Results

This chapter explains how VoIP networks are deployed in real-world scenarios. It covers the essential hardware and software components, such as IP phones, session initiation protocol (SIP) servers, and network configurations. Additionally, the process of setting up codecs for compression and quality assurance techniques to minimize latency and packet loss is detailed.

3.1 Implementation

The project's network infrastructure was implemented using Cisco Packet Tracer, a simulation tool for network design and testing. Key components utilized included routers, switches, and IP phones. Configurations included:

- Dynamic Host Configuration Protocol (DHCP): Enabled automated IP address allocation for efficient network management.
- Secure Shell (SSH): Implemented to enhance network security by providing encrypted remote access for configuration and monitoring. The setup ensured optimal functionality and security for simulated real-world network scenarios.

3.2 Performance Analysis

Performance analysis focused on validating critical network features and testing overall efficiency within the simulated environment:

- VLAN Segmentation: Verified effective traffic separation and secure data communication across Virtual LANs.
- Inter-VLAN Routing: Ensured proper connectivity between VLANs using Layer 3 routing techniques.
- VoIP Call Quality: Simulated and assessed the quality of Voice over IP calls for clarity and latency.

Key parameters such as latency and reliability were monitored, keeping in mind the inherent constraints of simulation in Packet Tracer, such as limited real-world variability.

3.3 Results and Discussion

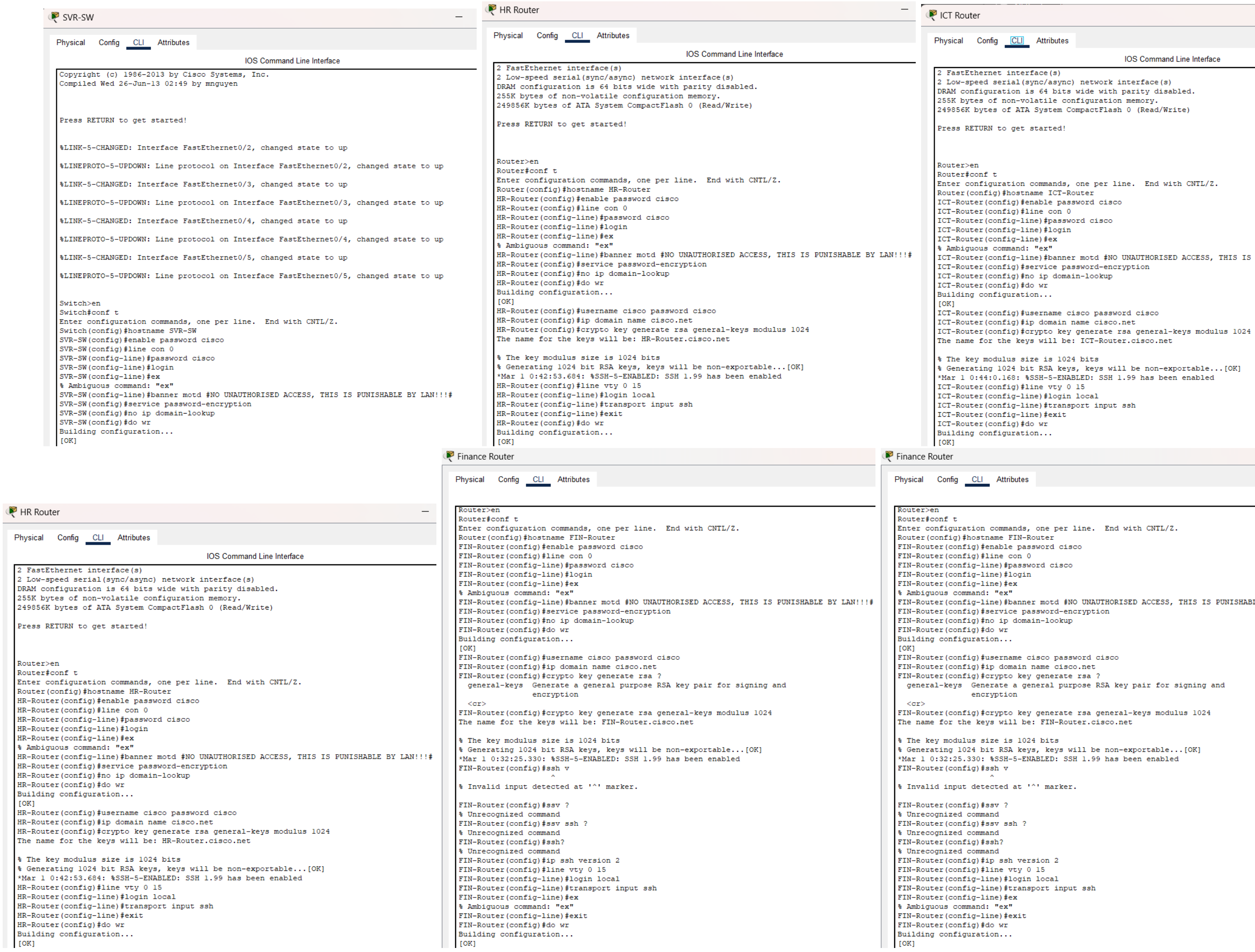
The simulation demonstrated successful deployment of a secure and segmented network infrastructure. Major findings include:

• VLAN Segmentation: Achieved efficient data isolation and improved security between network segments.

• Inter-VLAN Connectivity: Enabled seamless communication across different VLANs, proving routing configuration effectiveness.

• VoIP Viability: The network supported high-quality VoIP calls within the simulated conditions, affirming the feasibility of such setups for small to medium-sized networks.

While Packet Tracer's constraints limit real-world parameter precision, the outcomes indicate robust design principles and configurations, highlighting their adaptability for real implementation.



```
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen



Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%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


Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SVR-SW
SVR-SW(config)#enable password cisco
SVR-SW(config)#line con 0
SVR-SW(config-line)#password cisco
SVR-SW(config-line)#login
SVR-SW(config-line)#ex
% Ambiguous command: "ex"
SVR-SW(config-line)#banner motd #NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!#
SVR-SW(config)#service password-encryption
SVR-SW(config)#no ip domain-lookup
SVR-SW(config)#do wr
Building configuration...
[OK]
```

```
2 FastEthernet interface(s)
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!



Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname HR-Router
HR-Router(config)#enable password cisco
HR-Router(config)#line con 0
HR-Router(config-line)#password cisco
HR-Router(config-line)#login
HR-Router(config-line)#ex
% Ambiguous command: "ex"
HR-Router(config-line)#banner motd #NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!#
HR-Router(config)#service password-encryption
HR-Router(config)#no ip domain-lookup
HR-Router(config)#do wr
Building configuration...
[OK]
HR-Router(config)#username cisco password cisco
HR-Router(config)#ip domain name cisco.net
HR-Router(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: HR-Router.cisco.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:42:53.684: %SSH-5-ENABLED: SSH 1.99 has been enabled
HR-Router(config)#line vty 0 15
HR-Router(config-line)#login local
HR-Router(config-line)#transport input ssh
HR-Router(config-line)#exit
HR-Router(config)#do wr
Building configuration...
[OK]
```

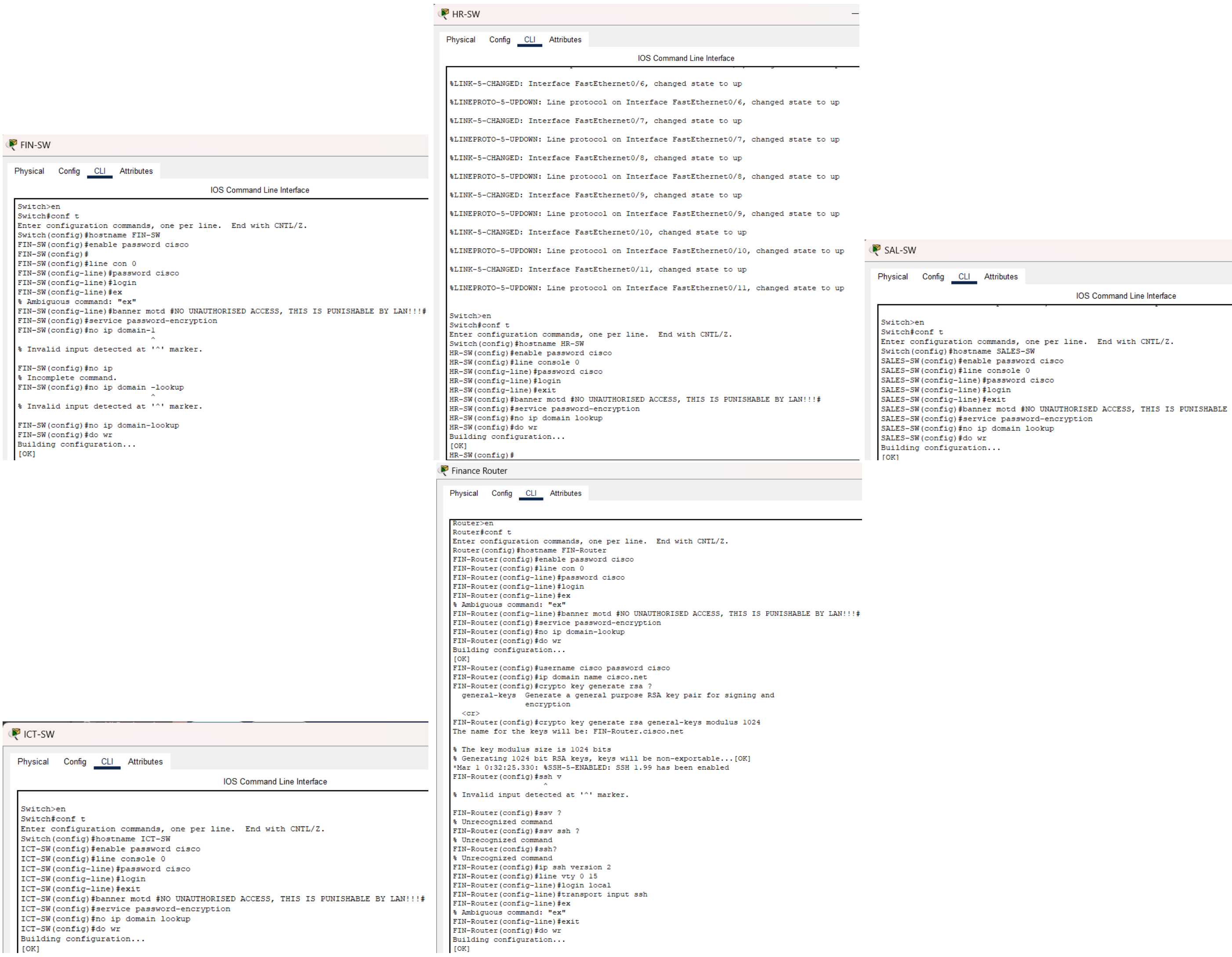
```
2 FastEthernet interface(s)
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!



Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname ICT-Router
ICT-Router(config)#enable password cisco
ICT-Router(config)#line con 0
ICT-Router(config-line)#password cisco
ICT-Router(config-line)#login
ICT-Router(config-line)#ex
% Ambiguous command: "ex"
ICT-Router(config-line)#banner motd #NO UNAUTHORISED ACCESS, THIS IS
ICT-Router(config)#service password-encryption
ICT-Router(config)#no ip domain-lookup
ICT-Router(config)#do wr
Building configuration...
[OK]
ICT-Router(config)#username cisco password cisco
ICT-Router(config)#ip domain name cisco.net
ICT-Router(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: ICT-Router.cisco.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:44:0.168: %SSH-5-ENABLED: SSH 1.99 has been enabled
ICT-Router(config)#line vty 0 15
ICT-Router(config-line)#login local
ICT-Router(config-line)#transport input ssh
ICT-Router(config-line)#exit
ICT-Router(config)#do wr
Building configuration...
[OK]
```

```
2 FastEthernet interface(s)
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!



Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname HR-Router
HR-Router(config)#enable password cisco
HR-Router(config)#line con 0
HR-Router(config-line)#password cisco
HR-Router(config-line)#login
HR-Router(config-line)#ex
% Ambiguous command: "ex"
HR-Router(config-line)#banner motd #NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!#
HR-Router(config)#service password-encryption
HR-Router(config)#no ip domain-lookup
HR-Router(config)#do wr
Building configuration...
[OK]
HR-Router(config)#username cisco password cisco
HR-Router(config)#ip domain name cisco.net
HR-Router(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: HR-Router.cisco.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:42:53.684: %SSH-5-ENABLED: SSH 1.99 has been enabled
HR-Router(config)#line vty 0 15
HR-Router(config-line)#login local
HR-Router(config-line)#transport input ssh
HR-Router(config-line)#exit
HR-Router(config)#do wr
Building configuration...
[OK]
```

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname FIN-Router
FIN-Router(config)#enable password cisco
FIN-Router(config)#line con 0
FIN-Router(config-line)#password cisco
FIN-Router(config-line)#login
FIN-Router(config-line)#ex
% Ambiguous command: "ex"
FIN-Router(config-line)#banner motd #NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!#
FIN-Router(config)#service password-encryption
FIN-Router(config)#no ip domain-lookup
FIN-Router(config)#do wr
Building configuration...
[OK]
FIN-Router(config)#username cisco password cisco
FIN-Router(config)#ip domain name cisco.net
FIN-Router(config)#crypto key generate rsa ?
  general-keys  Generate a general purpose RSA key pair for signing and
                encryption
  <cr>
FIN-Router(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: FIN-Router.cisco.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:32:25.330: %SSH-5-ENABLED: SSH 1.99 has been enabled
FIN-Router(config)#ssh v
                      ^
% Invalid input detected at '^' marker.

FIN-Router(config)#ssv ?
% Unrecognized command
FIN-Router(config)#ssv ssh ?
% Unrecognized command
FIN-Router(config)#ssh?
% Unrecognized command
FIN-Router(config)#ip ssh version 2
FIN-Router(config)#line vty 0 15
FIN-Router(config-line)#login local
FIN-Router(config-line)#transport input ssh
FIN-Router(config-line)#ex
% Ambiguous command: "ex"
FIN-Router(config-line)#exit
FIN-Router(config)#do wr
Building configuration...
[OK]
```

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname FIN-Router
FIN-Router(config)#enable password cisco
FIN-Router(config)#line con 0
FIN-Router(config-line)#password cisco
FIN-Router(config-line)#login
FIN-Router(config-line)#ex
% Ambiguous command: "ex"
FIN-Router(config-line)#banner motd #NO UNAUTHORISED ACCESS, THIS IS PUNISHABL
FIN-Router(config)#service password-encryption
FIN-Router(config)#no ip domain-lookup
FIN-Router(config)#do wr
Building configuration...
[OK]
FIN-Router(config)#username cisco password cisco
FIN-Router(config)#ip domain name cisco.net
FIN-Router(config)#crypto key generate rsa ?
  general-keys  Generate a general purpose RSA key pair for signing and
                encryption
  <cr>
FIN-Router(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: FIN-Router.cisco.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:32:25.330: %SSH-5-ENABLED: SSH 1.99 has been enabled
FIN-Router(config)#ssh v
                      ^
% Invalid input detected at '^' marker.

FIN-Router(config)#ssv ?
% Unrecognized command
FIN-Router(config)#ssv ssh ?
% Unrecognized command
FIN-Router(config)#ssh?
% Unrecognized command
FIN-Router(config)#ip ssh version 2
FIN-Router(config)#line vty 0 15
FIN-Router(config-line)#login local
FIN-Router(config-line)#transport input ssh
FIN-Router(config-line)#ex
% Ambiguous command: "ex"
FIN-Router(config-line)#exit
FIN-Router(config)#do wr
Building configuration...
[OK]
```

Figure 3.1: Serial 2 basic router config



```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname FIN-SW
FIN-SW(config)#enable password cisco
FIN-SW(config)#
FIN-SW(config)#line con 0
FIN-SW(config-line)#password cisco
FIN-SW(config-line)#login
FIN-SW(config-line)#ex
% Ambiguous command: "ex"
FIN-SW(config-line)#banner motd #NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!#
FIN-SW(config)#service password-encryption
FIN-SW(config)#no ip domain-l
                           ^
% Invalid input detected at '^' marker.

FIN-SW(config)#no ip
% Incomplete command.
FIN-SW(config)#no ip domain -lookup
                           ^
% Invalid input detected at '^' marker.

FIN-SW(config)#no ip domain-lookup
FIN-SW(config)#do wr
Building configuration...
[OK]
```

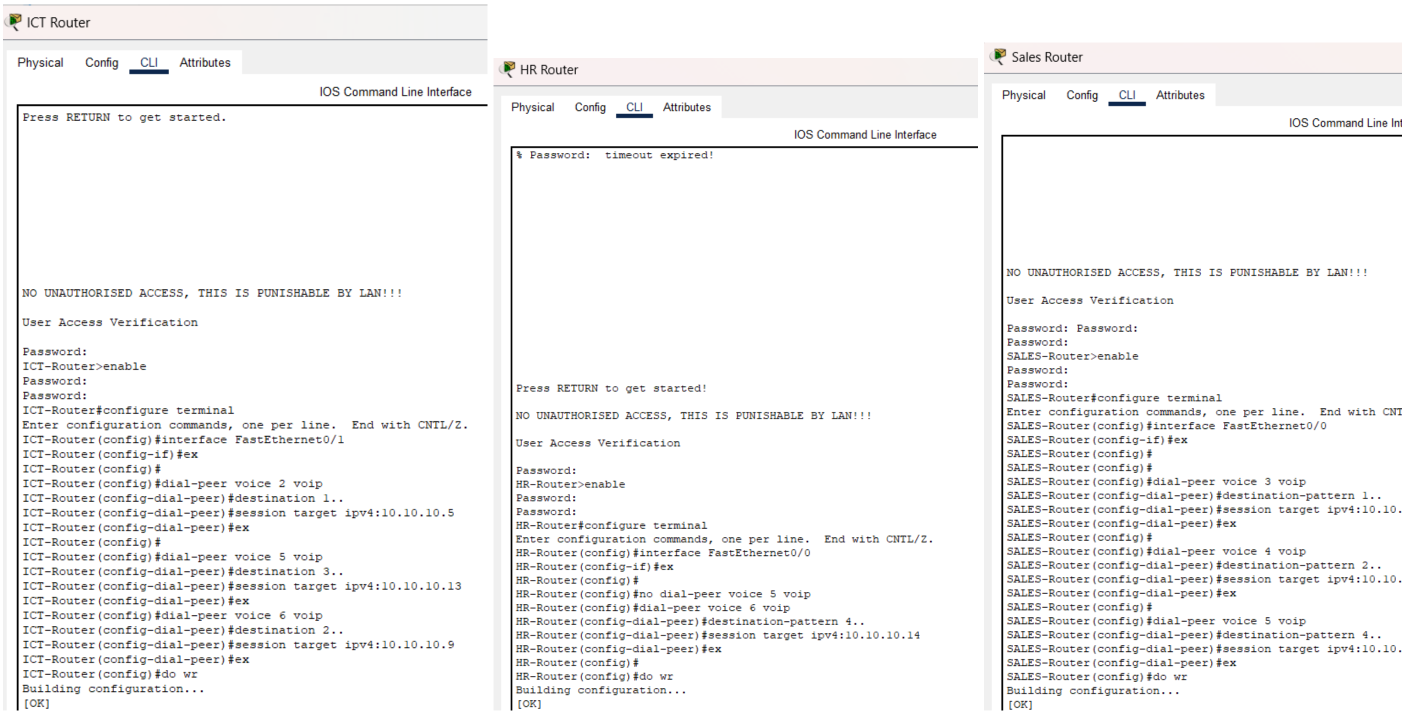
```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname ICT-SW
ICT-SW(config)#enable password cisco
ICT-SW(config)#line console 0
ICT-SW(config-line)#password cisco
ICT-SW(config-line)#login
ICT-SW(config-line)#exit
ICT-SW(config)#banner motd #NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!#
ICT-SW(config)#service password-encryption
ICT-SW(config)#no ip domain lookup
ICT-SW(config)#do wr
Building configuration...
[OK]
```

```
%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 FastEthernet0/7, changed state to up

%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 FastEthernet0/9, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to up


Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname HR-SW
HR-SW(config)#enable password cisco
HR-SW(config)#line console 0
HR-SW(config-line)#password cisco
HR-SW(config-line)#login
HR-SW(config-line)#exit
HR-SW(config)#banner motd #NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!#
HR-SW(config)#service password-encryption
HR-SW(config)#no ip domain lookup
HR-SW(config)#do wr
Building configuration...
[OK]
HR-SW(config)#
```

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname FIN-Router
FIN-Router(config)#enable password cisco
FIN-Router(config)#line con 0
FIN-Router(config-line)#password cisco
FIN-Router(config-line)#login
FIN-Router(config-line)#ex
% Ambiguous command: "ex"
FIN-Router(config-line)#banner motd #NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!#
FIN-Router(config)#service password-encryption
FIN-Router(config)#no ip domain-lookup
FIN-Router(config)#do wr
Building configuration...
[OK]
FIN-Router(config)#username cisco password cisco
FIN-Router(config)#ip domain name cisco.net
FIN-Router(config)#crypto key generate rsa ?
  general-keys  Generate a general purpose RSA key pair for signing and
                encryption
  <cr>
FIN-Router(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: FIN-Router.cisco.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:32:25.330: %SSH-5-ENABLED: SSH 1.99 has been enabled
FIN-Router(config)#ssh v
                    ^
% Invalid input detected at '^' marker.

FIN-Router(config)#ssv ?
% Unrecognized command
FIN-Router(config)#ssv ssh ?
% Unrecognized command
FIN-Router(config)#ssh?
% Unrecognized command
FIN-Router(config)#ip ssh version 2
FIN-Router(config)#line vty 0 15
FIN-Router(config-line)#login local
FIN-Router(config-line)#transport input ssh
FIN-Router(config-line)#ex
% Ambiguous command: "ex"
FIN-Router(config-line)#exit
FIN-Router(config)#do wr
Building configuration...
[OK]
```

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SALES-SW
SALES-SW(config)#enable password cisco
SALES-SW(config)#line console 0
SALES-SW(config-line)#password cisco
SALES-SW(config-line)#login
SALES-SW(config-line)#exit
SALES-SW(config)#banner motd #NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE
SALES-SW(config)#service password-encryption
SALES-SW(config)#no ip domain lookup
SALES-SW(config)#do wr
Building configuration...
[OK]
```

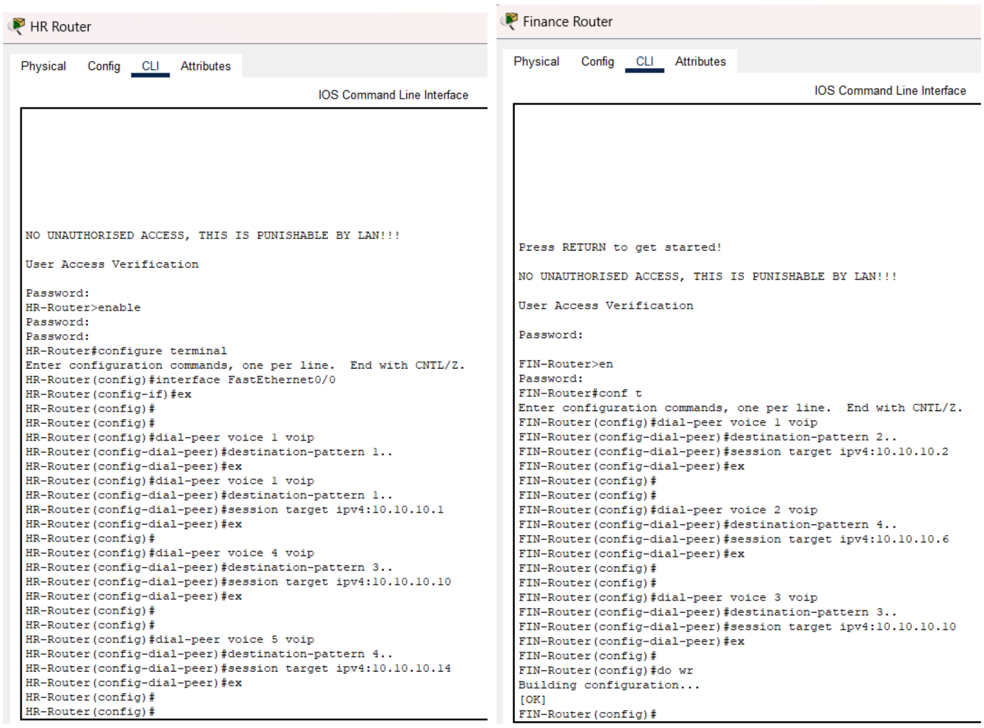
Figure 3.2: Serial 1 switch first part



```
Press RETURN to get started.









NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!

User Access Verification

Password:
ICT-Router>enable
Password:
Password:
ICT-Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ICT-Router(config)#interface FastEthernet0/1
ICT-Router(config-if)#ex
ICT-Router(config)#
ICT-Router(config)#dial-peer voice 2 voip
ICT-Router(config-dial-peer)#destination 1..
ICT-Router(config-dial-peer)#session target ipv4:10.10.10.5
ICT-Router(config-dial-peer)#ex
ICT-Router(config)#
ICT-Router(config)#dial-peer voice 5 voip
ICT-Router(config-dial-peer)#destination 3..
ICT-Router(config-dial-peer)#session target ipv4:10.10.10.13
ICT-Router(config-dial-peer)#ex
ICT-Router(config)#dial-peer voice 6 voip
ICT-Router(config-dial-peer)#destination 2..
ICT-Router(config-dial-peer)#session target ipv4:10.10.10.9
ICT-Router(config-dial-peer)#ex
ICT-Router(config)#do wr
Building configuration...
[OK]
```

```
% Password:  timeout expired!













Press RETURN to get started!

NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!

User Access Verification

Password:
HR-Router>enable
Password:
Password:
HR-Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HR-Router(config)#interface FastEthernet0/0
HR-Router(config-if)#ex
HR-Router(config)#
HR-Router(config)#no dial-peer voice 5 voip
HR-Router(config)#dial-peer voice 6 voip
HR-Router(config-dial-peer)#destination-pattern 4..
HR-Router(config-dial-peer)#session target ipv4:10.10.10.14
HR-Router(config-dial-peer)#ex
HR-Router(config)#
HR-Router(config)#do wr
Building configuration...
[OK]
```

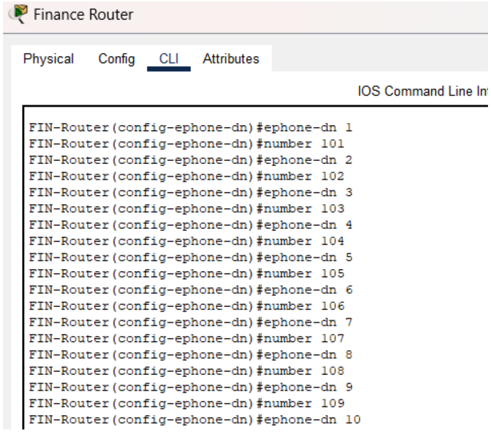
```
NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!

User Access Verification

Password: Password:
Password:
SALES-Router>enable
Password:
Password:
SALES-Router#configure terminal
Enter configuration commands, one per line.  End with CNT
SALES-Router(config)#interface FastEthernet0/0
SALES-Router(config-if)#ex
SALES-Router(config)#
SALES-Router(config)#
SALES-Router(config)#dial-peer voice 3 voip
SALES-Router(config-dial-peer)#destination-pattern 1..
SALES-Router(config-dial-peer)#session target ipv4:10.10.
SALES-Router(config-dial-peer)#ex
SALES-Router(config)#
SALES-Router(config)#dial-peer voice 4 voip
SALES-Router(config-dial-peer)#destination-pattern 2..
SALES-Router(config-dial-peer)#session target ipv4:10.10.
SALES-Router(config-dial-peer)#ex
SALES-Router(config)#
SALES-Router(config)#dial-peer voice 5 voip
SALES-Router(config-dial-peer)#destination-pattern 4..
SALES-Router(config-dial-peer)#session target ipv4:10.10.
SALES-Router(config-dial-peer)#ex
SALES-Router(config)#do wr
Building configuration...
[OK]
```



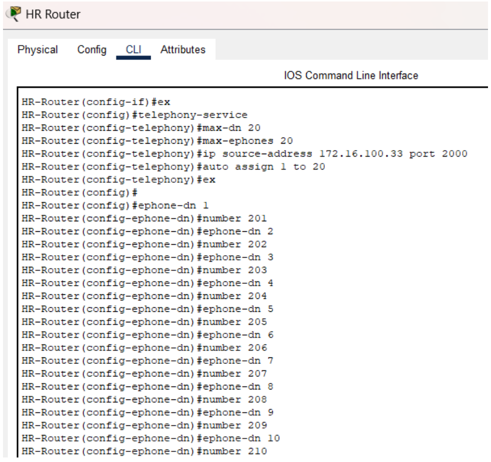
```
NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!

User Access Verification

Password:
HR-Router>enable
Password:
Password:
HR-Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HR-Router(config)#interface FastEthernet0/0
HR-Router(config-if)#ex
HR-Router(config)#
HR-Router(config)#
HR-Router(config)#dial-peer voice 1 voip
HR-Router(config-dial-peer)#destination-pattern 1..
HR-Router(config-dial-peer)#ex
HR-Router(config)#dial-peer voice 1 voip
HR-Router(config-dial-peer)#destination-pattern 1..
HR-Router(config-dial-peer)#session target ipv4:10.10.10.1
HR-Router(config-dial-peer)#ex
HR-Router(config)#
HR-Router(config)#dial-peer voice 4 voip
HR-Router(config-dial-peer)#destination-pattern 3..
HR-Router(config-dial-peer)#session target ipv4:10.10.10.10
HR-Router(config-dial-peer)#ex
HR-Router(config)#
HR-Router(config)#
HR-Router(config)#dial-peer voice 5 voip
HR-Router(config-dial-peer)#destination-pattern 4..
HR-Router(config-dial-peer)#session target ipv4:10.10.10.14
HR-Router(config-dial-peer)#ex
HR-Router(config)#
HR-Router(config)#
```

```
Press RETURN to get started!

NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!

User Access Verification

Password:

FIN-Router>en
Password:
FIN-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
FIN-Router(config)#dial-peer voice 1 voip
FIN-Router(config-dial-peer)#destination-pattern 2..
FIN-Router(config-dial-peer)#session target ipv4:10.10.10.2
FIN-Router(config-dial-peer)#ex
FIN-Router(config)#
FIN-Router(config)#
FIN-Router(config)#dial-peer voice 2 voip
FIN-Router(config-dial-peer)#destination-pattern 4..
FIN-Router(config-dial-peer)#session target ipv4:10.10.10.6
FIN-Router(config-dial-peer)#ex
FIN-Router(config)#
FIN-Router(config)#
FIN-Router(config)#dial-peer voice 3 voip
FIN-Router(config-dial-peer)#destination-pattern 3..
FIN-Router(config-dial-peer)#session target ipv4:10.10.10.10
FIN-Router(config-dial-peer)#ex
FIN-Router(config)#
FIN-Router(config)#do wr
Building configuration...
[OK]
FIN-Router(config)#
```

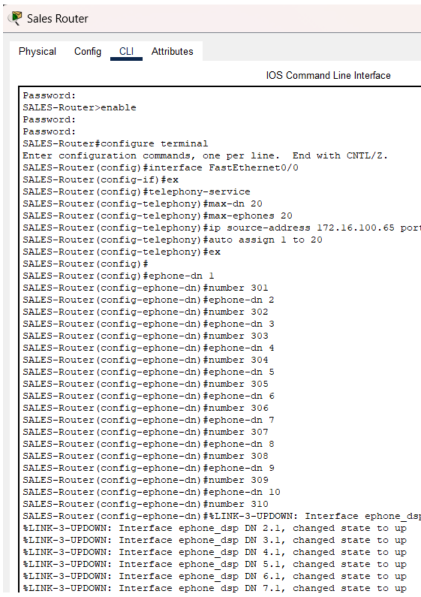
Figure 3.3: Serial 8(Dial peering configuration in all routers)



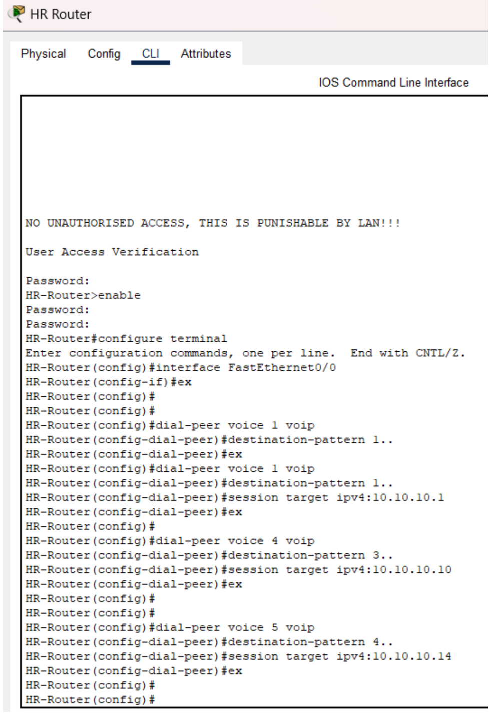
```
FIN-Router(config-ephone-dn)#ephone-dn 1
FIN-Router(config-ephone-dn)#number 101
FIN-Router(config-ephone-dn)#ephone-dn 2
FIN-Router(config-ephone-dn)#number 102
FIN-Router(config-ephone-dn)#ephone-dn 3
FIN-Router(config-ephone-dn)#number 103
FIN-Router(config-ephone-dn)#ephone-dn 4
FIN-Router(config-ephone-dn)#number 104
FIN-Router(config-ephone-dn)#ephone-dn 5
FIN-Router(config-ephone-dn)#number 105
FIN-Router(config-ephone-dn)#ephone-dn 6
FIN-Router(config-ephone-dn)#number 106
FIN-Router(config-ephone-dn)#ephone-dn 7
FIN-Router(config-ephone-dn)#number 107
FIN-Router(config-ephone-dn)#ephone-dn 8
FIN-Router(config-ephone-dn)#number 108
FIN-Router(config-ephone-dn)#ephone-dn 9
FIN-Router(config-ephone-dn)#number 109
FIN-Router(config-ephone-dn)#ephone-dn 10
```



```
HR-Router(config-if)#ex
HR-Router(config)#telephony-service
HR-Router(config-telephony)#max-dn 20
HR-Router(config-telephony)#max-ephones 20
HR-Router(config-telephony)#ip source-address 172.16.100.33 port 2000
HR-Router(config-telephony)#auto assign 1 to 20
HR-Router(config-telephony)#ex
HR-Router(config)#
HR-Router(config)#ephone-dn 1
HR-Router(config-ephone-dn)#number 201
HR-Router(config-ephone-dn)#ephone-dn 2
HR-Router(config-ephone-dn)#number 202
HR-Router(config-ephone-dn)#ephone-dn 3
HR-Router(config-ephone-dn)#number 203
HR-Router(config-ephone-dn)#ephone-dn 4
HR-Router(config-ephone-dn)#number 204
HR-Router(config-ephone-dn)#ephone-dn 5
HR-Router(config-ephone-dn)#number 205
HR-Router(config-ephone-dn)#ephone-dn 6
HR-Router(config-ephone-dn)#number 206
HR-Router(config-ephone-dn)#ephone-dn 7
HR-Router(config-ephone-dn)#number 207
HR-Router(config-ephone-dn)#ephone-dn 8
HR-Router(config-ephone-dn)#number 208
HR-Router(config-ephone-dn)#ephone-dn 9
HR-Router(config-ephone-dn)#number 209
HR-Router(config-ephone-dn)#ephone-dn 10
HR-Router(config-ephone-dn)#number 210
```

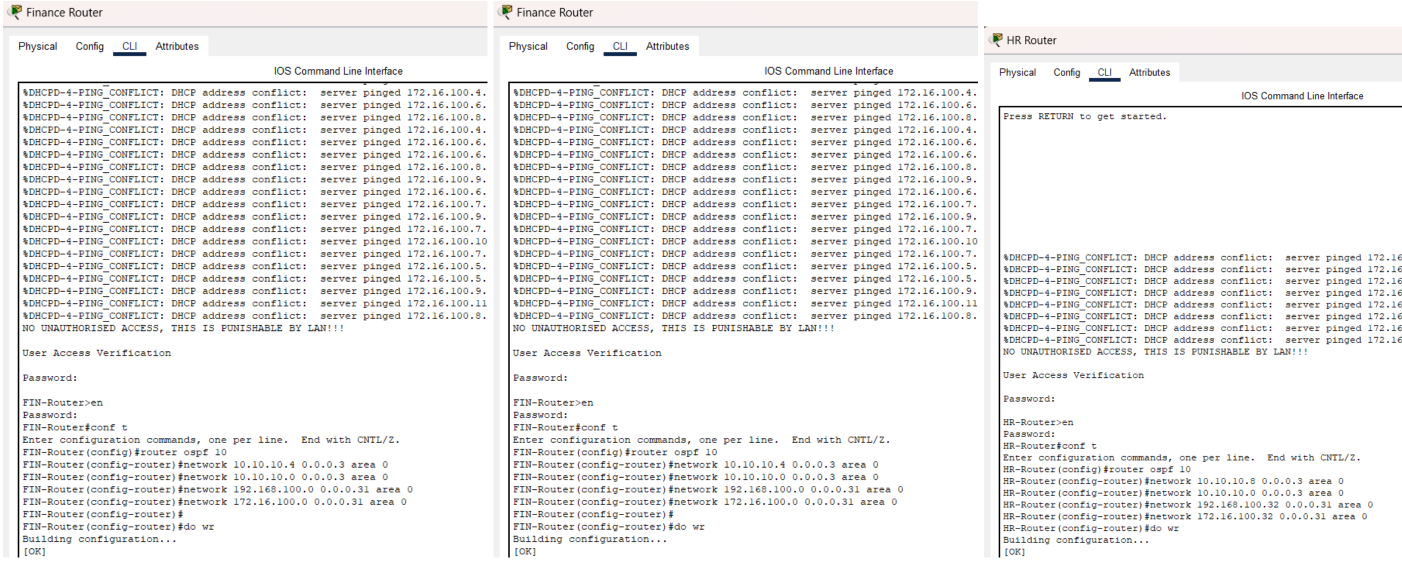


```
Password:
SALES-Router>enable
Password:
Password:
SALES-Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SALES-Router(config)#interface FastEthernet0/0
SALES-Router(config-if)#ex
SALES-Router(config)#telephony-service
SALES-Router(config-telephony)#max-dn 20
SALES-Router(config-telephony)#max-ephones 20
SALES-Router(config-telephony)#ip source-address 172.16.100.65 port
SALES-Router(config-telephony)#auto assign 1 to 20
SALES-Router(config-telephony)#ex
SALES-Router(config)#
SALES-Router(config)#ephone-dn 1
SALES-Router(config-ephone-dn)#number 301
SALES-Router(config-ephone-dn)#ephone-dn 2
SALES-Router(config-ephone-dn)#number 302
SALES-Router(config-ephone-dn)#ephone-dn 3
SALES-Router(config-ephone-dn)#number 303
SALES-Router(config-ephone-dn)#ephone-dn 4
SALES-Router(config-ephone-dn)#number 304
SALES-Router(config-ephone-dn)#ephone-dn 5
SALES-Router(config-ephone-dn)#number 305
SALES-Router(config-ephone-dn)#ephone-dn 6
SALES-Router(config-ephone-dn)#number 306
SALES-Router(config-ephone-dn)#ephone-dn 7
SALES-Router(config-ephone-dn)#number 307
SALES-Router(config-ephone-dn)#ephone-dn 8
SALES-Router(config-ephone-dn)#number 308
SALES-Router(config-ephone-dn)#ephone-dn 9
SALES-Router(config-ephone-dn)#number 309
SALES-Router(config-ephone-dn)#ephone-dn 10
SALES-Router(config-ephone-dn)#number 310
SALES-Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp
%LINK-3-UPDOWN: Interface ephone_dsp DN 2.1, changed state to up
%LINK-3-UPDOWN: Interface ephone_dsp DN 3.1, changed state to up
%LINK-3-UPDOWN: Interface ephone_dsp DN 4.1, changed state to up
%LINK-3-UPDOWN: Interface ephone_dsp DN 5.1, changed state to up
%LINK-3-UPDOWN: Interface ephone_dsp DN 6.1, changed state to up
%LINK-3-UPDOWN: Interface ephone_dsp DN 7.1, changed state to up
```



```
NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!

User Access Verification

Password:
HR-Router>enable
Password:
Password:
HR-Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HR-Router(config)#interface FastEthernet0/0
HR-Router(config-if)#ex
HR-Router(config)#
HR-Router(config)#
HR-Router(config)#dial-peer voice 1 voip
HR-Router(config-dial-peer)#destination-pattern 1..
HR-Router(config-dial-peer)#ex
HR-Router(config)#dial-peer voice 1 voip
HR-Router(config-dial-peer)#destination-pattern 1..
HR-Router(config-dial-peer)#session target ipv4:10.10.10.1
HR-Router(config-dial-peer)#ex
HR-Router(config)#
HR-Router(config)#dial-peer voice 4 voip
HR-Router(config-dial-peer)#destination-pattern 3..
HR-Router(config-dial-peer)#session target ipv4:10.10.10.10
HR-Router(config-dial-peer)#ex
HR-Router(config)#
HR-Router(config)#
HR-Router(config)#dial-peer voice 5 voip
HR-Router(config-dial-peer)#destination-pattern 4..
HR-Router(config-dial-peer)#session target ipv4:10.10.10.14
HR-Router(config-dial-peer)#ex
HR-Router(config)#
HR-Router(config)#
```

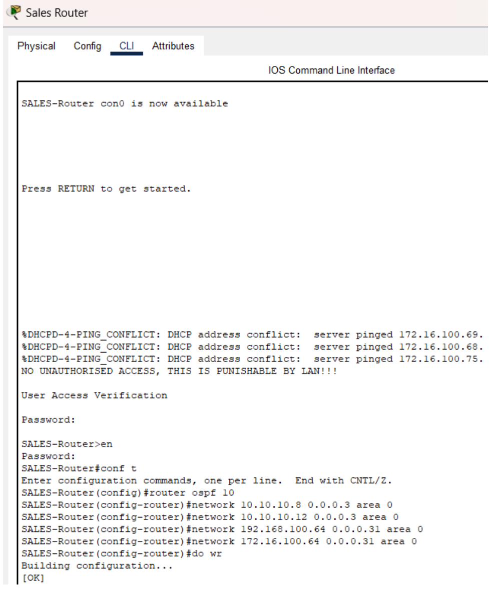
Figure 3.4: Serial 7(Configure VoIP configuration in all routers)



```
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.4.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.6.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.8.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.4.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.6.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.6.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.8.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.9.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.6.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.7.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.9.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.7.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.10
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.7.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.5.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.5.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.9.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.11
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.8.
NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!

User Access Verification

Password:

FIN-Router>en
Password:
FIN-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
FIN-Router(config)#router ospf 10
FIN-Router(config-router)#network 10.10.10.4 0.0.0.3 area 0
FIN-Router(config-router)#network 10.10.10.0 0.0.0.3 area 0
FIN-Router(config-router)#network 192.168.100.0 0.0.0.31 area 0
FIN-Router(config-router)#network 172.16.100.0 0.0.0.31 area 0
FIN-Router(config-router)#
FIN-Router(config-router)#do wr
Building configuration...
[OK]
```

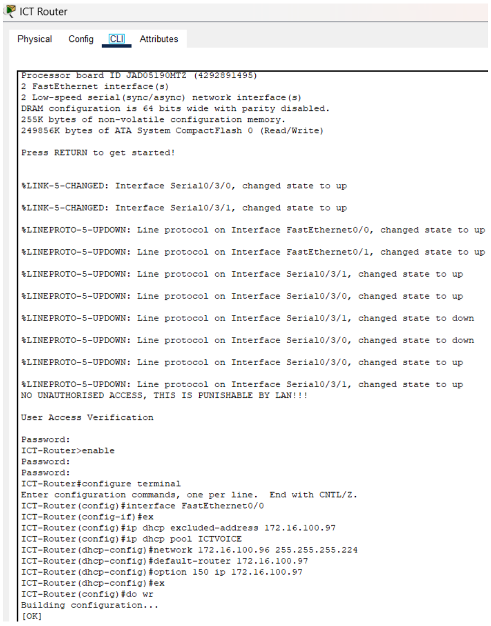
```
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.4.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.6.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.8.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.4.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.6.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.6.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.8.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.9.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.6.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.7.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.9.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.7.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.10
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.7.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.5.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.5.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.9.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.11
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.8.
NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!

User Access Verification

Password:

FIN-Router>en
Password:
FIN-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
FIN-Router(config)#router ospf 10
FIN-Router(config-router)#network 10.10.10.4 0.0.0.3 area 0
FIN-Router(config-router)#network 10.10.10.0 0.0.0.3 area 0
FIN-Router(config-router)#network 192.168.100.0 0.0.0.31 area 0
FIN-Router(config-router)#network 172.16.100.0 0.0.0.31 area 0
FIN-Router(config-router)#
FIN-Router(config-router)#do wr
Building configuration...
[OK]
```

```
Press RETURN to get started.









%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16
NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!

User Access Verification

Password:

HR-Router>en
Password:
HR-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HR-Router(config)#router ospf 10
HR-Router(config-router)#network 10.10.10.8 0.0.0.3 area 0
HR-Router(config-router)#network 10.10.10.0 0.0.0.3 area 0
HR-Router(config-router)#network 192.168.100.32 0.0.0.31 area 0
HR-Router(config-router)#network 172.16.100.32 0.0.0.31 area 0
HR-Router(config-router)#do wr
Building configuration...
[OK]
```

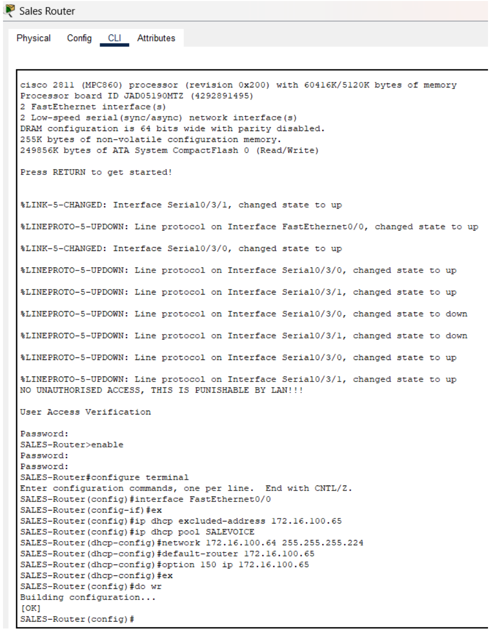


```
SALES-Router con0 is now available




Press RETURN to get started.










%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.69.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.68.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.75.
NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!

User Access Verification

Password:

SALES-Router>en
Password:
SALES-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SALES-Router(config)#router ospf 10
SALES-Router(config-router)#network 10.10.10.8 0.0.0.3 area 0
SALES-Router(config-router)#network 10.10.10.12 0.0.0.3 area 0
SALES-Router(config-router)#network 192.168.100.64 0.0.0.31 area 0
SALES-Router(config-router)#network 172.16.100.64 0.0.0.31 area 0
SALES-Router(config-router)#do wr
Building configuration...
[OK]
```

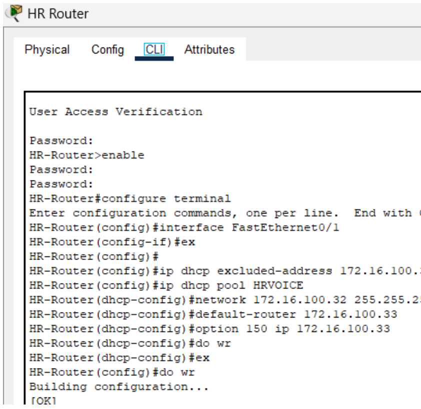
Figure 3.5: Serial 6(OSPF on the routers)



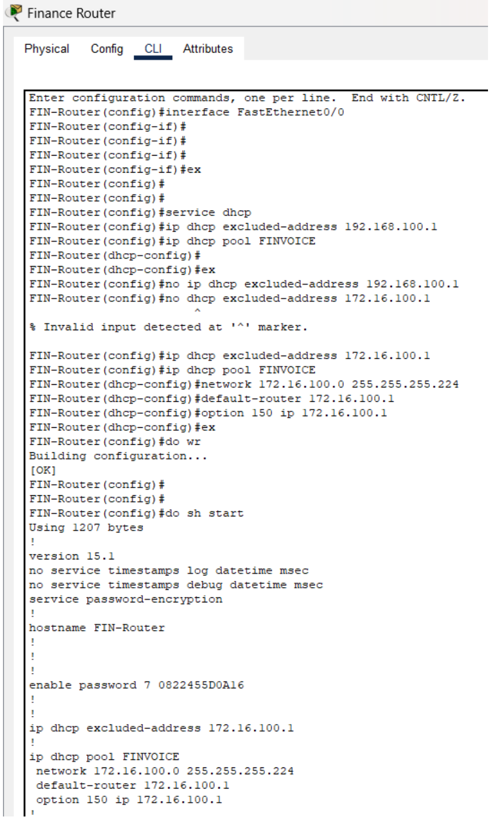
```
Processor board ID JAD05190MTZ (4292891495)
2 FastEthernet interface(s)
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!


%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up

%LINK-5-CHANGED: Interface Serial0/3/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/1, changed state to up
NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!

User Access Verification

Password:
ICT-Router>enable
Password:
Password:
ICT-Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ICT-Router(config)#interface FastEthernet0/0
ICT-Router(config-if)#ex
ICT-Router(config)#ip dhcp excluded-address 172.16.100.97
ICT-Router(config)#ip dhcp pool ICTVOICE
ICT-Router(dhcp-config)#network 172.16.100.96 255.255.255.224
ICT-Router(dhcp-config)#default-router 172.16.100.97
ICT-Router(dhcp-config)#option 150 ip 172.16.100.97
ICT-Router(dhcp-config)#ex
ICT-Router(config)#do wr
Building configuration...
[OK]
```



```
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
2 FastEthernet interface(s)
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!


%LINK-5-CHANGED: Interface Serial0/3/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/1, changed state to up
NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!

User Access Verification

Password:
SALES-Router>enable
Password:
Password:
SALES-Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SALES-Router(config)#interface FastEthernet0/0
SALES-Router(config-if)#ex
SALES-Router(config)#ip dhcp excluded-address 172.16.100.65
SALES-Router(config)#ip dhcp pool SALEVOICE
SALES-Router(dhcp-config)#network 172.16.100.64 255.255.255.224
SALES-Router(dhcp-config)#default-router 172.16.100.65
SALES-Router(dhcp-config)#option 150 ip 172.16.100.65
SALES-Router(dhcp-config)#ex
SALES-Router(config)#do wr
Building configuration...
[OK]
SALES-Router(config)#
```

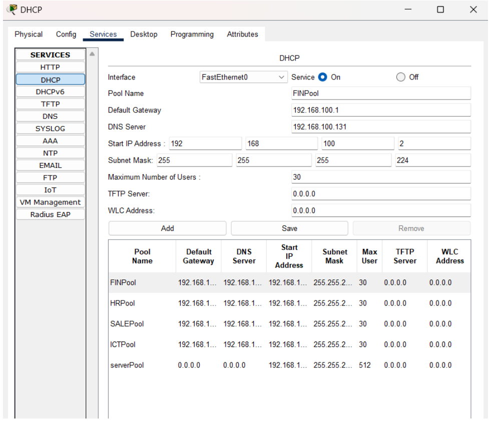


```
User Access Verification

Password:
HR-Router>enable
Password:
Password:
HR-Router#configure terminal
Enter configuration commands, one per line.  End with
HR-Router(config)#interface FastEthernet0/1
HR-Router(config-if)#ex
HR-Router(config)#
HR-Router(config)#ip dhcp excluded-address 172.16.100.
HR-Router(config)#ip dhcp pool HRVOICE
HR-Router(dhcp-config)#network 172.16.100.32 255.255.2
HR-Router(dhcp-config)#default-router 172.16.100.33
HR-Router(dhcp-config)#option 150 ip 172.16.100.33
HR-Router(dhcp-config)#do wr
HR-Router(dhcp-config)#ex
HR-Router(config)#do wr
Building configuration...
[OK]
```



```
Enter configuration commands, one per line.  End with CNTL/Z.
FIN-Router(config)#interface FastEthernet0/0
FIN-Router(config-if)#
FIN-Router(config-if)#
FIN-Router(config-if)#
FIN-Router(config-if)#ex
FIN-Router(config)#
FIN-Router(config)#
FIN-Router(config)#service dhcp
FIN-Router(config)#ip dhcp excluded-address 192.168.100.1
FIN-Router(config)#ip dhcp pool FINVOICE
FIN-Router(dhcp-config)#
FIN-Router(dhcp-config)#ex
FIN-Router(config)#no ip dhcp excluded-address 192.168.100.1
FIN-Router(config)#no dhcp excluded-address 172.16.100.1
                        ^
% Invalid input detected at '^' marker.

FIN-Router(config)#ip dhcp excluded-address 172.16.100.1
FIN-Router(config)#ip dhcp pool FINVOICE
FIN-Router(dhcp-config)#network 172.16.100.0 255.255.255.224
FIN-Router(dhcp-config)#default-router 172.16.100.1
FIN-Router(dhcp-config)#option 150 ip 172.16.100.1
FIN-Router(dhcp-config)#ex
FIN-Router(config)#do wr
Building configuration...
[OK]
FIN-Router(config)#
FIN-Router(config)#
FIN-Router(config)#do sh start
Using 1207 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname FIN-Router
!
!
!
enable password 7 0822455D0A16
!
!
ip dhcp excluded-address 172.16.100.1
!
ip dhcp pool FINVOICE
 network 172.16.100.0 255.255.255.224
 default-router 172.16.100.1
 option 150 ip 172.16.100.1
!
```

Figure 3.6: Serial 4(Configure DHCP for Voice)



DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name FINPool

Default Gateway 192.168.100.1

DNS Server 192.168.100.131

Start IP Address : 192 168 100 2

Subnet Mask: 255 255 255 224

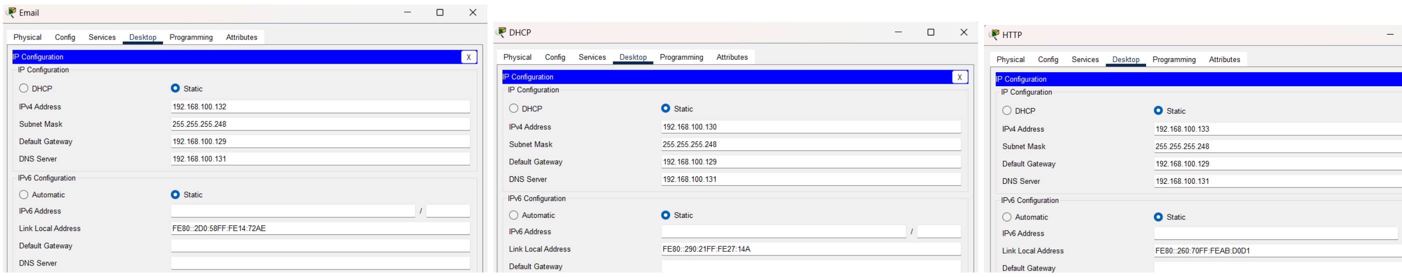
Maximum Number of Users : 30

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
FINPool	192.168.1...	192.168.1...	192.168.1...	255.255.2...	30	0.0.0.0	0.0.0.0
HRPool	192.168.1...	192.168.1...	192.168.1...	255.255.2...	30	0.0.0.0	0.0.0.0
SALEPool	192.168.1...	192.168.1...	192.168.1...	255.255.2...	30	0.0.0.0	0.0.0.0
ICTPool	192.168.1...	192.168.1...	192.168.1...	255.255.2...	30	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.1...	255.255.2...	512	0.0.0.0	0.0.0.0

Figure 3.7: Serial 3.2(DHCP server device configuration)



IP Configuration

○ DHCP ● Static

IPv4 Address 192.168.100.132

Subnet Mask 255.255.255.248

Default Gateway 192.168.100.129

DNS Server 192.168.100.131

IPv6 Configuration

○ Automatic ● Static

IPv6 Address /

Link Local Address FE80::2D0:58FF:FE14:72AE

Default Gateway

DNS Server

IP Configuration

○ DHCP ● Static

IPv4 Address 192.168.100.130

Subnet Mask 255.255.255.248

Default Gateway 192.168.100.129

DNS Server 192.168.100.131

IPv6 Configuration

○ Automatic ● Static

IPv6 Address /

Link Local Address FE80::290:21FF:FE27:14A

Default Gateway

IP Configuration

○ DHCP ● Static

IPv4 Address 192.168.100.133

Subnet Mask 255.255.255.248

Default Gateway 192.168.100.129

DNS Server 192.168.100.131

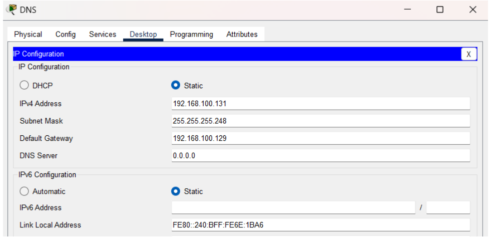
IPv6 Configuration

○ Automatic ● Static

IPv6 Address

Link Local Address FE80::260:70FF:FEAB:D0D1

Default Gateway



IP Configuration

○ DHCP ● Static

IPv4 Address 192.168.100.131

Subnet Mask 255.255.255.248

Default Gateway 192.168.100.129

DNS Server 0.0.0.0

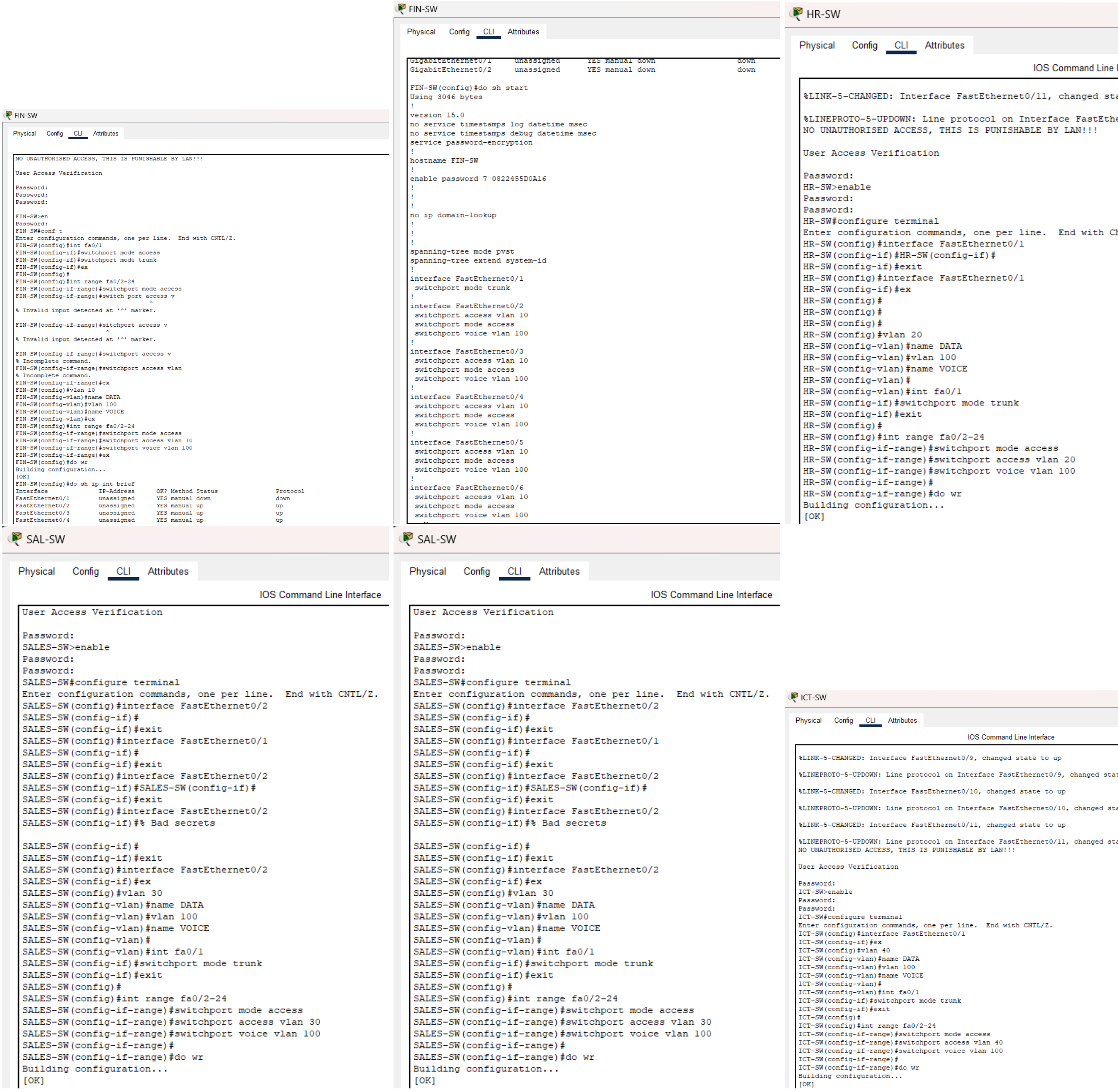
IPv6 Configuration

○ Automatic ● Static

IPv6 Address /

Link Local Address FE80::240:BFF:FE6E:1BA6

Figure 3.8: Serial 3.1(Static ip address to server room device)



```
NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!

User Access Verification

Password:
Password:
Password:

FIN-SW>en
Password:
FIN-SW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
FIN-SW(config)#int fa0/1
FIN-SW(config-if)#switchport mode access
FIN-SW(config-if)#switchport mode trunk
FIN-SW(config-if)#ex
FIN-SW(config)#
FIN-SW(config)#int range fa0/2-24
FIN-SW(config-if-range)#switchport mode access
FIN-SW(config-if-range)#switch port access v
                                    ^
% Invalid input detected at '^' marker.

FIN-SW(config-if-range)#sitchport access v
                         ^
% Invalid input detected at '^' marker.

FIN-SW(config-if-range)#switchport access v
% Incomplete command.
FIN-SW(config-if-range)#switchport access vlan
% Incomplete command.
FIN-SW(config-if-range)#ex
FIN-SW(config)#vlan 10
FIN-SW(config-vlan)#name DATA
FIN-SW(config-vlan)#vlan 100
FIN-SW(config-vlan)#name VOICE
FIN-SW(config-vlan)#ex
FIN-SW(config)#int range fa0/2-24
FIN-SW(config-if-range)#switchport mode access
FIN-SW(config-if-range)#switchport access vlan 10
FIN-SW(config-if-range)#switchport voice vlan 100
FIN-SW(config-if-range)#ex
FIN-SW(config)#do wr
Building configuration...
[OK]
FIN-SW(config)#do sh ip int brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual down                  down
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual up                    up
FastEthernet0/4        unassigned      YES manual up                    up
```

```
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down

FIN-SW(config)#do sh start
Using 3046 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname FIN-SW
!
enable password 7 0822455D0A16
!
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 100
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 100
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 100
!
interface FastEthernet0/5
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 100
!
interface FastEthernet0/6
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 100
```

```
%LINK-5-CHANGED: Interface FastEthernet0/11, changed sta

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthe
NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!

User Access Verification

Password:
HR-SW>enable
Password:
Password:
HR-SW#configure terminal
Enter configuration commands, one per line.  End with C
HR-SW(config)#interface FastEthernet0/1
HR-SW(config-if)#HR-SW(config-if)#
HR-SW(config-if)#exit
HR-SW(config)#interface FastEthernet0/1
HR-SW(config-if)#ex
HR-SW(config)#
HR-SW(config)#
HR-SW(config)#
HR-SW(config)#vlan 20
HR-SW(config-vlan)#name DATA
HR-SW(config-vlan)#vlan 100
HR-SW(config-vlan)#name VOICE
HR-SW(config-vlan)#
HR-SW(config-vlan)#int fa0/1
HR-SW(config-if)#switchport mode trunk
HR-SW(config-if)#exit
HR-SW(config)#
HR-SW(config)#int range fa0/2-24
HR-SW(config-if-range)#switchport mode access
HR-SW(config-if-range)#switchport access vlan 20
HR-SW(config-if-range)#switchport voice vlan 100
HR-SW(config-if-range)#
HR-SW(config-if-range)#do wr
Building configuration...
[OK]
```

```
User Access Verification

Password:
SALES-SW>enable
Password:
Password:
SALES-SW#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SALES-SW(config)#interface FastEthernet0/2
SALES-SW(config-if)#
SALES-SW(config-if)#exit
SALES-SW(config)#interface FastEthernet0/1
SALES-SW(config-if)#
SALES-SW(config-if)#exit
SALES-SW(config)#interface FastEthernet0/2
SALES-SW(config-if)#SALES-SW(config-if)#
SALES-SW(config-if)#exit
SALES-SW(config)#interface FastEthernet0/2
SALES-SW(config-if)#% Bad secrets

SALES-SW(config-if)#
SALES-SW(config-if)#exit
SALES-SW(config)#interface FastEthernet0/2
SALES-SW(config-if)#ex
SALES-SW(config)#vlan 30
SALES-SW(config-vlan)#name DATA
SALES-SW(config-vlan)#vlan 100
SALES-SW(config-vlan)#name VOICE
SALES-SW(config-vlan)#
SALES-SW(config-vlan)#int fa0/1
SALES-SW(config-if)#switchport mode trunk
SALES-SW(config-if)#exit
SALES-SW(config)#
SALES-SW(config)#int range fa0/2-24
SALES-SW(config-if-range)#switchport mode access
SALES-SW(config-if-range)#switchport access vlan 30
SALES-SW(config-if-range)#switchport voice vlan 100
SALES-SW(config-if-range)#
SALES-SW(config-if-range)#do wr
Building configuration...
[OK]
```

SAL-SW
Physical Config CLI Attributes
IOS Command Line Interface

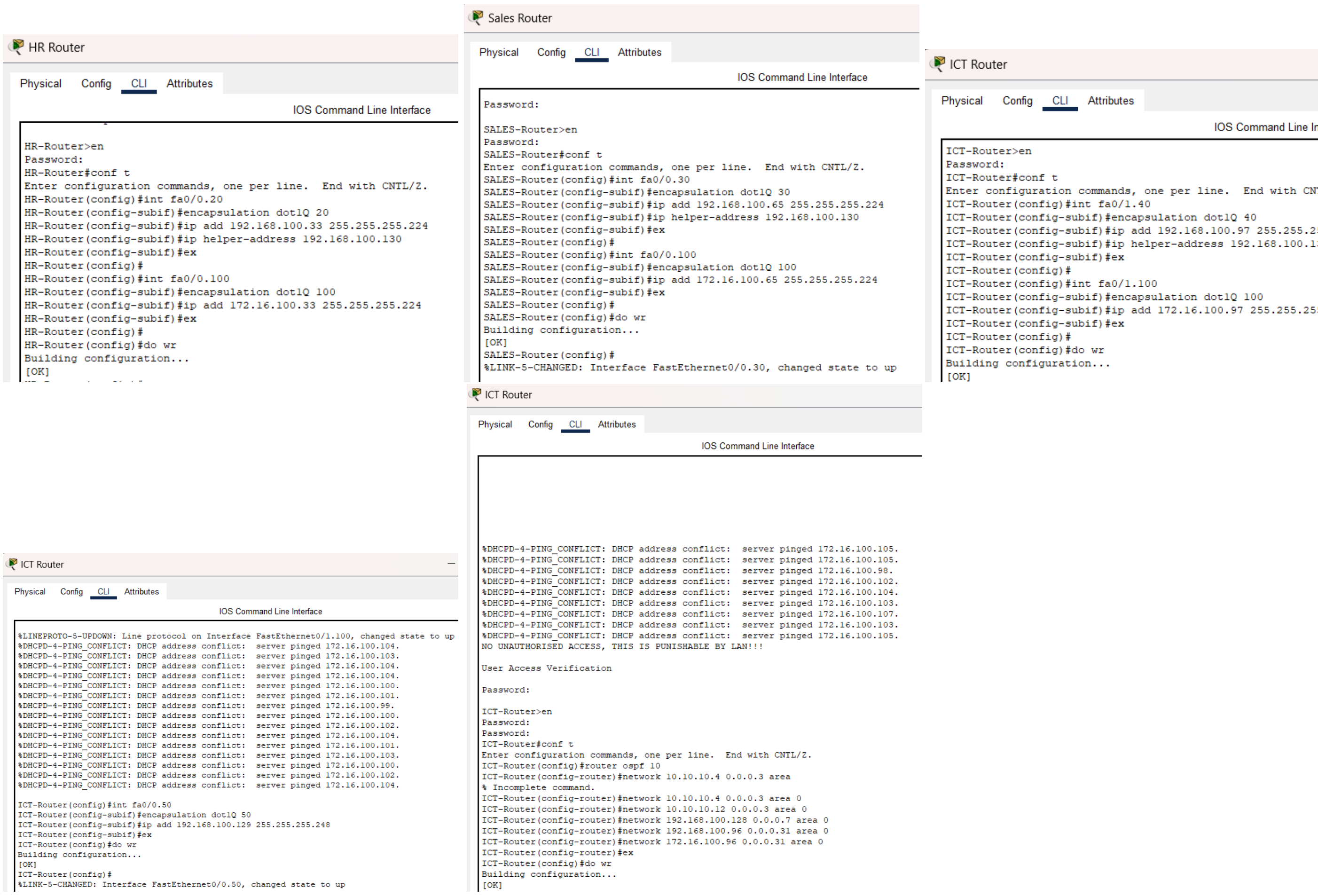
User Access Verification

Password:
SALES-SW>enable
Password:
Password:
SALES-SW#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SALES-SW(config)#interface FastEthernet0/2
SALES-SW(config-if)#
SALES-SW(config-if)#exit
SALES-SW(config)#interface FastEthernet0/1
SALES-SW(config-if)#
SALES-SW(config-if)#exit
SALES-SW(config)#interface FastEthernet0/2
SALES-SW(config-if)#SALES-SW(config-if)#
SALES-SW(config-if)#exit
SALES-SW(config)#interface FastEthernet0/2
SALES-SW(config-if)#% Bad secrets

SALES-SW(config-if)#
SALES-SW(config-if)#exit
SALES-SW(config)#interface FastEthernet0/2
SALES-SW(config-if)#ex
SALES-SW(config)#vlan 30
SALES-SW(config-vlan)#name DATA
SALES-SW(config-vlan)#vlan 100
SALES-SW(config-vlan)#name VOICE
SALES-SW(config-vlan)#
SALES-SW(config-vlan)#int fa0/1
SALES-SW(config-if)#switchport mode trunk
SALES-SW(config-if)#exit
SALES-SW(config)#
SALES-SW(config)#int range fa0/2-24
SALES-SW(config-if-range)#switchport mode access
SALES-SW(config-if-range)#switchport access vlan 30
SALES-SW(config-if-range)#switchport voice vlan 100
SALES-SW(config-if-range)#
SALES-SW(config-if-range)#do wr
Building configuration...
[OK]

```
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9, changed stat

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed sta

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed sta
NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!

User Access Verification

Password:
ICT-SW>enable
Password:
Password:
ICT-SW#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ICT-SW(config)#interface FastEthernet0/1
ICT-SW(config-if)#ex
ICT-SW(config)#vlan 40
ICT-SW(config-vlan)#name DATA
ICT-SW(config-vlan)#vlan 100
ICT-SW(config-vlan)#name VOICE
ICT-SW(config-vlan)#
ICT-SW(config-vlan)#int fa0/1
ICT-SW(config-if)#switchport mode trunk
ICT-SW(config-if)#exit
ICT-SW(config)#
ICT-SW(config)#int range fa0/2-24
ICT-SW(config-if-range)#switchport mode access
ICT-SW(config-if-range)#switchport access vlan 40
ICT-SW(config-if-range)#switchport voice vlan 100
ICT-SW(config-if-range)#
ICT-SW(config-if-range)#do wr
Building configuration...
[OK]
```

Figure 3.9: Serial 3(switch 2nd part)



```
HR-Router>en
Password:
HR-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HR-Router(config)#int fa0/0.20
HR-Router(config-subif)#encapsulation dot1Q 20
HR-Router(config-subif)#ip add 192.168.100.33 255.255.255.224
HR-Router(config-subif)#ip helper-address 192.168.100.130
HR-Router(config-subif)#ex
HR-Router(config)#
HR-Router(config)#int fa0/0.100
HR-Router(config-subif)#encapsulation dot1Q 100
HR-Router(config-subif)#ip add 172.16.100.33 255.255.255.224
HR-Router(config-subif)#ex
HR-Router(config)#
HR-Router(config)#do wr
Building configuration...
[OK]
```

```
Password:

SALES-Router>en
Password:
SALES-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SALES-Router(config)#int fa0/0.30
SALES-Router(config-subif)#encapsulation dot1Q 30
SALES-Router(config-subif)#ip add 192.168.100.65 255.255.255.224
SALES-Router(config-subif)#ip helper-address 192.168.100.130
SALES-Router(config-subif)#ex
SALES-Router(config)#
SALES-Router(config)#int fa0/0.100
SALES-Router(config-subif)#encapsulation dot1Q 100
SALES-Router(config-subif)#ip add 172.16.100.65 255.255.255.224
SALES-Router(config-subif)#ex
SALES-Router(config)#
SALES-Router(config)#do wr
Building configuration...
[OK]
SALES-Router(config)#
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up
```

```
ICT-Router>en
Password:
ICT-Router#conf t
Enter configuration commands, one per line.  End with CN
ICT-Router(config)#int fa0/1.40
ICT-Router(config-subif)#encapsulation dot1Q 40
ICT-Router(config-subif)#ip add 192.168.100.97 255.255.2
ICT-Router(config-subif)#ip helper-address 192.168.100.1
ICT-Router(config-subif)#ex
ICT-Router(config)#
ICT-Router(config)#int fa0/1.100
ICT-Router(config-subif)#encapsulation dot1Q 100
ICT-Router(config-subif)#ip add 172.16.100.97 255.255.25
ICT-Router(config-subif)#ex
ICT-Router(config)#
ICT-Router(config)#do wr
Building configuration...
[OK]
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.100, changed state to up
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.104.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.103.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.104.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.104.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.100.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.101.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.99.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.100.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.102.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.104.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.101.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.103.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.100.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.102.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.104.

ICT-Router(config)#int fa0/0.50
ICT-Router(config-subif)#encapsulation dot1Q 50
ICT-Router(config-subif)#ip add 192.168.100.129 255.255.255.248
ICT-Router(config-subif)#ex
ICT-Router(config)#do wr
Building configuration...
[OK]
ICT-Router(config)#
%LINK-5-CHANGED: Interface FastEthernet0/0.50, changed state to up
```

```
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.105.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.105.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.98.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.102.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.104.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.103.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.107.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.103.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.105.
NO UNAUTHORISED ACCESS, THIS IS PUNISHABLE BY LAN!!!

User Access Verification

Password:

ICT-Router>en
Password:
Password:
ICT-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ICT-Router(config)#router ospf 10
ICT-Router(config-router)#network 10.10.10.4 0.0.0.3 area
% Incomplete command.
ICT-Router(config-router)#network 10.10.10.4 0.0.0.3 area 0
ICT-Router(config-router)#network 10.10.10.12 0.0.0.3 area 0
ICT-Router(config-router)#network 192.168.100.128 0.0.0.7 area 0
ICT-Router(config-router)#network 192.168.100.96 0.0.0.31 area 0
ICT-Router(config-router)#network 172.16.100.96 0.0.0.31 area 0
ICT-Router(config-router)#ex
ICT-Router(config)#do wr
Building configuration...
[OK]
```

Figure 3.10: Serial 5(Inter-VLAN routing on the routers plus ip dhcp helper address)

Chapter 4

Engineering Standards and Mapping

This chapter provides an overview of the major protocols and standards that ensure interoperability and quality in VoIP systems. It discusses SIP, H.323, RTP (Real-Time Protocol), and other key frameworks that define call setup, media transmission, and security in VoIP communications.

4.1 Impact on Society, Environment and Sustainability

4.1.1 Impact on Life

The adoption of VoIP technology significantly enhances communication capabilities, especially in cost-sensitive environments. It provides efficient and affordable solutions for seamless communication, empowering organizations and individuals to remain connected.

4.1.2 Impact on Society & Environment

By reducing reliance on traditional telephony infrastructure, the project lowers operational costs and minimizes the environmental impact associated with the production and maintenance of conventional telephone systems. This shift contributes to a more sustainable communication ecosystem.

4.1.3 Ethical Aspects

The inclusion of Secure Shell (SSH) ensures that the network adheres to ethical standards by maintaining confidentiality and integrity in communication. This fosters trust and mitigates risks of data breaches or unauthorized access.

4.1.4 Sustainability Plan

The network design is scalable, allowing for future expansions without significant reconfigurations or additional resources. This adaptability ensures that the system remains relevant and functional over the long term, promoting sustainability.

4.2 Project Management and Team Work

The project followed a structured timeline, ensuring that milestones were met efficiently. Tasks were systematically distributed among team members based on expertise, promoting collaboration and optimizing resources. Regular meetings facilitated progress tracking and problem resolution, contributing to the project's success.

4.3 Complex Engineering Problem

4.3.1 Mapping of Program Outcome

In this section, provide a mapping of the problem and provided solution with targeted Program Outcomes (PO's).

Table 4.1: Justification of Program Outcomes

PO's	**Justification**
PO1	The hierarchical network design ensures scalability, enabling smooth integration of additional components as needed.
PO2	Configurations reflect advanced problem-solving skills, addressing specific requirements such as secure communication and efficient routing.
PO3	PO3 Simulation in Cisco Packet Tracer validates the system's reliability, ensuring performance consistency under various scenarios.

4.3.2 Complex Problem Solving

In this section, provide a mapping with problem solving categories. For each mapping add subsections to put rationale (Use Table 4.2). For P1, you need to put another mapping with Knowledge profile and rational thereof.

Table 4.2: Mapping with complex problem solving.

EP1 Dept of Knowledge	EP2 Range of Conflicting Requirements	EP3 Depth of Analysis	EP4 Familiarity of Issues	EP5 Extent of Applicable Codes	EP6 Extent of Stakeholder Involvement	EP7 Interdependence
√	√	√	√	√	√	

4.3.3 Engineering Activities

In this section, provide a mapping with engineering activities. For each mapping add subsections to put rationale (Use Table 4.3).

Table 4.3: Mapping with complex engineering activities.

EA1 Range of resources	EA2 Level of Interaction	EA3 Innovation	EA4 Consequences for society and environment	EA5 Familiarity
√	√	√	√	√

Chapter 5

Conclusion

This chapter summarizes the findings and insights gained from the study of VoIP networks. It highlights the transformative impact of VoIP on modern communication systems, addresses challenges such as latency and security, and suggests future improvements to enhance reliability and scalability.

5.1 Summary

This project successfully showcased the design, configuration, and implementation of a VoIP-enabled telephony network. The system ensured secure and efficient communication through the deployment of VLAN segmentation, Inter-VLAN routing, and SSH protocols. The simulation demonstrated the viability of VoIP technology for cost-effective and scalable communication solutions.

5.2 Limitation

The use of Cisco Packet Tracer imposed certain limitations on the project:

- Advanced testing scenarios, such as large-scale traffic simulations and complex QoS (Quality of Service) configurations, could not be fully explored due to simulation constraints.
- Hardware-level features like detailed packet behavior and processing delays were not emulated, limiting real-world applicability of some results.

5.3 Future Work

Future enhancements to the project could involve:

- Implementation of Quality of Service (QoS): Ensuring optimal performance for VoIP calls by prioritizing voice traffic over data traffic.
- Integration with Public Switched Telephone Network (PSTN): Expanding the system to connect with traditional telephony infrastructure, increasing its versatility.
- Advanced Security Protocols: Deploying protocols like Secure Real-Time Transport Protocol (SRTP) to enhance data encryption and integrity during VoIP communication.

These additions would extend the project's applicability and reliability in real-world scenarios, addressing current limitations and expanding functionality.

References

[1] Lingfen Sun and Emmanuel C Ifeachor. Voice quality prediction models and their application in voip networks. *IEEE transactions on multimedia*, 8(4):809–820, 2006.