TEAM 3 | CSE E

Computer Networks

Abirami Mam

Amrita Vishwa Vidyapeetham

# Networking

## With Cisco Packet Tracer

Dec 06, 2023

# COMPUTER NETWORKS

# Case Study

### VoIP and Dial Peering system

### Group Number - 3

| Registration No | Name | Email ID | Contribution |
|---|---|---|---|
| CB.EN.U4CSE21450 | S Harecharan | harecharan321@gmail.com | HR DEPT,<br>OSPF and Documentation |
| CB.EN.U4CSE21455 | Shreyas Visweshwaran | shreyasvisweshwaran@gmail.com | FINANCE , VLANs and Documentation |
| CB.EN.U4CSE21466 | Vignesh G | vgram2003@gmail.com | IT and VoIP Protocol and Documentation |
| CB.EN.U4CSE21468 | Viswaa Ramasubramanian | viswaofficial2003@gmail.com | SALES ,DHCP and Documentation |

# INTRODUCTION

## (a) Statistics related to Network Analysis

**Business Adoption of VOIP**: A 2018 survey revealed that 61% of businesses had transitioned to VOIP phone systems from traditional phone lines, indicating a significant shift towards digital communication solutions in the business sector.

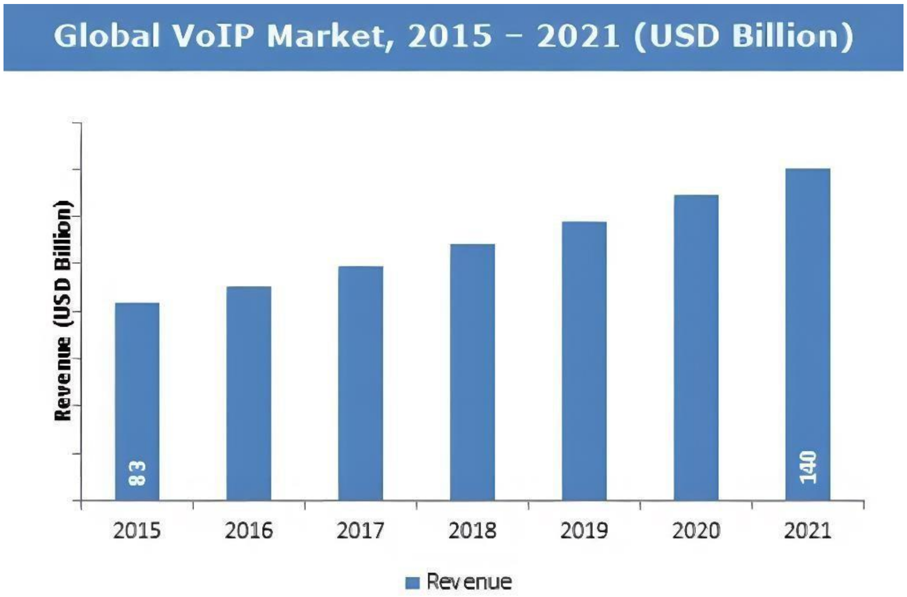
**Cost Savings**: VOIP systems offer substantial cost savings for businesses. On average, businesses save between 30% and 50% on their phone costs after switching to VOIP. This includes up to 40% savings on local calls and up to 90% on international calls. Furthermore, a business can save an average of 32 call minutes daily per team member, leading to increased efficiency and further cost reduction.

**Productivity and Profitability**: VOIP technology is not only about cost savings; it significantly boosts productivity. Businesses reported an improvement in productivity by as much as 77% after adopting VOIP systems. This increased productivity is particularly beneficial for small and medium businesses (SMBs), which are expected to grow more than 15% in the VOIP market by 2025.

**Reduced Costs for Businesses**: The average VOIP costs for businesses are around $20 to $30 per user per month, offering a cost-effective communication solution. This affordability is a driving factor for businesses, especially smaller ones, to adopt VOIP.

**Increase in VoIP Lines**: In the United States, more than 35 million VOIP lines were added between 2010 and 2018, reaching a total of 41.6 million. This significant growth in VOIP lines illustrates the rapid adoption of VOIP technology across various industries.

**Productivity and Profitability**: VOIP technology is not only about cost savings; it significantly boosts productivity. Businesses reported an improvement in productivity by as much as 77% after adopting VOIP systems. This increased productivity is particularly beneficial for small and medium businesses (SMBs), which are expected to grow more than 15% in the VOIP market by 2025.



## b) Why do we need networking in VoIP ?

**Data Transmission**: VoIP converts voice into digital data packets that are transmitted over a network. Without a network, these data packets cannot be sent or received.

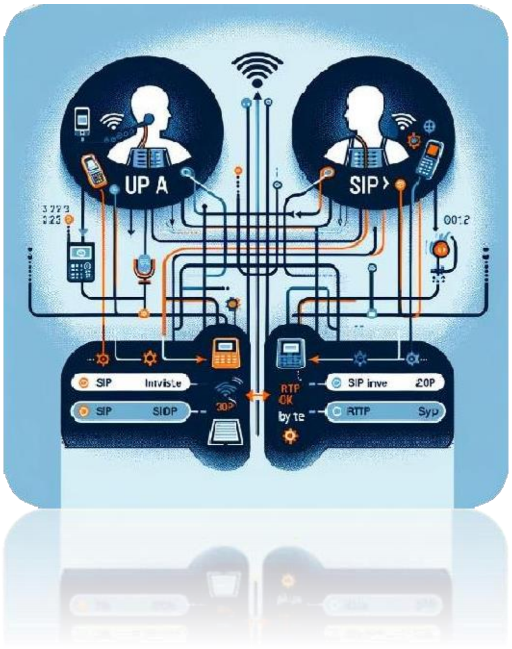
**Quality of Service (QoS)**: Effective networking ensures QoS by prioritizing voice data over other types of data. This is crucial for reducing latency, jitter, and packet loss, which are vital for maintaining the clarity and reliability of voice calls.

**Scalability and Flexibility**: Networks allow VoIP systems to easily scale up or down based on demand and enable integration with other services and applications, enhancing overall communication capabilities.

**Cost Efficiency**: Networking enables VoIP to use existing internet connections for communication, reducing the need for traditional telephone infrastructures and thereby lowering operational costs.

**Remote Connectivity**: With a network, VoIP services can be accessed from anywhere with an internet connection, facilitating remote work and global communication.

**Integration with Other Systems**: Networking allows VoIP to be integrated with other digital systems such as email, video conferencing, and customer relationship management (CRM) software, creating a unified communication platform.



# Problem statement

Develop and implement a robust and efficient Voice over Internet Protocol (VoIP) system with dial peering functionality within a multi-departmental organizational setup.

# Implementing VOIP with Dial Peering

The case study revolves around a hypothetical organization seeking to implement a VOIP system with dial peering. The goal is to create a seamless and efficient telephony network interlinking various departments such as Finance, ICT, Sales, and HR. The network design involves setting up VoIP-enabled routers, access layer switches, and configuring IP phones in each department.

Advanced configurations include subnetting and IP addressing strategies to create distinct network segments for each department, ensuring efficient and secure data transmission. Moreover, the setup incorporates the OSPF routing protocol, which enhances the network's ability to dynamically learn and adjust to changes.

A critical aspect of this implementation is the configuration of dial peering. This setup allows direct calls between departments without routing through a central exchange, significantly reducing call setup time and improving overall communication efficiency. The case study will delve into the technical configurations necessary for establishing dial peering, including the setup of telephony services and the configuration of each router and switch to support VOIP communications.

# Project Designing:

Our project revolves around the establishment of a Voice over Internet Protocol (VoIP) system tailored for business operations. The primary objective is to facilitate seamless communication among various departments within the organization. Despite each department functioning independently, they collectively serve a shared customer base. The need for high-frequency and immediate inter-departmental communication led us to prioritize voice-based communication over conventional methods such as text requests and emails. In light of the unique requirements outlined in our project's problem statement, which differentiates it from more mainstream topics like hospital or campus management systems, we have opted for a business model that aligns with the specific demands of our chosen problem statement.

## Hardware and Software Requirements

The successful implementation of a VOIP system requires specific hardware and software components. Key hardware components include:

- VOIP-enabled routers, which direct voice traffic through the network
- Access layer switches, which connect end-user devices to the network
- IP phones, which convert voice signals into digital packets

The case study will examine the types of routers (like the 2811 routers), switches (such as the 2960-24TT switches), and IP phones (like the 7960 model) necessary for a robust VOIP setup.

Software plays a crucial role in configuring and maintaining the VOIP network. Cisco's packet tracer software is essential for network design and simulation, allowing for virtual testing of network setups before implementation. The software enables visualization of network topology, helps in understanding the interaction between network devices, and is crucial for troubleshooting and optimizing network performance. This section will also cover the software configurations required for each device in the network, including the setup of protocols like OSPF for routing, SSH for secure remote management, and specific configurations for VLANs and DHCP services.

# Protocols and Configurations

Protocols are the backbone of any network, and for VOIP systems, they govern how data is transmitted and routed. The Open Shortest Path First (OSPF) protocol is critical for efficient routing within the VOIP network. OSPF, a type of Interior Gateway Protocol (IGP), helps in the rapid convergence of the network, ensuring that the most efficient paths are used for data transmission. This is especially important in VOIP systems, where delays can significantly impact call quality.

Dial peering configurations are essential in a VOIP network as they enable direct communication between different network segments or departments without routing through a central switchboard. This setup is critical for reducing call setup times and improving the overall efficiency of the telephony system. The configuration involves setting up dial-peer VOIP on the routers, specifying destination patterns, and defining session targets. This section will delve into the specific configurations necessary for OSPF and dial peering, outlining how these protocols contribute to the overall performance and efficiency of the VOIP system. It will cover the technical details of setting up OSPF in each router and the necessary steps to configure dial peering among different departments.

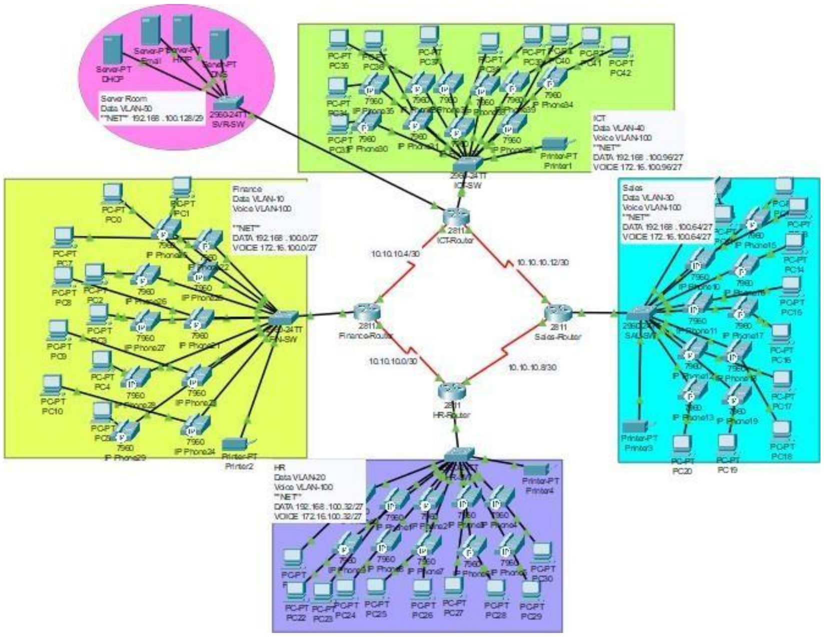
# Performance parameters

| Parameter | Meaning | Formula |
|---|---|---|
| **Bandwidth** | Bandwidth is the capacity of a wired or wireless network communications link to transmit the maximum amount of data from one point to another over a computer network or internet connection in a given amount of time | Expressed as bits per second (bps), modern network links have greater capacity, which is typically measured in millions of bits per second (megabits per second, or Mbps) or billions of bits per second (gigabits per second, or Gbps). |
| **Throughput** | Throughput measures the percentage of data packets that are successfully being sent; a low throughput means there are a lot of failed or dropped packets that need to be sent again. | |

| | | |
|---|---|---|
| **Packet Loss** | Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination.Due to network congestion | Efficiency = 100% * (transferred - retransmitted) / transferred<br>Network Loss = 100 - Efficiency |
| **Transmission time** | The time required for transmission of a message depends on the size of the message and the bandwidth of the channel. | Transmission time=Message size / Bandwidth |
| **Propagation Time** | Propagation time measures the time required for a bit to travel from the source to the destination. The propagation time is calculated by dividing the distance by the propagation speed. | Propagation time = Distance /Propagation speed |
| **Processing Delay** | Time taken by the processor to process the data packet is called processing delay. | |
| **Queuing Delay** | Time spent by the data packet waiting in the queue before it is taken for execution is called queuing delay. | |

| | | |
|---|---|---|
| **Jitter** | Jitter is defined as the variation in time delay for the data packets sent over a network. This variable represents an identified disruption in the normal sequencing of data packets. Jitter is related to latency, since the jitter manifests itself in increased or uneven latency between data packets, which can disrupt network performance and lead to packet loss and network congestion. Although some level of jitter is to be expected and can usually be tolerated, quantifying network jitter is an important aspect of comprehensive network | Latency=sum of all delays<br>To measure Jitter, we take the difference between samples, then divide by the number of samples (minus 1). |

**Architecture design:**



# Analytical questions

1. **How are different departments interconnected in the VoIP network?**
    - Each department is connected via VoIP-enabled routers and access layer switches, with specific IP configurations and VLAN settings to facilitate communication and data segmentation.

2. **What protocol is used for dynamic routing in the network, and why?**
    - OSPF (Open Shortest Path First) is used for dynamic routing to efficiently manage network traffic and ensure quick adaptation to changes in network topology.

3. **How does dial peering enhance the VoIP system?**
    - Dial peering allows direct calls between departments, bypassing the central exchange, which reduces call setup time and enhances communication efficiency.

4. **What role do VLANs play in this VoIP setup?**
    - VLANs segregate voice and data traffic, improving network security and performance by reducing congestion and prioritizing voice packets.

5. **How is network security ensured in the VoIP system?**
    - Network security is addressed through encryption, secure SIP protocols, firewall configurations, and secure network design principles.

6. **What cost savings are expected from implementing this VoIP system?**
    - The system is expected to significantly reduce costs on local and international calls, while also lowering maintenance costs compared to traditional telephony systems.

7. **How does the implementation support remote users or teleworkers?**
    - The VoIP system facilitates remote connectivity, allowing users to access telephony services from anywhere with an internet connection.

### 8. What are the key factors in ensuring Quality of Service (QoS) for VoIP?

- QoS is maintained by prioritizing voice packets, managing bandwidth, and configuring network devices to minimize latency and packet loss.

### 9. How are IP addresses managed across the departments?

- IP addresses are managed using subnetting and DHCP configurations, with distinct address ranges assigned to each department.

### 10. What measures are in place for network performance monitoring and troubleshooting?

- The network design includes monitoring tools and protocols for real-time performance assessment, along with predefined troubleshooting procedures for quick resolution of issues.

| **Department Name** | **Student** |
|---|---|
| Finance | Shreyas Visweshwaran – CB.EN.U4CSE21455 |
| HR | S Harecharan – CB.EN.U4CSE21450 |
| Sales | Viswaa Ramasubramanian – CB.EN.U4CSE21468 |
| ICT | Vignesh G – CB.EN.U4CSE21468 |

**CISCO packet tracer Network design**

# Base Network : 192.168.100.0

| Department | Network Address | Devices PDs + Printers | Subnet Mask | Host Address Range | Broadcast Address |
|---|---|---|---|---|---|
| Finance | 192.168.100.0 | 21 | 255.255.255.224/27 | 192.168.100.1 to 192.168.100.30 | 192.168.100.31 |
| HR | 192.168.100.32 | 21 | 255.255.255.224/27 | 192.168.100.33 to 192.168.100.62 | 192.168.100.63 |
| Sales | 192.168.100.64 | 21 | 255.255.255.224/27 | 192.168.100.65 to 192.168.100.94 | 192.168.100.96 |
| ICT | 192.168.100.96 | 21 | 255.255.255.224/27 | 192.168.100.97 to 192.168.100.126 | 192.168.100.127 |
| Server | 192.168.100.128 | 4 | 255.255.255.248/29 | 192.168.100.129 to 192.168.100.134 | 192.168.100.135 |

# IP Phones

| Department | Network Address | Phones | Subnet Mask | Host Address Range | Broadcast Address |
|---|---|---|---|---|---|
| Finance | 172.16.100.0 | 20 | 255.255.255.224/27 | 172.16.100.1 to 172.16.100.30 | 172.16.100.31 |
| HR | 172.16.100.32 | 20 | 255.255.255.224/27 | 172.16.100.33 to 172.16.100.62 | 172.16.100.63 |
| Sales | 172.16.100.64 | 20 | 255.255.255.224/27 | 172.16.100.65 to 172.16.100.94 | 172.16.100.96 |
| ICT | 172.16.100.96 | 20 | 255.255.255.224/27 | 172.16.100.97 to 172.16.100.126 | 172.16.100.127 |

## Between Routers

| Departments | Network Address |
|---|---|
| Finance to HR | 10.10.10.0/30 |
| Finance to ICT | 10.10.10.4/30 |
| Sales to HR | 10.10.10.8/30 |
| Sales to ICT | 10.10.10.12/30 |

# Routing Algorithm:

## 1)OSPF(open shortest path finder):

As mentioned before , the advantages of this protocol include dynamic route allocation for a more efficient system to connect across networks i.e; in this case, across departments. Let us look into its working mechanism:

**1. Hierarchical Routing**

OSPF organizes routers into hierarchical structures called areas. This hierarchical approach simplifies network management and reduces routing traffic, as routers within an area share summarized route information with routers outside the area.
OSPF introduces different types of areas, such as backbone areas (Area 0) and non-backbone areas. Backbone areas interconnect all other areas, and routers within an area share detailed topology information. Non-backbone areas receive summarized information, reducing the size of routing tables.

**2. Link-State Database**

OSPF routers maintain a Link-State Database (LSDB), which contains information about the state of all links in the network. Each router floods updates about its local state to other routers, ensuring all routers have a consistent view of the network topology.

**3. Shortest Path First Algorithm**

OSPF uses the Dijkstra Shortest Path First (SPF) algorithm to calculate the shortest path between routers. By considering link costs, OSPF determines the most efficient route for data packets to traverse the network, minimizing latency and maximizing bandwidth usage.

**4. Dynamic Routing**

OSPF adapts dynamically to changes in network topology. When a link or router fails, OSPF routers quickly update their LSDBs and recalculates the shortest path. This dynamic nature ensures optimal routing even in the presence of network changes.

**5. Router ID**

Each router in an OSPF domain is assigned a unique Router ID. The Router ID helps identify and distinguish routers within the OSPF network. This identifier is crucial for OSPF's operation and stability. It also supports scalability and authentication functionalies to it to ensure security.

## STEPS TO DO OSPF:

**1. Create Network Topology:**

- Open Cisco Packet Tracer and set up your network topology by placing routers and connecting them using appropriate interfaces.

**2. Assign IP Addresses:**

- Assign IP addresses to router interfaces. Enter the interface configuration mode on each router using the following commands:

  ```
  enable configure terminal interface [interface-type] [interface-number] ip address [ip-address] [subnet-mask] no shutdown
  ```

**3. Enable OSPF on Routers:**

- Enter OSPF configuration mode using the following commands:

```
router ospf [process-id]
```

Replace **[process-id]** with a numerical identifier for the OSPF process.

**4. Set Router ID:**

- Assign a router ID using the following command within OSPF router configuration mode:

  ```
  router-id [router-id]
  ```

  Replace **[router-id]** with a unique identifier for the router.

**5. Enable OSPF on Interfaces:**

- Enter interface configuration mode for each interface participating in OSPF and enable OSPF:

  ```
  interface [interface-type] [interface-number] ip ospf [process-id] area [area-id]
  ```

**6. Verify OSPF Configuration:**

- Use the following commands to verify OSPF configuration:
  - To check OSPF neighbor relationships:
    ```
    show ip ospf neighbor
    ```
  - To display OSPF routing information:
    ```
    show ip ospf
    ```

**7. Save Configuration:**

- Save your configuration to ensure that it persists after a reboot:

```
write memory
```

**8. Repeat for Additional Routers:**

- If your network has multiple routers, repeat steps 3-7 for each router, adjusting router IDs and area configurations as needed.

**9. Testing:**

- Test OSPF functionality by examining the routing table using the command:

```
show ip route
```

**10. Monitor OSPF:**

- Regularly monitor OSPF status using commands such as show ip ospf IInterface and show ip ospf neighbor. This allows you to ensure proper OSPF operation.

## 2) VoIP (Voice over Internet Protocol):

VoIP is a technology that enables voice communication and multimedia sessions over the Internet, providing an efficient and cost-effective alternative to traditional telephony. Let's delve into its workings:

1. **Packetization of Voice:** VoIP transforms analog voice signals into digital data packets. These packets are then transmitted over the IP network, facilitating real-time communication.
2. **Compression and Decompression:** To optimize bandwidth usage, VoIP employs various compression algorithms. Codecs (Coder-Decoder) are used to compress voice signals at the source and decompress them at the destination, ensuring efficient data transmission.
3. **Session Initiation Protocol (SIP):** SIP is a signaling protocol used in VoIP to initiate, modify, and terminate communication sessions. It facilitates the establishment of voice and video calls, conference calls, and other multimedia communication.
4. **Quality of Service (QoS):** VoIP relies on QoS mechanisms to prioritize voice traffic over the network. This ensures minimal latency, jitter, and packet loss, maintaining high-quality voice communication.

5. **Gateway Integration:** Gateways connect VoIP networks with traditional telephony networks. They handle the conversion of voice signals between digital and analog formats, enabling communication between VoIP users and traditional phone users.

**Steps to Implement VoIP:**

1. **Network Topology Setup:**
    - Design the network topology with IP phones, a VoIP server, and routers.
2. **IP Address Assignment:**
    - Assign IP addresses to all devices participating in the VoIP network.
3. **VoIP Server Configuration:**
    - Set up a VoIP server and configure SIP, ensuring proper user authentication and call routing.
4. **IP Phones Configuration:**
    - Configure IP phones with SIP accounts, specifying the address of the VoIP server.
5. **Quality of Service Configuration:**
    - Implement QoS policies on routers and switches to prioritize VoIP traffic.
6. **Testing:**
    - Conduct tests to ensure the quality of voice calls. Use tools like packet sniffers to monitor and analyze network traffic.
7. **Security Measures:**
    - Implement security measures such as encryption to protect voice communication from unauthorized access.
8. **Troubleshooting and Monitoring:**
    - Regularly monitor the VoIP network, troubleshoot issues promptly, and ensure optimal performance.

## 3) DHCP (Dynamic Host Configuration Protocol):

DHCP is a network protocol that automatically assigns IP addresses and other network configuration information to devices on a network. Let's explore its working mechanism:

1. **Address Leasing:** DHCP leases IP addresses to devices on a network for a specific duration. This dynamic allocation allows efficient utilization of IP addresses.
2. **Client Request:** When a device (DHCP client) joins a network, it sends a DHCP request to the DHCP server, seeking an IP address and other configuration details.
3. **DHCP Discover and Offer:** The DHCP server responds with a DHCP Offer, proposing an IP address and other configuration parameters. The client receives multiple offers if multiple DHCP servers are present.
4. **Request and Acknowledgment:** The client selects one offer and sends a DHCP Request to the chosen server. The server responds with a DHCP Acknowledgment, confirming the lease of the offered IP address.

5. **Configuration Parameters:** Along with the IP address, DHCP provides additional configuration parameters, including subnet mask, default gateway, DNS servers, and more.

**Steps to Implement DHCP:**

1. **DHCP Server Setup:**
    - Set up a DHCP server on a designated machine in the network.
2. **Configuration of DHCP Pool:**
    - Configure a DHCP pool on the server, specifying the range of IP addresses to be leased.
3. **Router Configuration:**
    - Configure the default gateway and DNS servers on the DHCP server if applicable.
4. **Client Configuration:**
    - Ensure that client devices are set to obtain IP addresses automatically.
5. **Testing:**
    - Connect new devices to the network and verify that they receive IP addresses and other configuration details from the DHCP server.
6. **Monitoring and Maintenance:**
    - Regularly monitor DHCP leases, address utilization, and renewals. Perform routine maintenance, such as updating the DHCP pool if necessary.

### 4) VLAN (Virtual Local Area Network):

VLANs enable the segmentation of a physical network into multiple logical networks, providing enhanced security, manageability, and flexibility. Let's explore how VLANs work:

1. **Logical Network Segmentation:** VLANs divide a physical network into isolated logical networks, allowing different groups of devices to communicate as if they were on separate physical networks.
2. **Membership by Port or MAC Address:** Devices are assigned to VLANs based on the switch port they are connected to (port-based VLAN) or based on their MAC addresses (MAC-based VLAN). This assignment facilitates grouping devices with similar communication requirements.
3. **Inter-VLAN Routing:** For communication between VLANs, a router or Layer 3 switch is required. This device performs inter-VLAN routing, allowing traffic to flow between different VLANs while maintaining isolation.

4. **Broadcast Domain Isolation:** VLANs reduce the size of broadcast domains. Broadcast traffic is confined to devices within the same VLAN, preventing unnecessary broadcast propagation throughout the entire network.

**Steps to Implement VLANs:**

1. **Switch VLAN Configuration:**
    - Enter switch configuration mode and create VLANs using commands like **vlan [vlan-id]** and **name [vlan-name]**.

2. **Port Configuration:**
    - Assign switch ports to specific VLANs using commands like **interface range [interface-range]** and **switchport mode access** followed by **switchport access vlan [vlan-id]**.

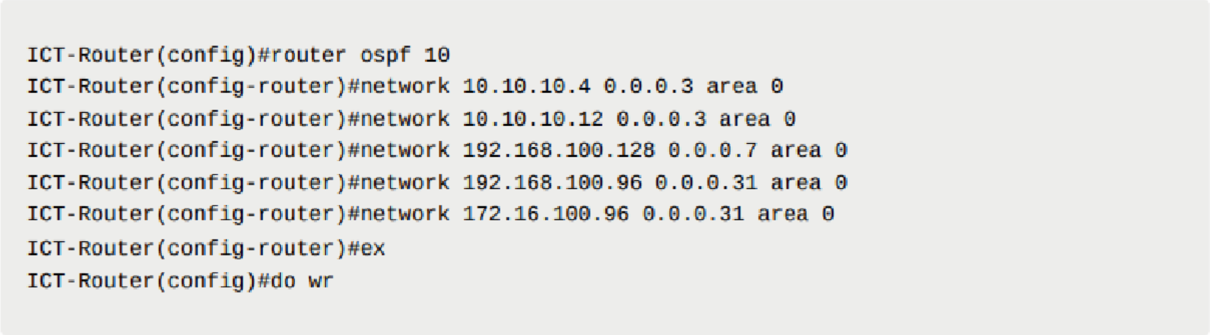
3. **Router or Layer 3 Switch Configuration:**
    - Configure the router or Layer 3 switch with subinterfaces for each VLAN to enable inter-VLAN routing.
4. **Testing:**
    - Connect devices to the configured VLANs and verify their ability to communicate within the same VLAN and across VLANs through the router.
5. **Monitoring and Maintenance:**
    - Regularly monitor VLAN configurations, verify connectivity, and make adjustments as needed. Consider network growth and make appropriate VLAN adjustments.

In this way, VoIP, DHCP, and VLANs play crucial roles in optimizing network communication, managing IP address allocation, and providing logical network segmentation for improved security and efficiency.

# CISCO PACKET DESIGNING STEPS:

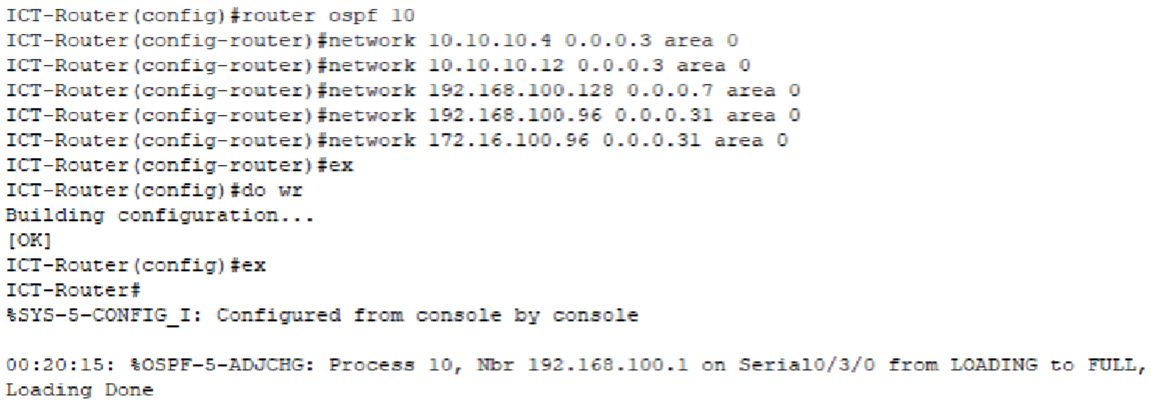
## 1)SET UP ICT ROUTER:

### ICT ROUTER



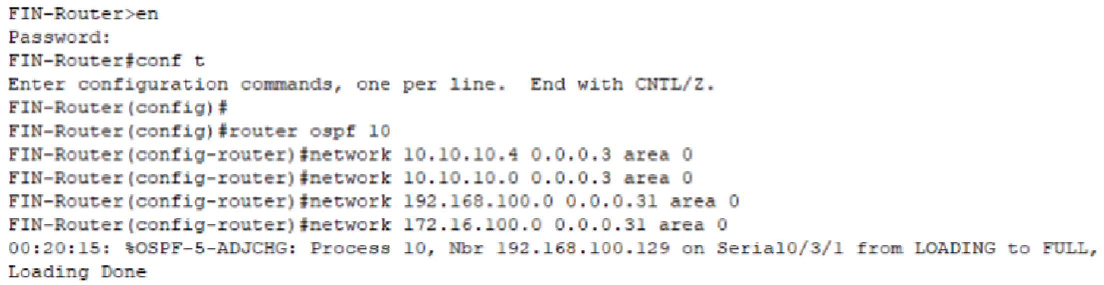
```
ICT-Router(config)#router ospf 10
ICT-Router(config-router)#network 10.10.10.4 0.0.0.3 area 0
ICT-Router(config-router)#network 10.10.10.12 0.0.0.3 area 0
ICT-Router(config-router)#network 192.168.100.128 0.0.0.7 area 0
ICT-Router(config-router)#network 192.168.100.96 0.0.0.31 area 0
ICT-Router(config-router)#network 172.16.100.96 0.0.0.31 area 0
ICT-Router(config-router)#ex
ICT-Router(config)#do wr
```

### OSPF CONFIG FOR ICT



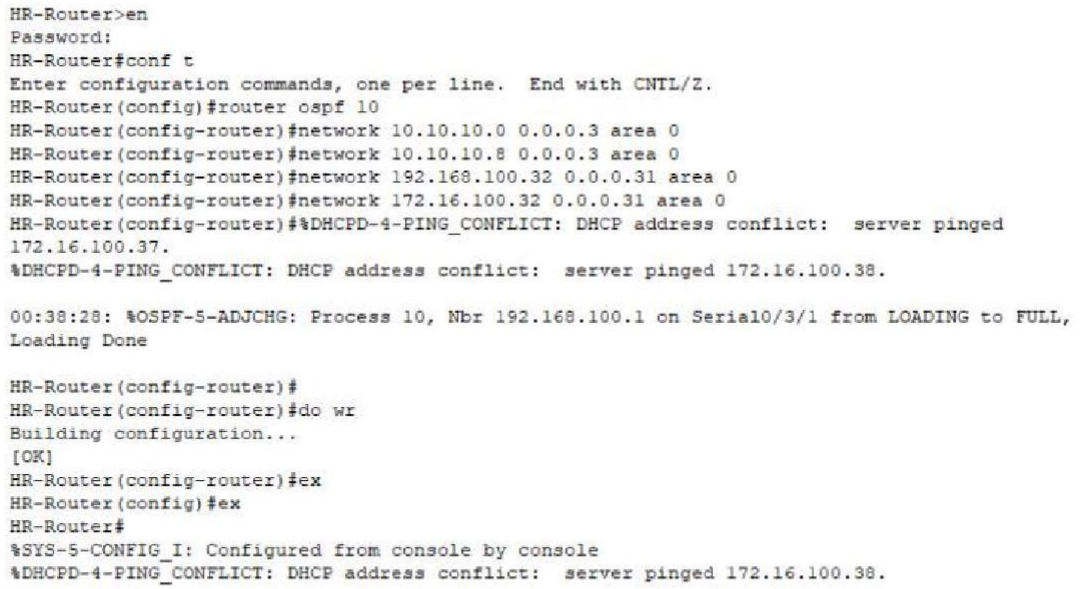
```
ICT-Router(config)#router ospf 10
ICT-Router(config-router)#network 10.10.10.4 0.0.0.3 area 0
ICT-Router(config-router)#network 10.10.10.12 0.0.0.3 area 0
ICT-Router(config-router)#network 192.168.100.128 0.0.0.7 area 0
ICT-Router(config-router)#network 192.168.100.96 0.0.0.31 area 0
ICT-Router(config-router)#network 172.16.100.96 0.0.0.31 area 0
ICT-Router(config-router)#ex
ICT-Router(config)#do wr
Building configuration...
[OK]
ICT-Router(config)#ex
ICT-Router#
%SYS-5-CONFIG_I: Configured from console by console

00:20:15: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.100.1 on Serial0/3/0 from LOADING to FULL,
Loading Done
```

# OSPF CONFIG FOR FIN



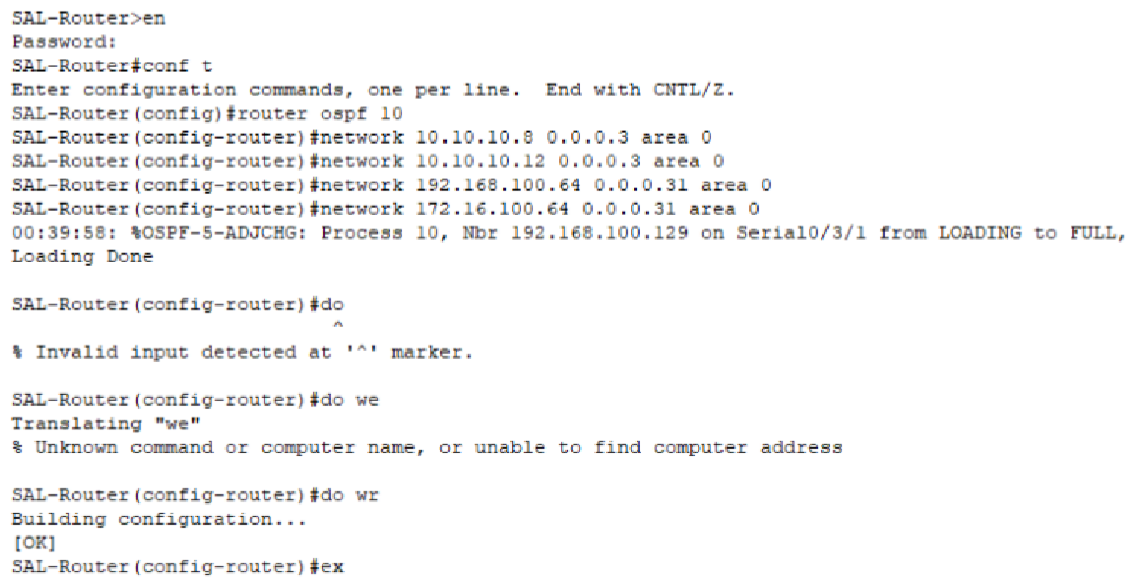
```
FIN-Router>en
Password:
FIN-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
FIN-Router(config)#
FIN-Router(config)#router ospf 10
FIN-Router(config-router)#network 10.10.10.4 0.0.0.3 area 0
FIN-Router(config-router)#network 10.10.10.0 0.0.0.3 area 0
FIN-Router(config-router)#network 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
00:20:15: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.100.129 on Serial0/3/1 from LOADING to FULL,
Loading Done
```

# OSPF CONFIG FOR HR



```
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 10.10.10.0 0.0.0.3 area 0
HR-Router(config-router)#network 10.10.10.8 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)#%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged
172.16.100.37.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.38.

00:38:28: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.100.1 on Serial0/3/1 from LOADING to FULL,
Loading Done

HR-Router(config-router)#
HR-Router(config-router)#do wr
Building configuration...
[OK]
HR-Router(config-router)#ex
HR-Router(config)#ex
HR-Router#
%SYS-5-CONFIG_I: Configured from console by console
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.38.
```

# OSPF CONFIG FOR SALES



```
SAL-Router>en
Password:
SAL-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SAL-Router(config)#router ospf 10
SAL-Router(config-router)#network 10.10.10.8 0.0.0.3 area 0
SAL-Router(config-router)#network 10.10.10.12 0.0.0.3 area 0
SAL-Router(config-router)#network 192.168.100.64 0.0.0.31 area 0
SAL-Router(config-router)#network 172.16.100.64 0.0.0.31 area 0
00:39:58: %OSPF-5-ADJCHG: Process 10, Nbr 192.168.100.129 on Serial0/3/1 from LOADING to FULL,
Loading Done

SAL-Router(config-router)#do
                           ^
% Invalid input detected at '^' marker.

SAL-Router(config-router)#do we
Translating "we"
% Unknown command or computer name, or unable to find computer address

SAL-Router(config-router)#do wr
Building configuration...
[OK]
SAL-Router(config-router)#ex
```

## CALLER RANGES:

HR: 201-210

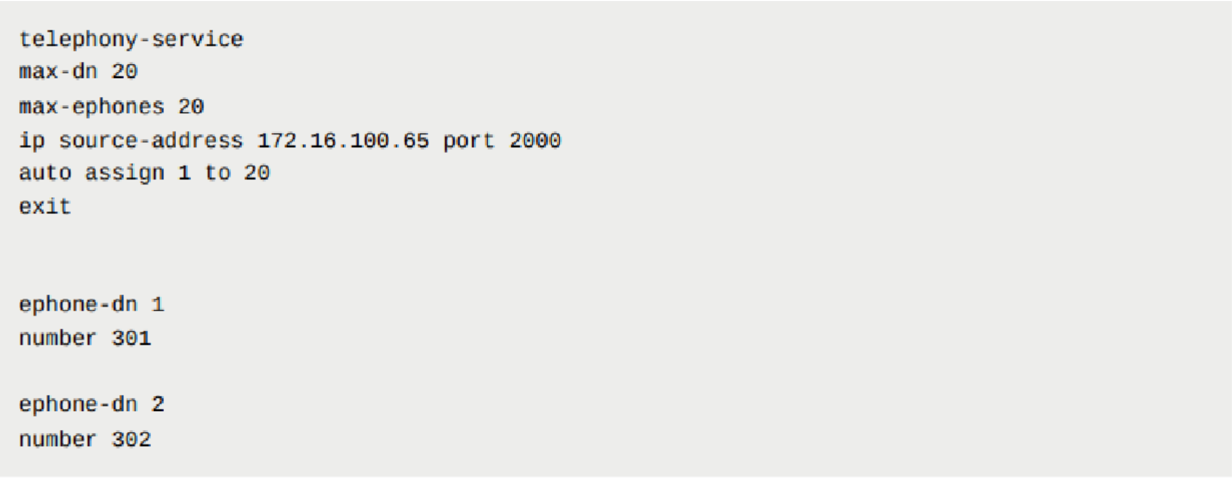
Sales: 301-310

Finance: 101-110

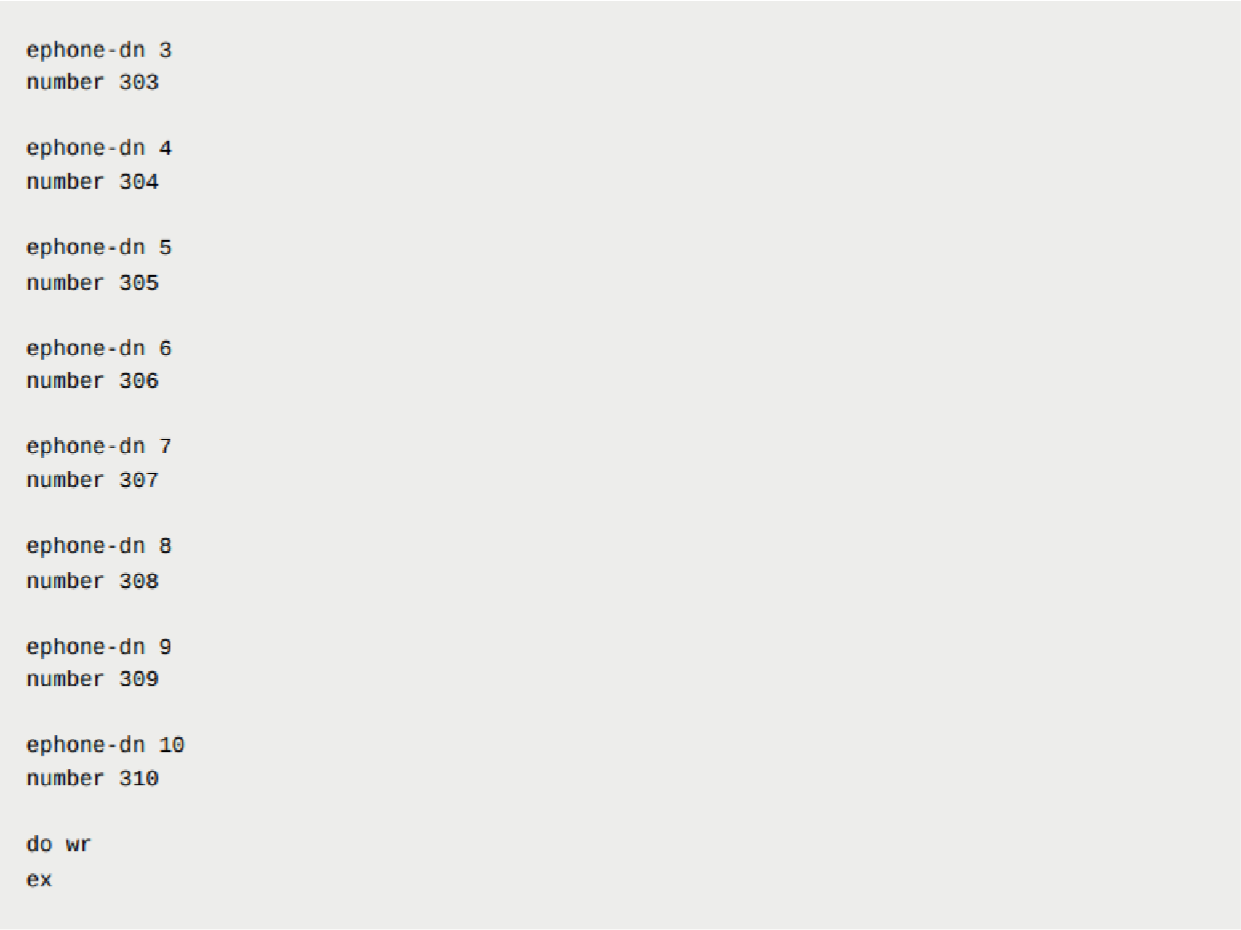
ICT: 401-410

Now the second step is to setup VoIP.

## 2)SET UP VOIP:

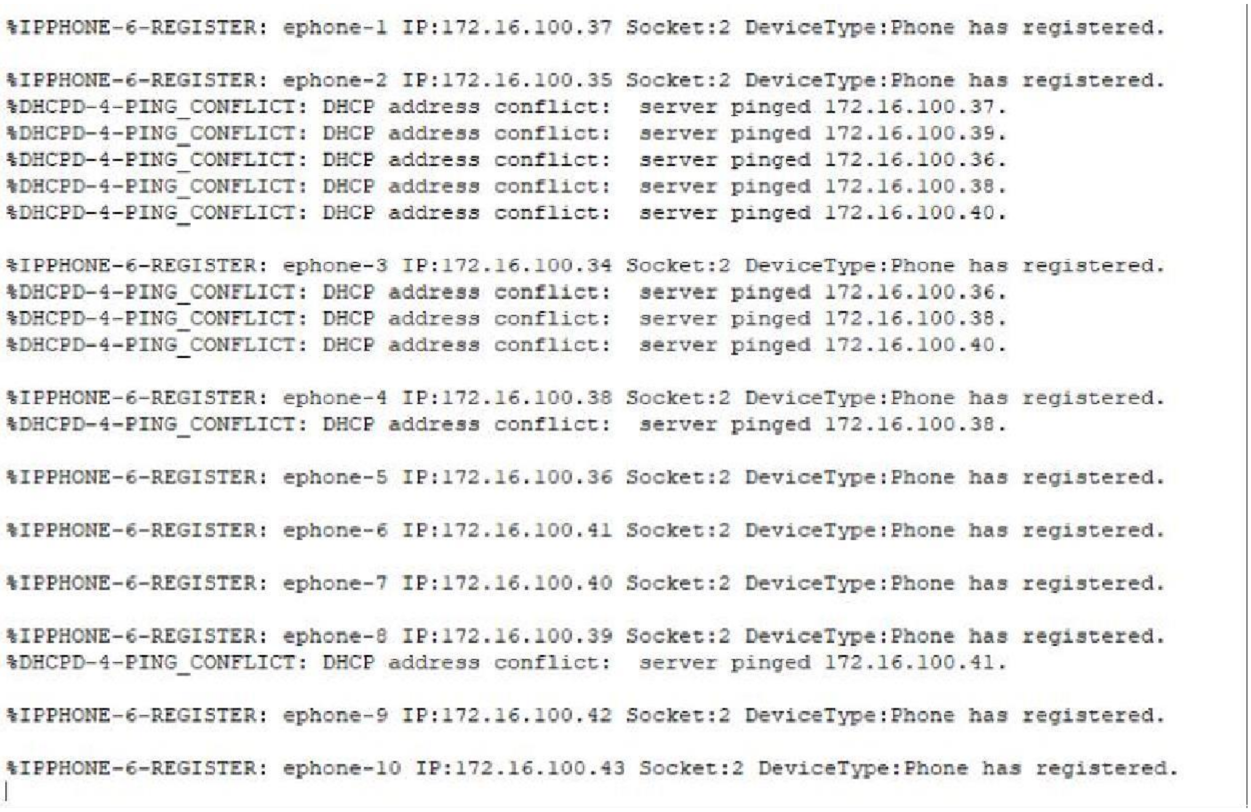


```
telephony-service
max-dn 20
max-ephones 20
ip source-address 172.16.100.65 port 2000
auto assign 1 to 20
exit


ephone-dn 1
number 301

ephone-dn 2
number 302
```



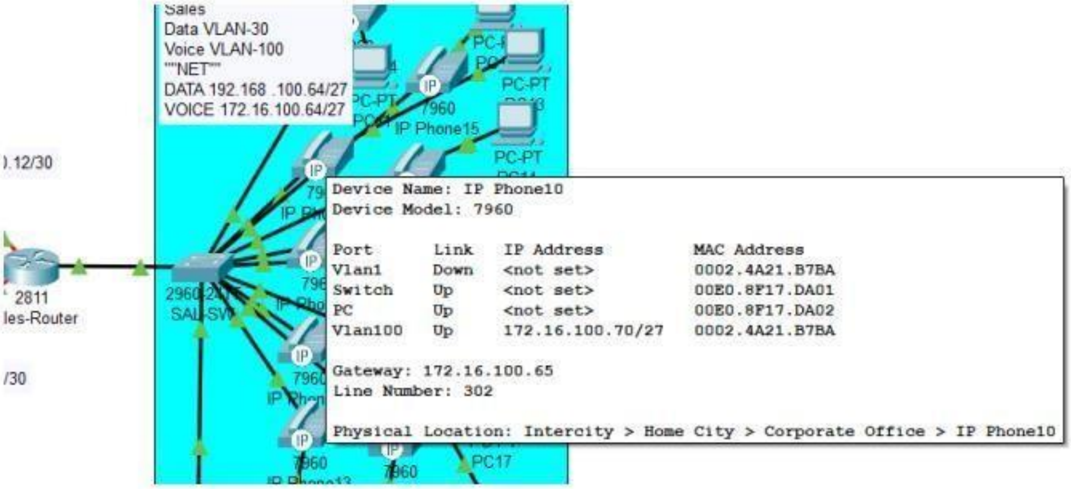
```
ephone-dn 3
number 303

ephone-dn 4
number 304

ephone-dn 5
number 305

ephone-dn 6
number 306

ephone-dn 7
number 307

ephone-dn 8
number 308

ephone-dn 9
number 309

ephone-dn 10
number 310

do wr
ex
```

After the setup, you should be getting somewhat like below

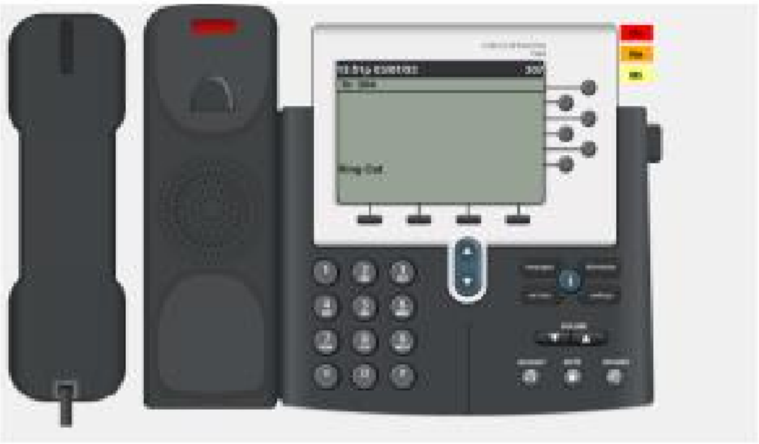


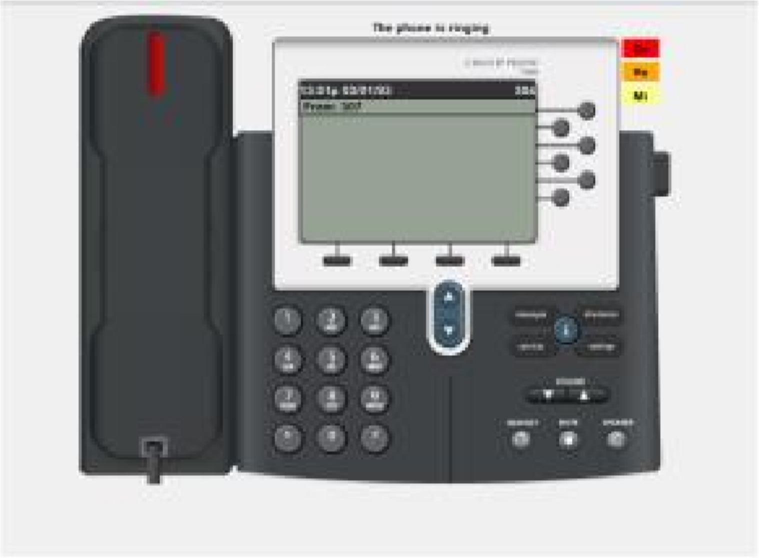
```
%IPPHONE-6-REGISTER: ephone-1 IP:172.16.100.37 Socket:2 DeviceType:Phone has registered.

%IPPHONE-6-REGISTER: ephone-2 IP:172.16.100.35 Socket:2 DeviceType:Phone has registered.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.37.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.39.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.36.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.38.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.40.

%IPPHONE-6-REGISTER: ephone-3 IP:172.16.100.34 Socket:2 DeviceType:Phone has registered.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.36.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.38.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.40.

%IPPHONE-6-REGISTER: ephone-4 IP:172.16.100.38 Socket:2 DeviceType:Phone has registered.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.38.

%IPPHONE-6-REGISTER: ephone-5 IP:172.16.100.36 Socket:2 DeviceType:Phone has registered.

%IPPHONE-6-REGISTER: ephone-6 IP:172.16.100.41 Socket:2 DeviceType:Phone has registered.

%IPPHONE-6-REGISTER: ephone-7 IP:172.16.100.40 Socket:2 DeviceType:Phone has registered.

%IPPHONE-6-REGISTER: ephone-8 IP:172.16.100.39 Socket:2 DeviceType:Phone has registered.
%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 172.16.100.41.

%IPPHONE-6-REGISTER: ephone-9 IP:172.16.100.42 Socket:2 DeviceType:Phone has registered.

%IPPHONE-6-REGISTER: ephone-10 IP:172.16.100.43 Socket:2 DeviceType:Phone has registered.
```

# **FINAL OUTPUT:**



```
Device Name: IP Phone10
Device Model: 7960

Port       Link   IP Address          MAC Address
Vlan1      Down   <not set>           0002.4A21.B7BA
Switch     Up     <not set>           00E0.8F17.DA01
PC         Up     <not set>           00E0.8F17.DA02
Vlan100    Up     172.16.100.70/27    0002.4A21.B7BA

Gateway: 172.16.100.65
Line Number: 302

Physical Location: Intercity > Home City > Corporate Office > IP Phone10
```




The phone is ringing

Now VoIP is possible within the department, what happens when you dial number which is outside the department, well since we haven’t configured dial peering among various groups, we cannot dial from HR to Sales etc.. Last step now is configuring Dial Peering among groups Below are the commands to setup dial peering from one dept to another and you can follow the similar approach to setup dial peering for all:

```
FIN-Router(config)#dial-peer voice 1 voip
```

- Enters dial-peer configuration mode for voice over IP (VoIP) with dial-peer number 1.

```
FIN-Router(config-dial-peer)#destination-pattern 2..
```

- Sets the destination pattern for this dial-peer to 2.., indicating that this dial-peer will match calls with destination numbers starting with the digit 2 and having any additional digits.

```
FIN-Router(config-dial-peer)#session target ipv4:10.10.10.2
```

- Sets the session target for this dial-peer to the IPv4 address 10.10.10.2. This specifies the destination IP address for the VoIP session.

```
FIN-Router(config-dial-peer)#ex
```

- Exits the dial-peer configuration mode and returns to global configuration mode.

```
FIN-Router(config)#do wr
```

- Executes the "write memory" command, saving the current running configuration to the startup configuration. This ensures that the changes made to the configuration are saved and will persist after a reboot.

```
Building configuration...
[OK]
```

- Indicates that the configuration has been successfully saved.

```
FIN-Router(config)#dial-peer voice 2 voip
```

- Enters dial-peer configuration mode for voice over IP with dial-peer number 2.

```
FIN-Router(config-dial-peer)#destination-pattern 4..
```

- Sets the destination pattern for this dial-peer to 4.., indicating that this dial-peer will match calls with destination numbers starting with the digit 4 and having any additional digits.

```
FIN-Router(config-dial-peer)#session target ipv4:10.10.10.6
```

- Sets the session target for this dial-peer to the IPv4 address 10.10.10.6.

```
FIN-Router(config-dial-peer)#ex
```

- Exits the dial-peer configuration mode.

```
FIN-Router(config)#dial-peer voice 3 voip
```

- Enters dial-peer configuration mode for voice over IP with dial-peer number 3.

```
FIN-Router(config-dial-peer)#destination-pattern 3..
```

- Sets the destination pattern for this dial-peer to 3.., indicating that this dial-peer will match calls with destination numbers starting with the digit 3 and having any additional digits.

```
FIN-Router(config-dial-peer)#session target ipv4:10.10.10.10
```

- Sets the session target for this dial-peer to the IPv4 address 10.10.10.10.

```
FIN-Router(config-dial-peer)#ex
```

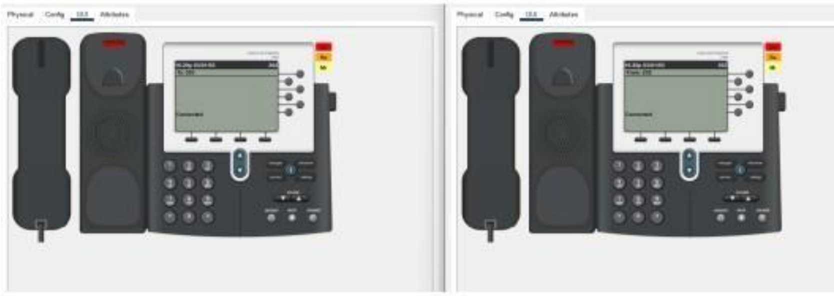
- Exits the dial-peer configuration mode.

```
FIN-Router(config)#do wr
```

- Executes the "write memory" command, saving the current running configuration to the startup configuration.

This configuration sets up three dial-peers for VoIP on the router, each with a different destination pattern and associated destination IP address.

Below is an example



As you can see, now the dial peering between different departments is possible.

# CONCLUSION:

In conclusion, the exploration of the Voice over Internet Protocol (VoIP) protocol, as outlined in the documentation and simulated in the attached Cisco Packet Tracer scenario, provides a comprehensive understanding of its inner workings. VoIP represents a transformative technology that facilitates efficient and cost-effective voice communication over IP networks. The advantages of VoIP lie in its ability to packetize voice, utilize compression algorithms, and leverage the Session Initiation Protocol (SIP) for seamless initiation and termination of communication sessions.

One of the key strengths of VoIP is its implementation of Quality of Service (QoS) mechanisms, ensuring prioritization of voice traffic and minimizing latency, jitter, and packet loss. Additionally, the integration of gateways allows interoperability between VoIP networks and traditional telephony systems, enabling a smooth transition and coexistence between different communication technologies.

However, it is imperative to acknowledge that VoIP is not without its challenges. The dependence on network quality and reliability underscores the importance of robust infrastructure to maintain optimal voice communication. Security concerns, such as unauthorized access and potential eavesdropping, necessitate the implementation of encryption and other security measures to safeguard sensitive communication.Despite these challenges, the benefits of VoIP in providing fast, reliable communication and overcoming geographical limitations are substantial. The dynamic nature of VoIP allows for scalability, making it suitable for a variety of organizational sizes and structures. The ability to transmit voice data as packets over existing IP networks contributes to cost savings and resource optimization.

In the professional realm, a nuanced understanding of VoIP's advantages and challenges is crucial for network administrators and IT professionals. This knowledge empowers them to design, implement, and maintain VoIP systems that align with organizational requirements, ensuring efficient and secure voice communication across departments and geographical locations.

As technology continues to evolve, the continued refinement of VoIP protocols and the integration of emerging technologies will likely address current challenges and enhance the overall reliability and security of VoIP systems. This exploration underscores the importance of staying abreast of technological advancements in the realm of communication protocols for creating and sustaining efficient and secure networking environments.

## ReĪerences :

1) Zion Research Analysis 2016
2) Kurose , neĪworks, a Īop-down approach
3) GeeksĪorgeeks.com
4) GuruĪech SoluĪions
5) Neso Academy

# THANK YOU

TEAM 3