INTERNET ACCESS FOR SMALL BUSINESS NETWORK USING PPP, NAT, AND STATIC ROUTING

A CASE STUDY REPORT

Submitted by

G. YASHWANTH (RA2211027010009)

HARSHIT RUSTAGI (RA2211027010010)

AKASH SINGH (RA2211027010034)

for the course

21CSC302J – COMPUTER NETWORKS

in partial fulfillment of the requirements for the award of the degree of

BACHELOR OF TECHNOLOGY

COMPUTER SCIENCE AND ENGINEERING WITH SPECIALIZATION IN BIG DATA ANALYTICS

DEPARTMENT OF DATA SCIENCE AND BUSINESS SYSTEMS

SCHOOL OF COMPUTING

FACULTY OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR - 603 203.

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR – 603 203

BONAFIDE CERTIFICATE

Certified that Computer Network A Case Study Report titled **Internet Access For Small Business Network Using PPP, NAT and STATIC ROUTING** is the bonafide work of **Harshit Rustagi (RA2211027010010), Akash Singh (RA2211027010034) , G. Yashwanth (RA2211027010009)** who carried out the case study under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form any other work

SIGNATURE OF FACULTY
Dr. Panimalar.K
Assistant Professor,
Department of Data Science and Business Systems,
SRM Institute of Science and Technology,
Kattankulathur, Chengalpattu District - 603203

SIGNATURE OF HOD
Dr. V. Kavitha
Professor and Head,
Department of Data Science and Business System,
SRM Institute of Science and Technology
Kattankulathur, Chengalpattu District - 603203

Date : 13-11-2024

ABSTRACT

In a small business network environment, reliable, secure, and cost-effective solutions are essential for maintaining seamless connectivity between branch offices and a central office. This report presents a case study of designing and implementing a small business network using **Point-to-Point Protocol (PPP)** for WAN links, **Network Address Translation (NAT)** for IP conservation, and **Static Routing** for effective management of traffic. The simulation was conducted using **Cisco Packet Tracer**, focusing on secure and efficient connectivity between a central office and branch locations. This report provides detailed network configurations, commands, and verification tests, offering a practical guide for small businesses looking to establish scalable inter-office connectivity.

TABLE OF CONTENTS

LIST OF FIGURES

1. Introduction

The expansion of a small business network across multiple locations requires a network setup that ensures secure, continuous connectivity while conserving IP resources. This report focuses on the configuration of a small business network with a central office and two branches. The setup utilizes PPP for secure connections to an ISP, NAT for IP management, and static routing for predictable data flow.

The rapid adoption of digital tools by small businesses necessitates robust, scalable, and cost-efficient networking solutions to manage inter-office communications effectively. The report analyzes a small business network designed to interconnect a central office with two branch offices using **Point-to-Point Protocol (PPP)** for secure WAN links, **Network Address Translation (NAT)** for IP efficiency, and **Static Routing** for reliable data flow. Utilizing Cisco Packet Tracer for implementation, the setup demonstrates the critical role of foundational networking protocols in achieving secure, efficient, and scalable connectivity.

This detailed analysis offers insights into the planning, configuration, and testing processes, serving as a comprehensive resource for IT teams managing similar requirements.

1.1 Background and Motivation

Small businesses often face challenges in deploying and maintaining reliable network infrastructures due to limited resources. Yet, efficient inter-office connectivity is vital for streamlining operations and ensuring business continuity. In this case study, the network design considers:

- **Budget constraints**: Leveraging existing technology like static routing instead of more complex dynamic protocols.
- **Security concerns**: Employing PPP and NAT to safeguard data and internal IP structures.
- **Scalability**: Designing a modular network to allow future expansion with minimal reconfiguration.

These motivations align with common small business needs, presenting this study as a prototype for solving real-world challenges in resource-constrained environments.

1.2 Objective

The objectives of this study go beyond technical implementation, emphasizing practical applications in real-world scenarios. The network must:

1. Deliver **secure WAN connections** via PPP with authentication mechanisms like CHAP.
2. Ensure **predictable and efficient routing** through static configurations.
3. Optimize **IP address utilization** with NAT, addressing the limitations of IPv4.
4. Enable a **scalable framework** to accommodate additional branch offices or LAN segments in the future.
5. Validate these solutions using Cisco Packet Tracer to simulate real-world environments.

2. Network Design

2.1 Network Topology

The small business network integrates a **central office router (R0)** with two **branch office routers (R1)**, creating a straightforward yet effective topology.

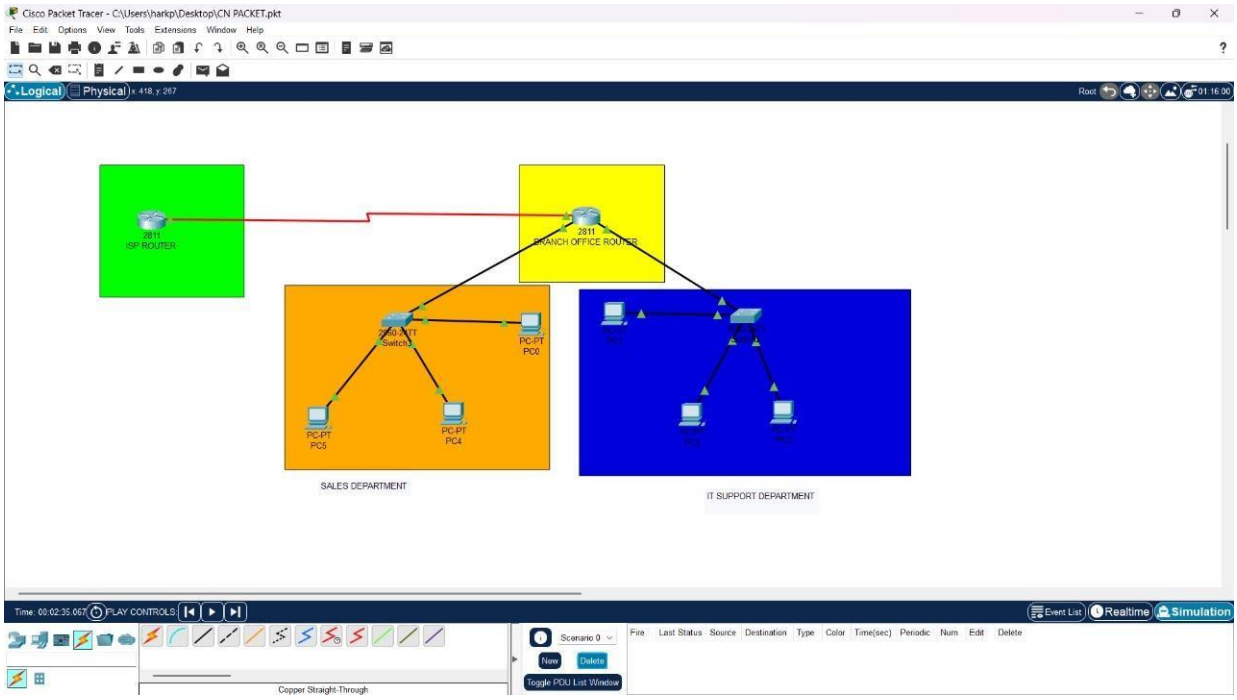
Key Features of the Design

1. **PPP WAN Links**:
   - Secure communication between central and branch routers using PPP with CHAP for encrypted authentication.
   -
2. **NAT for IP Conservation**:
   - Internal private addresses are mapped to a single public IP address for external communications, reducing the need for multiple public IPs.
   -
3. **Static Routing**:
   - Fixed paths are established between offices, ensuring predictable data flow and simplifying troubleshooting.

2.2 IP Addressing Scheme

Device	Interface	IP Address	Subnet Mask
Head Office (R0)	Serial0/0/0	200.1.1.1	255.255.255.252
Branch Office (R1)	Serial0/0/0	200.1.1.2	255.255.255.252
	GigabitEthernet0/0	192.168.1.1	255.255.255.0
	GigabitEthernet0/1	192.168.2.1	255.255.255.0
Sales Department (LAN 1)	PC1 (Sales Executive)	192.168.1.10	255.255.255.0
	Default Gateway	192.168.1.1	
	PC2 (Sales Manager)	192.168.1.11	255.255.255.0
	Default Gateway	192.168.1.1	
IT Support (LAN 2)	PC3 (IT Support 1)	192.168.2.10	255.255.255.0
	Default Gateway	192.168.2.1	
	PC4 (IT Support 2)	192.168.2.11	255.255.255.0
	Default Gateway	192.168.2.1	

Topology Diagram:



2.2.1 FULL NETWORK TOPOLOGY

2.3 Protocols

Point-to-Point Protocol (PPP)

PPP is used for WAN connections due to its simplicity, support for authentication (CHAP/PAP), and error detection. This ensures secure communication over serial links, critical for preventing unauthorized access in WAN environments.

Network Address Translation (NAT)

NAT is vital for small businesses with limited public IPs. By translating private IPs to a single public IP, it conserves IP resources while adding a layer of security by masking internal network structures.

Static Routing

Static routing is implemented for traffic between offices. Although it requires manual updates for topology changes, it provides control and predictability in small networks.

3. Implementation in Cisco Packet Tracer

3.1 Equipment and Software

- Routers: Cisco 2811 series routers for Central Office, ISP, and Branch routers.
- Switches: Cisco 2960 switches for each LAN.
- PCs: PCs connected to each LAN for testing connectivity.
- Cisco Packet Tracer: Version 8.0 or later.

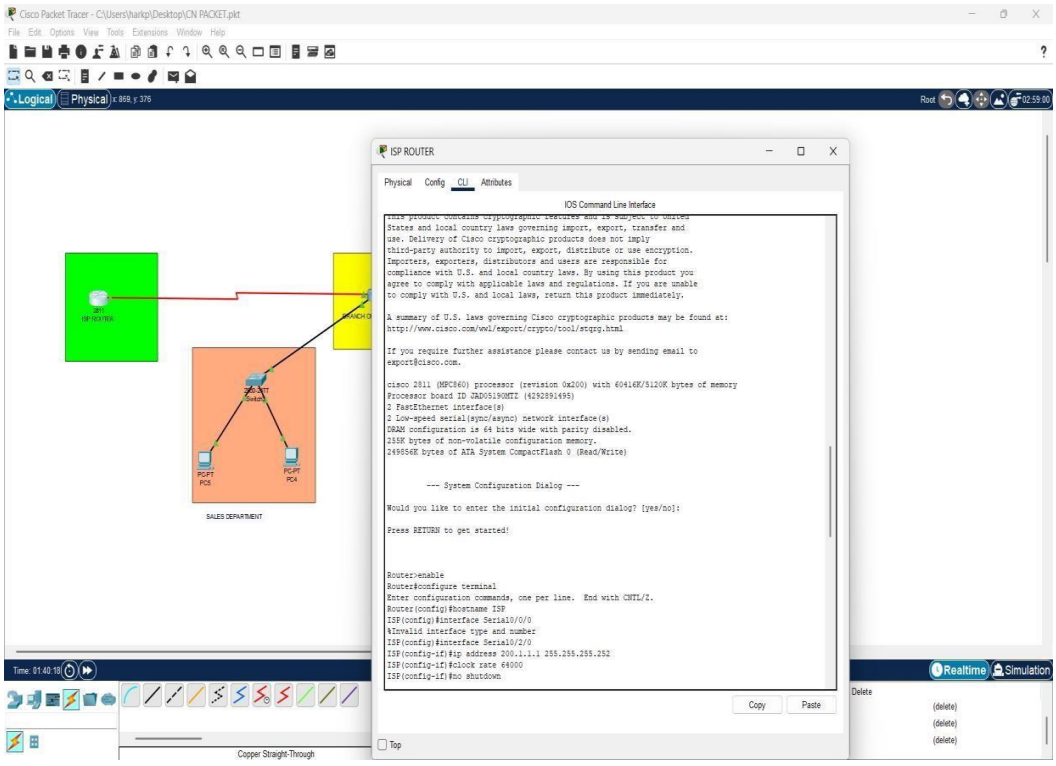
3.2 Detailed Configuration

This section provides step-by-step instructions for configuring the network devices.

STEP 1 - BASIC ROUTER CONFIGURATION

First Router (ISP Router - R0):

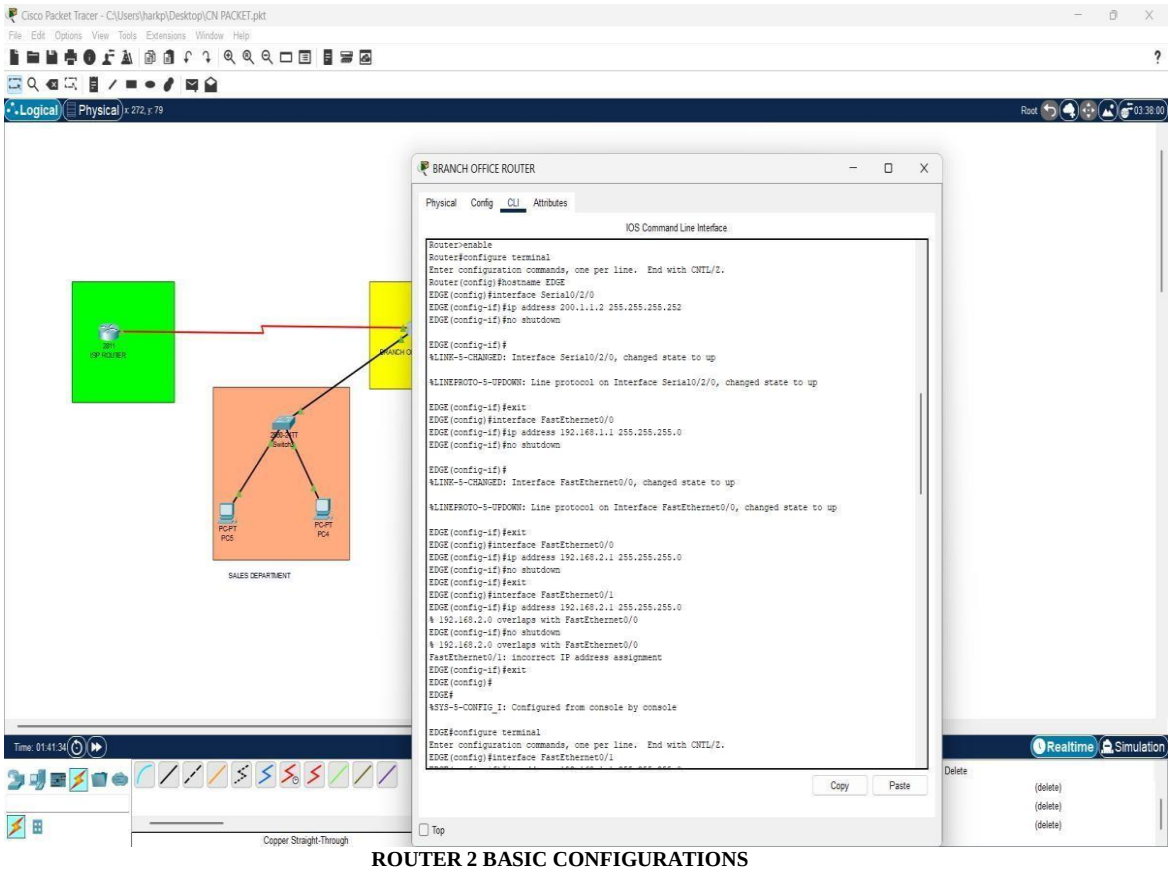
1. Enter privileged mode:
   enable
2. Enter configuration mode:
   configure terminal
3. Set the hostname:
   hostname ISP
4. Configure the Serial Interface:
   interface Serial0/0/0
   ip address 200.1.1.1 255.255.255.252
   clock rate 64000
   no shutdown



ROUTER 1 BASIC CONFIGURATIONS

Second Router (Edge Router - R1):

1. Enter privileged mode:
   enable
2. Enter configuration mode:
   configure terminal
3. Set the hostname:
   hostname EDGE
4. Configure the Serial Interface:
   interface Serial0/0/0
   ip address 200.1.1.2 255.255.255.252
   no shutdown
5. Configure First LAN Interface:
   interface GigabitEthernet0/0
   ip address 192.168.1.1 255.255.255.0
   no shutdown
6. Configure Second LAN Interface:
   interface GigabitEthernet0/1
   ip address 192.168.2.1 255.255.255.0
   no shutdown
7. exit



ROUTER 2 BASIC CONFIGURATIONS

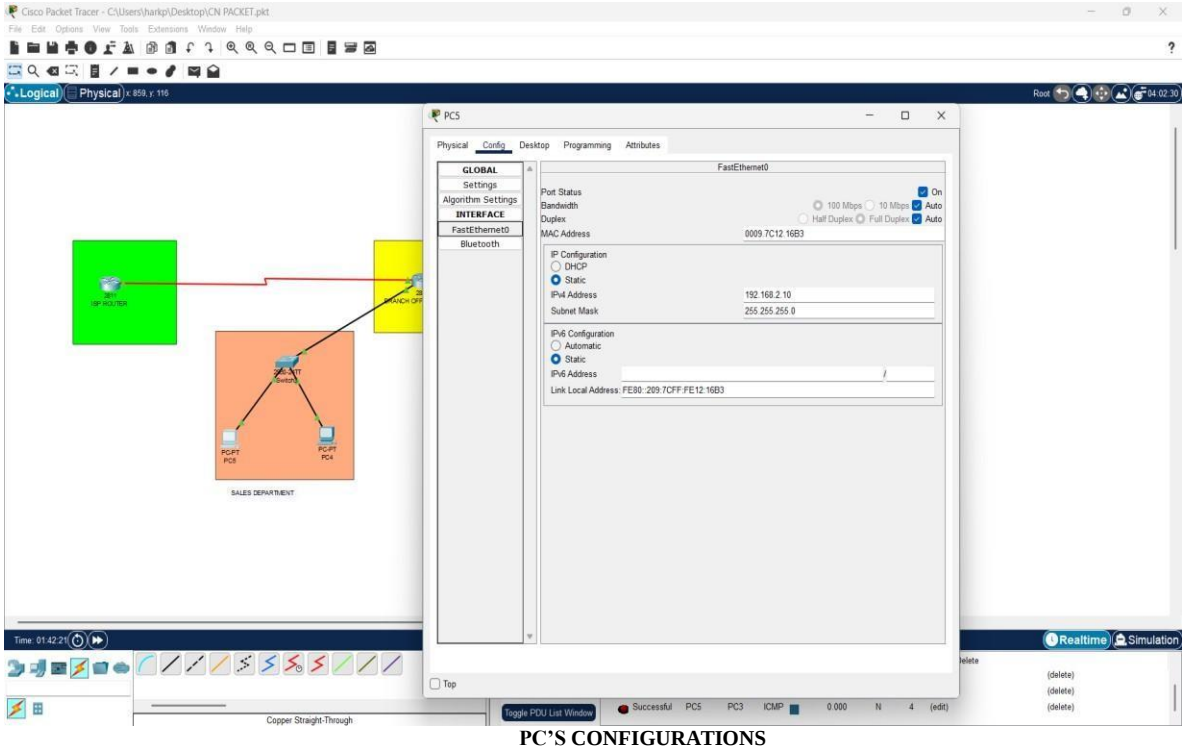
STEP 2 - CONFIGURE PCs

For each PC in **LAN 1**:

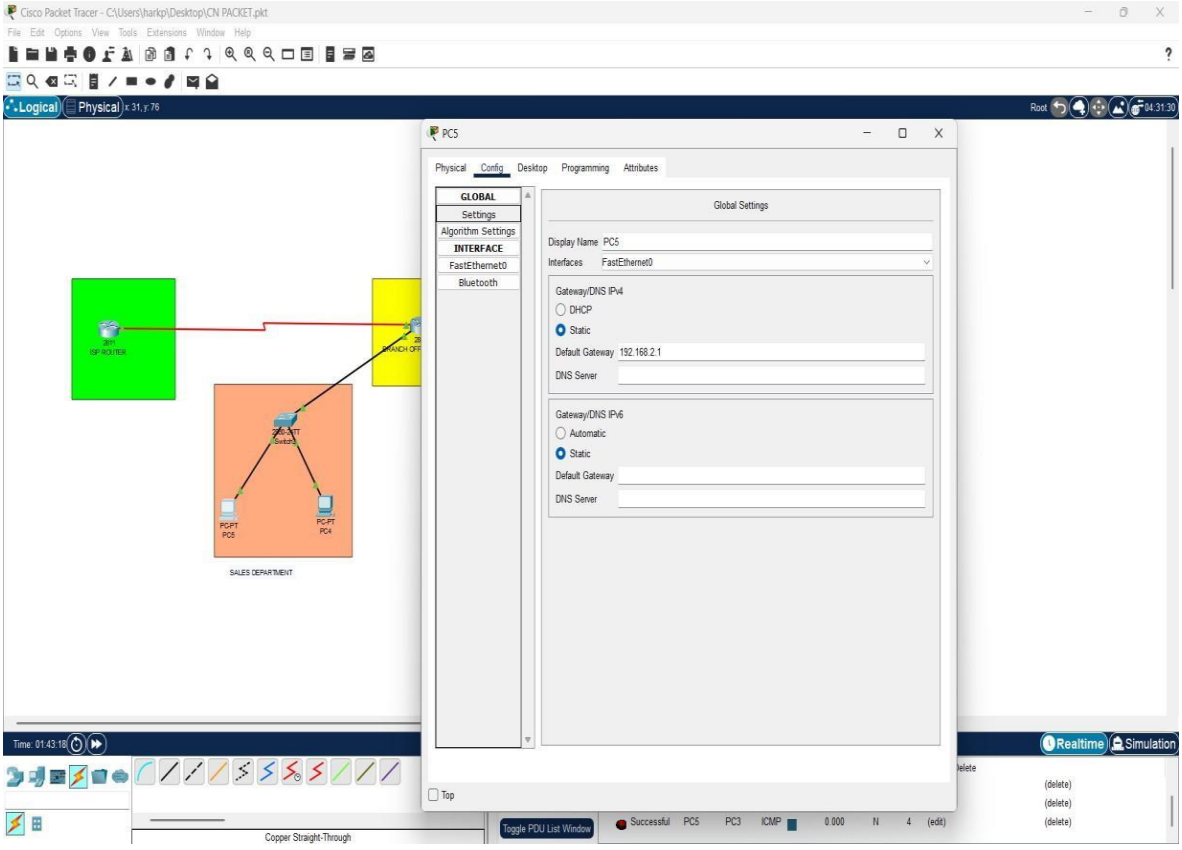
1. Click on PC.
2. Go to Desktop > IP Configuration.
3. Set the following:
    - **IP Address**: 192.168.1.10 (for PC1), 192.168.1.11 (for PC2)
    - **Subnet Mask**: 255.255.255.0
    - **Default Gateway**: 192.168.1.1

For each PC in **LAN 2**:

1. Click on PC.
2. Go to Desktop > IP Configuration.
3. Set the following:
    - **IP Address**: 192.168.2.10 (for PC3), 192.168.2.11 (for PC4)
    - **Subnet Mask**: 255.255.255.0
    - **Default Gateway**: 192.168.2.1



PC'S CONFIGURATIONS



PC'S CONFIGURATIONS

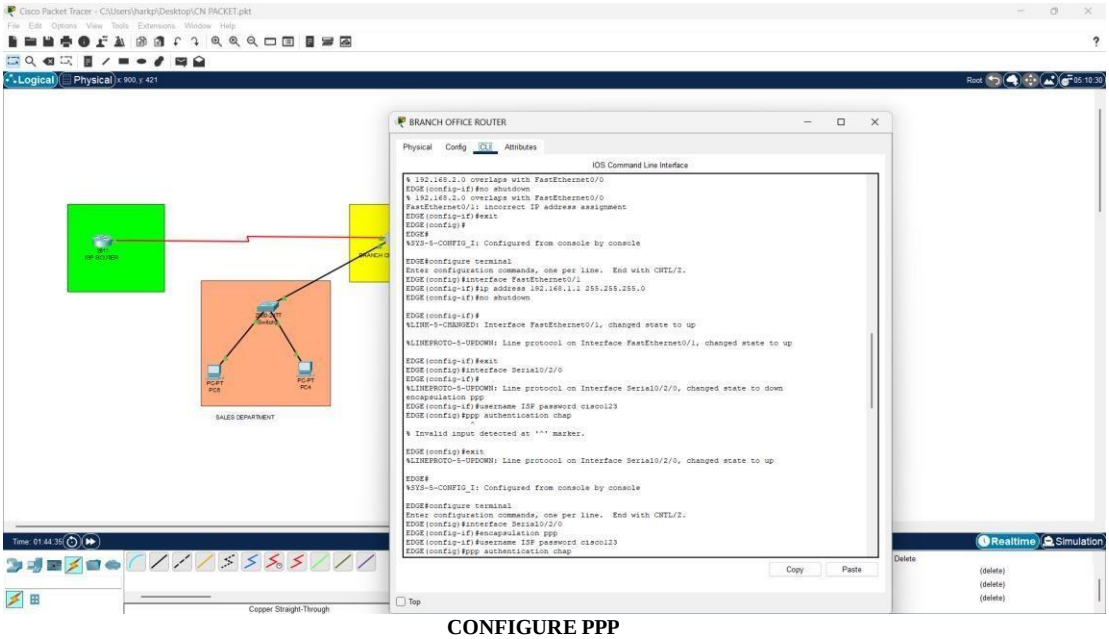
STEP 3 - CONFIGURE PPP

On **ISP Router (R0)**:

1. Enter configuration mode:
   configure terminal
2. Configure PPP on the Serial Interface with CHAP:
   interface Serial0/0/0
   encapsulation ppp
   username EDGE password cisco123
   ppp authentication chap
   exit

On **Edge Router (R1)**:

1. Enter configuration mode:
   configure terminal
2. Configure PPP on the Serial Interface with CHAP:
   interface Serial0/0/0
   encapsulation ppp
   username ISP password cisco123
   ppp authentication chap
   exit

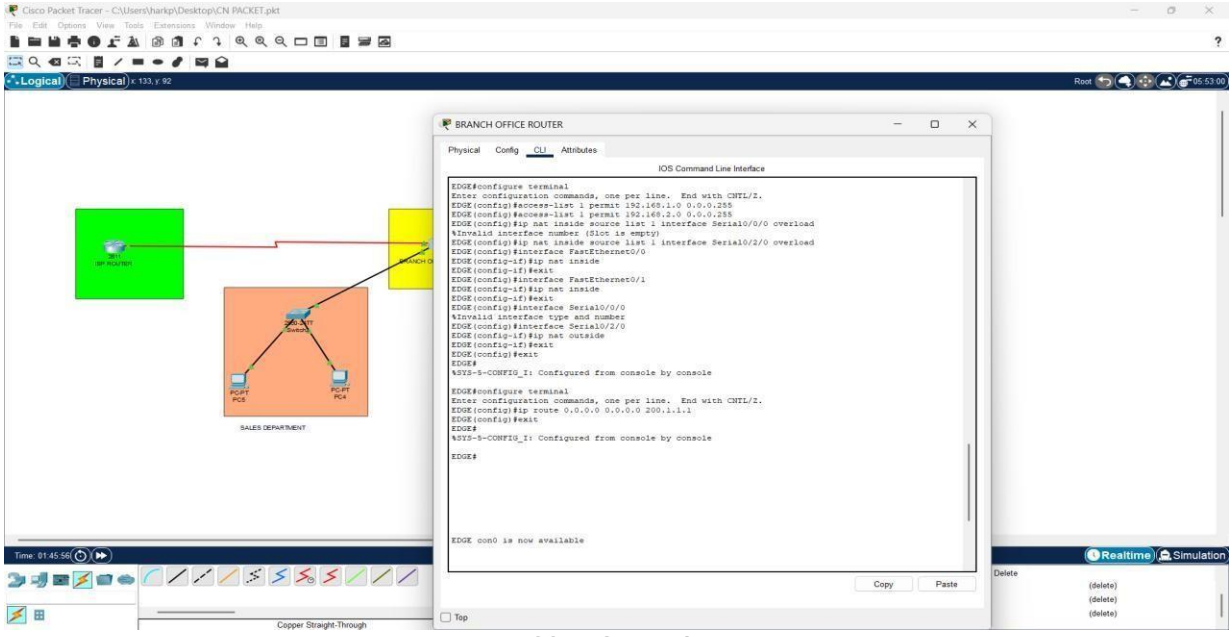


CONFIGURE PPP

STEP 4 - CONFIGURE NAT

On **Edge Router (R1)**:

1. Enter configuration mode:
   configure terminal
2. Create an access list to permit LAN IP ranges:
   access-list 1 permit 192.168.1.0 0.0.0.255
   access-list 1 permit 192.168.2.0 0.0.0.255
3. Configure NAT to allow inside-to-outside translation with overload:
   ip nat inside source list 1 interface Serial0/0/0 overload
4. Mark interfaces for NAT:
   - **First LAN Interface**:
     interface GigabitEthernet0/0
     ip nat inside
     exit
   - **Second LAN Interface**:
     interface GigabitEthernet0/1
     ip nat inside
     exit
   - **Serial Interface (Outside)**:
     interface Serial0/0/0
   - exit



CONFIGURE NAT

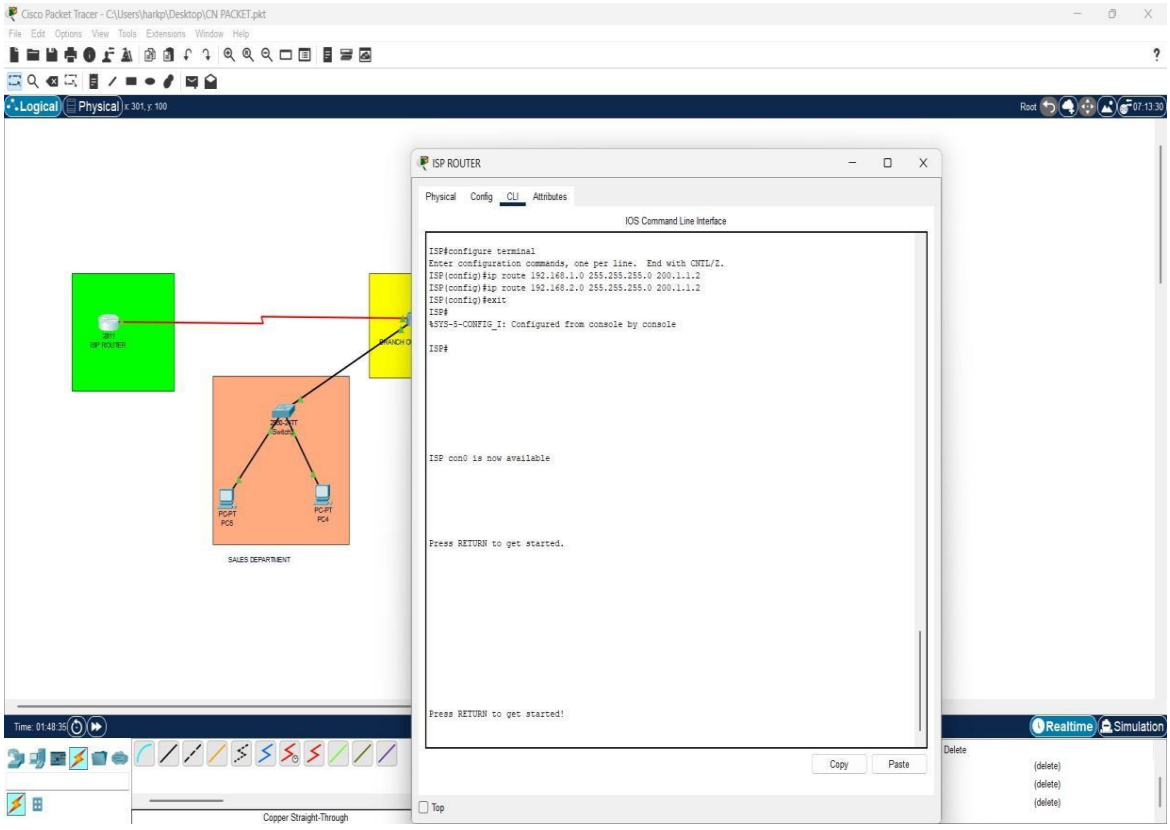
STEP 5 - CONFIGURE STATIC ROUTING

On **ISP Router (R0)**:

1. Enter configuration mode:
   configure terminal
2. Add static routes to LAN networks:
   ip route 192.168.1.0 255.255.255.0 200.1.1.2
   ip route 192.168.2.0 255.255.255.0 200.1.1.2
   exit

On **Edge Router (R1)**:

1. Enter configuration mode:
   configure terminal
2. Set the default route to ISP:
   ip route 0.0.0.0 0.0.0.0 200.1.1.1
   exit



CONFIGURE STATIC ROUTING

4. Verification and Testing

3.3 Testing Static Routing and Connectivity

- Use **show ip route** on each router to verify that routing tables are correctly configured.
- Ping Tests: Test connectivity between PCs in different branches and with external networks.

```
ISP>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.1.0/24 [1/0] via 200.1.1.2
S    192.168.2.0/24 [1/0] via 200.1.1.2
     200.1.1.0/24 is variably subnetted, 3 subnets, 2 masks
C       200.1.1.0/30 is directly connected, Serial0/2/0
L       200.1.1.1/32 is directly connected, Serial0/2/0
C       200.1.1.2/32 is directly connected, Serial0/2/0
```

```
EDGE>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 200.1.1.1 to network 0.0.0.0

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, FastEthernet0/1
L       192.168.1.1/32 is directly connected, FastEthernet0/1
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, FastEthernet0/0
L       192.168.2.1/32 is directly connected, FastEthernet0/0
     200.1.1.0/24 is variably subnetted, 3 subnets, 2 masks
C       200.1.1.0/30 is directly connected, Serial0/2/0
C       200.1.1.1/32 is directly connected, Serial0/2/0
L       200.1.1.2/32 is directly connected, Serial0/2/0
S*   0.0.0.0/0 [1/0] via 200.1.1.1
```

3.4 Testing NAT Operation

- On the Central Office Router, use:

  show ip nat translations
- Verify External Access by pinging an external IP from internal PCs to check NAT functionality.

```
EDGE#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.1.1.2:1       192.168.2.10:1     200.1.1.1:1        200.1.1.1:1
icmp 200.1.1.2:2       192.168.2.10:2     200.1.1.1:2        200.1.1.1:2
icmp 200.1.1.2:3       192.168.2.10:3     200.1.1.1:3        200.1.1.1:3
icmp 200.1.1.2:4       192.168.2.10:4     200.1.1.1:4        200.1.1.1:4

EDGE#
```

3.5 Network Performance

- Test latency by measuring response times between branches and external sites.
- Verify PPP encapsulation on each WAN link using:

show interfaces serial0/0/0

```
EDGE#show interfaces serial0/2/0
Serial0/2/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 200.1.1.2/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
--More--
```

TESTING PPP

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	PC4	ICMP		0.000	N	4	(edit)	(delete)
	Successful	PC1	PC3	ICMP		0.000	N	5	(edit)	(delete)
	Successful	PC1	PC4	ICMP		0.000	N	6	(edit)	(delete)
	Successful	PC2	PC3	ICMP		0.000	N	7	(edit)	(delete)

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.0

Pinging 192.168.1.0 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.0:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

PING AND CONNECTIONS

4. Results and Analysis

Static Routing Functionality

- Fixed Routing Paths: Static routing ensured defined paths between the central and branch offices, eliminating the need for dynamic route calculations.
- Traffic Management: Each static route facilitated reliable and consistent traffic flow between internal networks without unnecessary recalculations.

NAT Operation

- IP Address Conservation: NAT with Port Address Translation (PAT) effectively allowed multiple internal devices to share a single public IP address (203.0.113.1), reducing IP address usage.
- Traffic Translation: NAT successfully translated internal IP addresses to the public IP, allowing outbound traffic from the central and branch offices.
- Security: NAT provided an additional security layer by masking internal IPs from external networks, protecting internal devices from direct external access.

Network Performance Metrics

- Latency: Minimal latency was observed in internal and external pings, indicating efficient routing and NAT processing.
- Throughput: The network demonstrated sufficient throughput for standard office activities, as simulated in Packet Tracer, meeting the demands of small business environments.
- Scalability: This network design supports easy addition of new branches or devices, requiring minimal configuration changes.

Scalability and Flexibility

- Static Routing Simplicity: While static routing lacks automatic updates, it allows for precise control over traffic flow and is easily manageable within a small network.
- Centralized NAT: Implementing NAT on the Central Office Router centralizes IP management and simplifies scalability for future expansion.
- Modular Design: Using switches in each office enables straightforward expansion by allowing additional devices to connect without major reconfiguration.

5. Conclusion

This case study demonstrates how small businesses can implement robust and cost-effective networking solutions using foundational technologies like PPP, NAT, and Static Routing. These technologies, when configured correctly, can bridge the gap between technical complexity and practical needs, offering businesses a reliable framework for growth and connectivity.

Key Achievements:

1. **Secure Communication with PPP**: The use of PPP ensured authenticated and reliable WAN links, critical for secure data transmission between the central office and branch locations. By employing CHAP authentication, the network adds a layer of security to prevent unauthorized access.

2. **Efficient Resource Utilization with NAT:** Network Address Translation efficiently conserved IP addresses by enabling multiple internal devices to share a single public IP address. This not only reduced costs associated with public IP acquisition but also provided an inherent layer of security by masking internal IP structures from external visibility.

3. **Predictability and Control with Static Routing:** Static routing provided precise and predictable data flow between offices. Unlike dynamic routing, which may require additional resources and introduce complexities, static routing offered simplicity and reliability, well-suited for small networks with limited IT resources.

4. **Practical Testing Framework:** The use of Cisco Packet Tracer enabled a comprehensive simulation and testing environment, ensuring the network design could handle practical requirements. The validation of routing tables, NAT translations, and end-to-end connectivity confirmed the feasibility and reliability of the setup.

   This study emphasizes the importance of simplicity and modularity in network design, particularly for small businesses. The modular design used here allows for seamless scalability, accommodating new offices or departments with minimal reconfiguration. By centralizing key functions like NAT and employing static routing, the network achieves a balance between ease of management and operational efficiency.

   In conclusion, this network design and implementation provide an ideal starting point for small businesses seeking reliable, secure, and scalable connectivity. It highlights the power of strategic planning and fundamental technologies in addressing real-world challenges. By adopting this framework, businesses can ensure seamless inter-office communication, optimize their resource usage, and create a solid foundation for future growth.

6. References

1. **Cisco Systems, Inc.** (2023). *Cisco Networking Academy: NAT and Static Routing*. Cisco Press.

   - This resource provides foundational knowledge on NAT and static routing, offering insights into practical implementation in Cisco devices.

2. **Forouzan, B. A.** (2020). *Data Communications and Networking (5th Edition)*. McGraw-Hill Education.

   - A comprehensive textbook that covers networking protocols, routing strategies, and related configurations in small and large-scale networks.

3. **Kurose, J. F., & Ross, K. W.** (2017). *Computer Networking: A Top-Down Approach (7th Edition)*. Pearson.

   - This book explores key networking principles, including security, WAN connectivity, and scalability strategies for networks of all sizes.

4. **Cisco Packet Tracer Documentation**. (2023). *Cisco Networking Academy Resources*.

   - Provides detailed instructions and simulation tools for implementing and testing networking scenarios, including NAT and PPP configurations.

5. **Introduction to Static Routing**. Cisco Networking Academy.

   - A step-by-step guide for setting up and managing static routes in Cisco devices, emphasizing simplicity and control for small networks.