

Infrastructure Setup Offer

Dear Noventra SA Team,

We are delighted to present our proposal for the modernization and expansion of your IT infrastructure.

Recognizing the significant growth of Noventra SA and the need to support an ever-increasing number of staff, our proposal is designed to transcend the current limits of the local network. We propose a comprehensive solution to enable professional Internet access throughout your organization, ensuring seamless connectivity for local branches and international expansions. Our goal is to create a robust and scalable network that will allow your team and teleworkers to securely and efficiently access critical company resources, no matter where they are located.

This strategic enhancement is not just a step towards empowering your staff but also a leap towards the sustainability of your business in the digital age.

With Best Regards

avysakyuz@gmail.com

Table of Contents

Introduction.....	3
Objectives.....	3
Constraints.....	3
Desired Services.....	3
Hardware.....	4
Infrastructure Diagrams.....	5
Logical.....	5
Physical.....	6
Budgetary Offer.....	7
Cisco Packet Tracer Implementation.....	9
Objectives.....	9
Network Topology and Device Placement.....	9
IP Addressing and Interface Configuration.....	11
CLI Configuration.....	12
Explanation of Static Route Commands.....	13
Laptop Manual IP Configuration (Using Packet Tracer Desktop Tab).....	13
VPN Configuration Using Cisco 2811 Routers.....	14
VPN Test and Output Verification.....	16
Full Router Configuration Export.....	18
Optional Task: Dial-Up VPN Setup with Cloud and Teleworker.....	21

Introduction

Objectives

Our primary goal is to design a state-of-the-art IT infrastructure that will facilitate seamless Internet connectivity across all Zytech SA branches, including the new international office. This infrastructure must be robust enough to support a high-speed secure network capable of handling the complex data and communication needs of over a hundred employees. Additionally, we aim to implement solutions that enable efficient remote access, ensuring that teleworkers have reliable and secure connections to the company's central resources. We will also set up dedicated servers for hosting our web services and for printing capabilities, further enhancing our operational efficiency. The main objective is to provide an infrastructure that is not only resilient and secure but also scalable to accommodate future growth and technological advancements.

Constraints

As we chart the course for Noventra SA's IT expansion, we must contend with a set of critical constraints to ensure the success of our implementation. First, we recognize the need to facilitate secure remote access to our internal resources, especially for our foreign branches and teleworkers. This requires a robust VPN solution that adheres to international security standards. We are also faced with the challenge of integrating this extended network into our current LAN configuration while maintaining uninterrupted service. These constraints guide the design of our infrastructure to be highly secure, reliable, and capable of supporting seamless international collaboration. Our commitment is to provide an infrastructure solution that overcomes these constraints and propels Noventra SA into its next phase of growth.

Desired Services

To support the expansion of Noventra SA, our proposal includes the setup and enhancement of the following key services:

- **Internet Access (ISP DHCP):** Reliable and fast internet access provided via Dynamic Host Configuration Protocol to automatically assign IP addresses to all devices on the company's network.
- **Active Directory (AD):** A centralized domain management service that allows managing and storing information about network resources and application data in a distributed database, thus facilitating user logins and access to resources.
- **Domain Name System (DNS):** A scalable service that resolves names to IP addresses, ensuring that network resources are seamlessly accessible to users.
- **Web Server:** A dedicated server for hosting the company's website, ensuring that it is accessible from outside the network and capable of handling the expected traffic.

- **VPN (dial-up and site-to-site):** Virtual Private Network services for secure remote access, allowing encrypted connections between the main office, remote branches, and individual teleworkers.
- **Network Address Translation (NAT):** A method for modifying network address information in the headers of IP datagram packets, allowing devices on a private network to share a single public IP address. .
- **Print Server:** Infrastructure for managing printers and print jobs within the network, enabling employees to efficiently perform printing tasks.
- **File and Storage Services:** Robust solutions for storing, organizing, and sharing files within the company, ensuring that data is accessible only to authorized personnel.

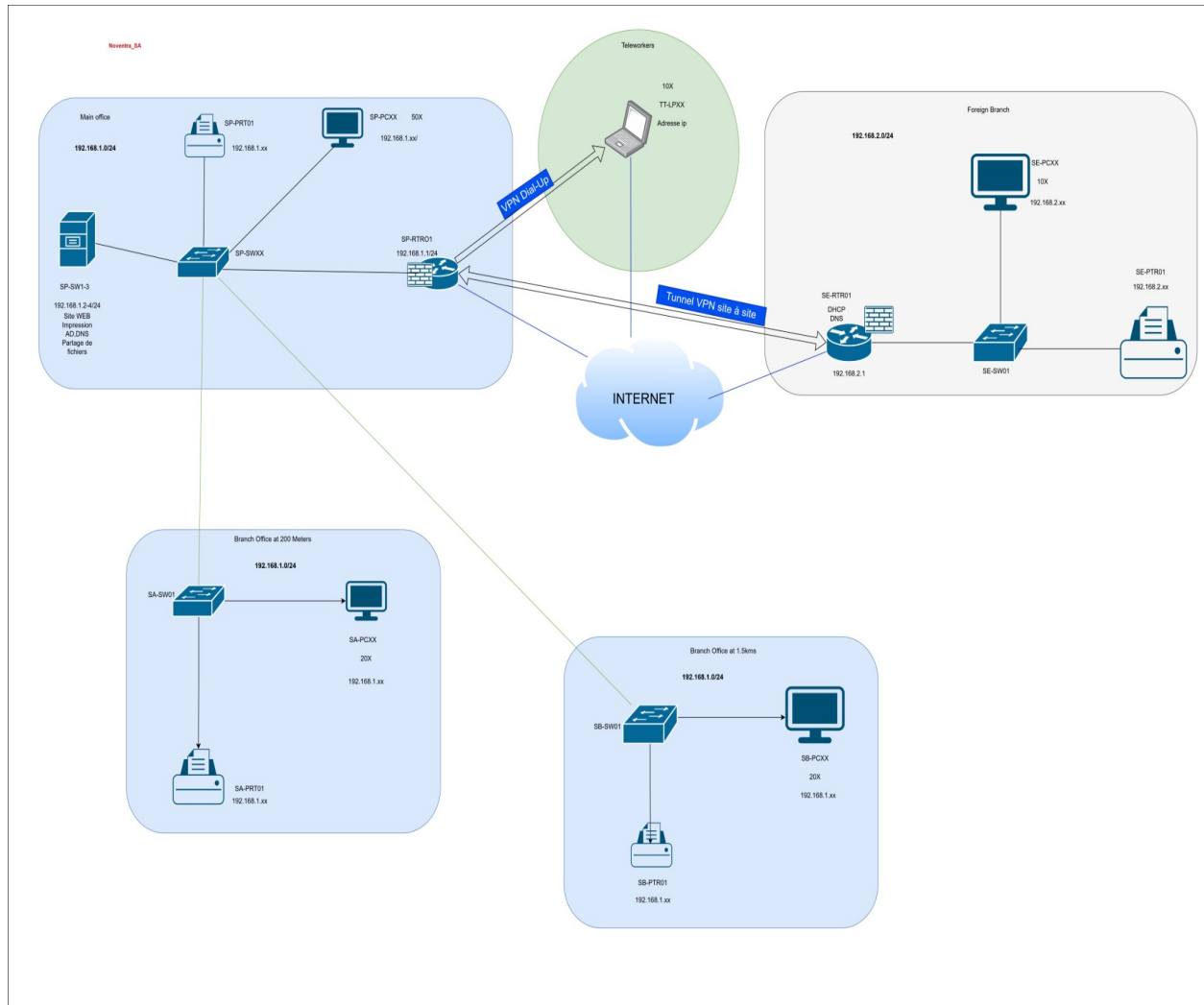
Hardware

The hardware configuration of the enhanced IT infrastructure for Noventra SA is meticulously selected to ensure optimal performance, security, and scalability. It includes:

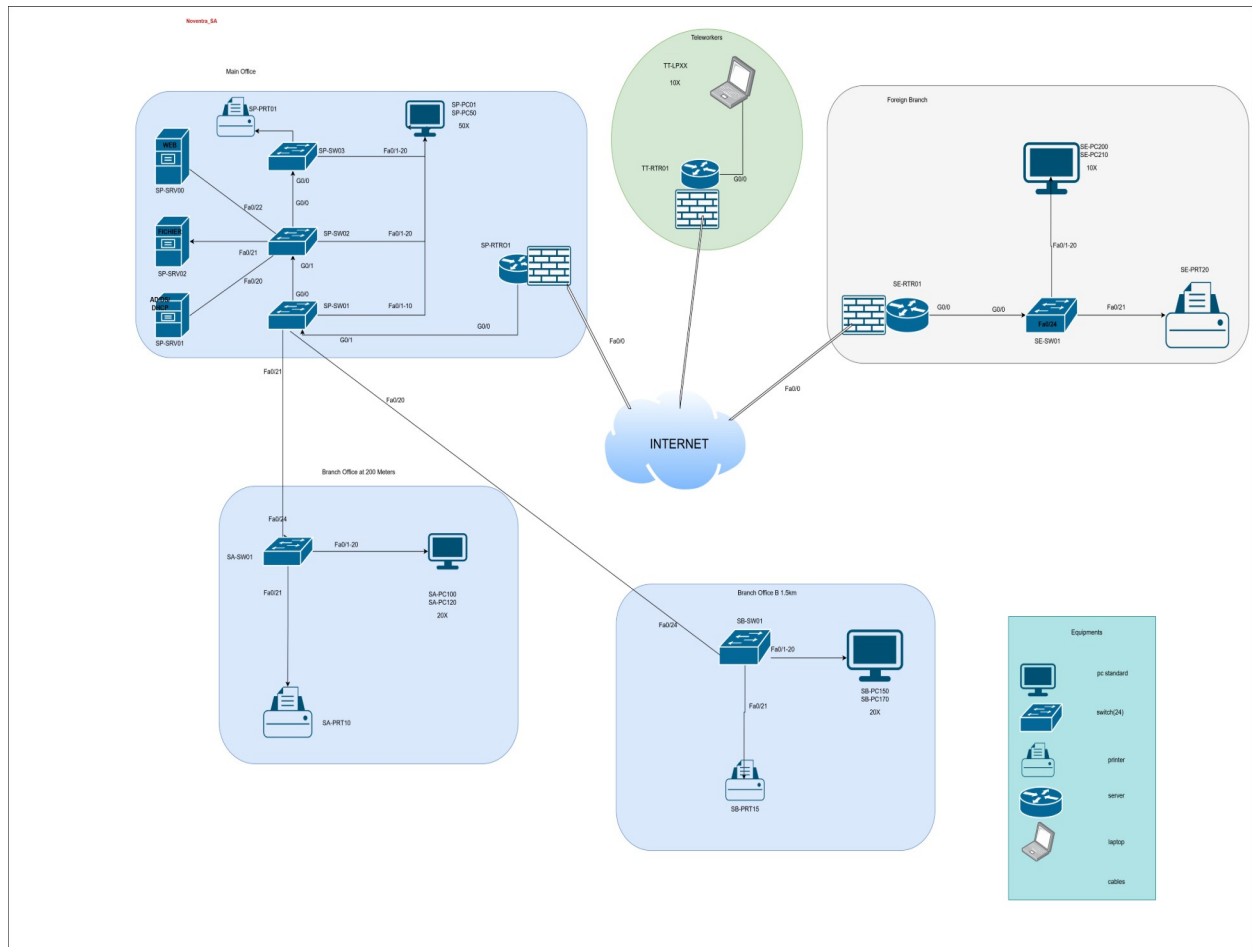
- **Servers:** Utilization of Windows Server 2019 Standard editions, strategically deployed to manage Active Directory services, domain name system management, web hosting, file sharing, and storage management.
- **Routers:** High-performance Cisco routers equipped with SNAT, DNAT, PAT, and PPPoE capabilities to efficiently manage internal and external network traffic.
- **Switches:** A fleet of Cisco switches with 24 ports each, providing fast Ethernet and Gigabit Ethernet interfaces for high-speed internal connectivity.
- **Network Cabinets (Racks):** Durable 19-inch racks to house patch panels, switches, and routers, facilitating organized cable management and easy maintenance.
- **Patch Panels:** To provide a centralized location for all network cables, making it easier to modify the network structure as needed.
- **Computing Devices:** Upgrading desktops and laptops to replace obsolete systems, thereby ensuring all employees have access to modern and efficient workstations.
- **Printers:** Advanced laser printers to meet the company's printing needs with high efficiency and reliability.
- **Cabling:** High-quality single-mode fiber optic cables for long-distance connections between branches and UTP CAT6 cables for reliable and rapid local networking.
- **Additional Equipment:** Extra hardware components to ensure redundancy and business continuity in the event of device failure.

Infrastructure Diagrams

Logical



Physical



Budgetary Offer

Services and Hardware	Quantities	Model	Unit Price	Time/Explanation	Sub-Total
Web Server Installation/Configuration	1		100/h	2h	200*
Installation / Configuration Server (AD, DNS)	3		100/h	3h	300*
Installation of Patch Panel Cabinets (cabling, etc.)	4		150/h	4h/cabinet	2'400*
Router Configuration (sNAT, PAT, PPPoE)	2		100/h	1h/router	200*
Switch Configuration	6		100/h	1h/switch	600*
Operating System Installation	110		100/h	1h/2os	-----
Dial-up VPN Configuration on Router	1		100/h	1h	100*
Configuration VPN site-site sur routeur	1		100/h	1h	100*
Site-to-Site VPN Configuration on Router	10		100/h	5h	500*
Router	2	CISCO Catalyst 8200-1N-4T Routeur	2315		4630*
Switch	6	Cisco 24 Port Rail PoE+ Switch C1000-24P-4G-L	685		4110*
Patch Panel Cabinet	4	Digitus DN-19 32U-6/6-1 Armoire réseau	678		2712*
Patch panel	4	Delock 19" Coupling Patch Panel 24 Port Cat.6	62		248*

Optical Fiber Cable	20	Ubiquiti Netzwerkkabel 100 m	314.-		6280*
GBIC Module High-speed	6	Cisco GLC-LH-SM-RGD, SFP GBIC Modul	852	Optional	-----
RJ45 Patch Cables 10m	100	digitec Ethernet- Patchkabel RJ45 S/FTP, CAT6a, 10 m	19.40		1940*
RJ45 Patch Cables 50cm	10	digitec Ethernet- Patchkabel RJ45 S/FTP, CAT6a, 0.50 m	10.10		101*
Server	3	Cisco UCS C220M4S W/2XE52609V3	3,119		9357*
Printer	4	HP M479fdw Color LaserJet Pro	517		2068*
Complete Computer	100 + 10	Lenovo ThinkStation P3 Tiny i7-13700T 1x16/512GB T400 W11P Intel Core i7-13700T, 16 GB, 512 GB, SSD +Écran, clavier, mause	1182		130020*
Laptop	10	Lenovo ThinkPad E16 Gen 1 16", Intel Core i7- 13700H, 16 Go, 512 Go, CH +empreinte digitale	1000		10000*
Service and Control	1		100/h	Facultatif	---
Total					175866*

The preferred computers will be equipped with Windows 11 Pro pre-installed. If the Enterprise version is required, the computers will be purchased without an operating system and the Enterprise version will then be installed.

Cisco Packet Tracer Implementation

Objectives

This report outlines the step-by-step process of designing and implementing a secure, scalable network for Noventra SA using Cisco Packet Tracer. The main objective is to enable professional internet access, site-to-site VPN communication between remote branches, and secure remote access for teleworkers.

To achieve this, the project involves:

- Selecting appropriate routers (Cisco 2811) for VPN support.
- Configuring IP addressing and routing for internal LAN and WAN segments.
- Establishing a site-to-site IPsec VPN tunnel between the Principal Office (Router0) and the Remote Office (Router2).
- Preparing a secondary task to implement Dial-Up VPN via cloud for remote users.

The report includes CLI configurations, IP schemas, VPN outputs, and a task proposal for cloud-based VPN access to extend real-world scenarios.

Network Topology and Device Placement

The network topology of Noventra SA is designed to reflect a realistic, scalable business environment with both central and remote connectivity. The infrastructure includes a Principal Office, a Remote Branch, and a proposed cloud-based Dial-Up VPN solution for teleworkers.

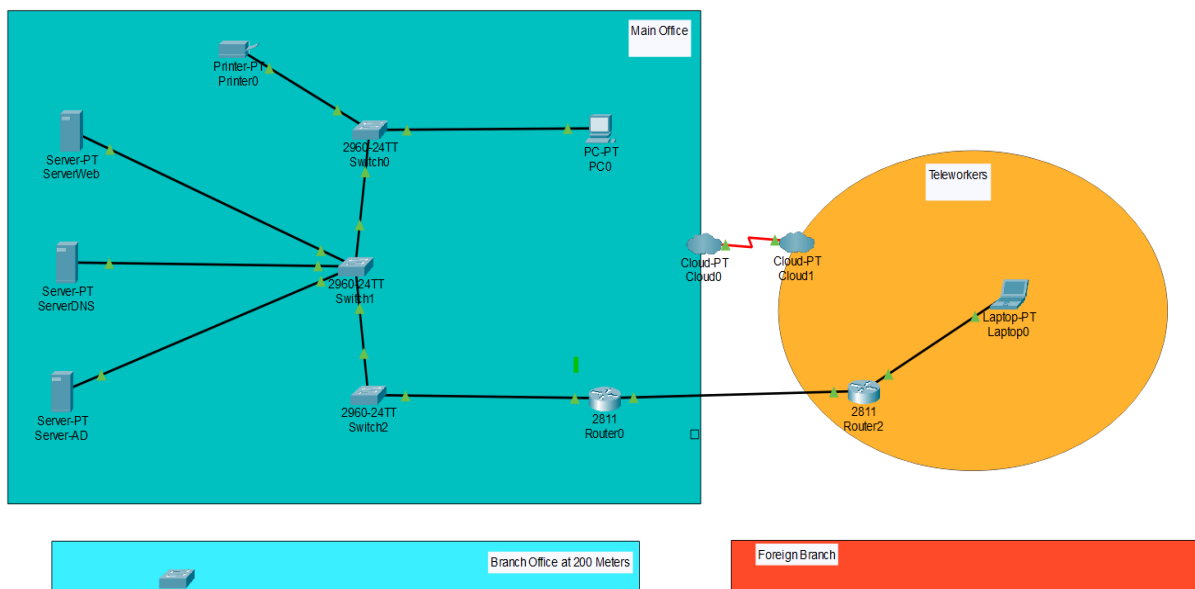
Devices Used in the Topology:

Device Type	Quantity	Purpose / Location
Cisco 2811 Routers	2	VPN-enabled routers for site-to-site connection (Router0 & Router2)
Switches	2	One in each branch, for LAN connectivity
Laptops	2	One in each branch, for user simulation
Clouds	2	Simulated WAN/Internet segments
DSL Modem	1	For Dial-Up VPN task simulation
Optional Server	1	For testing reachability and internal services (DHCP/DNS/Web)

Description of Topology Layout:

- Router0 (Principal Office) is connected to:
 - A local LAN switch
 - A laptop (192.168.1.100)

- FastEthernet0/0 → 192.168.1.1/24 (LAN)
- FastEthernet0/1 → 10.0.0.1/30 (VPN WAN link to Router2)
- Connected to Cloud1 for internet simulation
- Router2 (Remote Office) is connected to:
 - A LAN switch
 - A laptop (192.168.3.2)
 - FastEthernet0/0 → 192.168.3.1/24 (LAN)
 - FastEthernet0/1 → 10.0.0.2/30 (VPN WAN link to Router0)
 - Connected to Cloud2 for dial-up VPN testing scenario
- Cloud1 ↔ Cloud2 are connected using a serial or Ethernet link to simulate WAN communication.



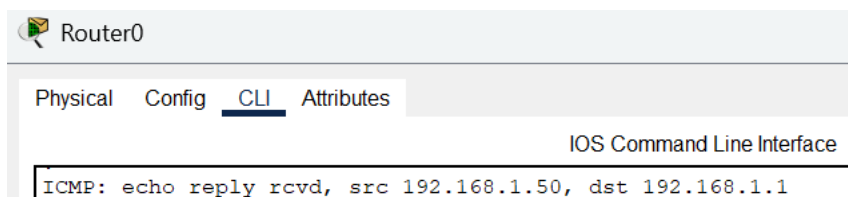
IP Addressing and Interface Configuration

This section provides detailed information about the IP addressing scheme and interface-level configurations performed on both Cisco 2811 routers. Static IP addressing has been used to maintain control over routing and ensure VPN compatibility.

IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Purpose
Router0	FastEthernet0/0	192.168.1.1	255.255.255.0	LAN (Principal Office)
	FastEthernet0/1	10.0.0.1	255.255.255.252	VPN link to Router2
PC0	NIC	192.168.1.100	255.255.255.0	Host in Principal Office
Router2	FastEthernet0/0	192.168.3.1	255.255.255.0	LAN (Remote Office)
	FastEthernet0/1	10.0.0.2	255.255.255.252	VPN link to Router0
Laptop1	NIC	192.168.3.2	255.255.255.0	Host in Remote Office

All configurations below were performed on Cisco 2811 routers using the Command Line Interface (CLI) within Cisco Packet Tracer.



```
enable>configure terminal>show running-config
```

This command provides a complete view of all current settings, including IP addresses, interfaces, routing, and VPN configurations.

CLI Configuration

All of the following commands were entered via the CLI terminal of Router0 in Cisco Packet Tracer.

Router0 (PrincipalRouter)

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
interface FastEthernet0/1
ip address 10.0.0.1 255.255.255.252
no shutdown
ip route 192.168.3.0 255.255.255.0 10.0.0.2
exit
write memory
```

Router2

```
interface FastEthernet0/0
ip address 192.168.3.1 255.255.255.0
no shutdown
interface FastEthernet0/1
ip address 10.0.0.2 255.255.255.252
no shutdown
ip route 192.168.1.0 255.255.255.0 10.0.0.1
exit
write memory
```

Explanation of Static Route Commands

In both routers, a **static route** was configured to enable communication between the two LANs (192.168.1.0/24 and 192.168.3.0/24) over the VPN link. Without these routes, the routers would not know how to reach the network that is not directly connected to them.

On Router0:

```
ip route 192.168.3.0 255.255.255.0 10.0.0.2
```

This command tells **Router0**:

"To reach the 192.168.3.0/24 network (the remote office LAN), send traffic to the next hop IP address 10.0.0.2" (which is the FastEthernet0/1 interface of Router2).

Since 192.168.3.0 is not directly connected to Router0, this static route forwards matching packets across the VPN tunnel via the WAN interface.

On Router2:

```
ip route 192.168.1.0 255.255.255.0 10.0.0.1
```

This command tells **Router2**:

"To reach the 192.168.1.0/24 network (the principal office LAN), send traffic to the next hop IP address 10.0.0.1" (which is the FastEthernet0/1 interface of Router0).

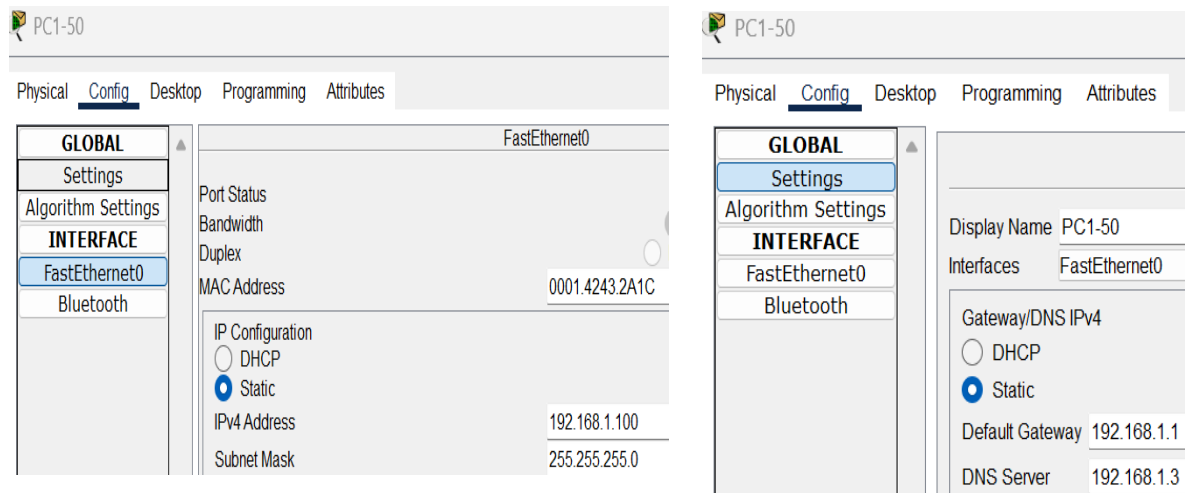
This ensures return traffic from the remote office can find its way back to the main office network.

These two static routes are essential for **bidirectional communication** between the two LANs. They work together with VPN policies to ensure that encrypted traffic is routed correctly through the tunnel.

Laptop Manual IP Configuration (Using Packet Tracer Desktop Tab)

Configuration was done manually via the **Desktop → IP Configuration** tab in Packet Tracer.

- **PC (Principal Office):**
 - IP Address: 192.168.1.100
 - Subnet Mask: 255.255.255.0
 - Default Gateway: 192.168.1.1
- **Laptop1 (Remote Office):**
 - IP Address: 192.168.3.2
 - Subnet Mask: 255.255.255.0
 - Default Gateway: 192.168.3.1



VPN Configuration Using Cisco 2811 Routers

To ensure secure communication between the main office and the remote branch, an **IPsec VPN tunnel** is established using **Cisco 2811 routers**. The configuration includes ISAKMP policy definition, IPsec transform sets, access-lists for interesting traffic, and the application of crypto maps on the WAN interfaces.

All configurations were performed in CLI mode inside Cisco Packet Tracer.

Step 1: ISAKMP Configuration (IKE Policy)

Defines **Phase 1** of VPN negotiation using AES encryption, pre-shared key authentication, and Diffie-Hellman Group 2.

- The pre-shared key (mykey123) must match on both routers.
- The address indicates the peer IP.

On **Router0**:

```
crypto isakmp policy 1
```

```
encr aes
```

```
authentication pre-share
```

```
group 2
```

```
crypto isakmp key mykey123 address 10.0.0.2
```

On Router2:

```
crypto isakmp policy 1
  encr aes
  authentication pre-share
  group 2
crypto isakmp key mykey123 address 10.0.0.1
```

Step 2: Define IPsec Transform Set

Both routers: `crypto ipsec transform-set myset esp-aes esp-sha-hmac`

Specifies how traffic will be encrypted (AES) and authenticated (SHA-HMAC) in Phase 2.

Step 3: Create Access Lists for "Interesting Traffic"

On Router0: `access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255`

On Router2: `access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255`

These ACLs define which traffic should be encrypted. Only traffic between the two LANs will go through the VPN tunnel.

Step 4: Apply Crypto Map

On Router0:

```
crypto map mymap 10 ipsec-isakmp
  set peer 10.0.0.2
  set transform-set myset
  match address 100
interface FastEthernet0/1
  crypto map mymap
```

On Router2:

```
crypto map mymap 10 ipsec-isakmp
  set peer 10.0.0.1
  set transform-set myset
  match address 100
interface FastEthernet0/1
  crypto map mymap
```

crypto map binds all the previous elements together: peer IP, transform set, and ACL.

It is applied to the external interface (WAN) where the VPN tunnel will be built.

Step 5: Static Routing (Recap)

As explained in Section 3, these commands ensure traffic between the two LANs is routed correctly:

- On Router0:
ip route 192.168.3.0 255.255.255.0 10.0.0.2
- On Router2:
ip route 192.168.1.0 255.255.255.0 10.0.0.1

Once these steps are completed, an IPsec VPN tunnel will be successfully established between the two routers.

VPN Test and Output Verification

To validate that the IPsec VPN tunnel between **Router0** and **Router2** is working correctly, we used a combination of ping tests and show crypto diagnostic commands.

```
router#ping 192.168.1.1
-----
Router#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

The ping from **Router2** (192.168.3.1) to **Router0** (192.168.1.1) was **successful**, with 100% reply rate.

This confirms basic Layer 3 connectivity and that traffic between the local subnets is flowing properly through the VPN tunnel.

ISAKMP SA Status : show crypto isakmp sa

```
PrincipalRouter#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
10.0.0.2     10.0.0.1     QM_IDLE        1099      0  ACTIVE
IPv6 Crypto ISAKMP SA
```

QM_IDLE (Quick Mode Idle): VPN Phase 2 is successfully established.

ACTIVE: The ISAKMP (IKE) session is up and operational.

This means that the tunnel negotiation was successful using the correct policies and pre-shared key.

IPsec SA Status : show crypto ipsec sa

```
PrincipalRouter#show crypto ipsec sa
interface: FastEthernet0/1
  Crypto map tag: mymap, local addr 10.0.0.1

  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.1.0/255.255.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 10.0.0.2 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 22, #pkts encrypt: 22, #pkts digest: 0
    #pkts decaps: 22, #pkts decrypt: 22, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 10.0.0.1, remote crypto endpt.:10.0.0.2
    path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
    current outbound spi: 0xC2E23C7B(3269606523)
```

These values confirm that real encrypted traffic is being passed through the VPN tunnel.

encaps and encrypt represent packets sent *through the VPN tunnel*.

decaps and decrypt represent packets received *from the other side of the VPN tunnel*.

Important Note:

These packets are **not normal ICMP pings**, but specifically the encrypted VPN traffic flowing between the private subnets 192.168.1.0/24 and 192.168.3.0/24 — as defined in the access list (access-list 100).

However, local traffic exchanged between end devices within the same subnet (e.g., between two PCs behind Router0, or between Router0 and a local server) does not pass through the VPN tunnel and therefore is not counted in these VPN packet statistics.

As a result, values like:

- #pkts encaps:
- #pkts encrypt:
- #pkts decaps:
- #pkts decrypt:

represent only the IP packets that were encrypted, tunneled, and decrypted between the two routers — not internal subnet communication.

Full Router Configuration Export

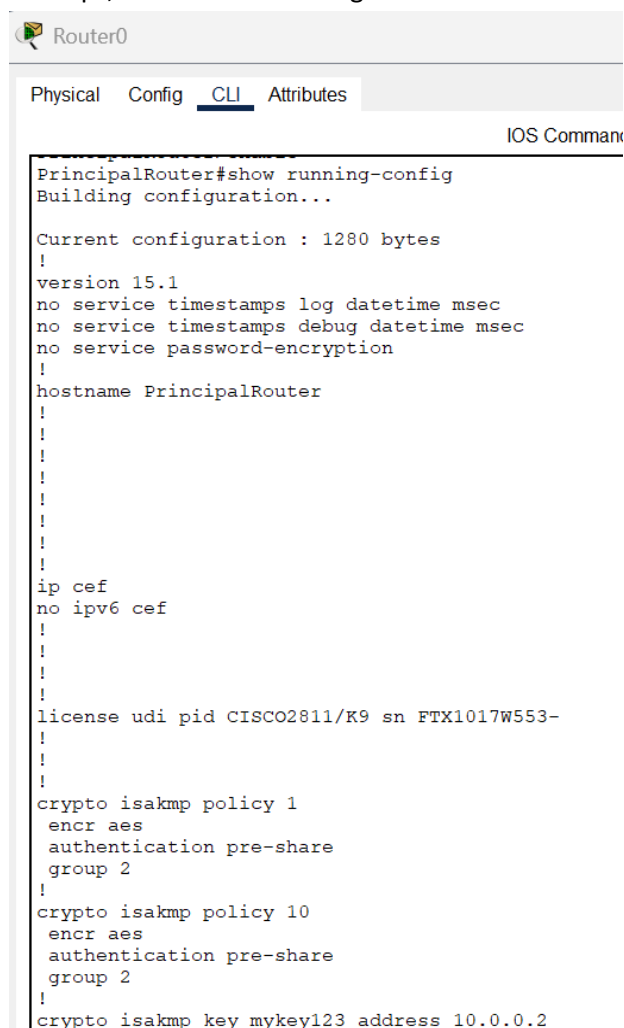
At this stage of the project, I would like to share the complete CLI configuration of the main router (Router0) for documentation and reproducibility purposes. This configuration reflects all essential elements such as:

- IP address assignments
- Static routing
- VPN (ISAKMP and IPsec) parameters
- Access control lists
- Interface settings
- Crypto map application

You can retrieve the full configuration of any router in Cisco Packet Tracer (or on a real device) using the following command in privileged EXEC mode:

```
router> enable -> Router# show running-config
```

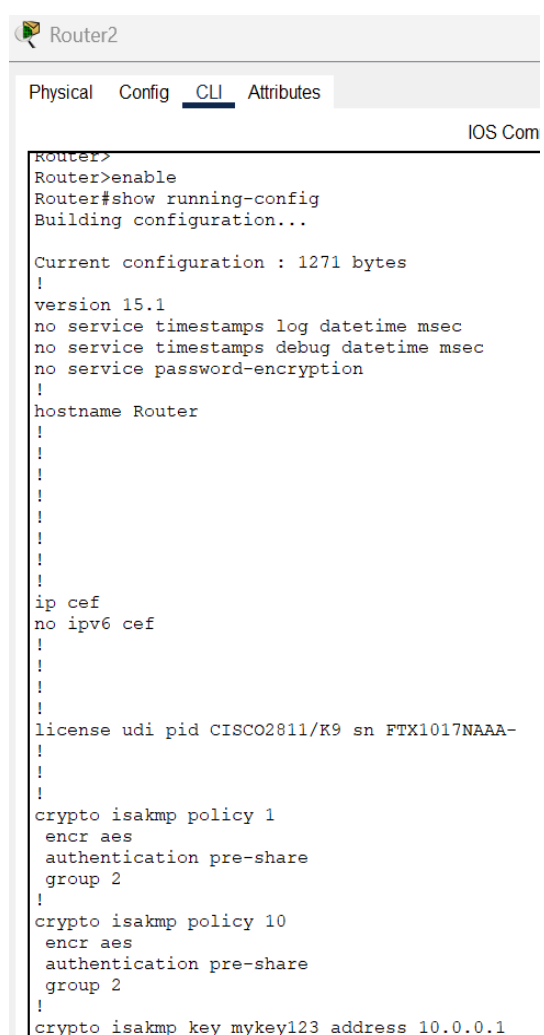
This command displays the entire active configuration of the router, which includes all interface settings, security policies, routing rules, and VPN definitions. It is extremely useful for auditing, backups, and troubleshooting.



The screenshot shows the CLI window for Router0. The tabs at the top are Physical, Config, CLI (selected), and Attributes. The text 'IOS Command' is visible in the top right corner. The command 'PrincipalRouter#show running-config' has been entered, and the output shows the current configuration, which is 1280 bytes. The configuration includes version 15.1, service timestamps, hostname PrincipalRouter, IP CEF, license information, and two ISAKMP policies with AES encryption and pre-share authentication. The first policy is for address 10.0.0.2.

```
PrincipalRouter#show running-config
Building configuration...

Current configuration : 1280 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname PrincipalRouter
!
!
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2811/K9 sn FTX1017W553-
!
!
!
crypto isakmp policy 1
  encr aes
  authentication pre-share
  group 2
!
crypto isakmp policy 10
  encr aes
  authentication pre-share
  group 2
!
crypto isakmp key mykey123 address 10.0.0.2
```



The screenshot shows the CLI window for Router2. The tabs at the top are Physical, Config, CLI (selected), and Attributes. The text 'IOS Com' is visible in the top right corner. The command 'Router#show running-config' has been entered, and the output shows the current configuration, which is 1271 bytes. The configuration includes version 15.1, service timestamps, hostname Router, IP CEF, license information, and two ISAKMP policies with AES encryption and pre-share authentication. The first policy is for address 10.0.0.1.

```
Router#show running-config
Building configuration...

Current configuration : 1271 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2811/K9 sn FTX1017NAAA-
!
!
!
crypto isakmp policy 1
  encr aes
  authentication pre-share
  group 2
!
crypto isakmp policy 10
  encr aes
  authentication pre-share
  group 2
!
crypto isakmp key mykey123 address 10.0.0.1
```

```
PrincipalRouter>enable

PrincipalRouter#show running-config
Building configuration...
Current configuration : 1280 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname PrincipalRouter
!
ip cef
no ipv6 cef
!
license udi pid CISCO2811/K9 sn FTX1017W553-
!
crypto isakmp policy 1
  encr aes
  authentication pre-share
  group 2
!
crypto isakmp policy 10
  encr aes
  authentication pre-share
  group 2
!
crypto isakmp key mykey123 address 10.0.0.2
!
crypto ipsec transform-set myset esp-aes esp-sha-hmac
!
crypto map mymap 10 ipsec-isakmp
  set peer 10.0.0.2
  set transform-set myset
  match address 100
!
spanning-tree mode pvst
!
interface FastEthernet0/0
  ip address 192.168.1.1 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 10.0.0.1 255.255.255.252
```

```
duplex auto
speed auto
crypto map mymap
!
interface Serial0/3/0
no ip address
clock rate 2000000
!
interface Serial0/3/1
no ip address
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 192.168.3.0 255.255.255.0 10.0.0.2
!
ip flow-export version 9
!
access-list 100 permit ip 192.168.1.0 0.0.0.255 any
access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
end
PrincipalRouter#
```

- crypto isakmp policy and transform-set blocks define the VPN protocols.
- crypto map applies the VPN settings to interface Fa0/1, which connects to the peer router.
- Static route ip route 192.168.3.0 255.255.255.0 10.0.0.2 ensures traffic to the remote LAN is forwarded into the tunnel.
- Access-list 100 ensures only LAN-to-LAN traffic is encrypted.

Optional Task: Dial-Up VPN Setup with Cloud and Teleworker

In addition to the site-to-site IPsec VPN tunnel, an optional scenario is proposed to support remote workers via Dial-Up VPN through a simulated cloud environment. This model is useful for employees working from home or in the field.

Topology Overview

The following components are added to the network:

Cloud0 & Cloud1: Simulated internet via Packet Tracer's Cloud device.

Router0: Still acts as the VPN server.

Router2: Replaced by a teleworker laptop connected via an intermediate router and a Cloud.

Laptop (Teleworker): A client device that initiates VPN connection using the Desktop → VPN tab.

Physical Connection Guide

Device	Interface Used	Cable Type	Notes
Router0	Fa0/1	Copper Straight	Connect to Cloud0 → Ethernet6
Cloud0	Ethernet6	---	Connects to Router0
Cloud0	Serial0	DCE	Connects to Cloud1 → Serial0
Router2	Fa0/1	Copper Straight	Connect to Cloud1 → Ethernet6
Laptop	NIC	Copper Straight	Connect to Router2 → Fa0/0

Note: Cloud's Ethernet6 interface must be manually enabled (Config tab), and Serial ports must be DCE/DTE paired correctly.

VPN Setup (on Laptop)

Navigate to **Desktop → VPN Configuration** tab and enter:

- **Group Name:** MyVPNGroup
- **Group Key:** mykey123
- **Host IP (Server IP):** 10.0.0.1
- **Username:** user1
- **Password:** pass1

Server-Side Configuration (on Router0)

The following should be added in addition to existing site-to-site VPN setup:

```
crypto isakmp client configuration group MyVPNGroup
```

```
key mykey123
```

```
dns 192.168.1.1
```

```
domain noentra.local
```

```
pool VPN-POOL
```

```
ip local pool VPN-POOL 192.168.xx.xx 192.168.xx.xx
```

```
username user1 password pass1
```