[UNIVERSIDAD TECNOLOGICA NACIONAL]

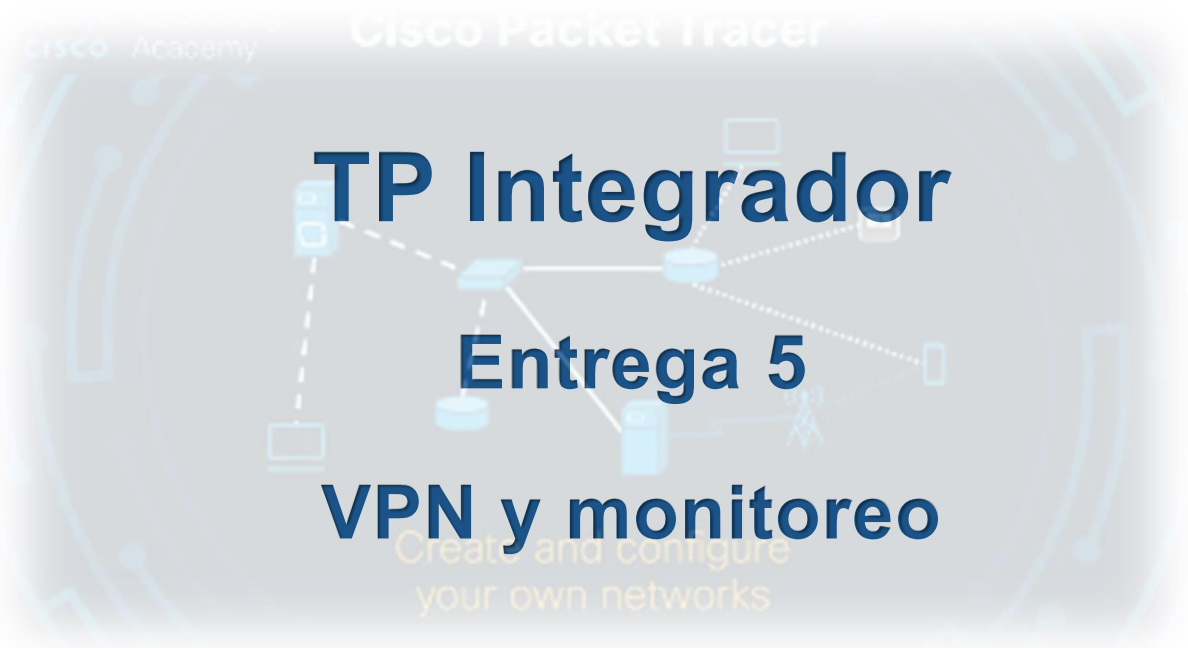
[FACULTAD REGIONAL DELTA]

Carrera: Ing. Sistemas de información

Materia: Redes de datos

Profesor: Ing. Juan Antonio González

Docente Laboratorio: Ing. Carlos José Alberto Carrizo



TP Integrador

Entrega 5

VPN y monitoreo

Alumna:

Apellido y Nombre	legajo
Enriquez, Sylvina	

Curso: 2025

Contenido

CONSIGNA TRABAJO PRÁCTICO INTEGRADOR

Tema: **Diseño y Configuración de red de un DATACENTER**

Objetivo General

El objetivo de este trabajo práctico es que los estudiantes diseñen y configuren una red para un DATACENTER estándar en Cisco Packet Tracer. El diseño debe incluir redundancia en la conectividad a internet mediante dos ISP y dar servicio de DHCP, DNS, WWW y monitoreo mediante SNMP.

El trabajo se desarrollará en **5 entregas parciales**, cada una acumulando sobre la anterior, hasta lograr una red operativa, segura y documentada.

Escenario: Se debe diseñar un nuevo DATACENTER que cumpla con los siguientes requerimientos mínimos:

- La red tenga **alta disponibilidad**, conectada a 2 ISP.
- Exista segmentación interna en **4 VLANs** (Aplicaciones, Producción, Administración y Producción).
- Los servicios **DHCP, DNS, Web interno y SNMP** estén correctamente configurados y accesibles.
- Se implementen **medidas de seguridad** (ACLs, SSH) y conectividad remota segura mediante **VPN**.

Herramienta:

- **Cisco Packet Tracer**.

Criterios generales de aprobación:

- Cumplimiento funcional de cada etapa.
- Buena documentación y evidencias (capturas, pruebas de conectividad, descripciones claras).
- Organización y claridad en la configuración.

💡 **Tip:** Piensa cada entrega como un "módulo" que, al final, ensamblará la red completa.

Entregas (en etapas)

Cada entrega debe incluir:

o Archivo .pkt de Cisco Packet Tracer.

o Informe técnico con capturas, configuraciones y justificación de decisiones.

Entrega 5 – VPN y Monitoreo

🎯 **Objetivo:** Configurar VPN de acceso remoto y SNMP básico.

Pasos:

1. Configurar túnel VPN IPSec entre Router ISP y Router Corporativo.
2. Validar el envío de paquetes encriptados a través del túnel.
3. Configurar servidor SNMP y agentes en los dispositivos de red.
4. Validar status de interfaces desde Browser MIB.

Checklist:

✅ VPN activa.

✅ SNMP configurado.

✅ Browse MIB.

Desarrollo del trabajo práctico integrador

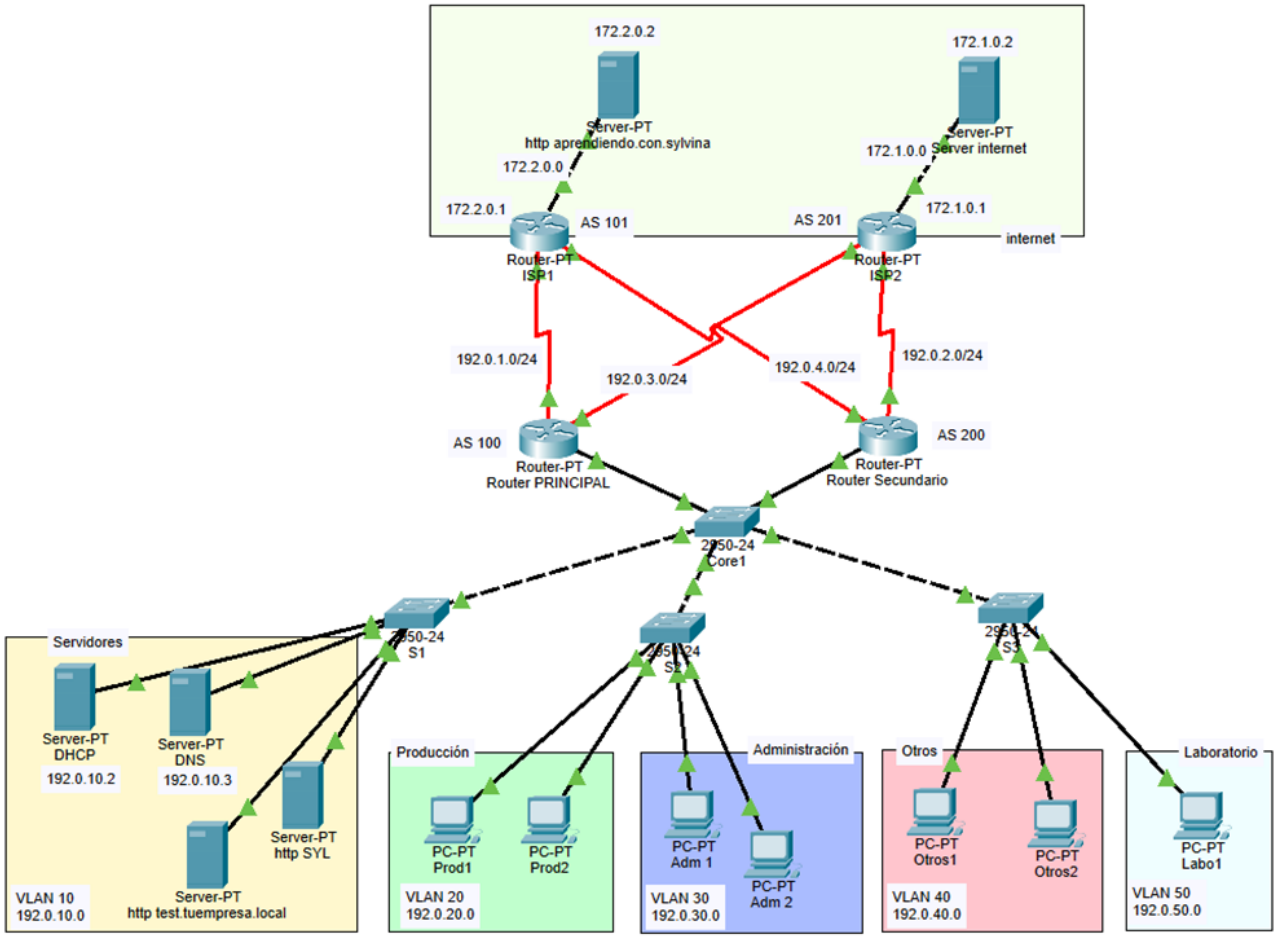
ENTREGA 5 – VPN y monitoreo

Objetivo: Configurar VPN de acceso remoto y SNMP básico

Diseño en Packet Tracer

Para realizar los requerimientos de esta nueva entrega se usa, como base el diseño final de la cuarta entrega.

Diseño INICIAL:



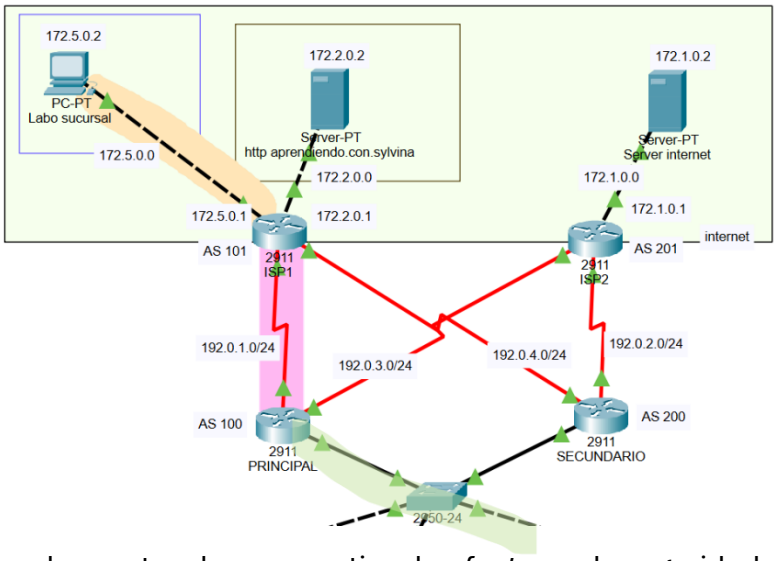
1. Configurar túnel VPN IPSec entre Router ISP y Router Corporativo.

Una VPN es una red virtual privada que utiliza internet (un medio inseguro) para realizar una transferencia de paquetes con seguridad. Es una herramienta que encripta la conexión a internet y, de esta manera, se puede enviar paquetes en forma segura y privada, evitando que terceros espíen estas actividades. Para esto vamos a utilizar IPSec, que es la seguridad del protocolo de internet.

Para llevar a cabo una VPN se utiliza un "túnel" que hace que el tráfico de paquetes sea seguro. Existen dos tipos de túneles VPN

a) Punto a punto
b) Cliente-servidor

Para el desarrollo de este trabajo práctico se utilizará el tipo "punto a punto". Esta conexión se realizará entre los routers ISP1 y los dos frontera (para el diagrama realizado en las entregas anteriores, existe una comunicación cruzada entre los routers frontera y los de ISP). Además, se agregará una red en el router ISP1 para responder a la consigna planteada en clases de permitir que una red pase por el túnel mientras que la otra no.



Antes de configurar los routers hay que activar los *features* de seguridad. Con *show ver* se puede observar si están activados o no:

```
Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      disable       None          None
uc            disable       None          None
data          disable       None          None

Configuration register is 0x2102
```

Están desactivadas. Se activan con el comando:

R1(config)# ***license boot module c2900 technology-package securityk9***

Esto debe observarse y/o configurarse en cada router que intervendrán en el *túnel*.

```
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]: yes
```

Ejecutando, nuevamente, el comando *show ver*:

```
-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      disable       None          securityk9
uc            disable       None          None
data          disable       None          None

Configuration register is 0x2102
```

Una vez que están configuradas las *features* de seguridad, se deben **reiniciar los modems** *(reload* en modo privilegiado).

Existen dos fases a ejecutar:

- **Fase 1**: IKE (intercambio de claves): se utiliza para autenticar los dispositivos y negociar los parámetros de seguridad para crear un canal seguro de gestión de claves.

  Router(config)# ***crypto isakmp policy 10***
  Router(config-isakmp)# ***encr aes***
  Router(config-isakmp)# ***hash sha***
  Router(config-isakmp)# ***authentication pre-share***
  Router(config-isakmp)# ***group 2***
  Router(config-isakmp)# ***lifetime 86400***
  Router(config)# ***crypto isakmp key cisco123 address 100.0.0.1*** (esta dirección IP sería la que está en el otro extremo de la conexión)
  Router(config)# ***access-list 110 permit ip 10.0.0.0 0.255.255.255 192.168.40.0 0.0.0.25***

  Para limitar el acceso al túnel, creo la lista ACL 110 que solo permita el paso de paquetes desde y hacia VLAN 50 (Laboratorio) con la PC de Laboratorio de la sucursal.

  En router PRINCIPAL:

  access-list 110 permit ip 192.0.50.0 0.0.0.255 172.5.0.0 0.0.0.255

  Solo permite el paso de los paquetes desde la VLAN 50 (Laboratorio) hacia la red de Laboratorio de la sucursal.

  En router ISP1:

  access-list 110 permit ip 172.5.0.0 0.0.0.255 192.0.50.0 0.0.0.255

  Solo permite el paso de los paquetes desde la red de Laboratorio de la sucursal hacia la VLAN 50 (Laboratorio).

- **Fase 2**: Ipsec: Establecer el túnel de datos que protegerá el tráfico entre las redes.

  Router(config)# ***crypto ipsec transform-set TS esp-aes esp-sha-hmac***
  Router(config)# ***crypto map CMAP 10 ipsec-isakmp***
  Router(config-crypto-map)# ***set peer 100.0.0.1*** (interfaz extremo opuesto)
  Router(config-crypto-map)# ***set transform-set TS***
  Router(config-crypto-map)# ***match address 110***

  En esta red las interfaces utilizadas para conectar el túnel son de tipo *serial*:

  Router frontera:

  R(config)# ***interface se 0/0/1***
  R(config-if)# ***crypto map CMAP***

  Router IPS1:

  R(config)# ***interface se 0/0/0***
  R(config-if)# ***crypto map CMAP***

El comando ***match address 110*** hace referencia a la ACL 110 (declaradas previamente)

2. Validar el envío de paquetes encriptados a través del túnel.

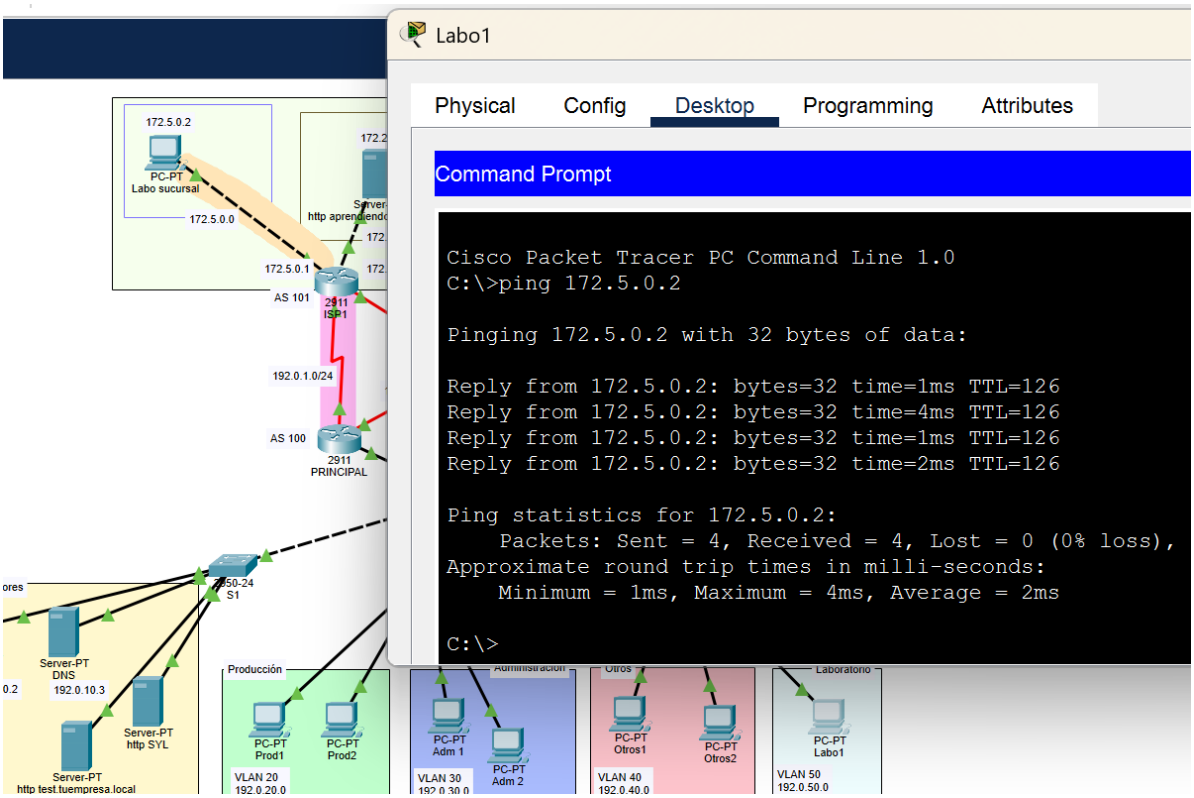
Para validar los envíos, primero se realiza una captura de pantalla antes de hacer las conexiones (pings) correspondientes para mostrar la encriptación del túnel.

ISP1# ***show crypto ipsec sa***

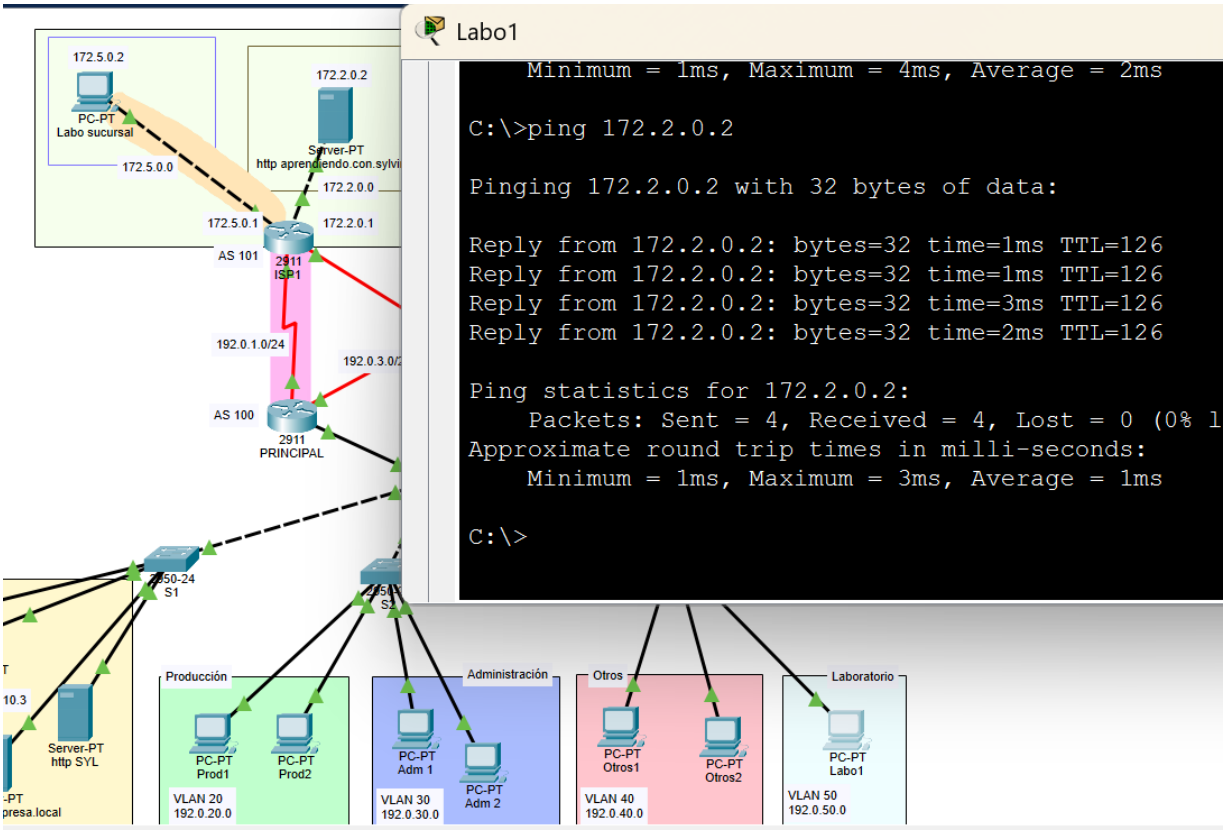
```
PRINCIPAL#show crypto ipsec sa

interface: Serial0/0/1
    Crypto map tag: CMAP, local addr 192.0.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.0.30.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.5.0.0/255.255.255.0/0/0)
   current_peer 192.0.1.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #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.: 192.0.1.1, remote crypto endpt.:192.0.1.2
```

```
ISP1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: CMAP, local addr 192.0.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.5.0.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port):
(192.0.30.0/255.255.255.0/0/0)
   current_peer 192.0.1.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #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
```

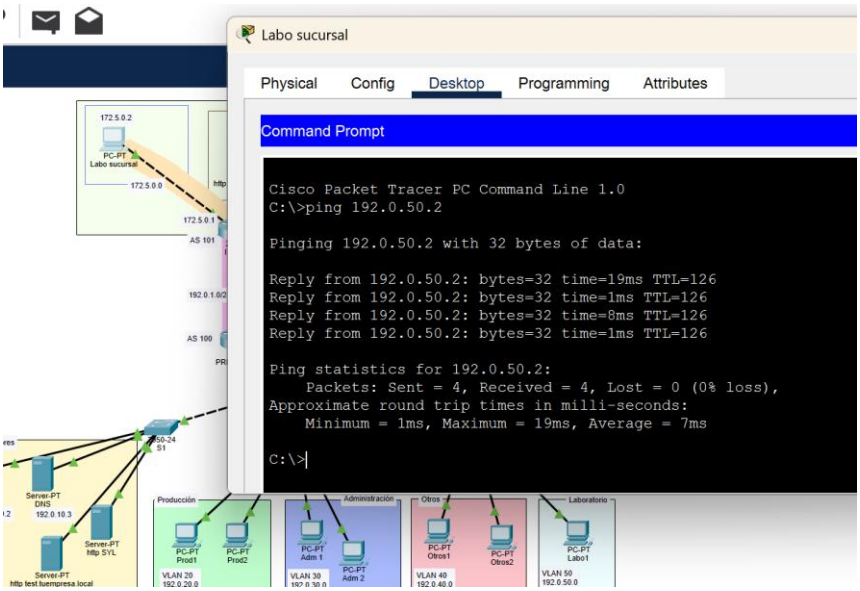
Se hace *ping* desde la PC de laboratorio (VLAN 50) hacia el área Laboratorio de la sucursal en forma exitosa:



y desde la misma PC hacia el server de internet:



Conexión desde PC Labo sucursal hacia la PC de la VLAN 50:



*ISP1# **show crypto ipsec sa:***

```
ISP1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: CMAP, local addr 192.0.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.5.0.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.0.50.0/255.255.255.0/0/0)
   current_peer 192.0.1.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 2, #pkts decrypt: 2, #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.: 192.0.1.2, remote crypto endpt.:192.0.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x93BC57D3(2478594003)

     inbound esp sas:
```

```
PRINCIPAL#show crypto ipsec sa

interface: Serial0/0/1
    Crypto map tag: CMAP, local addr 192.0.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.0.50.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.5.0.0/255.255.255.0/0/0)
   current_peer 192.0.1.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #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 1, #recv errors 0

     local crypto endpt.: 192.0.1.1, remote crypto endpt.:192.0.1.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/1
     current outbound spi: 0x1EBDC8CA(515754186)

     inbound esp sas:
      spi: 0x93BC57D3(2478594003)
```

Se puede observar que solo dos paquetes pasaron por el túnel. El *ping* que se dirigió desde PC Labo al server NO fue encriptado (no pasó por el túnel)

3. Configurar servidor SNMP y agentes en los dispositivos de red.

SNMP (Simple Network Management Protocol) es un protocolo que permite gestionar los equipos que están conectados en la red.

Este protocolo tiene una estructura basada en ***agentes*** instalados y un equipo que ejerce el rol de NMS que se encarga de conectar a los distintos agentes para recopilar información que estos proporcionan. Esta información se registra en una base de datos llamada ***MIB***.

Las órdenes básicas de SNMP son:

- *GetRequest*
- *GetNextRequest*
- *SetRequest*
- *GetBulkRequest*
- *Trap*

Para que los equipos sean monitoreados hay que configurar los mismos:

Router(config)# ***snmp-server community redes_ro ro*** (ro: read only)
Router(config)# ***snmp-server community redes_rw rw*** (rw: read and write)

4. Validar status de interfaces desde Browser MIB.

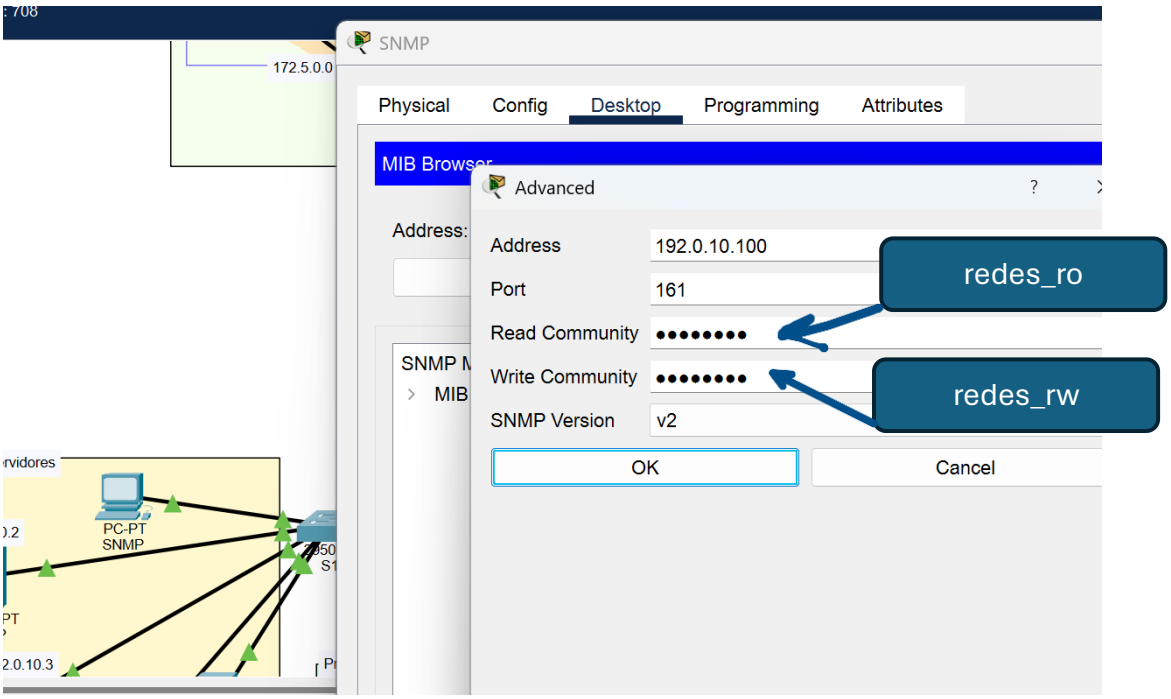
Para ver las líneas que tienen la palabra SNMP se utiliza el siguiente comando:

show running | include snmp

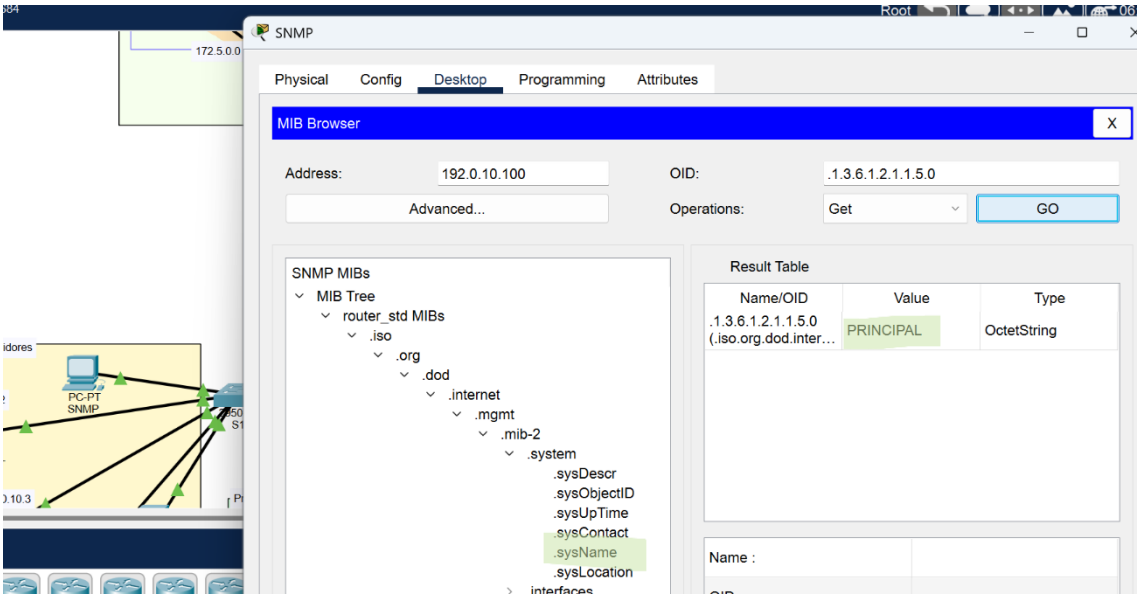
```
PRINCIPAL#show running | include snmp
snmp-server community redes_ro RO
snmp-server community redes_rw RW

SECUNDARIO#show running | include snmp
snmp-server community redes_rw RW
snmp-server community redes_ro RO

CORE#show running | include snmp
snmp-server community redes_ro RO
snmp-server community redes_rw RW

S1#show running | include snmp
snmp-server community redes_ro RO
snmp-server community redes_rw RW

S2#show running | include snmp
snmp-server community redes_ro RO
snmp-server community redes_rw RW

S3#show running | include snmp
snmp-server community redes_ro RO
snmp-server community redes_rw RW
```

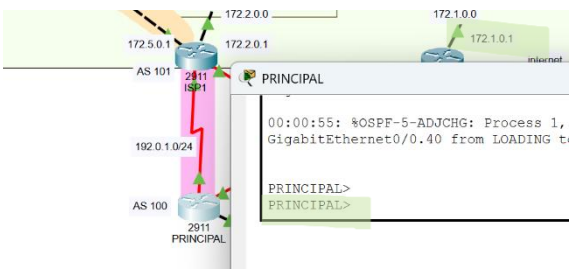
Ahora voy a acceder a los dispositivos a través de la PC conectada (agregada) a la VLAN 10, que se utilizará solamente para monitorear.

Puntualmente, en este caso, monitoreo el router PRINCIPAL, (se puede acceder desde la dirección IP 192.0.10.100):

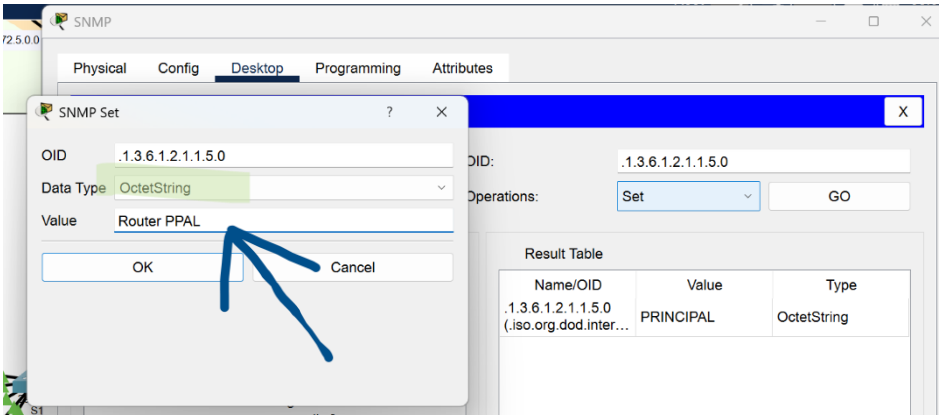


Accedo a ver el nombre del router:

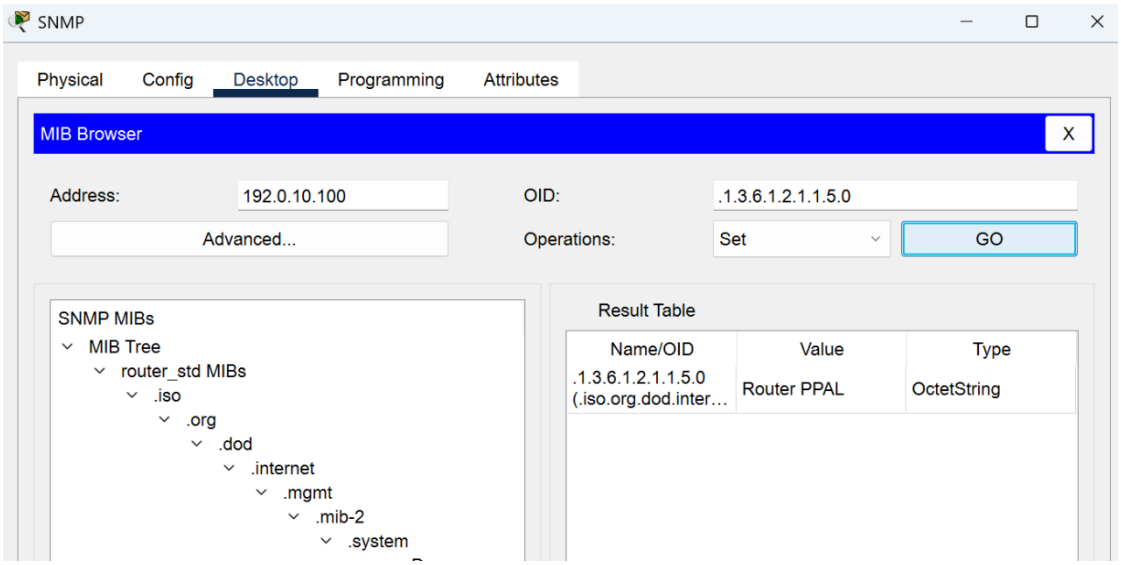


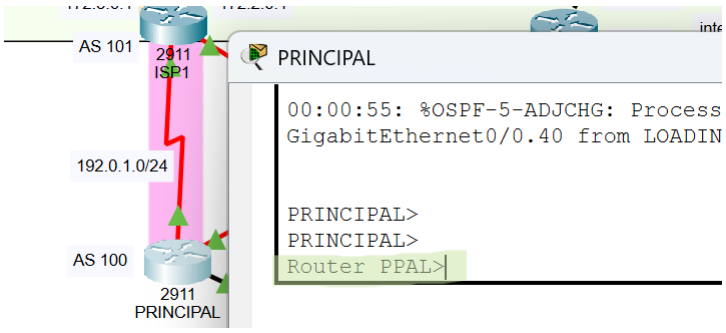


A continuación, accedo al router y le cambio el nombre a ***Router PPAL***

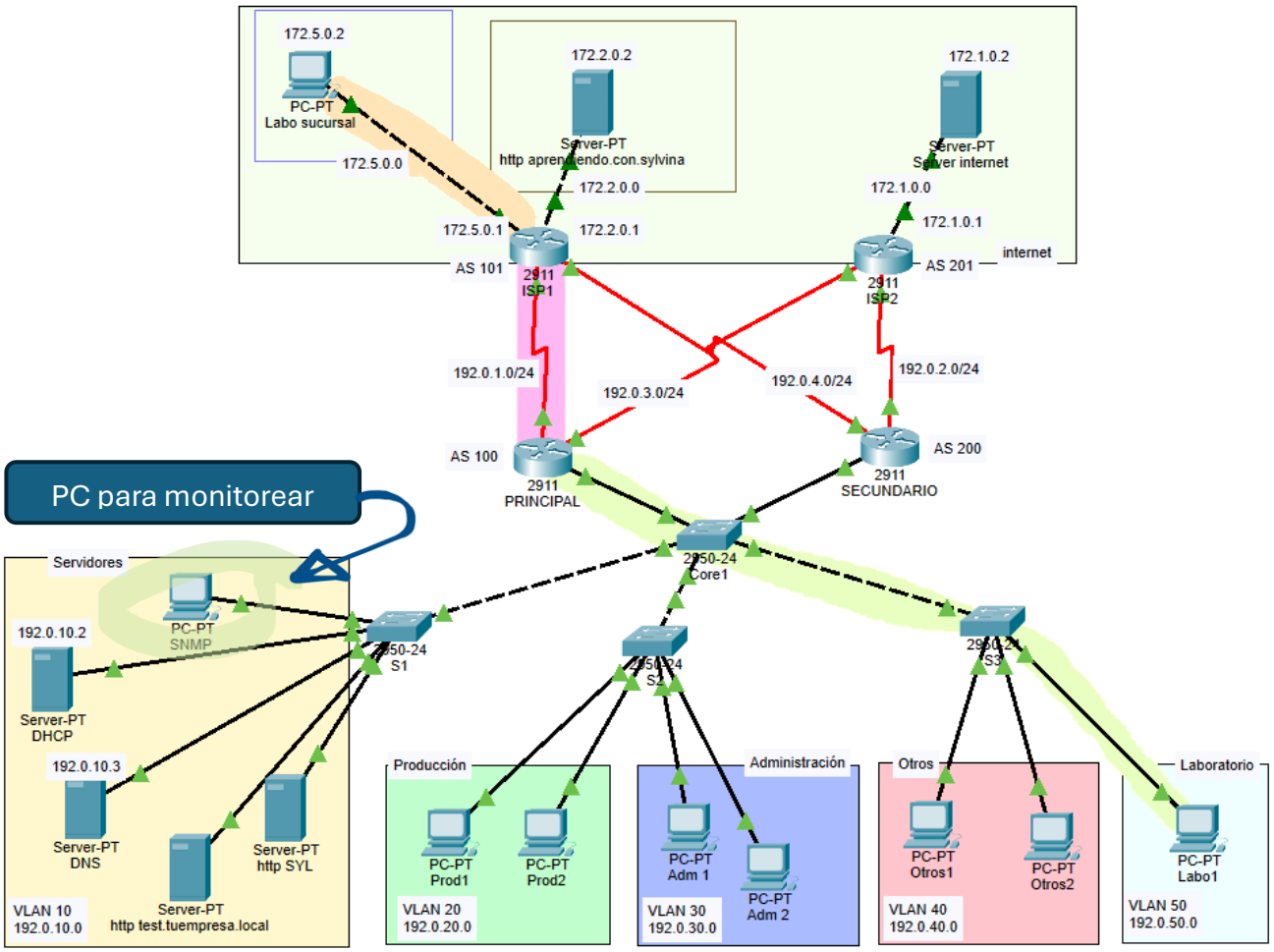


Cambio el nombre. Primero dar OK en donde indica la flecha azul y después *go* indicado con la flecha verde:





5. Configuración final de la red:



6. Conclusiones

Con el desarrollo de esta quinta entrega del trabajo práctico integrador se presentó un gran desafío: cambiar los cuatro routers utilizados. Esto se debió a que el diagrama lo hice con routers del tipo **Router-PT** pero resulta que este tipo de routers, en Packet tracer, no soporta **isakmp.** Esto me presentó un desafío de tener que cambiar los routers y volver a configurar los cuatro con los protocolos e interfaces que ya había elegido. Pero lo realicé y pude continuar con el desarrollo de esta última entrega.

Me resultó muy interesante observar cómo pasan los paquetes encriptados cuando la lista de acceso indica que debe utilizar el túnel creado.

Por otro lado, me resultó, también MUY INTERESANTE poder observar cómo poder monitorear los dispositivos de la red, pudiendo observar varias configuraciones y hasta realizar cambios.

Realizar todo el trabajo práctico, con sus distintas etapas, me permitió volcar, en un ejemplo práctico, todo lo aprendido en la teoría, de una forma muy dinámica fijando más los conocimientos adquiridos.

7. Claves

Router PRINCIPAL	→ enable: facundo
	→ para acceder al router en forma remota SSH: cisco
Router SECUNDARIO	→ enable: facundo
	→ para acceder al router en forma remota SSH: sylvina
Switch (todos)	→ enable: sylvina
	→ para acceder al router en forma remota SSH: facundo