[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 4

Seguridad y ACL

Alumna:

Apellido y Nombre	legajo
Enriquez, Sylvina	

Curso: 2025

Índice etapa 4

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 4 – Seguridad y ACL

🎯 **Objetivo:** Implementar ACLs, SSH y contraseñas seguras.

Pasos:

1. ACL bloquea la conectividad entre VLAN Otros y VLAN Servidores (Excepto el servicio Web).
2. Habilitar SSH en routers y switches.
3. Asegurar contraseñas.

Mini-desafío extra: ACL que solo deje ping hacia VLAN servidores desde VLAN Producción.

Checklist:

✅ ACL correctas.

✅ SSH operativo.

✅ Contraseñas seguras.

DESARROLLO DEL TRABAJO PRÁCTICO INTEGRADOR

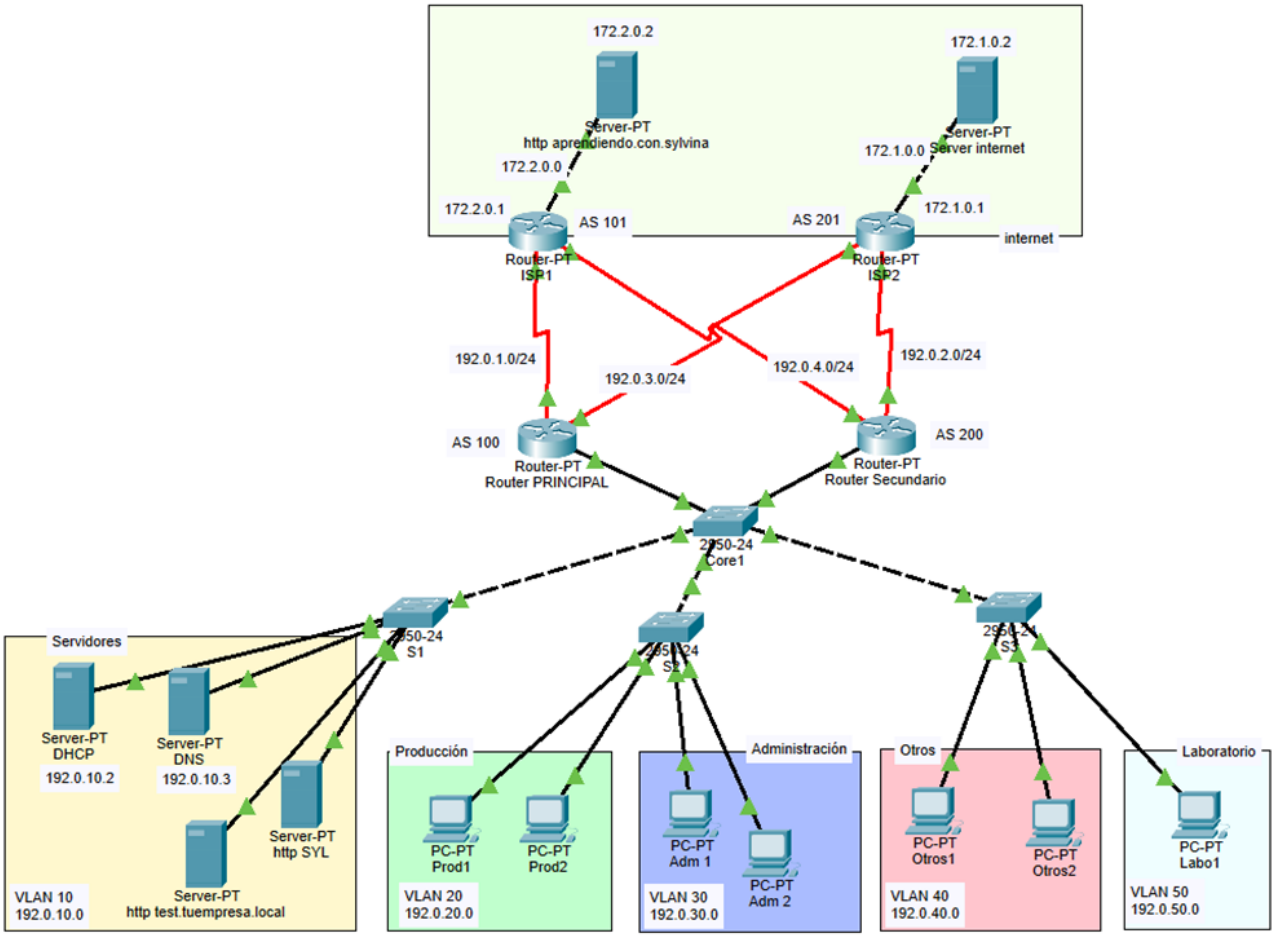
ENTREGA 4 – Seguridad y ACL

Objetivo: Implementar ACLs, SSH y contraseñas seguras.

1. Diseño en Packet Tracer

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

Diseño INICIAL:



2. ACL bloquea la conectividad entre VLAN Otros y VLAN Servidores (Excepto el servicio Web).

Una lista de control de acceso (ACL) es un filtro de paquetes que se crean en los routers que deniega o permite el pase en la interfaz según algunas reglas que se deben especificar (IP y puertos).

Existen dos tipos de listas de acceso:

- **Standard**: Para permitir o denegar el pase con reglas solo de una dirección IP:
  - *Router(config)# **access-list [número 1/99] [permit/deny] [número de IP] [wilcard]***
- **Extended**: Para permitir o denegar el pase con reglas con direcciones IP y/o puertos:
  - *Router(config)# **access-list [número 100/199] [permit/deny] [protocolo] [número de IP origen] [wilcard] [número de IP destino] [wilcard] eq [Num Puerto destino]***
  - ***eq** y **Num Puerto destino** son opcionales. Si se utiliza protocolo IP no hay que agregarlos.*
  - *http: protocolos TCP y UDP, puerto 80*
  - *ping: protocolo IMCP (sin especificación de puerto)*
  - *FTP: protocolo TCP, puertos 29 y 21*

Existen algunos "**comodines**" para reemplazar algunas direcciones y/o especificaciones:

- Si la regla se aplica a un host específico se puede reemplazar IP + wilcard escribiendo ***host Núm IP.***
- Si la regla aplica a cualquier dirección IP, se puede utilizar "any" para reemplazar IP+Wildcard

La creación de la ACL se realiza en modo configuración. El listado de listas creadas se puede ver estando en modo privilegiado.

Para aplicar ACL a una interfaz se debe ingresar al modo configuración de la misma:

- *Router(config)# **int Fa0/0***
- *Router(config-if)# **ip access-group [número lista 1/99] [in/out]***

  In: indica que la regla aplica a los paquetes entrantes

  Out: indica que la regla aplica a los paquetes salientes

Siempre hay que recordar que, por defecto, hay una regla final que deniega todo, por lo que, si no se desea que eso suceda, hay que agregar la regla ***permit any***.

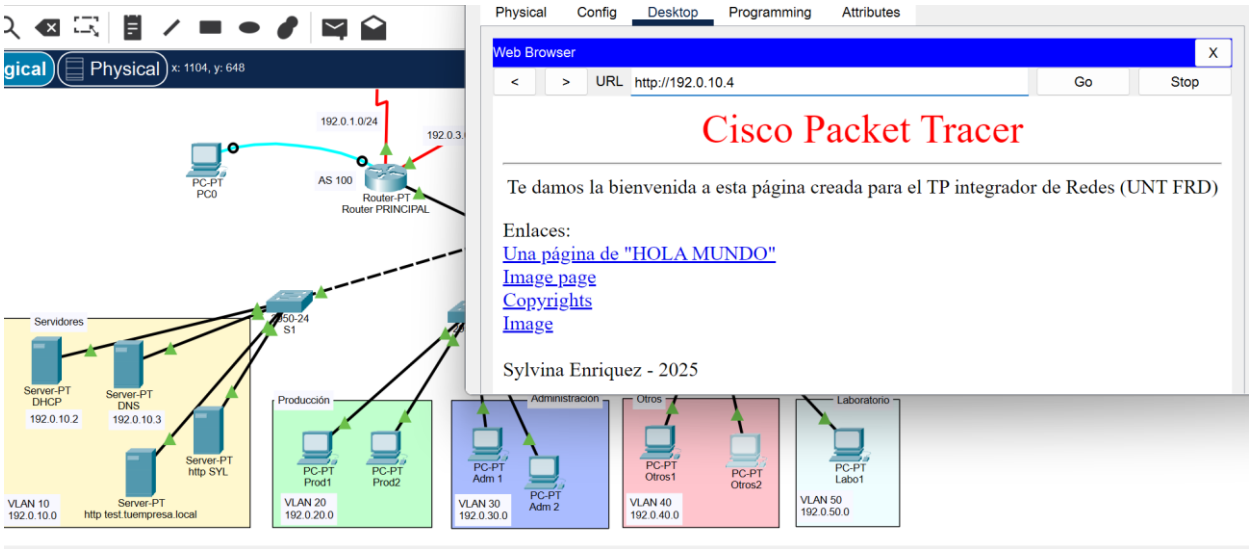
La lectura de las reglas es "top-down" por lo que una vez que encuentra una regla, se ejecuta y sale de la lista. Por este motivo es que hay que escribir primero, el permiso de uso del servicio web y luego bloquear la conectividad entre VLANs Otros y Servidores. Como por defecto la última regla deniega el resto de los accesos, no es necesario escribir otra regla.

```
show access-list
Extended IP access list 100
    10 permit tcp 192.0.40.0 0.0.0.255 192.0.10.0 0.0.0.255 eq www
    20 permit udp 192.0.40.0 0.0.0.255 192.0.10.0 0.0.0.255 eq www
    30 deny ip 192.0.40.0 0.0.0.255 192.0.10.0 0.0.0.255
    40 permit ip any any (1 match(es))
```

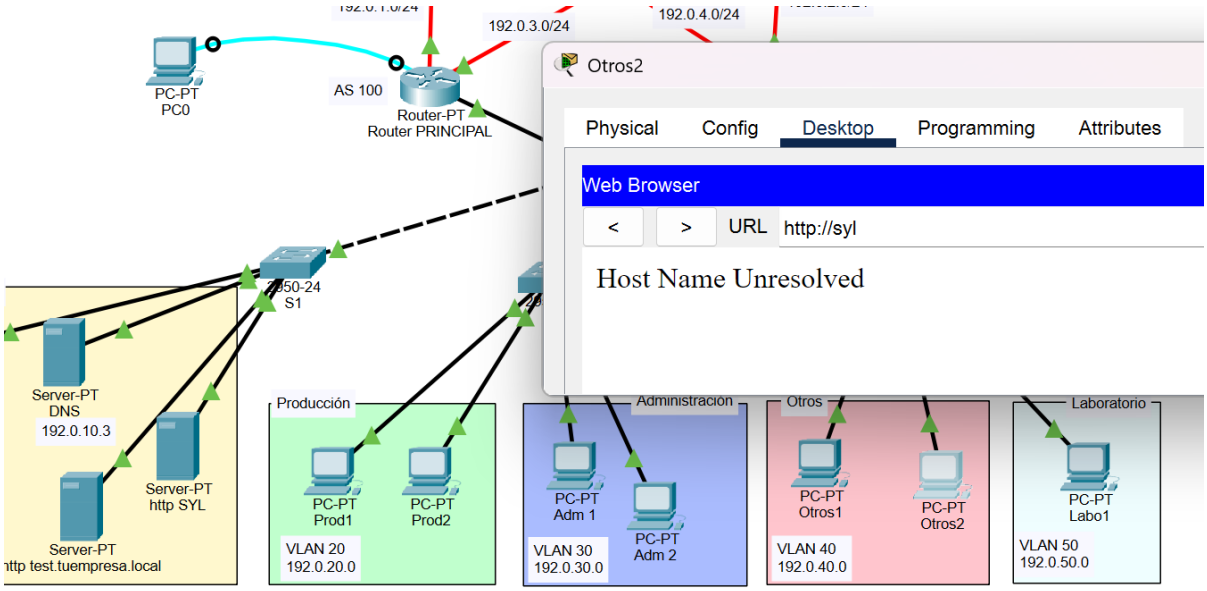
Se asigna a la interfaz correspondiente:

```
RouterPRINCIPAL#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
RouterPRINCIPAL(config)#int fa0/0.40
RouterPRINCIPAL(config-subif)#ip access-group 100 in
RouterPRINCIPAL(config-subif)#
```

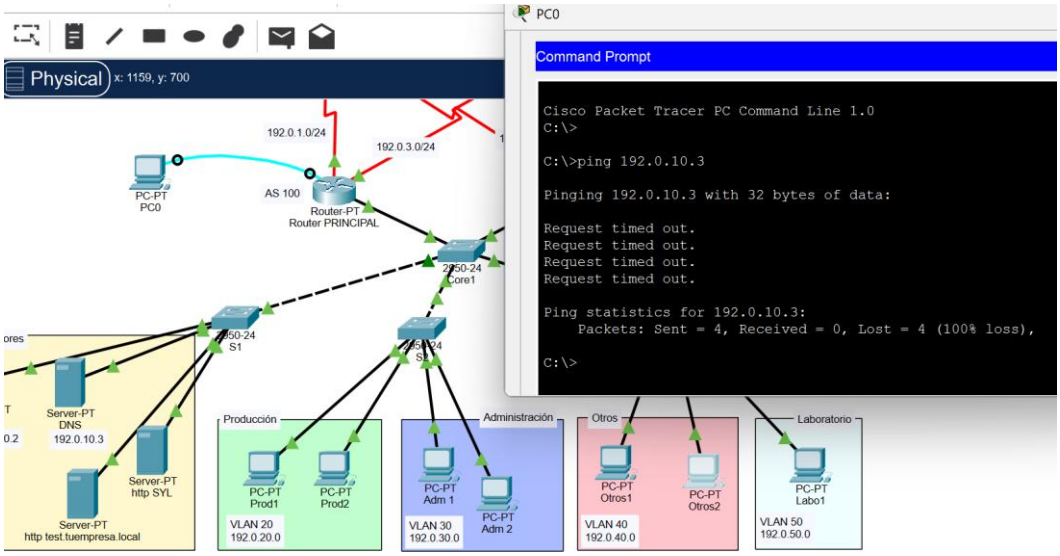
Uso del servicio web desde PC Otros 2:



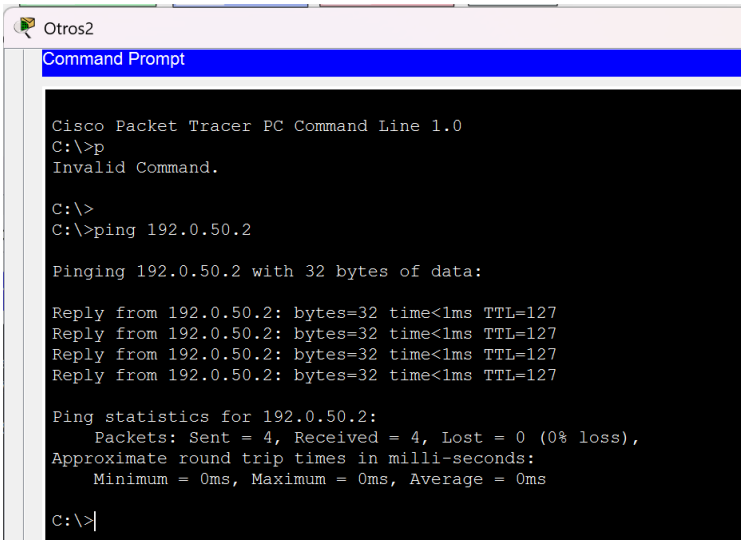
Pero no se puede utilizar el servicio DNS desde PC Otros 2:



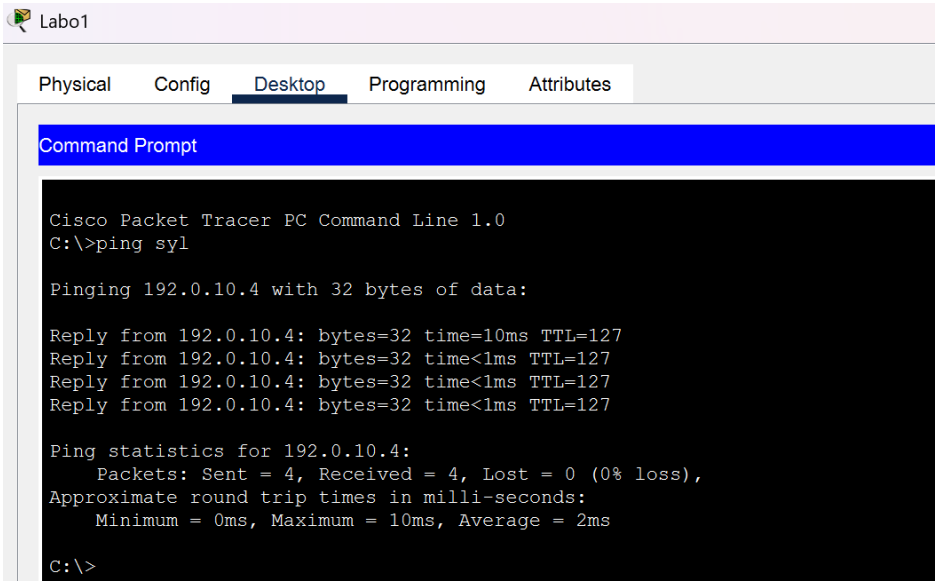
Tampoco se puede conectar desde PC Otros 2 hacia 192.0.10.3 con un ping:



pero se puede conectar PC Otros 2 con PC Labo1:



y PC Labo1 con 192.0.10.3, mediante el uso de DNS:



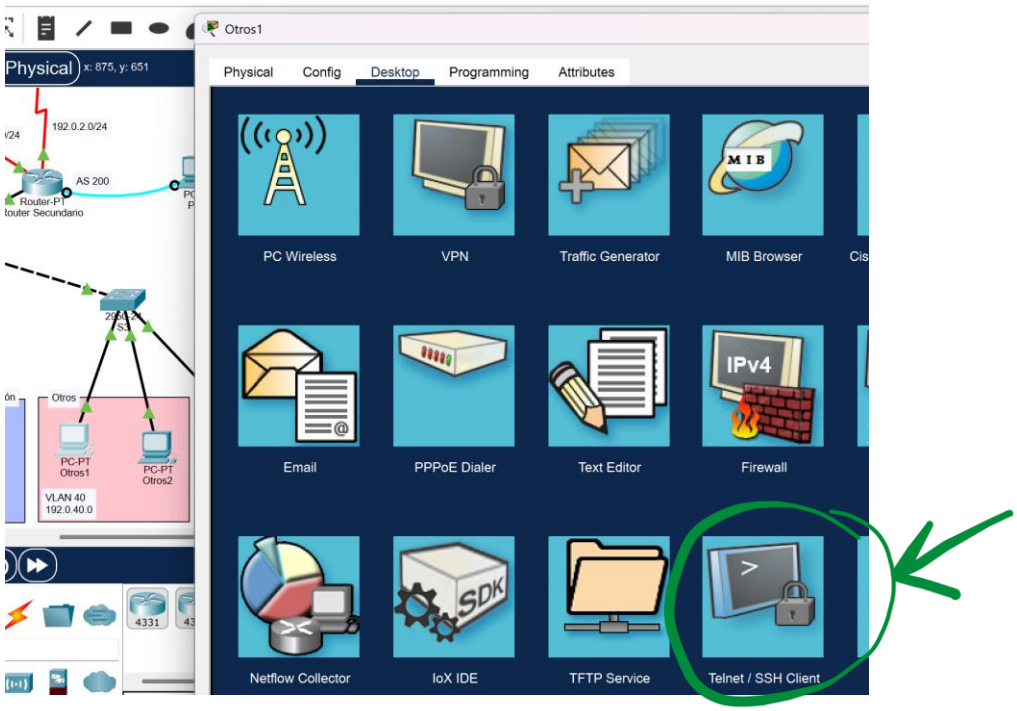
3. Habilitar SSH en routers y switches.

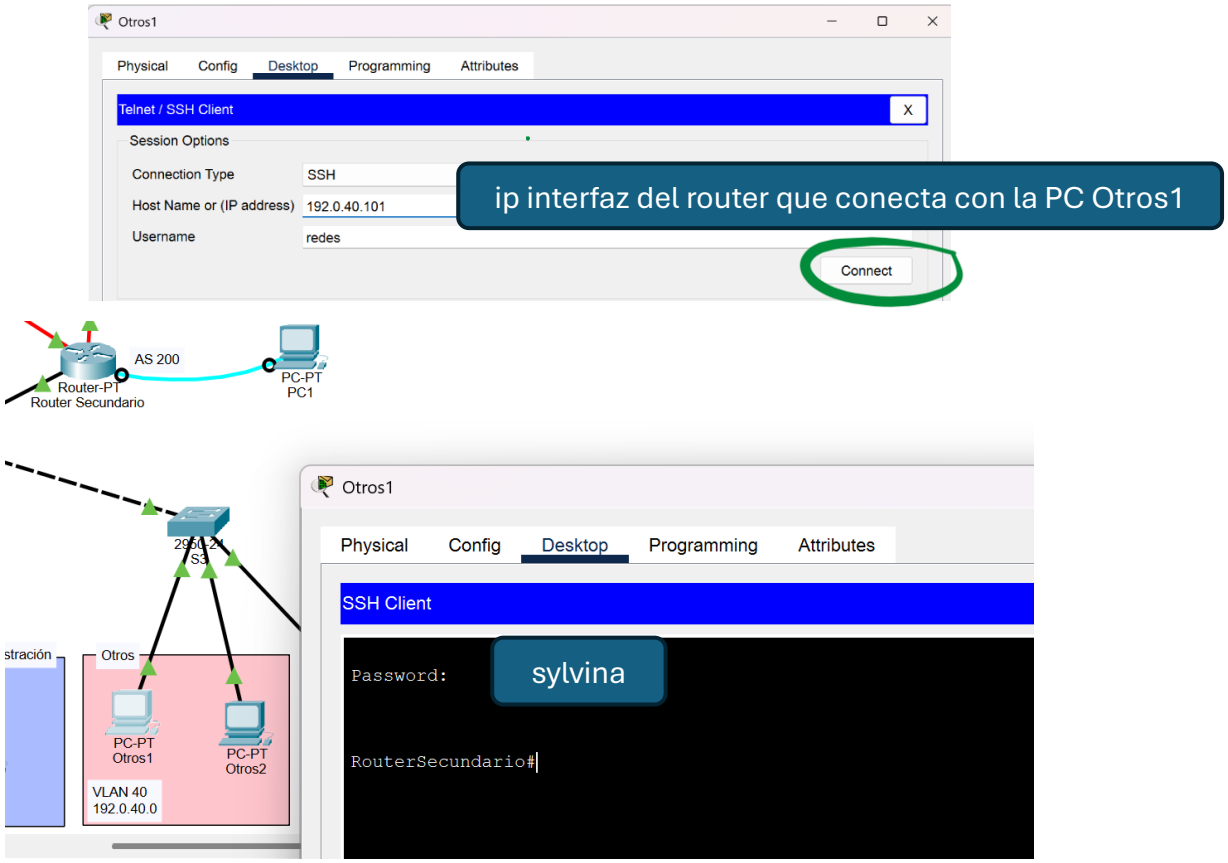
Para habilitar el protocolo SSH (creando conexiones cifradas para el acceso remoto seguro) en un switch o en un router, se debe:

- Configurar un nombre de host (ya está hecho en otra entrega)
- Generar claves SSH RSA
- Establecer un nombre de dominio
- Crear un usuario local
- Configurar las líneas VTY para que utilicen el protocolo SSH y el método login local.

*RouterSecundario#**conf ter***
*RouterSecundario(config)#**ip domain-name sylvina.com***
*RouterSecundario(config)#**crypto key generate rsa***
*How many bits in the modulus [512]: **1024***
*RouterSecundario(config)#**ip ssh version 2***
*RouterSecundario(config)#**line vty 0*** → 0: admite solo un acceso a la vez
*RouterSecundario(config-line)#**transport input ssh***
*RouterSecundario(config-line)#**login local***
*RouterSecundario(config-line)#**username redes privilege 15 password sylvina***
*RouterSecundario(config)#**enable secret facundo***

Luego de guardar la configuración en el router, intento acceder desde una PC de la VLAN 40:





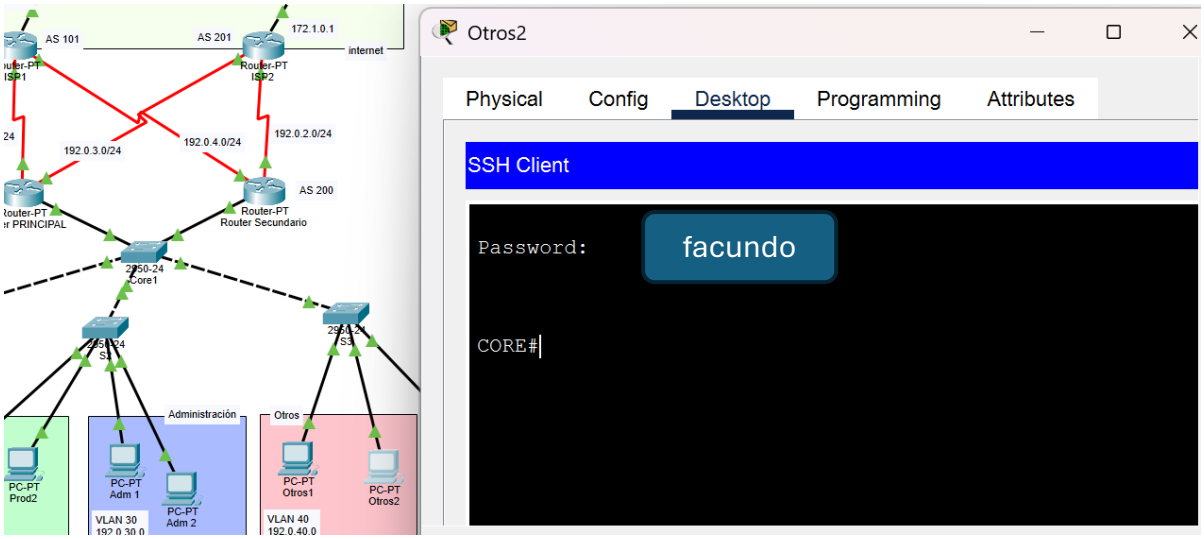
La contraseña que se pide en la consola de la PC Otros es el que se indica cuando se crea el usuario y clave:

*RouterSecundario(config-line)#**username redes privilege 15 password sylvina***

Luego de ese paso, se accede al modo privilegiado del Router secundario.

Este mismo procedimiento se realiza en los routers y switches de todo el diagrama.

Conexión remota desde PC Otros2 para configurar el Switch CORE:



En cada switch configuré IP para cada interfaz conectadas con las VLANs

*S3(config)#**int vlan 40***
*S3(config-if)#**ip address 192.0.40.152 255.255.255.0***
*S3(config-if)#**no shutdown***
*S3(config-if)#**exit***

4. Asegurar contraseñas.

Para asegurar que el uso de los routers no sea accesible para cualquier persona, le agrego una contraseña. Además, para que esta no aparezca (en forma "plana") al ejecutar el comando *show running-config* la voy a configurar de modo que sea secreta.

Estando en modo configuración, agrego la contraseña ***sylvina*** (para que sea fácil de recordar, aunque sea una contraseña débil)

*RouterPRINCIPAL#**conf ter***
*RouterPRINCIPAL(config)#**enable password sylvina***
*RouterPRINCIPAL(config)#**service password-encryption***
*RouterPRINCIPAL(config)#**exit***
RouterPRINCIPAL#

En modo privilegiado ejecuto el comando *show running-config* y se puede observar que la contraseña no queda como texto plano, sino encriptada:

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

Current configuration : 2968 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname RouterPRINCIPAL
!
!
!
enable password 7 083255421F100B16
!
```

Una vez comprobado que la contraseña está encriptada, se vuelve a modo global para intentar pasar al modo privilegiado, en donde se debe requerir una contraseña:

```
RouterPRINCIPAL>enable
Password:
RouterPRINCIPAL#
```

La contraseña se escribe, pero no se ve como texto plano. Si, al intentar cambiar de modo global a privilegiado, se falla tres veces ocurre esto:

```
RouterPRINCIPAL>enab
Password:
Password:
Password:
% Bad secrets

RouterPRINCIPAL>
```

Existen otras maneras de crear y encriptar una contraseña:

- ***enable password [clave]***, y luego encriptar la clave
- ***enable secret [clave]***
- ***line console 0***
  password [clave]
  login
  do write

De esta última forma se genera una clave para ingresar al modo global del router (antes de escribir ***enable***).

Mini-desafío extra: ACL que solo deje ping hacia VLAN servidores desde VLAN Producción.

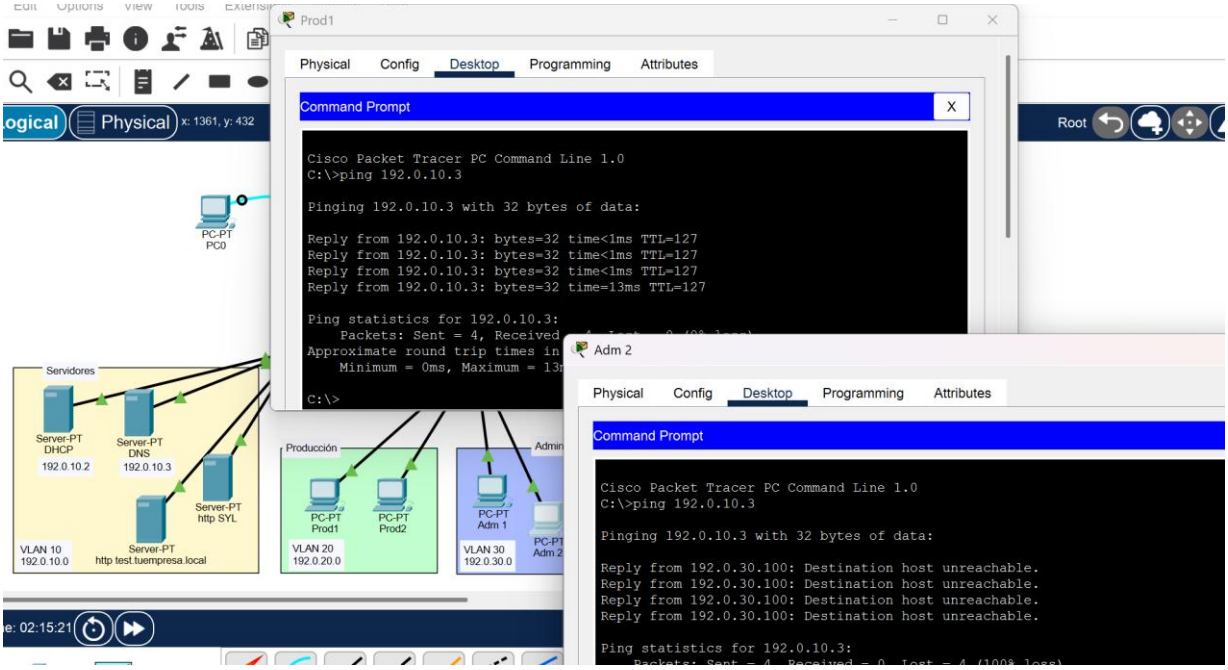
Se agrega una ACL extendida (en cada router):

```
RouterPRINCIPAL#show access-list
Extended IP access list 100
    10 permit tcp 192.0.40.0 0.0.0.255 192.0.10.0 0.0.0.255 eq www
    20 permit udp 192.0.40.0 0.0.0.255 192.0.10.0 0.0.0.255 eq www
    30 deny ip 192.0.40.0 0.0.0.255 192.0.10.0 0.0.0.255 (2 match(es))
    40 permit ip any any (2388 match(es))
Extended IP access list 101
    10 permit icmp 192.0.20.0 0.0.0.255 192.0.10.0 0.0.0.255 (1 match(es))
    20 deny icmp any 192.0.10.0 0.0.0.255 (2 match(es))
    30 permit tcp any any
    40 permit udp any any
    50 permit ip any any
```

se asigna la lista 101 a la interfaz con IP 192.0.10.100, como “out”

```
RouterPRINCIPAL(config-subif)#no ip access-group 101 in
RouterPRINCIPAL(config-subif)#ip access-group 101 out
RouterPRINCIPAL(config-subif)#
```

Desde la PC Prod1 se hace un ping exitoso hacia un servidor de la VLAN 10 pero no es exitoso cuando se hace ping desde la PC Adm 2 hacia el mismo servidor:



Conclusiones

Con el desarrollo de esta cuarta entrega del trabajo práctico integrador he podido configurar distintas formas de darle más seguridad al sistema autónomo, a las distintas redes.

Además, aprendí el hecho de poner en práctica cómo poder configurar un switch o router para poder acceder de forma remota, sin tener que conectar una consola para configurar (solo se utiliza al principio, para configurar el acceso remoto).

La creación de listas de acceso, con sus reglas, también le agrega seguridad a la red, según políticas que se pueden establecer en la organización.

Claves

Router PRINCIPAL	→ enable: sylvina
	→ 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