[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 3

Redundancia y Enrutamiento BGP

Alumna:

Apellido y Nombre	legajo
Enriquez, Sylvina	------

Curso: 2025

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 3 – Redundancia y enrutamiento BGP

🎯 **Objetivo:** Configurar BGP entre routers e ISP y simular falla en uno de los routers.

Pasos:

1. Configurar alta disponibilidad hacia ISP1 e ISP2 mediante HSRP.
2. Verificar ruta principal.
3. Simular caída de router principal y comprobar failover.
4. Enviar paquetes fuera de la red y confirmar enrutamiento BGP.

Checklist:

✅ BGP activo.

✅ Failover OK.

Índice etapa 3

CONSIGNA TRABAJO PRÁCTICO INTEGRADOR 2

DESARROLLO TRABAJO PRÁCTICO INTEGRADOR..... 5

1. Diseño en Packet Tracer 5
2. Configurar alta disponibilidad hacia ISP1 e ISP2 mediante HSRP. 5
3. Verificar ruta principal. 7
4. Simular caída de router principal y comprobar failover. 8
5. Enviar paquetes fuera de la red y confirmar enrutamiento BGP. 10
6. Diseño FINAL de esta entrega: 12

Conclusiones..... 12

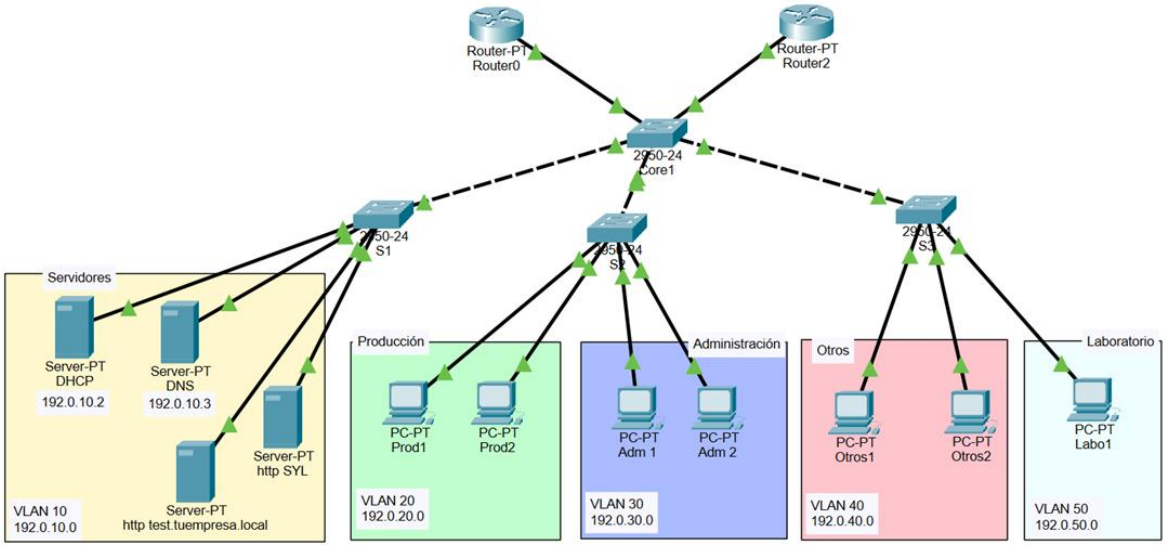
DESARROLLO TRABAJO PRÁCTICO INTEGRADOR

ENTREGA 3 – Redundancia y enrutamiento BGP

1. Diseño en Packet Tracer

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

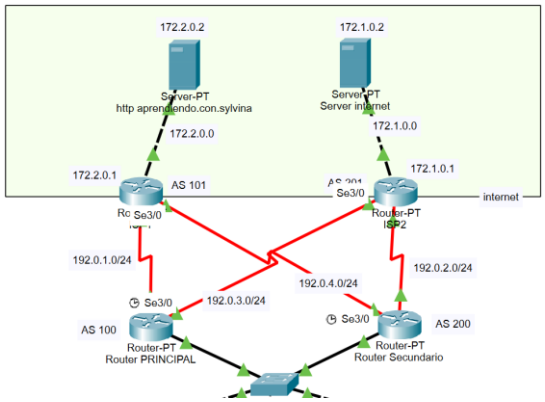
Diseño INICIAL:



2. Configurar alta disponibilidad hacia ISP1 e ISP2 mediante HSRP.

Desde la primera entrega se tuvo en cuenta el requerimiento de contar con dos direcciones ISP, por eso el diagrama cuenta con dos Routers. Se agregan dos routers para simular distintos sistemas autónomos (AS) de internet (ISP1 e ISP2). Además, se incorporan dos servers, con el fin de simular que forman parte de Internet.

Por otro lado, se comenta que es necesario conectar ambos router (los que funcionan como frontera de la AS) a los dos ISPs. De esta manera, se aplicará el protocolo HSRP para darle prioridad a uno de los routers. El secundario actuará si el principal se cae.



Para aplicar el protocolo HSRP se configura el Router *PRINCIPAL* de la siguiente manera:

***NV**: número de VLAN*

Las direcciones IP configuradas en el trabajo práctico anterior tienen la forma:

192.0. ***NV***.1

y quedaron de esta manera (en la etapa 2):

```
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.0.10.1 255.255.255.0
 ip helper-address 192.0.10.2
```

Ahora se debe modificar la dirección IP para que tome la que corresponde al Gateway de cada VLAN. Además, se debe agregar el protocolo HSRP (*standby*):

ROUTER PRINCIPAL:

```
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.0.10.100 255.255.255.0
 ip helper-address 192.0.10.2
 standby 10 ip 192.0.10.1
 standby 10 priority 110
 standby 10 preempt
!
```

- *ip address 192.0.NV.101 255.255.255.0*: cambio el 1 por el 101
- *standby NV ip 192.0.NV.1*: aquí se utiliza el .1 que indica el gateway de la VLAN
- *standby NV priority 110*: indica que tomará la prioridad 110 (podría ser otro número)
- *standby NV preempt*: el protocolo HSRP permite, con el comando *preempt,* estar escuchando si el otro router está activo. Esto se realiza en cada interfaz del router principal

ROUTER SECUNDARIO:

Show running-config

```
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.0.10.101 255.255.255.0
 ip helper-address 192.0.10.2
 standby 10 ip 192.0.10.1
 standby preempt
!
```

Si hubiese más de un router de respaldo, se le podría asignar un valor de prioridad menor que el principal pero con una secuencia de valores según cómo se determine su importancia.

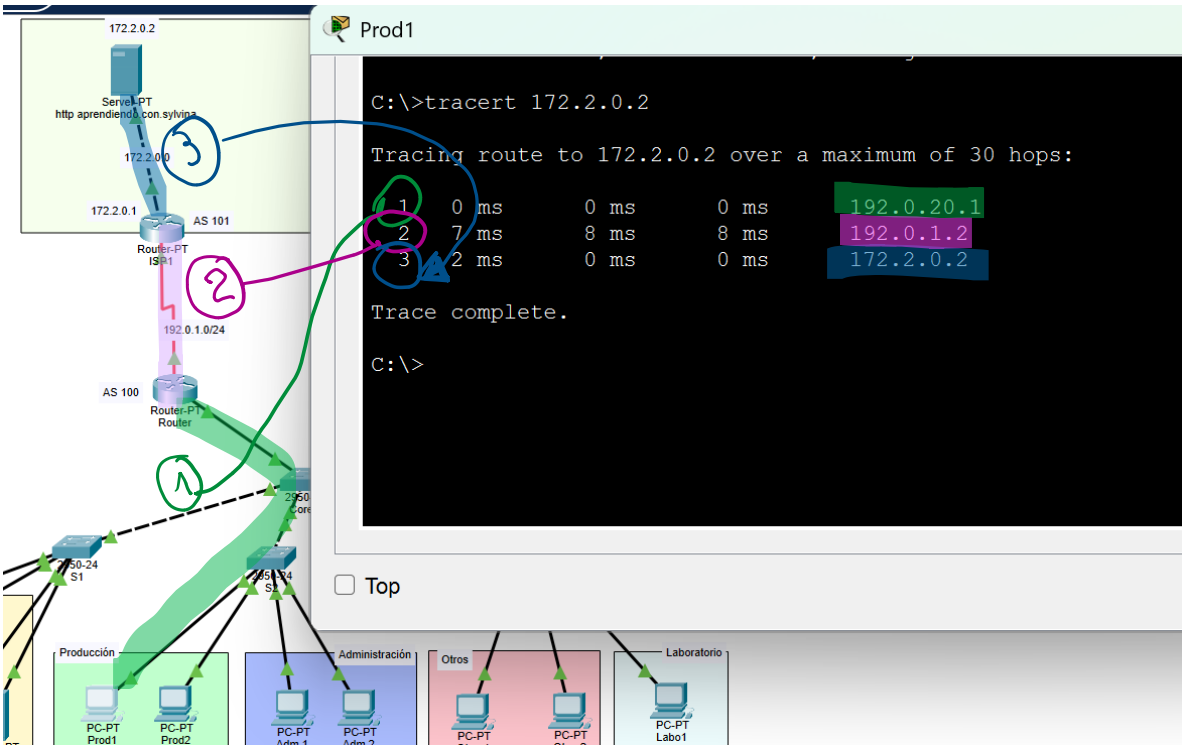
Se configura el protocolo BGP entre los routers de Internet (ISP1 e ISP2) y los routers frontera de nuestro sistema.

Nota: en el valor de standby ***NV*** no es necesario que varíe (puede ser 1 para todos los casos)

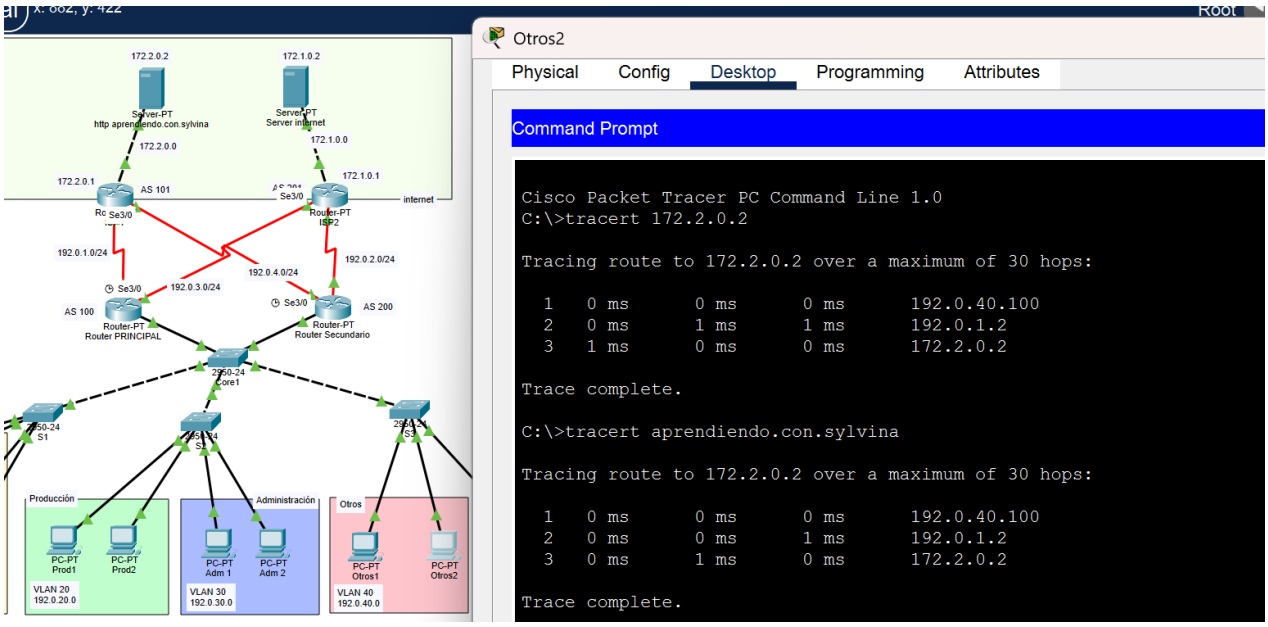
3. Verificar ruta principal.

Se utiliza el comando *tracert [IP destino]* en la consola de la PC desde la que se desea trazar la ruta para verificar la ruta principal.

Desde PC Prod1 hasta Server 172.2.0.2:

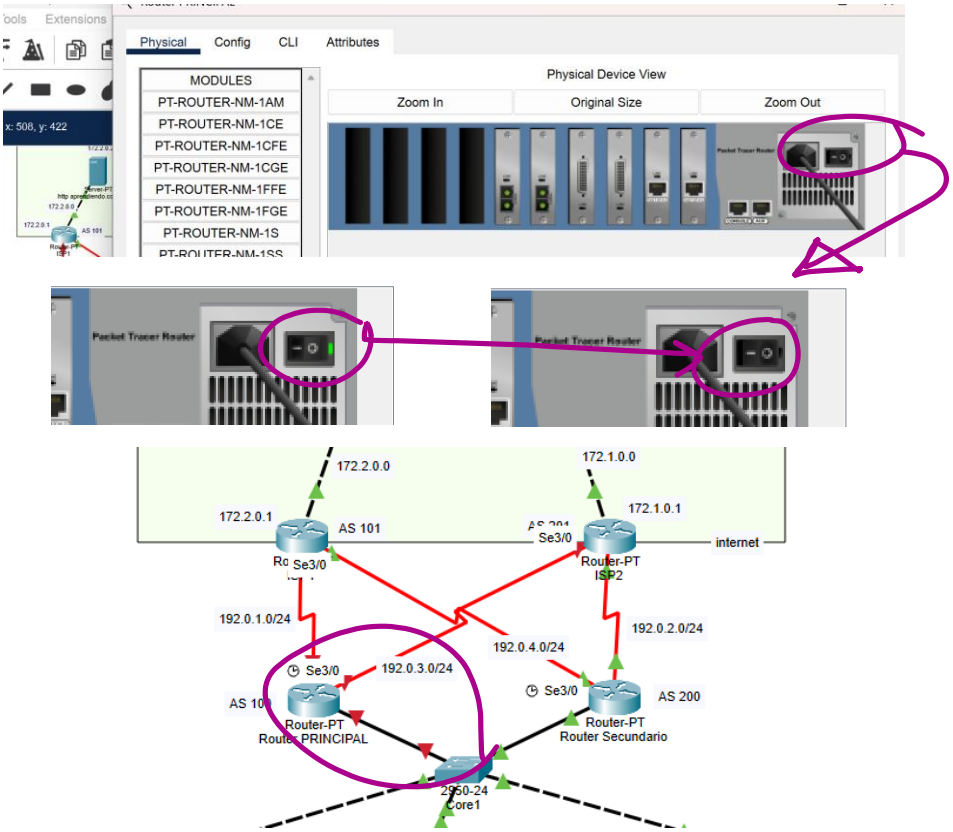


En esta imagen se puede observar el trazado de la ruta entre la PC “Otros 2” con el Server que está en internet. El mismo se solicita a través del comando *tracert 172.2.0.2* (IP del server) y también a través del uso del servicio de DNS (utilizando el mismo comando, pero con el nombre del sitio a consultar)



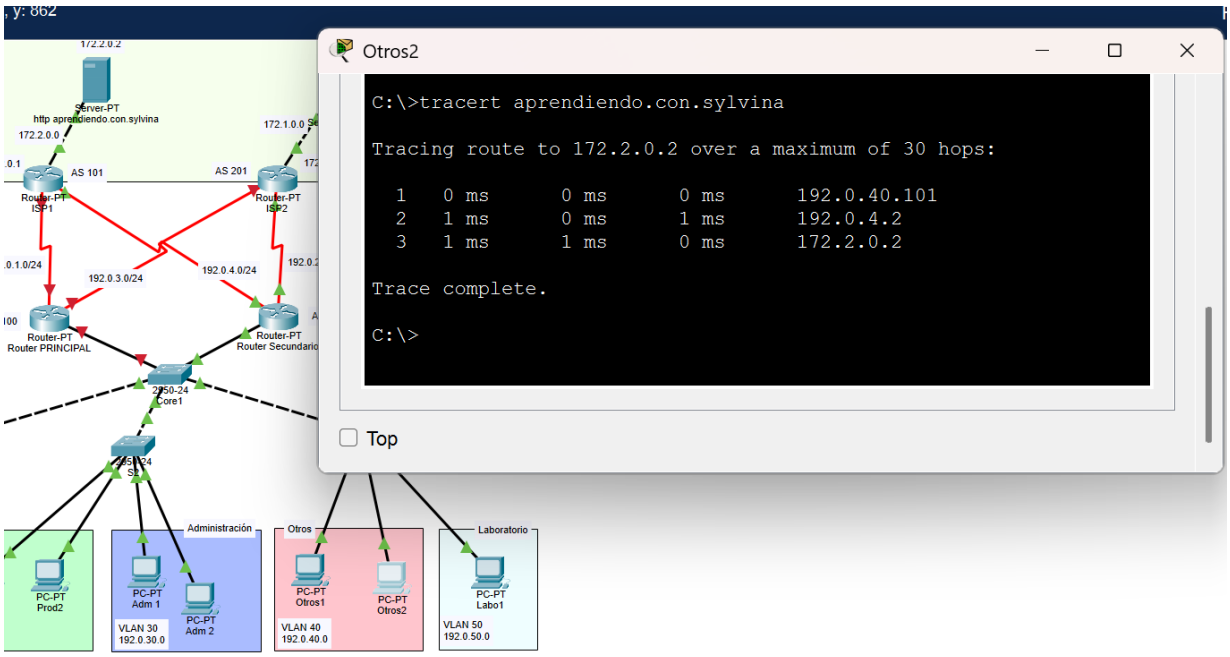
4. Simular caída de router principal y comprobar failover.

Se procede a apagar el router principal para simular la caída del mismo:

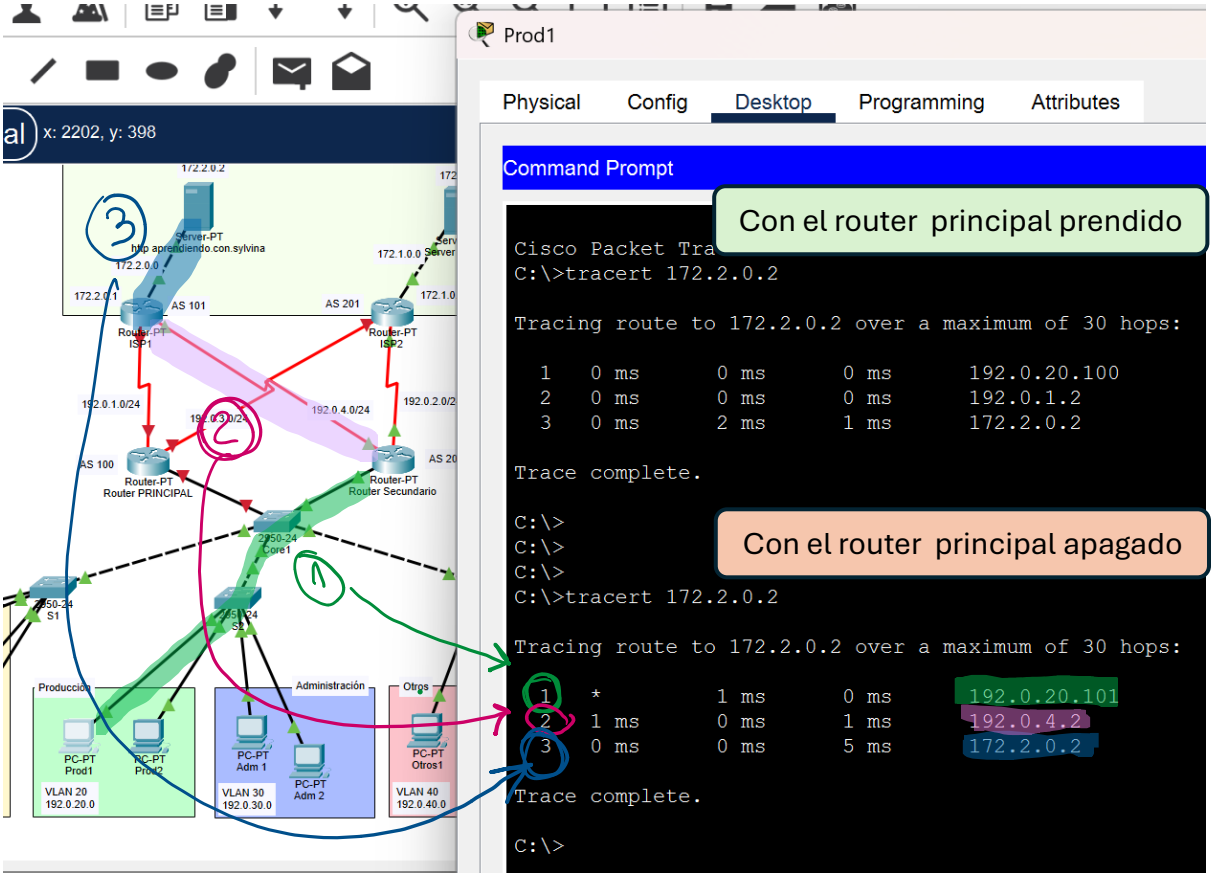


Se puede observar cómo, luego de apagarlo, las conexiones (triángulos) que antes estaban en verde, ahora aparecen en rojo (muestra que no funcionan esas conexiones). Ahora se verifica la ruta principal como en el ejemplo mostrado anteriormente:

- desde *PC Otros 2* hacia el sitio *aprendiendo.con.sylvina*:



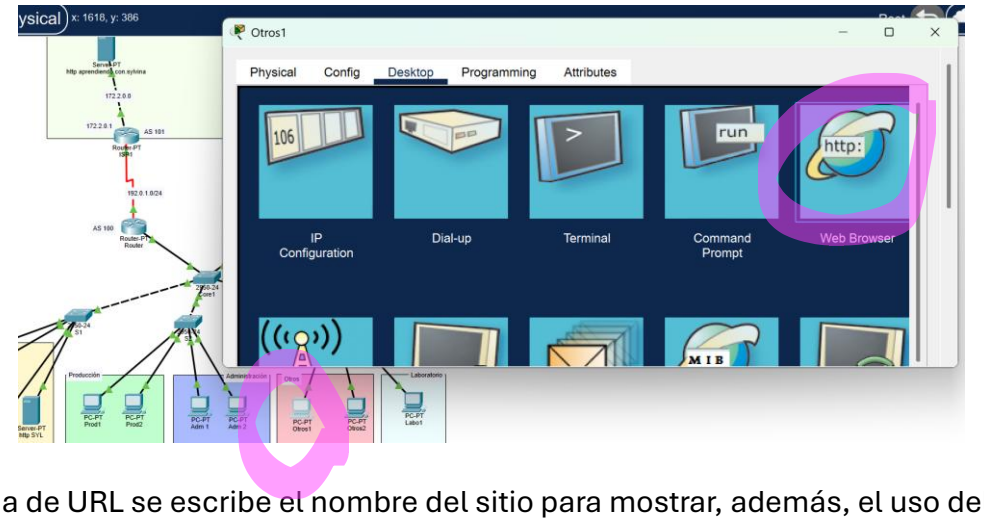
- Desde PC Prod1 hasta Server 172.2.0.2:



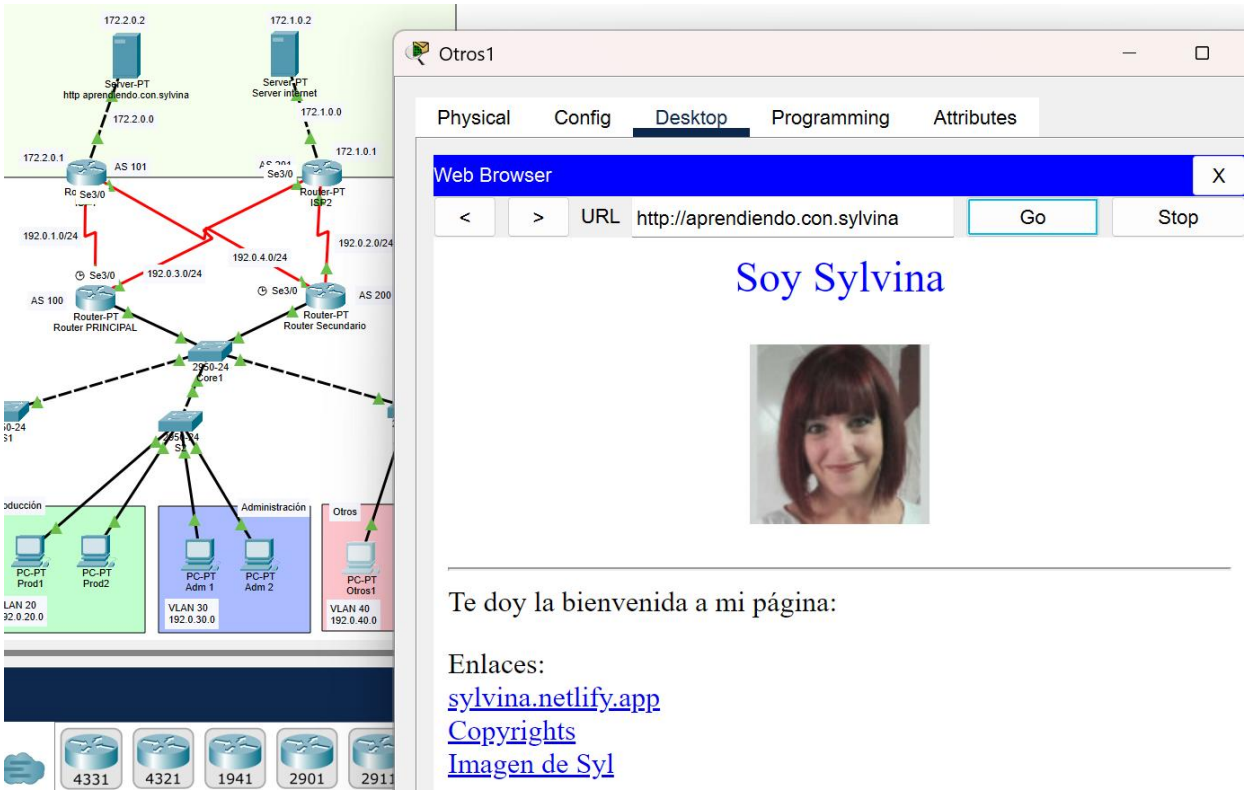
5. Enviar paquetes fuera de la red y confirmar enrutamiento BGP.

Se puede observar que, desde la PC *Otros1* se accede al sitio *aprendiendo.con.sylvina* que está en el Server fuera de nuestro sistema aislado (en internet). Para ello, debe estar activo el protocolo BGP, pues el pedido sale de nuestra red por medio del router principal:

Se accede mediante el uso del Web Browser de la PC:



En la línea de URL se escribe el nombre del sitio para mostrar, además, el uso del servicio DNS:



- Router ISP1:

```
ISP1#show ip bgp summary
BGP router identifier 192.0.4.2, local AS number 101
BGP table version is 56, main routing table version 6
26 network entries using 3432 bytes of memory
26 path entries using 1352 bytes of memory
22/18 BGP path/bestpath attribute entries using 3680 bytes of memory
4 BGP AS-PATH entries using 96 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 8592 total bytes of memory
BGP activity 12/0 prefixes, 26/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.0.1.1       4   100      62      19        56    0    0 00:17:14        4
192.0.4.1       4   200     174      21        56    0    0 00:12:21        4
```

- Router ISP2:

```
ISP2#show ip bgp summary
BGP router identifier 192.0.3.2, local AS number 201
BGP table version is 54, main routing table version 6
26 network entries using 3432 bytes of memory
26 path entries using 1352 bytes of memory
22/18 BGP path/bestpath attribute entries using 3680 bytes of memory
4 BGP AS-PATH entries using 96 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 8592 total bytes of memory
BGP activity 12/0 prefixes, 26/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.0.2.1       4   200     167      22        54    0    0 00:12:51        4
192.0.3.1       4   100      61      19        54    0    0 00:17:46        4
```

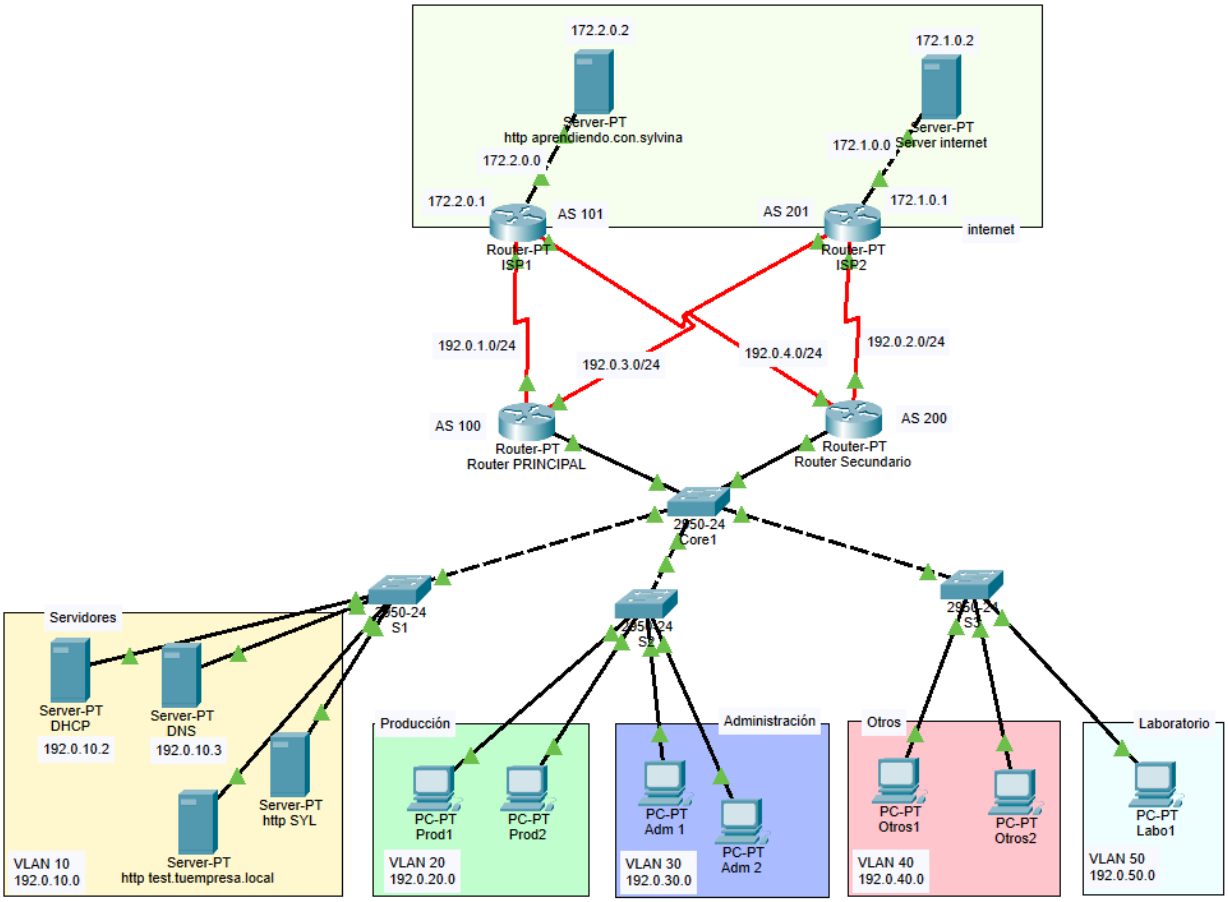
- Router Principal:

```
RouterPRINCIPAL#show ip bgp summary
BGP router identifier 192.0.99.100, local AS number 100
BGP table version is 98, main routing table version 6
41 network entries using 5412 bytes of memory
41 path entries using 2132 bytes of memory
22/8 BGP path/bestpath attribute entries using 2760 bytes of memory
4 BGP AS-PATH entries using 96 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 10432 total bytes of memory
BGP activity 12/0 prefixes, 41/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.0.1.2       4   101      83      20        98    0    0 00:18:18        4
192.0.3.2       4   201      77      20        98    0    0 00:18:20        4
```

- Router Secundario:

```
RouterSecundario#show ip bgp summary
BGP router identifier 192.0.99.101, local AS number 200
BGP table version is 135, main routing table version 6
54 network entries using 7128 bytes of memory
54 path entries using 2808 bytes of memory
35/8 BGP path/bestpath attribute entries using 3956 bytes of memory
4 BGP AS-PATH entries using 96 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 14020 total bytes of memory
BGP activity 12/0 prefixes, 54/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.0.2.2       4   201      81      23       135    0    0 00:14:03        4
192.0.4.2       4   101      88      23       135    0    0 00:14:03        4
```

6. Diseño FINAL de esta entrega:



Conclusiones

Con el desarrollo de esta tercera entrega del trabajo práctico integrador he podido entender cómo configurar el protocolo BGP (para conectar distintos AS) y cómo solucionar, a través del protocolo HSRP y poder comprobar la alta disponibilidad a pesar de la caída de un router.