



Universidad Tecmilenio Campus Cumbres

Infraestructura de Novared para Tecmicorp



Maestra : Blanca Aracely Aranda Machorro

Lugar: Monterrey Nuevo León

Fecha: 14 de Enero 2025

ÍNDICE

INTRODUCCIÓN DEL NEGOCIO.....	3
NOMBRE DE PROYECTO.....	4
ALCANCE.....	4
ANÁLISIS Y DISEÑO.....	4
TOPOLOGÍA DE RED.....	6
DESARROLLO DEL NEGOCIO.....	7
DESARROLLO.....	8
IMPLEMENTACIÓN.....	8
TESTEO DEL PROYECTO.....	16
PRUEBAS Y RESULTADOS DE LAS PRUEBAS.....	17
CONCLUSIÓN DEL PROYECTO.....	34
GLOSARIO DE TÉRMINOS Y CONDICIONES.....	35
BIBLIOGRAFÍA.....	44
AUTORES.....	45
CONCLUSIÓN.....	46

INTRODUCCIÓN DEL NEGOCIO



ANÁLISIS DE DISEÑO Y TOPOLOGÍA DE RED

INFRAESTRUCTURA DE NOVARED PARA TECMICROP

ALCANCE

Este proyecto tiene como objetivo lograr crear una infraestructura de red para Tecmicorp segura y escalable esto mediante diferentes servicios como SSH para tema de seguridad y DHCP para temas de escalabilidad.

ANÁLISIS Y DISEÑO

El diseño que se usó para la red de Tecmicorp, fue de una sede principal y 5 sucursales, la red de cada una de estas, tanto la sede como las sucursales se basa en uno modelo jerárquico de tres niveles, donde los routers actúan como el núcleo, facilitando la interconexión entre diferentes segmentos de red, los switches se encargan de distribuir el tráfico dentro de cada subred, conectando a los dispositivos finales, como PCs, laptops y servidores. La red WAN tambien usa la topología de estrella ya que consta de un router central que es el de la sede principal conectado a los otros nodos que son las sucursales.

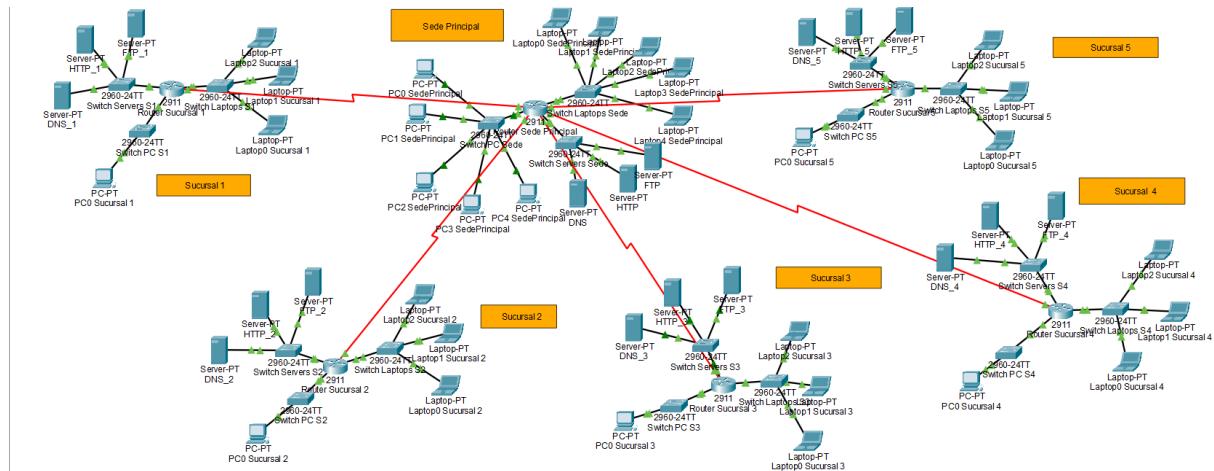


Figura 1. Diagrama de Red WAN

Cada red está dividida en 3 subredes, una para los dispositivos finales PCs, una para las laptops y uno para los servidores, esto con el fin de hacer una red más segura y generar menos tráfico de red.

Ejemplo de infraestructura de una sucursal

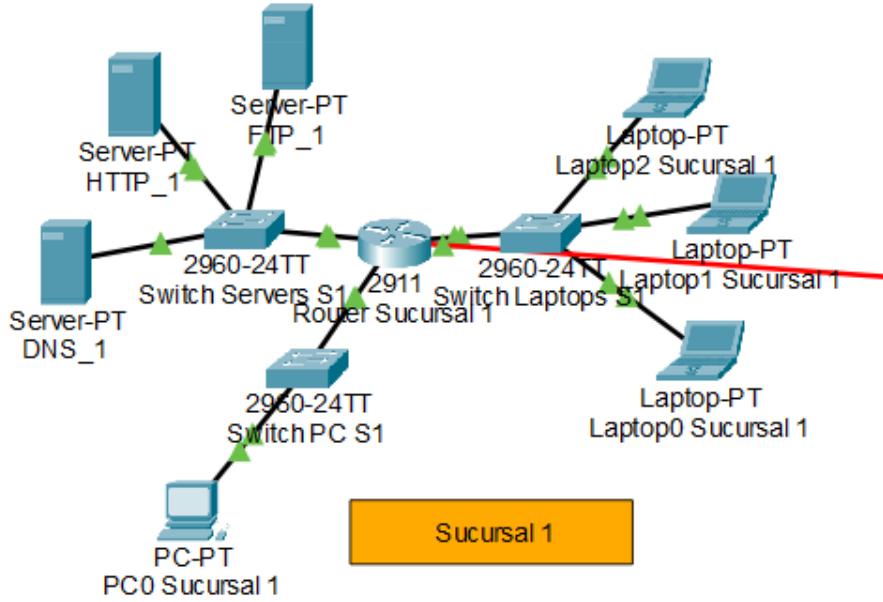


Figura 2. Arquitectura de Sucursal 1

Infraestructura de la sede principal:

- Router
- Switches para conectar algunos dispositivos finales por ethernet
- Dispositivos finales conectados con cable de cobre por ethernet (PCs, Laptops y Servidores)

Infraestructura de la sede principal, estructurada igual que las sucursales pero con mas dispositivos finales.

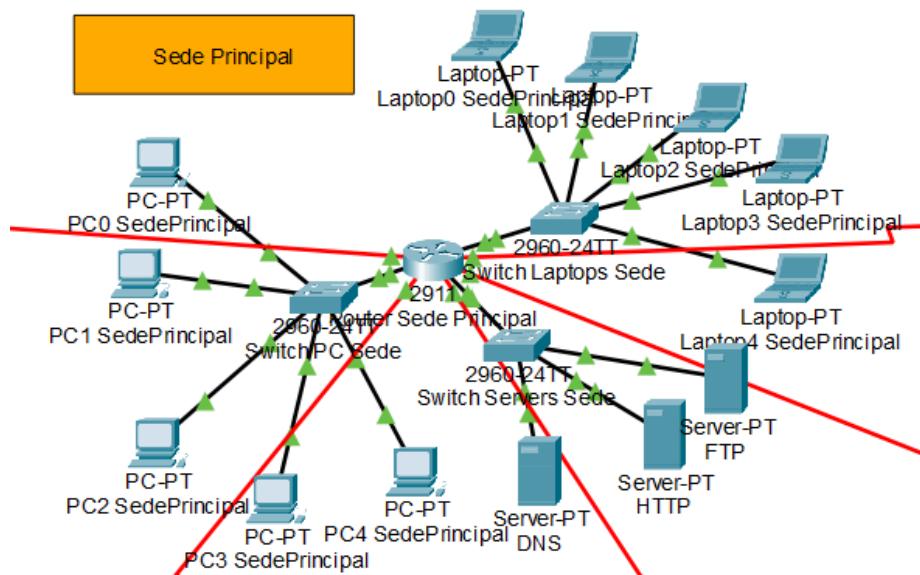


Figura 3. Arquitectura de sede principal

TOPOLOGÍA DE RED

La infraestructura de red de NovaRed para Tecmicorp está diseñada con una topología jerárquica de tres niveles y una WAN en estrella, conectando una sede principal con cinco sucursales. Cada sitio cuenta con sus propios dispositivos de red, asegurando independencia y redundancia en la comunicación.

Estructura de la Red

- Sede Principal:
 - Servidores DNS, HTTP y FTP que gestionan el acceso y distribución de servicios en la red.
 - Un router central (2911) que actúa como nodo principal de la WAN, manejando el ruteo y la segmentación de tráfico hacia las sucursales.
 - Switches de alta capacidad (2960-24TT) que interconectan equipos finales como PC y laptops.
- Sucursales:
 - Cada sucursal tiene su propio router (modelo 2911), encargado de la comunicación con la sede principal.
 - Switches para segmentación de redes de usuarios y servidores.
 - Servidores DNS, HTTP y FTP locales para optimizar el acceso a servicios internos y reducir la dependencia de la sede principal.
 - Equipos finales como PC y laptops conectados mediante enlaces Ethernet.

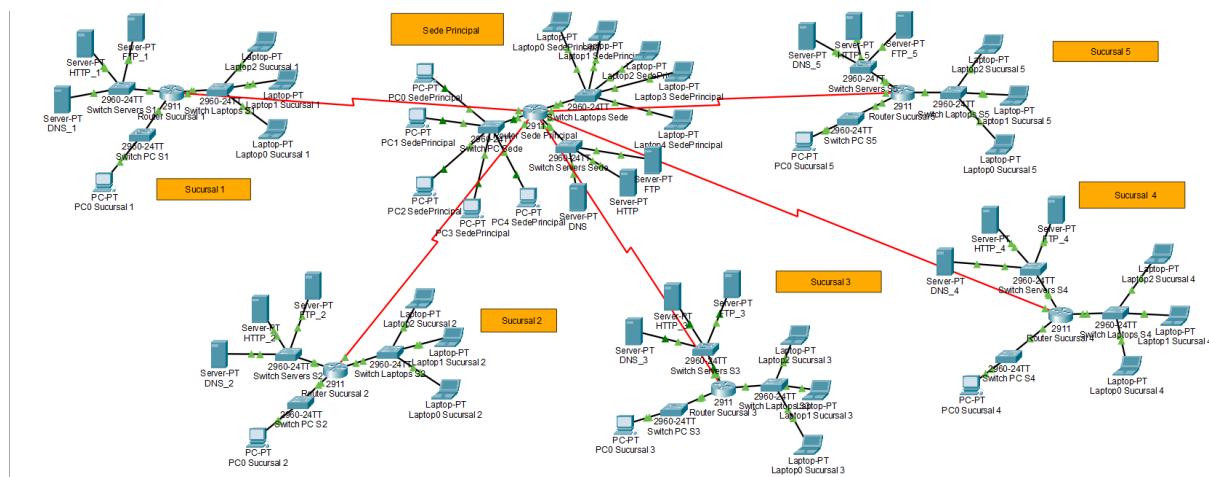
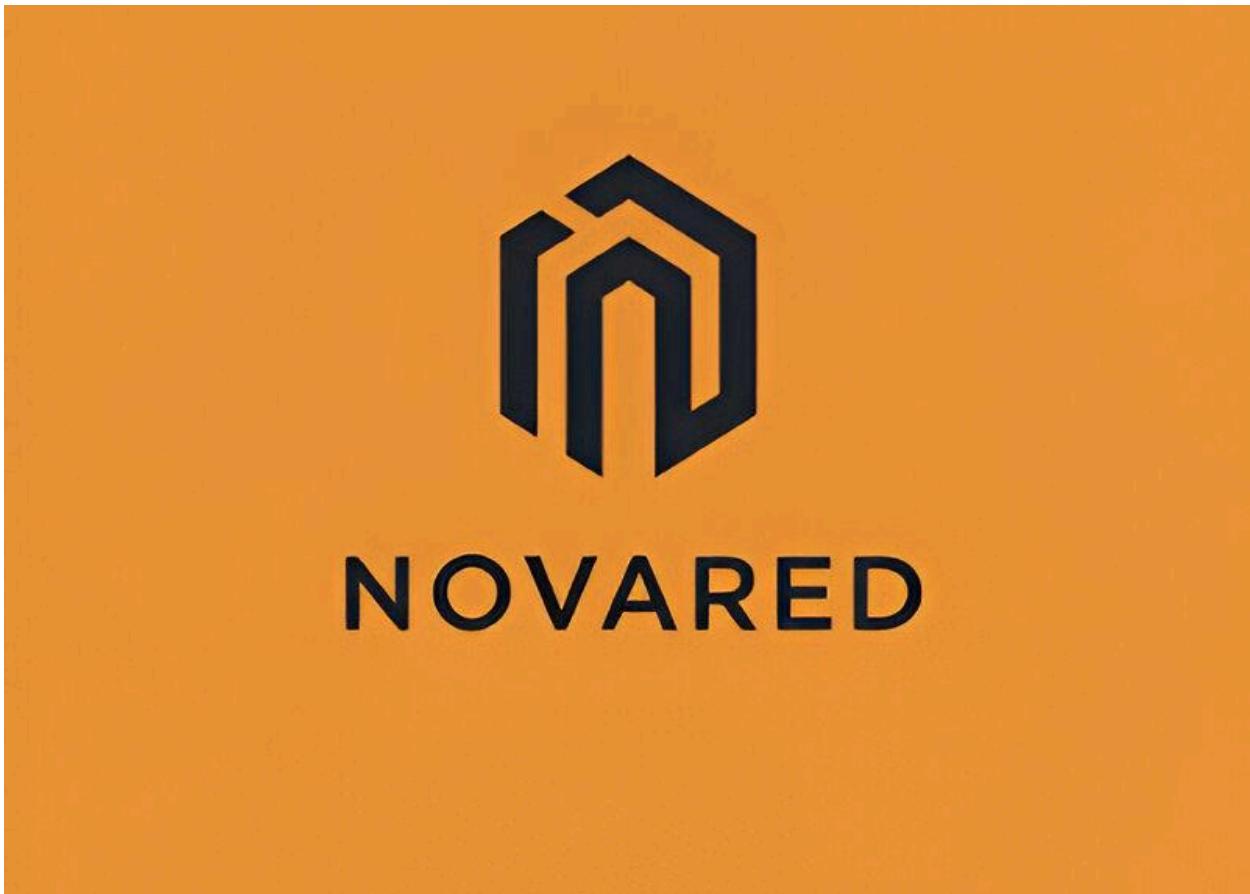


Figura 1. Diagrama de Red WAN

DESARROLLO DEL NEGOCIO



IMPLEMENTACIONES DEL PROYECTO

DESARROLLO

La implementación de la red para Tecmicorp se diseñó con un enfoque en escalabilidad, seguridad y eficiencia, garantizando una conectividad óptima entre la sede principal y las sucursales. Para ello, se implementaron diversas tecnologías y configuraciones que optimizan el rendimiento y la administración de la infraestructura.

Uno de los principales avances fue la configuración de DHCP para la asignación dinámica de direcciones IPv4, lo que facilita la escalabilidad de la red al evitar configuraciones manuales y reducir errores. Asimismo, se adoptó un esquema dual stack con IPv6, lo que no solo garantiza compatibilidad con futuras tecnologías, sino que también mejora la seguridad y permite la conexión de un mayor número de dispositivos.

En cuanto a la seguridad, se implementó SSH (Secure Shell) en los routers para evitar vulnerabilidades presentes en protocolos como Telnet, asegurando así una administración remota cifrada. Además, se integraron servicios clave como DNS, HTTP y FTP, permitiendo una mejor gestión de recursos internos, la resolución de nombres de dominio y la transferencia de archivos de manera eficiente dentro de la red.

Para optimizar la conectividad entre las distintas sucursales, se configuró RIP (Routing Information Protocol), lo que permite que los routers intercambien información de rutas de forma dinámica sin necesidad de intervenciones manuales. Esto garantiza una mayor adaptabilidad ante cambios en la topología de la red y mejora la eficiencia del enrutamiento.

IMPLEMENTACIÓN

Para mejorar la eficiencia, escalabilidad y seguridad de la red de Tecmicorp, se implementaron diversas configuraciones y protocolos clave. Entre estas mejoras se encuentra la asignación dinámica de direcciones IPv4 e IPv6 mediante DHCP, lo que optimiza la gestión de direcciones IP y facilita la expansión de la red. Además, se configuró SSH en cada router para garantizar conexiones remotas seguras y evitar accesos no autorizados. También se habilitaron los servicios DNS, HTTP y FTP, permitiendo la resolución de nombres de dominio, la transferencia de archivos y el alojamiento web dentro de la red. Para mejorar la comunicación entre routers y permitir que las sucursales reconozcan dinámicamente los dispositivos de la red, se implementa el protocolo de enrutamiento RIP (Routing Information Protocol). Gracias a estas

configuraciones, la red de Tecmicorp ahora cuenta con mayor seguridad, mejor administración de recursos y una conectividad más eficiente entre sus diferentes sedes.

DHCP:

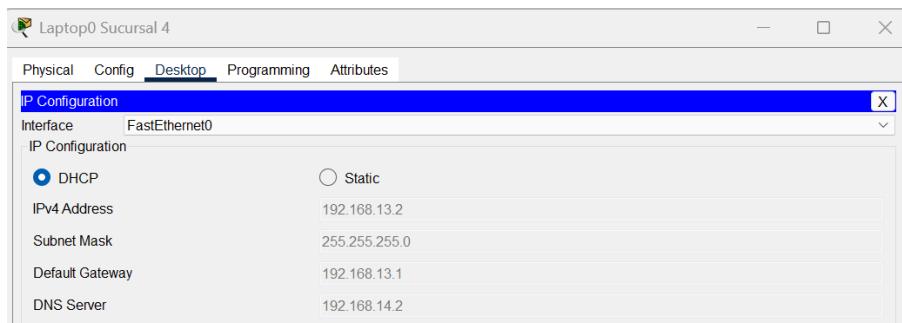
Se configuró DHCP en el router de la sede principal y las sucursales para permitir la asignación automática de direcciones IPv4 dinámicas a los dispositivos de la red. Esto facilita la escalabilidad, evitando la necesidad de asignar direcciones manualmente y reduciendo posibles errores de configuración.

Ejemplo de comandos utilizados para la configuración de una ip dinámica.

```
Router (config) #ip dhcp pool sucursal4_lap
Router (dhcp-config) #network 192.168.13.0 255.255.255.0
Router (dhcp-config) #default-router 192.168.13.1
Router (dhcp-config) #dns-server 192.168.14.2
Router (dhcp-config) #ip dhcp excluded-address 192.168.13.1
```

En estos comandos se especifica la subred en donde vamos a activar DHCP, el default gateway y el servidor DNS.

Una vez ejecutados estos comandos, se activa el DHCP dentro de los dispositivos finales esto desde la opción desktop > Ip Configuración del equipo en el que queramos activar este servicio. Cabe destacar que solo las subredes en las que se haya ejecutado la configuración de DHCP podrán asignar IP dinámicas .



IPv6 Dinámica:

Para mejorar la seguridad y escalabilidad de la red, también se implementó IPv6 utilizando el método Dual Stack, lo que permite la coexistencia de IPv4 e IPv6 en la misma infraestructura. La principal ventaja de IPv6 es su mayor espacio de direcciones, lo que evita problemas de agotamiento de IP y ofrece mecanismos de seguridad integrados, como IPsec para cifrado de datos.

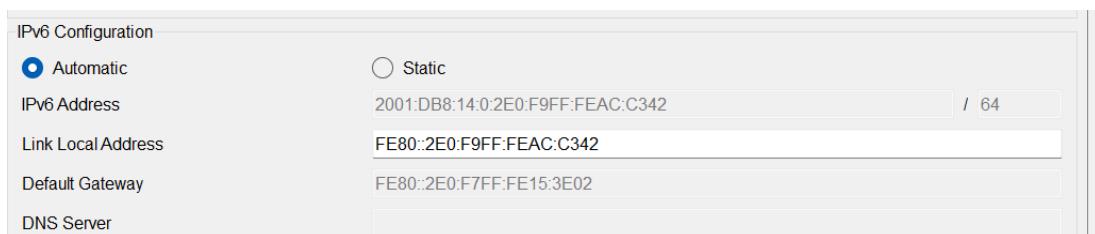
Para configurar la IPv6 dentro de nuestro router de forma dinámica, se utilizaron una serie de comandos en el CLI de router.

Ejemplo de comandos utilizados para la configuración de IPv6 dinámica.

```
Router(config)#interface GigabitEthernet0/2
Router(config-if)#ipv6 address 2001:db8:15::1/64
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ipv6 unicast-routing
```

En estos comandos se le asigna una dirección IPv6 a una subred y se activa el DHCP para esta misma subred pero para la dirección IPv6 asignada.

Una vez ejecutados los comandos igual que con el DHCP, se activa la opción de IPv6 automática dentro de los dispositivos desde la opción desktop > Ip Configuración de los equipos donde queramos añadir la red IPv6. Sólo los dispositivos dentro de una subred configurada con DHCPv6 podrán recibir una dirección dinámica. .



SSH:

Se implementó el servicio de SSH dentro de cada router, esto para poder hacer conexiones remotas desde cualquier equipo dentro de la red del router de forma segura.

La configuración del servicio SSH fue mediante unos comandos en el CLI del router, para especificar la línea virtual, username, password y otras cosas más, esto en cada router para que sea aún más seguro cada establecimiento.

```

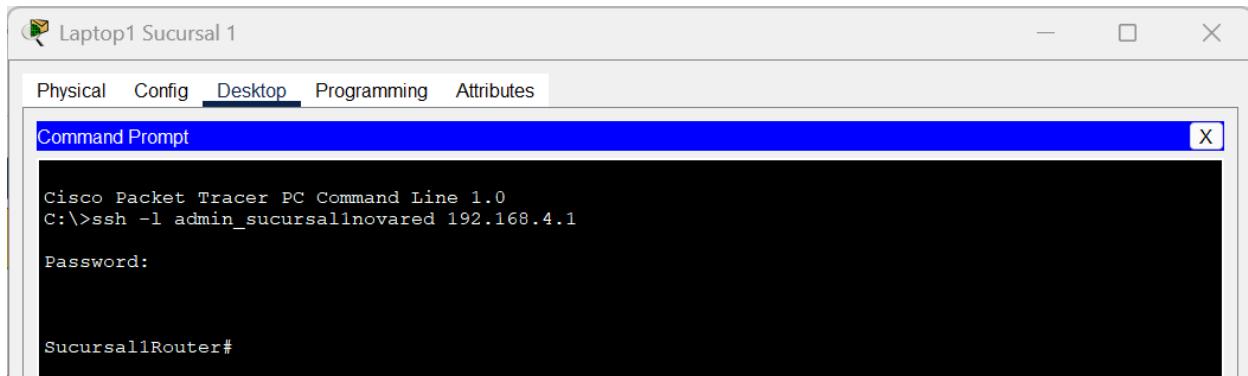
Router(config)#line vty 0 5
Router(config-line)#login local
Router(config-line)#transport input ssh
Router(config-line)#exit
Router(config)#username admin_sucursal5novared privilege 15 secret passsucursal5novared
Router(config)#ip domain-name novared.com
Router(config)#hostname
% Incomplete command.
Router(config)#hostname Sucursal5Router
Sucursal5Router(config)#crypto key generate rsa
The name for the keys will be: Sucursal5Router.novared.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Sucursal5Router(config)#ip ssh version 2
*Mar 2 17:28:1.411: %SSH-5-ENABLED: SSH 1.99 has been enabled

```

Para poder acceder al servicio ssh, tenemos que ir hacia el command prompt de un equipo que esté en la misma red del router en el que activamos el ssh y poner el comando de ssh -l más el username asignado en los comandos para la activación del servicio ssh y mas la ip del router. Para acceder a este servicio también se tiene que poner la contraseña asignada anteriormente, una vez fue ejecutado el comando anterior dentro de un equipo.



DNS:

Configuración:

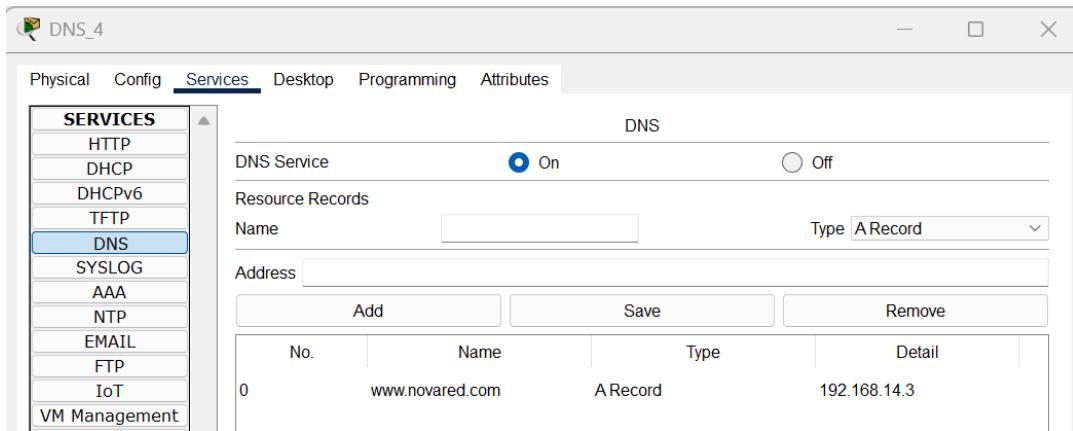
Para configurar correctamente el servicio de DNS, primero se asignó la IP del servidor DNS, después desde la CLI del router se configuró para que cuando se active el DHCP dentro de cualquier equipo automáticamente en el apartado de DNS Server se coloca la dirección IPv4 del servidor DNS.

```

Router(config)#ip dhcp pool sucursal4_lap
Router(dhcp-config)#network 192.168.13.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.13.1
Router(dhcp-config)#dns-server 192.168.14.2
Router(dhcp-config)#ip dhcp excluded-address 192.168.13.1

```

Tras configurar IPv4 en el servidor, activamos el servicio DNS en la pestaña de *Services*. Luego, añadimos el dominio www.novared.com y lo vinculamos a la dirección IP del servidor web, permitiendo el acceso a la página mediante un navegador.



Se usó el comando nslookup para verificar que nuestro dominio estuviera activado correctamente desde el command prompt de una PC.

```
C:\>nslookup www.novared.com
Server: [192.168.8.2]
Address: 192.168.8.2

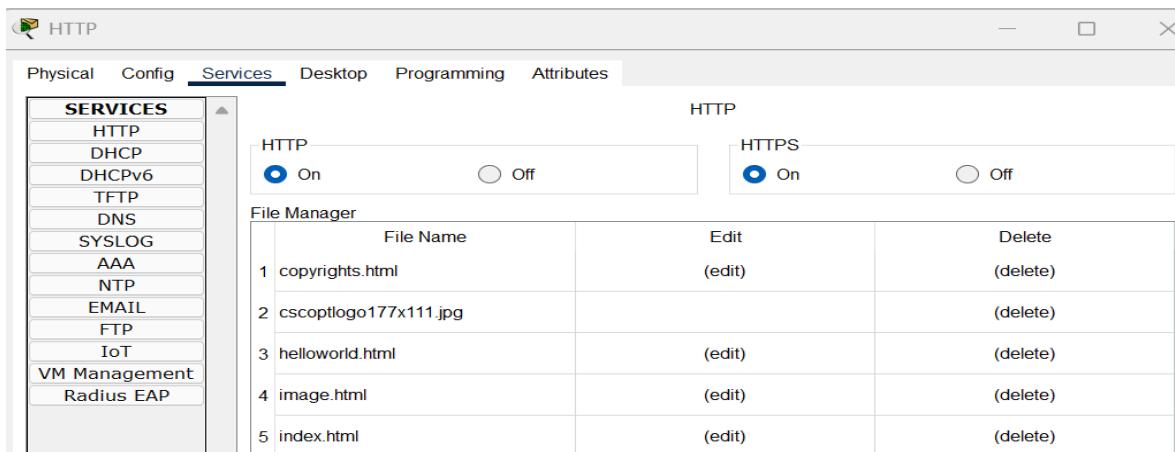
Non-authoritative answer:
Name:   www.novared.com
Address: 192.168.8.3

C:\>
```

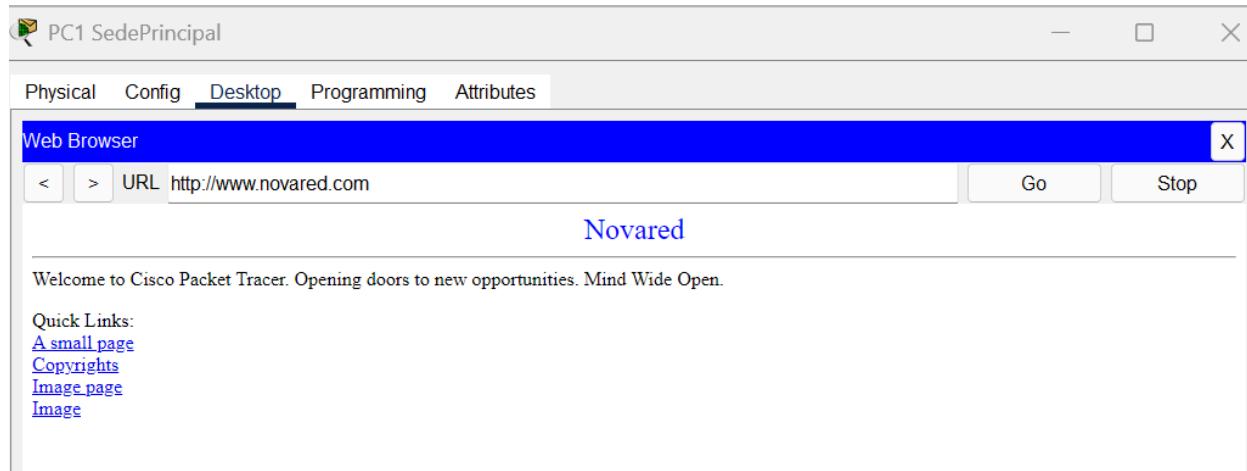
HTTP:

Configuración:

Para configurar el Servidor HTTP(web), al igual que en el servidor DNS, dentro del Servidor HTTP en la opción de Services se activó la opción del servicio HTTP.



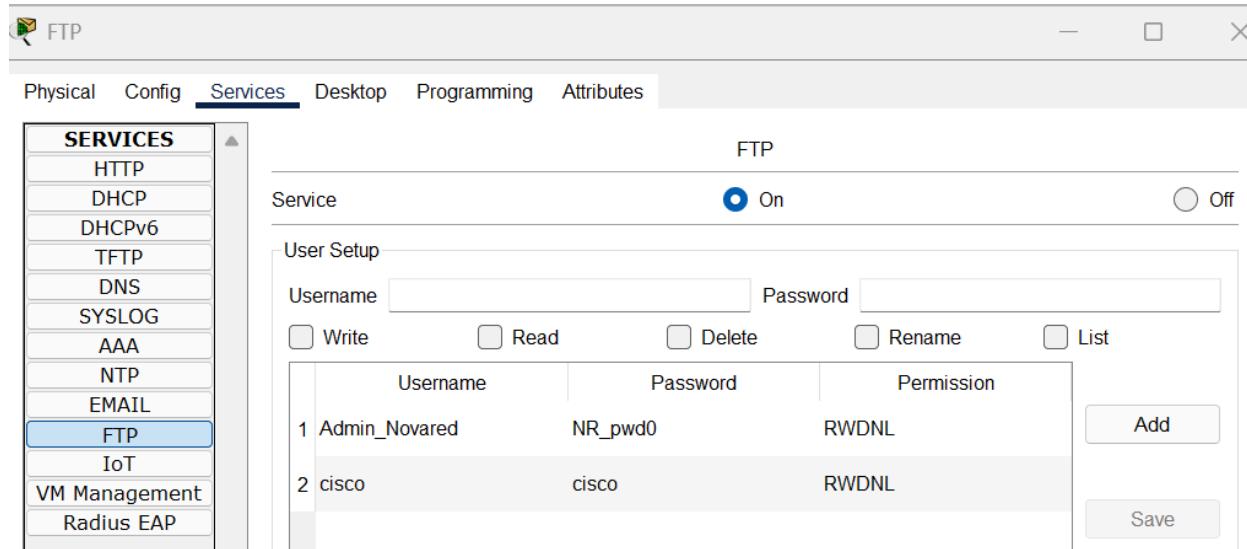
Para comprobar que el servicio funcionaba correctamente, desde un equipo PC en la opción Desktop > Web Browser, se ingresó el dominio previamente configurado en el Servidor DNS. Al dar clic en "Go", se cargó correctamente la página web del dominio.



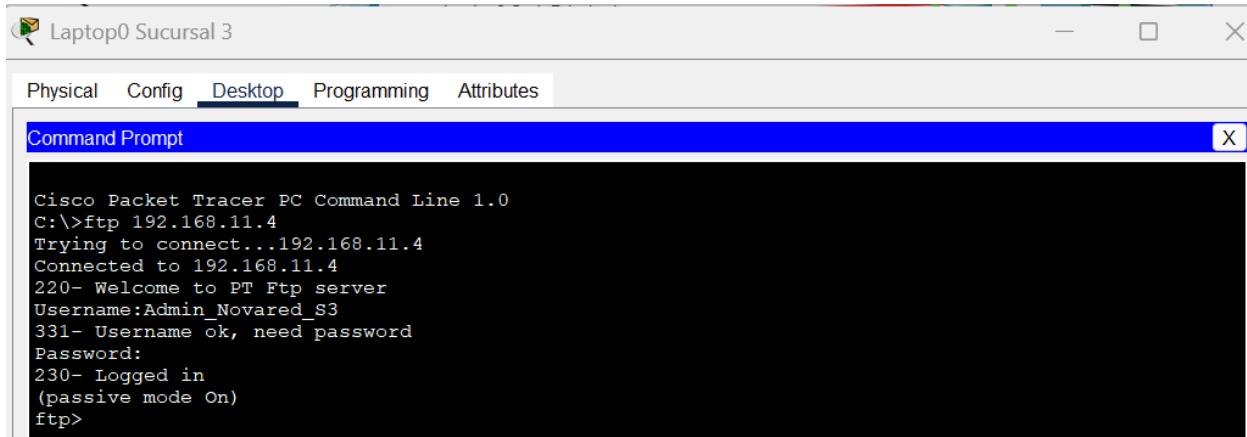
FTP:

Configuración:

Al igual que los dos servicios anteriores, para activar este servicio correctamente, dentro del servidor FTP en la opción de servicios se activó el servicio de FTP y creamos un nuevo usuario y contraseña.



Después para acceder al servicio de FTP, se usa el comando FTP más la IP del servidor FTP dentro del Command Prompt de un equipo PC. Para acceder al FTP se tiene que escribir correctamente el Username y Password ya anteriormente definidos en el Servidor.



Laptop0 Sucursal 3

Physical Config Desktop Programming Attributes

Command Prompt X

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.11.4
Trying to connect...192.168.11.4
Connected to 192.168.11.4
220- Welcome to PT Ftp server
Username:Admin_Novared_S3
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

RIP:

Para mejorar la eficiencia del enrutamiento entre routers y permitir que las sucursales reconozcan automáticamente los dispositivos de la red, se implementa el protocolo de enrutamiento RIP (Routing Information Protocol).

Configuración:

Para configurar RIP, se utilizaron comandos en el CLI del router para indicar las redes que participarán en el protocolo y permitir la distribución automática de rutas.

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.12.0
Router(config-router)#network 192.168.13.0
Router(config-router)#network 192.168.14.0
Router(config-router)#network 200.200.200.0
Router(config-router)#no auto-summary
Router(config-router)#exit
```

Con esta configuración, los routers intercambian información de enrutamiento y mantienen sus tablas de enrutamiento actualizadas automáticamente, mejorando la comunicación entre las sucursales de Tecnicorp.

TESTEO DEL PROYECTO



PRUEBAS Y RESULTADOS

PRUEBAS Y RESULTADOS DE LAS PRUEBAS

Se realizaron pruebas de conectividad entre dispositivos para probar que los dispositivos de la sede principal y de cada sucursal recibieron y enviaran datos entre ellos y también conectividad entre los routers.

Ping:

Prueba exitosa de conectividad de 5 dispositivos finales (laptops) y el dispositivo intermediario (router) de la sede principal de TecmiCorp.

PDU List Window											
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete	
●	Successful	Laptop0 SedePrincipal	Router Sede Principal	ICMP	■	0.000	N	0	(edit)		
●	Successful	Laptop1 SedePrincipal	Router Sede Principal	ICMP	■	0.000	N	1	(edit)		
●	Successful	Laptop2 SedePrincipal	Router Sede Principal	ICMP	■	0.000	N	2	(edit)		
●	Successful	Laptop3 SedePrincipal	Router Sede Principal	ICMP	■	0.000	N	3	(edit)		
●	Successful	Laptop4 SedePrincipal	Router Sede Principal	ICMP	■	0.000	N	4	(edit)		

Prueba exitosa de conectividad de 5 dispositivos finales (PCs) y el dispositivo intermediario (router) de la sede principal de TecmiCorp.

PDU List Window											
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete	
●	Successful	PC0 SedePrincipal	Router Sede Principal	ICMP	■	0.000	N	0	(edit)		
●	Successful	PC1 SedePrincipal	Router Sede Principal	ICMP	■	0.000	N	1	(edit)		
●	Successful	PC2 SedePrincipal	Router Sede Principal	ICMP	■	0.000	N	2	(edit)		
●	Successful	PC3 SedePrincipal	Router Sede Principal	ICMP	■	0.000	N	3	(edit)		
●	Successful	PC4 SedePrincipal	Router Sede Principal	ICMP	■	0.000	N	4	(edit)		

Prueba exitosa de conectividad de los 3 servidores y el dispositivo intermediario (router) de la sede principal de TecmiCorp.

PDU List Window											
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete	
●	Successful	DNS	Router Sede Principal	ICMP	■	0.000	N	0	(edit)		
●	Successful	HTTP	Router Sede Principal	ICMP	■	0.000	N	1	(edit)		
●	Successful	FTP	Router Sede Principal	ICMP	■	0.000	N	2	(edit)		

Prueba exitosa de conectividad de 4 dispositivos finales (3 laptops y una PC) y el dispositivo intermediario (router) de la primera sucursal de TecmiCorp.

PDU List Window												
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete		
●	Successful	PC0 Sucursal 1	Router Sucursal 1	ICMP	lightblue	0.000	N	0	(edit)			
●	Successful	Laptop0 Sucursal 1	Router Sucursal 1	ICMP	teal	0.000	N	1	(edit)			
●	Successful	Laptop1 Sucursal 1	Router Sucursal 1	ICMP	darkblue	0.000	N	2	(edit)			
●	Successful	Laptop2 Sucursal 1	Router Sucursal 1	ICMP	purple	0.000	N	3	(edit)			

Prueba exitosa de conectividad entre los 3 servidores y el dispositivo intermediario (router) de la primera sucursal de TecmiCorp.

PDU List Window												
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete		
●	Successful	DNS_1	Router Sucursal 1	ICMP	blue	0.000	N	0	(edit)			
●	Successful	HTTP_1	Router Sucursal 1	ICMP	teal	0.000	N	1	(edit)			
●	Successful	FTP_1	Router Sucursal 1	ICMP	darkblue	0.000	N	2	(edit)			

Prueba exitosa de conectividad de 4 dispositivos finales (3 laptops y una PC) y el dispositivo intermediario (router) de la segunda sucursal de TecmiCorp.

PDU List Window												
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete		
●	Successful	PC0 Sucursal 2	Router Sucursal 2	ICMP	blue	0.000	N	0	(edit)			
●	Successful	Laptop0 Sucursal 2	Router Sucursal 2	ICMP	green	0.000	N	1	(edit)			
●	Successful	Laptop1 Sucursal 2	Router Sucursal 2	ICMP	darkblue	0.000	N	2	(edit)			
●	Successful	Laptop2 Sucursal 2	Router Sucursal 2	ICMP	teal	0.000	N	3	(edit)			

Prueba exitosa de conectividad entre los 3 servidores y el dispositivo intermediario (router) de la segunda sucursal de TecmiCorp.

PDU List Window												
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete		
●	Successful	DNS_2	Router Sucursal 2	ICMP	green	0.000	N	0	(edit)			
●	Successful	DNS_2	Router Sucursal 2	ICMP	yellow	0.000	N	1	(edit)			
●	Successful	FTP_2	Router Sucursal 2	ICMP	blue	0.000	N	2	(edit)			

Prueba exitosa de conectividad de 4 dispositivos finales (3 laptops y una PC) y el dispositivo intermediario (router wireless) de la tercera sucursal de TecmiCorp.

PDU List Window												
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete		
●	Successful	PC0 Sucursal 3	Router Sucursal 3	ICMP	■	0.000	N	0	(edit)			
●	Successful	Laptop0 Sucursal 3	Router Sucursal 3	ICMP	■	0.000	N	1	(edit)			
●	Successful	Laptop1 Sucursal 3	Router Sucursal 3	ICMP	■	0.000	N	2	(edit)			
●	Successful	Laptop2 Sucursal 3	Router Sucursal 3	ICMP	■	0.000	N	3	(edit)			

Prueba exitosa de conectividad entre los 3 servidores y el dispositivo intermediario (router) de la tercera sucursal de TecmiCorp.

PDU List Window												
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete		
●	Successful	DNS_3	Router Sucursal 3	ICMP	■	0.000	N	0	(edit)			
●	Successful	HTTP_3	Router Sucursal 3	ICMP	■	0.000	N	1	(edit)			
●	Successful	FTP_3	Router Sucursal 3	ICMP	■	0.000	N	2	(edit)			

Prueba exitosa de conectividad de 4 dispositivos finales (3 laptops y una PC) y el dispositivo intermediario (router) de la cuarta sucursal de TecmiCorp.

PDU List Window												
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete		
●	Successful	PC0 Sucursal 4	Router Sucursal 4	ICMP	■	0.000	N	0	(edit)			
●	Successful	Laptop0 Sucursal 4	Router Sucursal 4	ICMP	■	0.000	N	1	(edit)			
●	Successful	Laptop1 Sucursal 4	Router Sucursal 4	ICMP	■	0.000	N	2	(edit)			
●	Successful	Laptop2 Sucursal 4	Router Sucursal 4	ICMP	■	0.000	N	3	(edit)			

Prueba exitosa de conectividad entre los 3 servidores y el dispositivo intermediario (router) de la cuarta sucursal de TecmiCorp.

PDU List Window												
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete		
●	Successful	DNS_4	Router Sucursal 4	ICMP	■	0.000	N	0	(edit)			
●	Successful	HTTP_4	Router Sucursal 4	ICMP	■	0.000	N	1	(edit)			
●	Successful	FTP_4	Router Sucursal 4	ICMP	■	0.000	N	2	(edit)			

Prueba exitosa de conectividad de 4 dispositivos finales (3 laptops y una PC) y el dispositivo intermediario (router) de la quinta sucursal de TecmiCorp.

PDU List Window										
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0 Sucursal 5	Router Sucursal 5	ICMP		0.000	N	0	(edit)	
	Successful	Laptop0 Sucursal 5	Router Sucursal 5	ICMP		0.000	N	1	(edit)	
	Successful	Laptop1 Sucursal 5	Router Sucursal 5	ICMP		0.000	N	2	(edit)	
	Successful	Laptop2 Sucursal 5	Router Sucursal 5	ICMP		0.000	N	3	(edit)	

Pruéba exitosa de conectividad entre los 3 servidores y el dispositivo intermediario (router) de la quinta sucursal de TecMiCorp.

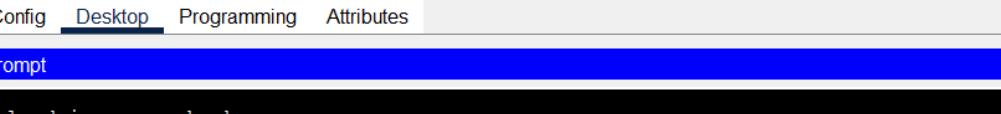
PDU List Window										
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	DNS_5	Router Sucursal 5	ICMP		0.000	N	0	(edit)	
	Successful	HTTP_5	Router Sucursal 5	ICMP		0.000	N	1	(edit)	
	Successful	FTP_5	Router Sucursal 5	ICMP		0.000	N	2	(edit)	

Prueba de Servicio SSH:

Sede Principal

Prueba exitosa de un equipo con el servicio ssh de la sede principal.

Credenciales: Username: **admin_sedenovared** - Password: **passsedenovared**



PC0 SedePrincipal

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>
C:\>ssh -l admin_novaredsede
Invalid Command.

C:\>ssh -l admin_sedenovared 192.168.0.1

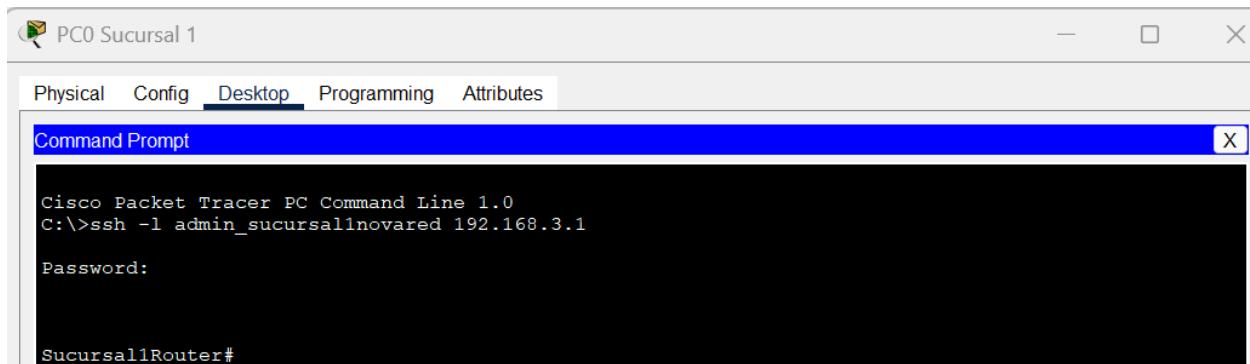
Password:

SedeRouter#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SedeRouter(config)#
```

Sucursal 1

Prueba exitosa de un equipo con el servicio ssh de la primera sucursal.

Credenciales: Username: **admin_sucursal1novared** - Password: **passsucursal1novared**

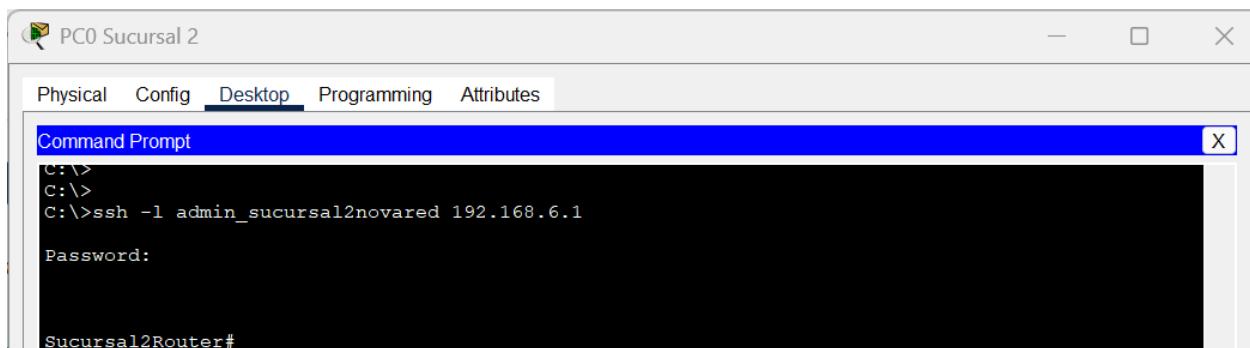


The screenshot shows a window titled "PC0 Sucursal 1". The tab bar at the top has "Physical", "Config", "Desktop" (which is selected), "Programming", and "Attributes". Below the tabs is a "Command Prompt" window with a blue header. The prompt shows the command "Cisco Packet Tracer PC Command Line 1.0" followed by "C:\>ssh -l admin_sucursal1novared 192.168.3.1" and a password prompt "Password:". At the bottom of the command window, it says "Sucursal1Router#".

Sucursal 2

Prueba exitosa de un equipo con el servicio ssh de la segunda sucursal.

Credenciales: Username: **admin_sucursal2novared** - Password: **passsucursal2novared**



The screenshot shows a window titled "PC0 Sucursal 2". The tab bar at the top has "Physical", "Config", "Desktop" (selected), "Programming", and "Attributes". Below the tabs is a "Command Prompt" window with a blue header. The prompt shows the command "Cisco Packet Tracer PC Command Line 1.0" followed by "C:\>" and "C:\>ssh -l admin_sucursal2novared 192.168.6.1" and a password prompt "Password:". At the bottom of the command window, it says "Sucursal2Router#".

Sucursal 3

Prueba exitosa de un equipo con el servicio ssh de la tercera sucursal.

Credenciales: Username: **admin_sucursal3novared** - Password: **passsucursal3novared**

```
C:\>
C:\>ssh -l admin_sucursal3novared 192.168.9.1
Password:

Sucursal3Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Sucursal3Router(config)#
```

Sucursal 4

Prueba exitosa de un equipo con el servicio ssh de la cuarta sucursal.

Credenciales: Username: **admin_sucursal4novared** - Password: **passsucursal4novared**

```
C:\>
C:\>ssh -l admin_sucursal4novared 192.168.12.1
Password:

Sucursal4Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Sucursal4Router(config)#
```

Sucursal 5

Prueba exitosa de un equipo con el servicio ssh de la quinta sucursal.

Credenciales: Username: **admin_sucursal5novared** - Password: **passsucursal5novared**

```
C:\>
C:\>ssh -l admin_sucursal5novared 192.168.15.1
Password:

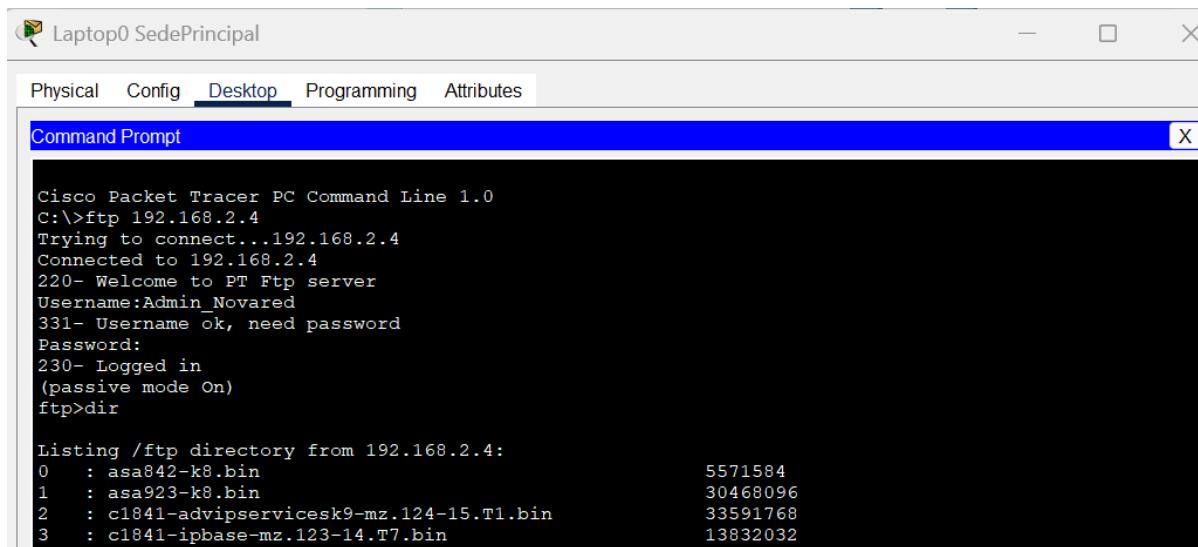
Sucursal5Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Sucursal5Router(config)#
```

Prueba de Servicio FTP:

Sede Principal

Prueba exitosa de un equipo con el servicio ftp de la sede principal.

Credenciales: Username: **Admin_Novared** - Password: **NR_pwd0**



Laptop0 SedePrincipal

Physical Config Desktop Programming Attributes

Command Prompt

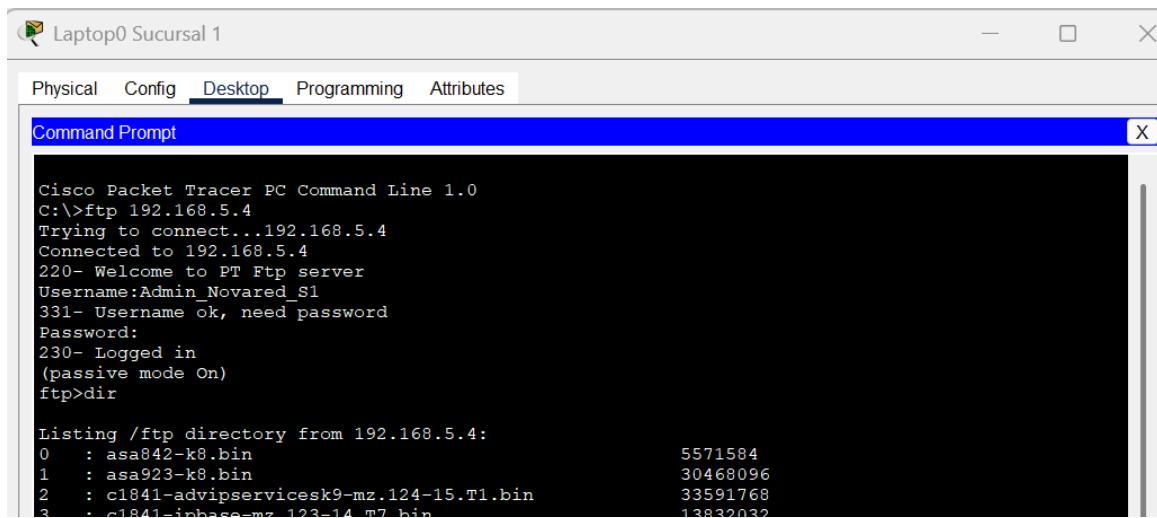
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.2.4
Trying to connect...192.168.2.4
Connected to 192.168.2.4
220- Welcome to PT Ftp server
Username:Admin_Novared
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 192.168.2.4:
0 : asa842-k8.bin          5571584
1 : asa923-k8.bin          30468096
2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
3 : c1841-ipbase-mz.123-14.T7.bin      13832032
```

Sucursal 1

Prueba exitosa de un equipo con el servicio ftp de la primera sucursal.

Credenciales: Username: **Admin_Novard_S1** - Password: **NR_pwd1**



Laptop0 Sucursal 1

Physical Config Desktop Programming Attributes

Command Prompt

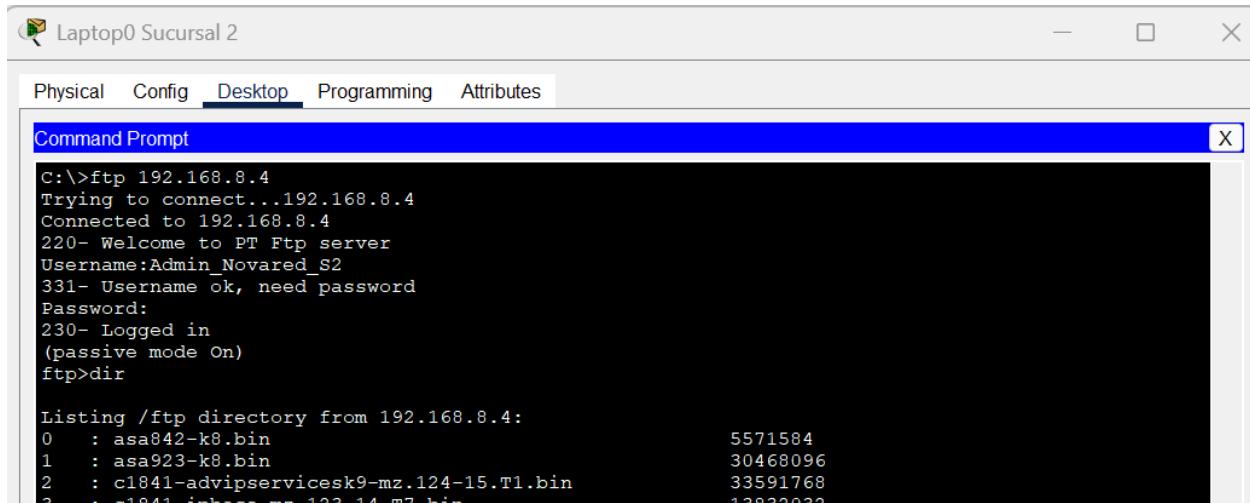
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.5.4
Trying to connect...192.168.5.4
Connected to 192.168.5.4
220- Welcome to PT Ftp server
Username:Admin_Novared_S1
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 192.168.5.4:
0 : asa842-k8.bin          5571584
1 : asa923-k8.bin          30468096
2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
3 : c1841-ipbase-mz.123-14.T7.bin      13832032
```

Sucursal 2

Prueba exitosa de un equipo con el servicio ftp de la segunda sucursal.

Credenciales: Username: **Admin_Novard_S2** - Password: **NR_pwd2**



```
Laptop0 Sucursal 2
Physical Config Desktop Programming Attributes
Command Prompt X

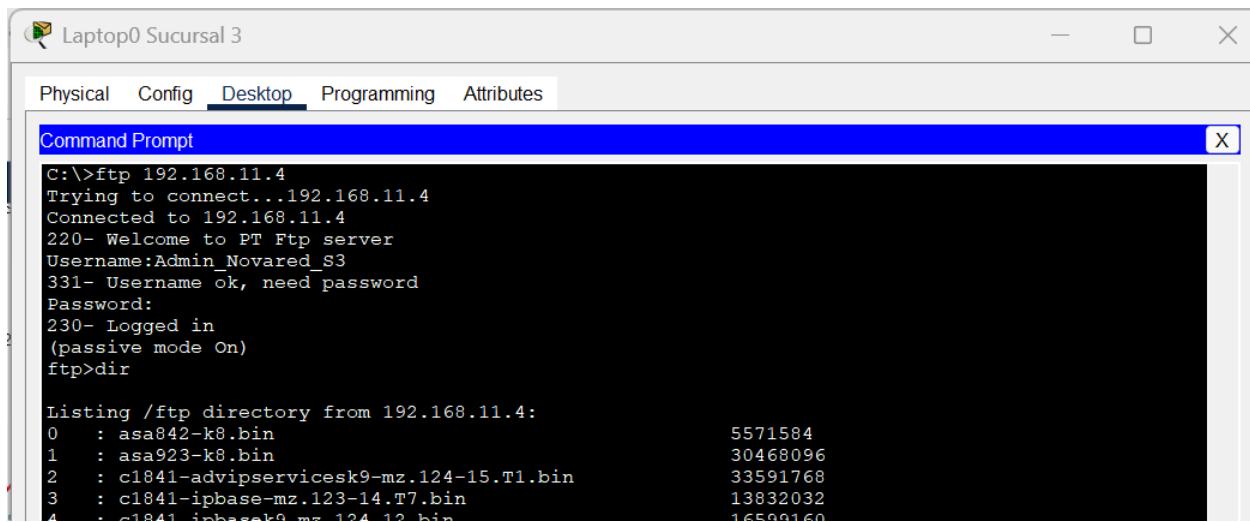
C:\>ftp 192.168.8.4
Trying to connect...192.168.8.4
Connected to 192.168.8.4
220- Welcome to PT Ftp server
Username:Admin_Novared_S2
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 192.168.8.4:
0 : asa842-k8.bin 5571584
1 : asa923-k8.bin 30468096
2 : c1841-advp�servicesk9-mz.124-15.T1.bin 33591768
3 : c1841-ipbase-mz.123-14.T7.bin 13832032
4 : c1841_ipbasek9_mz.124-12.bin 16500160
```

Sucursal 3

Prueba exitosa de un equipo con el servicio ftp de la tercera sucursal.

Credenciales: Username: **Admin_Novard_S3** - Password: **NR_pwd3**



```
Laptop0 Sucursal 3
Physical Config Desktop Programming Attributes
Command Prompt X

C:\>ftp 192.168.11.4
Trying to connect...192.168.11.4
Connected to 192.168.11.4
220- Welcome to PT Ftp server
Username:Admin_Novared_S3
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 192.168.11.4:
0 : asa842-k8.bin 5571584
1 : asa923-k8.bin 30468096
2 : c1841-advp�servicesk9-mz.124-15.T1.bin 33591768
3 : c1841-ipbase-mz.123-14.T7.bin 13832032
4 : c1841_ipbasek9_mz.124-12.bin 16500160
```

Sucursal 4

Prueba exitosa de un equipo con el servicio ftp de la cuarta sucursal.

Credenciales: Username: **Admin_Novard_S4** - Password: **NR_pwd4**

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.14.4
Trying to connect...192.168.14.4
Connected to 192.168.14.4
220- Welcome to PT Ftp server
Username:Admin_Novared_S4
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 192.168.14.4:
0  : asa842-k8.bin          5571584
1  : asa923-k8.bin          30468096
2  : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
3  : c1841-ipbase-mz.123-14.T7.bin    13832032
```

Sucursal 5

Prueba exitosa de un equipo con el servicio ftp de la quinta sucursal.

Credenciales: Username: **Admin_Novard_S5** - Password: **NR_pwd5**

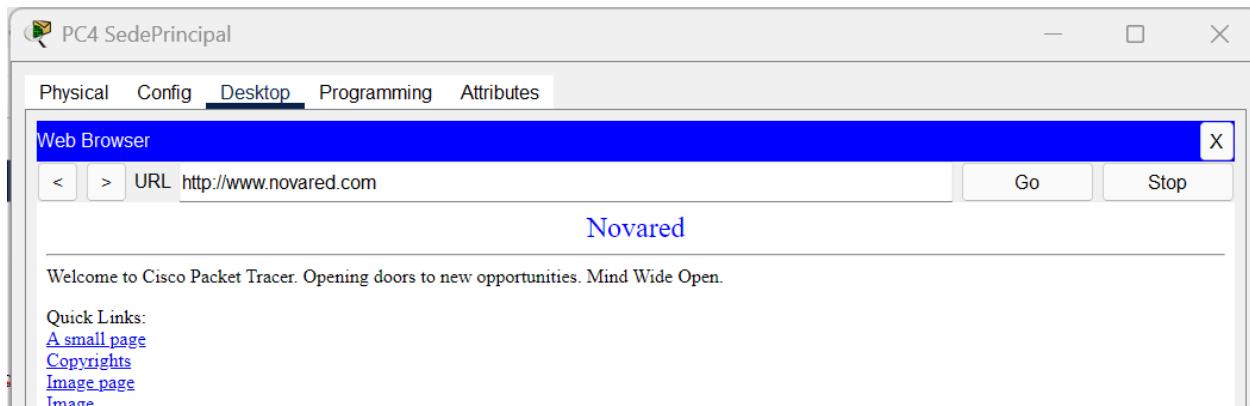
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.17.4
Trying to connect...192.168.17.4
Connected to 192.168.17.4
220- Welcome to PT Ftp server
Username:Admin_Novared_S5
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 192.168.17.4:
0  : asa842-k8.bin          5571584
1  : asa923-k8.bin          30468096
2  : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
3  : c1841-ipbase-mz.123-14.T7.bin    13832032
```

Prueba de Servicios DNS y HTTP:

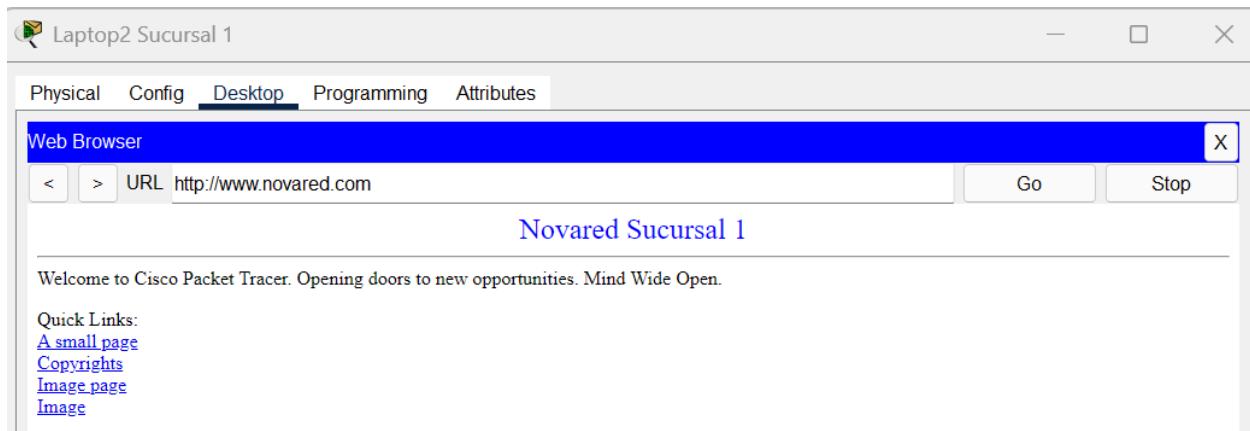
Sede Principal

Prueba exitosa de un equipo con los servicios de DNS y HTTP de la sede principal.



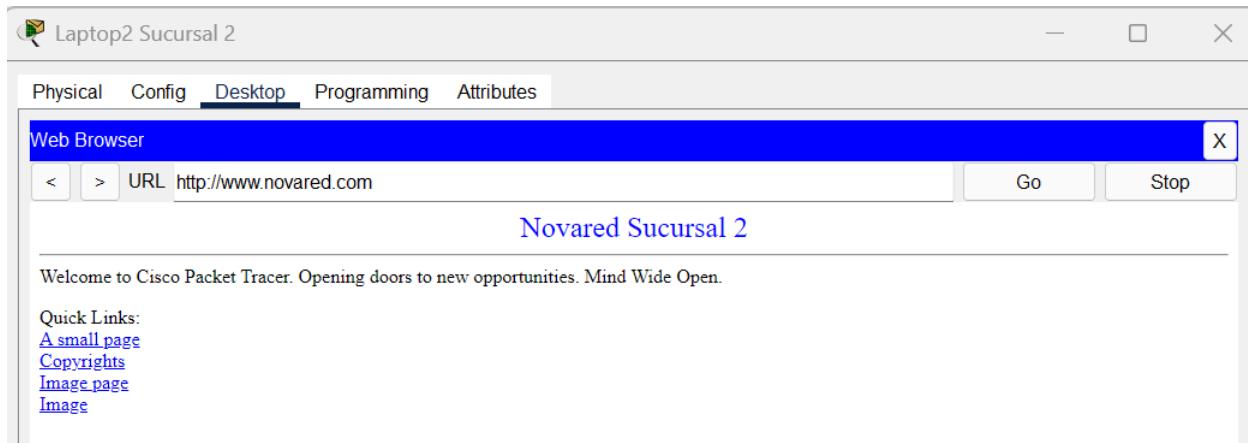
Sucursal 1

Prueba exitosa de un equipo con los servicios de DNS y HTTP de la primera sucursal.



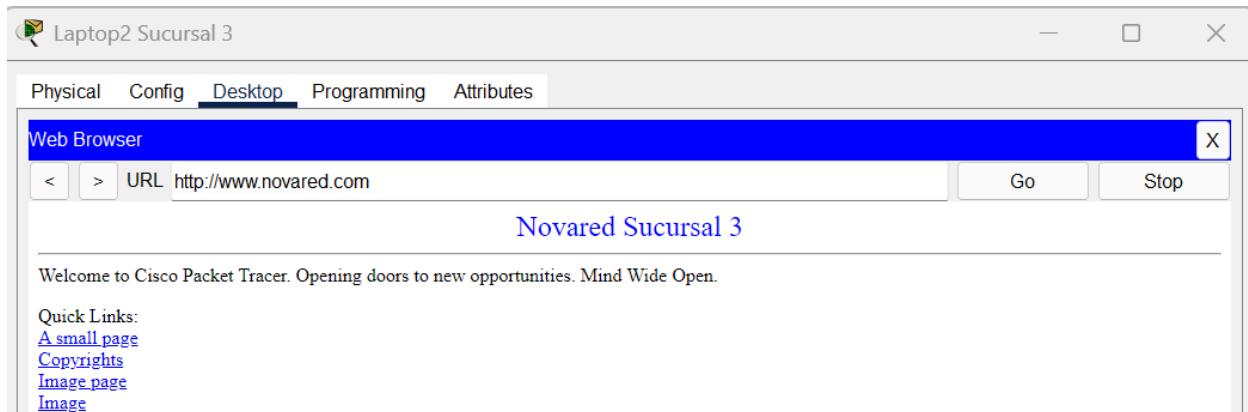
Sucursal 2

Prueba exitosa de un equipo con los servicios de DNS y HTTP de la segunda sucursal.



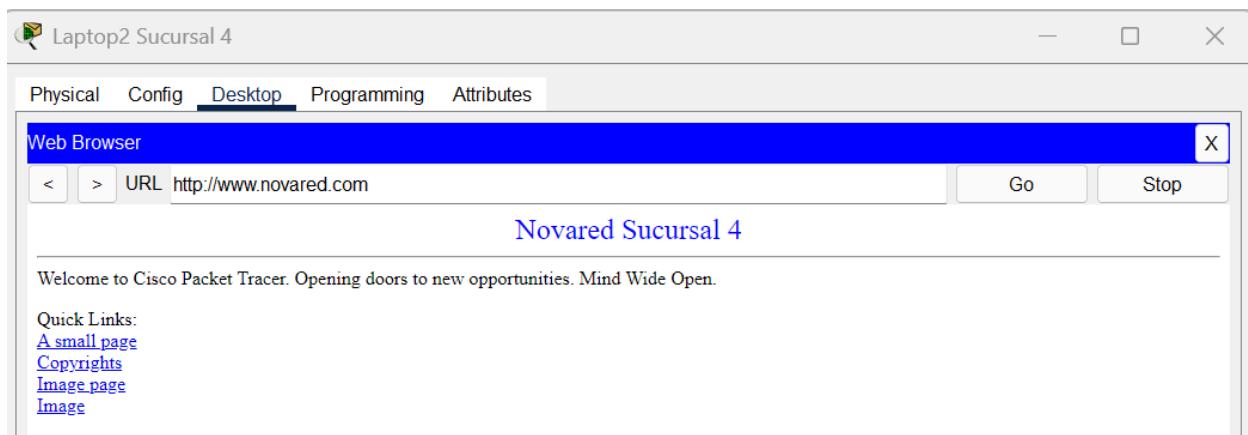
Sucursal 3

Prueba exitosa de un equipo con los servicios de DNS y HTTP de la tercera sucursal.



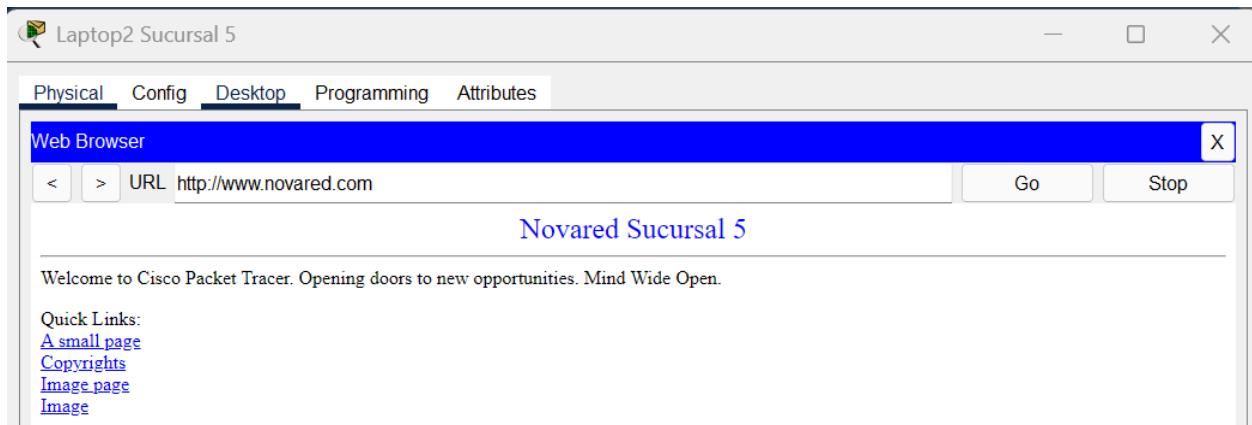
Sucursal 4

Prueba exitosa de un equipo con los servicios de DNS y HTTP de la cuarta sucursal.



Sucursal 5

Prueba exitosa de un equipo con los servicios de DNS y HTTP de la quinta sucursal.

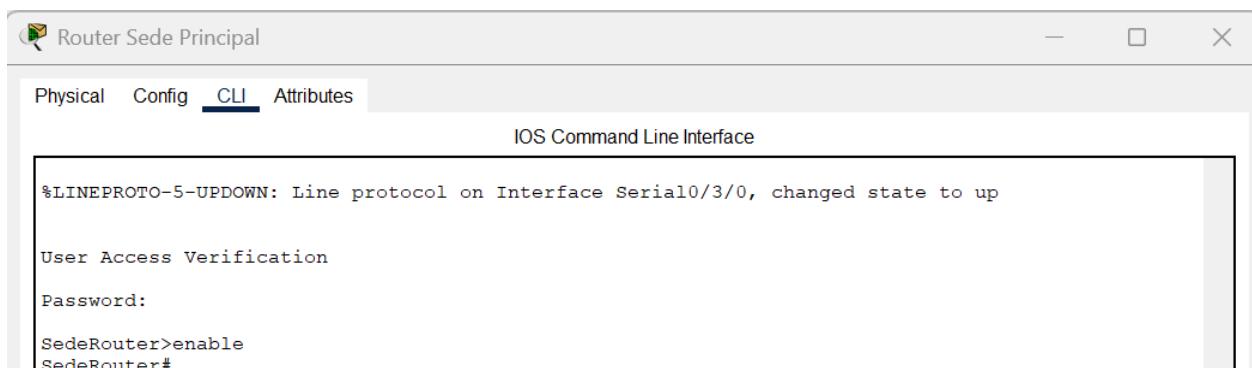


Prueba de contraseña para router:

Para más seguridad dentro de la sede como de las sucursales, se asignó una contraseña para el CLI de router, para que solo los que cuenten con esa contraseña puedan hacer configuraciones en la red.

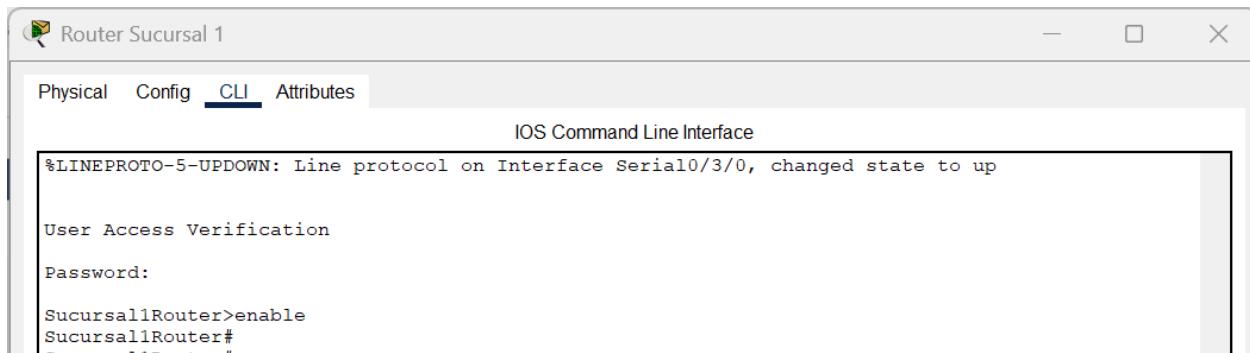
Sede Principal

Password: passnovared



Sucursal 1

Password: passnovareds1



Router Sucursal 1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up
```

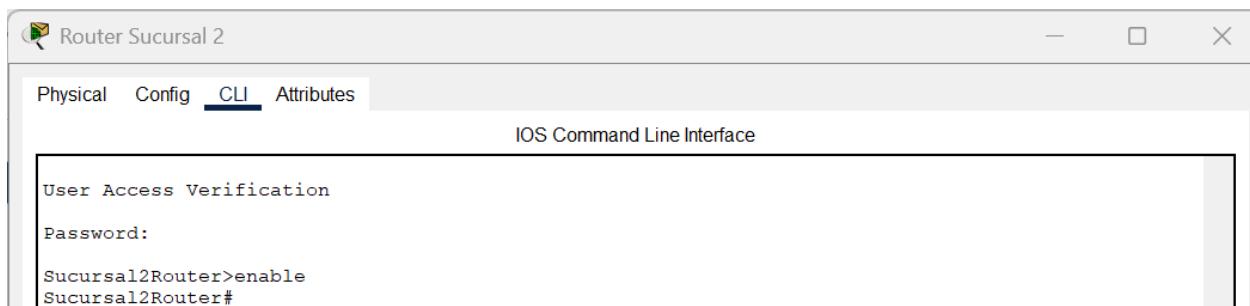
User Access Verification

Password:

```
Sucursal1Router>enable
Sucursal1Router#
```

Sucursal 2

Password: passnovareds2



Router Sucursal 2

Physical Config **CLI** Attributes

IOS Command Line Interface

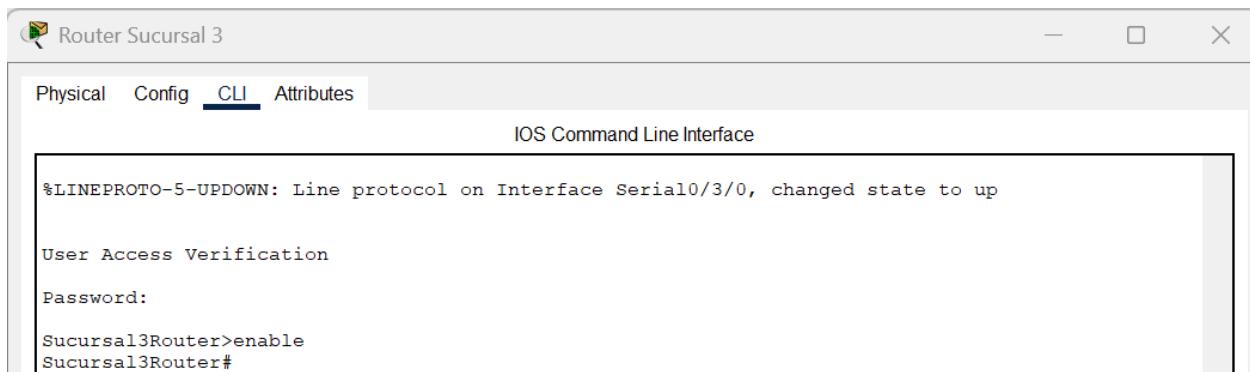
```
User Access Verification
```

Password:

```
Sucursal2Router>enable
Sucursal2Router#
```

Sucursal 3

Password: passnovareds3



Router Sucursal 3

Physical Config **CLI** Attributes

IOS Command Line Interface

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up
```

User Access Verification

Password:

```
Sucursal3Router>enable
Sucursal3Router#
```

Sucursal 4

Password: passnovareds4

Router Sucursal 4

Physical Config **CLI** Attributes

IOS Command Line Interface

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up

User Access Verification
Password:
Sucursal4Router>enable
Sucursal4Router#
```

Sucursal 5

Password: passnovareds5

Router Sucursal 5

Physical Config **CLI** Attributes

IOS Command Line Interface

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up

User Access Verification
Password:
Sucursal5Router>enable
Sucursal5Router#
```

Ping para RIP:

Gracias al uso de RIP se logró hacer comunicación exitosa entre dispositivos finales de sucursales con la sede principal y de sucursales con sucursales.

PDU List Window											
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete	
●	Successful	PC0 SedePrincipal	Laptop1 Sucursal 1	ICMP	■	0.000	N	0	(edit)		
●	Successful	Laptop0 Sucursal 1	PC4 SedePrincipal	ICMP	■	0.000	N	1	(edit)		
●	Successful	PC0 Sucursal 1	DNS	ICMP	■	0.000	N	2	(edit)		
●	Successful	Laptop4 SedePrincipal	HTTP_1	ICMP	■	0.000	N	3	(edit)		
●	Successful	Laptop1 Sucursal 1	PC0 SedePrincipal	ICMP	■	0.000	N	4	(edit)		
●	Successful	Laptop1 Sucursal 1	Laptop3 SedePrincipal	ICMP	■	0.000	N	5	(edit)		
●	Successful	Laptop0 SedePrincipal	Laptop0 Sucursal 1	ICMP	■	0.000	N	6	(edit)		

Conectividad exitosa entre dispositivos finales de la sede principal y dispositivos finales de la segunda sucursal de tecmicorp.

PDU List Window											
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete	
●	Successful	Laptop2 Sucursal 2	PC4 SedePrincipal	ICMP	■	0.000	N	0	(edit)		
●	Successful	Laptop2 SedePrincipal	PC0 Sucursal 2	ICMP	■	0.000	N	1	(edit)		
●	Successful	PC2 SedePrincipal	FTP_2	ICMP	■	0.000	N	2	(edit)		
●	Successful	Laptop4 SedePrincipal	HTTP_2	ICMP	■	0.000	N	3	(edit)		
●	Successful	Laptop0 Sucursal 2	DNS	ICMP	■	0.000	N	4	(edit)		
●	Successful	PC0 Sucursal 2	FTP	ICMP	■	0.000	N	5	(edit)		

Conectividad exitosa entre dispositivos finales de la sede principal y dispositivos finales de la tercera sucursal de tecmicorp.

PDU List Window											
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete	
●	Successful	PC3 SedePrincipal	Laptop0 Sucursal 3	ICMP	■	0.000	N	0	(edit)		
●	Successful	Laptop4 SedePrincipal	PC0 Sucursal 3	ICMP	■	0.000	N	1	(edit)		
●	Successful	PC0 Sucursal 3	PC4 SedePrincipal	ICMP	■	0.000	N	2	(edit)		
●	Successful	Laptop1 Sucursal 3	Laptop1 SedePrincipal	ICMP	■	0.000	N	3	(edit)		
●	Successful	PC0 Sucursal 3	HTTP	ICMP	■	0.000	N	4	(edit)		
●	Successful	Laptop0 SedePrincipal	FTP_3	ICMP	■	0.000	N	5	(edit)		

Conectividad exitosa entre dispositivos finales de la sede principal y dispositivos finales de la cuarta sucursal de tecmicorp.

PDU List Window											
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete	
●	Successful	PC4 SedePrincipal	Laptop2 Sucursal 4	ICMP	■	0.000	N	0	(edit)		
●	Successful	Laptop2 Sucursal 4	PC3 SedePrincipal	ICMP	■	0.000	N	1	(edit)		
●	Successful	Laptop4 SedePrincipal	PC0 Sucursal 4	ICMP	■	0.000	N	2	(edit)		
●	Successful	PC0 SedePrincipal	Laptop1 Sucursal 4	ICMP	■	0.000	N	3	(edit)		
●	Successful	Laptop1 Sucursal 4	DNS	ICMP	■	0.000	N	4	(edit)		
●	Successful	PC2 SedePrincipal	HTTP_4	ICMP	■	0.000	N	5	(edit)		

Conectividad exitosa entre dispositivos finales de la sede principal y dispositivos finales de la quinta sucursal de tecmicorp.

PDU List Window											
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete	
●	Successful	PC2 SedePrincipal	Laptop0 Sucursal 5	ICMP	■	0.000	N	0	(edit)		
●	Successful	PC0 Sucursal 5	Laptop0 SedePrincipal	ICMP	■	0.000	N	1	(edit)		
●	Successful	PC3 SedePrincipal	FTP_5	ICMP	■	0.000	N	2	(edit)		
●	Successful	Laptop2 Sucursal 5	HTTP	ICMP	■	0.000	N	3	(edit)		
●	Successful	Laptop0 SedePrincipal	Laptop1 Sucursal 5	ICMP	■	0.000	N	4	(edit)		
●	Successful	PC0 Sucursal 5	PC0 SedePrincipal	ICMP	■	0.000	N	5	(edit)		

Conectividad exitosa entre algunos dispositivos finales de las sucursales.

PDU List Window											
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete	
●	Successful	Laptop2 Sucursal 1	Laptop2 Sucursal 2	ICMP	■	0.000	N	0	(edit)		
●	Successful	PC0 Sucursal 2	PC0 Sucursal 3	ICMP	■	0.000	N	1	(edit)		
●	Successful	Laptop1 Sucursal 3	Laptop2 Sucursal 4	ICMP	■	0.000	N	2	(edit)		
●	Successful	PC0 Sucursal 4	PC0 Sucursal 5	ICMP	■	0.000	N	3	(edit)		
●	Successful	Laptop2 Sucursal 5	FTP_1	ICMP	■	0.000	N	4	(edit)		
●	Successful	Laptop2 Sucursal 1	Laptop2 Sucursal 3	ICMP	■	0.000	N	5	(edit)		
●	Successful	PC0 Sucursal 2	DNS_5	ICMP	■	0.000	N	6	(edit)		
●	Successful	PC0 Sucursal 1	DNS_4	ICMP	■	0.000	N	7	(edit)		

CONCLUSIÓN DEL PROYECTO



CONCLUSIONES

GLOSARIO DE TÉRMINOS Y CONDICIONES

- **Topología en estrella:**

Definición: Es un tipo de diseño de red en el que todos los dispositivos están conectados a un nodo central, generalmente un switch o un router. Este nodo central es responsable de administrar la comunicación entre los dispositivos.

Ejemplo: En la sede principal de TecmiCorp, la red está diseñada en estrella, donde todas las computadoras y laptops están conectadas a un switch, el cual a su vez se conecta al router principal.

- **Router:**

Definición: Es un dispositivo que gestiona el tráfico de datos en una red, permitiendo la comunicación entre diferentes redes. Su función principal es determinar la mejor ruta para enviar paquetes de información.

Ejemplo: Cada sucursal de TecmiCorp tiene un router wireless que se encarga de conectar los dispositivos locales con la sede principal a través de Internet.

- **Switch:**

Definición: Es un dispositivo de red que permite la comunicación entre múltiples dispositivos dentro de una misma red local (LAN). A diferencia de un hub, un switch envía datos solo al destinatario correcto en lugar de a todos los dispositivos.

Ejemplo: En la sede central de TecmiCorp, se utiliza un switch Cisco 2960-24TT para conectar las computadoras de escritorio mediante cables Ethernet.

- **Host:**

Definición: Es cualquier dispositivo conectado a una red que puede enviar o recibir datos. Un host puede ser una computadora, servidor, impresora, router, smartphone u otro dispositivo con una dirección IP asignada.

Ejemplo: En la red de TecmiCorp, cada PC y laptop funciona como un host con una dirección IP única para comunicarse con otros dispositivos dentro de la infraestructura de red.

- **Ethernet:**

Definición: Es un estándar de conexión de redes de área local (LAN) que permite la transmisión de datos a través de cables de cobre o fibra óptica.

Ejemplo: Las computadoras de escritorio en la sede de TecmiCorp están conectadas a la red mediante cables Ethernet, lo que proporciona una conexión más estable que la red inalámbrica.

- **Wireless (Inalámbrico):**

Definición: Tecnología que permite la comunicación de dispositivos sin necesidad de cables físicos, utilizando ondas de radio o infrarrojos.

Ejemplo: Las laptops de cada sucursal de TecmiCorp se conectan a Internet de forma wireless mediante el router de su respectiva sucursal.

- **IP (Protocolo de Internet):**

Definición: Es una dirección única que identifica a cada dispositivo dentro de una red, permitiendo su comunicación. Se presentan en formato IPv4 o IPv6.

Ejemplo: Cada computadora en la red de TecmiCorp tiene una dirección IP única, la cual se asignó durante la configuración del proyecto.

- **IPv4 (Protocolo de Internet versión 4):**

Definición: Es la cuarta versión del Protocolo de Internet y el más utilizado en la actualidad. Utiliza direcciones de 32 bits, lo que permite aproximadamente 4.3 mil millones de direcciones únicas. Se representa en formato decimal separado por puntos (ejemplo: 192.168.1.1).

Ejemplo: En la red de TecmiCorp, se asignaron direcciones IPv4 estáticas a los routers para mantener una configuración estable.

- **IPv6 (Protocolo de Internet versión 6):**

Definición: Es la versión más reciente del Protocolo de Internet, diseñada para reemplazar a IPv4 debido a la escasez de direcciones. Utiliza direcciones de 128 bits, permitiendo una cantidad prácticamente ilimitada de direcciones. Se representa en formato hexadecimal separado por dos puntos (ejemplo: 2001:0db8:8a3::8a2e:0370:7334).

Ejemplo: En futuras expansiones de la red de TecmiCorp, se podría implementar IPv6 para mejorar la eficiencia y la seguridad de la conectividad.

- **Tabla ARP (Address Resolution Protocol):**

Definición: Es una tabla que mantiene un registro de las direcciones IP y las direcciones MAC correspondientes de los dispositivos en la red.

Ejemplo: En las pruebas de red, los técnicos verificaron la tabla ARP para confirmar que los routers de las sucursales estaban detectando correctamente los dispositivos conectados.

- **Tabla de Enrutamiento:**

Definición: Es una tabla utilizada por los routers para determinar la mejor ruta que deben seguir los paquetes de datos en una red.

Ejemplo: En la red de TecmiCorp, se configuró una tabla de enrutamiento para dirigir correctamente los datos entre la sede principal y las sucursales.

- **CLI (Command Line Interface):**

Definición: Es una interfaz de usuario basada en texto que permite la administración y configuración de dispositivos de red, como routers y switches, mediante comandos en lugar de una interfaz gráfica.

Ejemplo: Durante la configuración de la infraestructura de red de TecmiCorp, los técnicos usaron la CLI para asignar direcciones IP a los routers y switches a través de comandos en la terminal.

- **Ping:**

Definición: Es una herramienta de diagnóstico utilizada para comprobar la conectividad entre dos dispositivos en una red. Si un ping es exitoso, significa que los dispositivos pueden comunicarse.

Ejemplo: En las pruebas de conectividad, se utilizó el comando ping para verificar que las computadoras de la sede central podían comunicarse con las de las sucursales.

- **MAC Address (Dirección MAC):**

Definición: Es un identificador único asignado a cada tarjeta de red de un dispositivo. Se expresa en un formato hexadecimal como 00:1A:2B:3C:4D:5E.

Ejemplo: Para gestionar la seguridad de la red en TecmiCorp, se registraron las direcciones MAC de cada laptop y computadora en la sede central y sucursales.

- **LAN (Red de Área Local):**

Definición: Es una red que conecta dispositivos dentro de un área geográfica limitada, como una oficina o una empresa.

Ejemplo: Cada sucursal de TecmiCorp tiene su propia LAN, que conecta los dispositivos de la sucursal mediante un switch y un router.

- **WAN (Red de Área Amplia):**

Definición: Es una red que cubre grandes áreas geográficas, conectando múltiples redes LAN. Internet es el mejor ejemplo de una WAN.

Ejemplo: La sede principal y las sucursales de TecmiCorp están conectadas a través de una WAN, utilizando routers para la comunicación entre ellas.

- **DHCP (Dynamic Host Configuration Protocol):**

Definición: Es un protocolo que asigna automáticamente direcciones IP a los dispositivos de una red, evitando la necesidad de configurarlas manualmente.

Ejemplo: En la red de TecmiCorp, el router de cada sucursal utiliza DHCP para asignar direcciones IP a las laptops conectadas de manera inalámbrica.

- **VLAN (Red de Área Local Virtual):**

Definición: Es una segmentación lógica dentro de una red física que permite separar el tráfico de datos sin necesidad de múltiples switches.

Ejemplo: Si TecmiCorp quisiera separar el tráfico de la red entre empleados administrativos y técnicos, podría crear dos VLANs en su switch gestionable.

- **SSID (Service Set Identifier):**

Definición: Es el nombre de una red WiFi que los dispositivos utilizan para conectarse.

Ejemplo: Cada sucursal de TecmiCorp tiene un SSID único, como por ejemplo "WiFi_TecmiCorp_Sucursal1", para que los empleados puedan identificar la red correcta.

- **Subred (Subnetting):**

Definición: Es una división dentro de una red más grande, utilizada para mejorar la eficiencia del tráfico y la seguridad.

Ejemplo: En TecmiCorp, se pueden usar subredes para separar el tráfico de los empleados administrativos y el tráfico de los servidores.

- **NAT (Network Address Translation):**

Definición: Es un método utilizado en routers para permitir que múltiples dispositivos de una red privada compartan una única dirección IP pública.

Ejemplo: En la sede principal de TecmiCorp, el router utiliza NAT para que todas las computadoras puedan acceder a Internet usando una sola dirección IP pública.

- **Red Mesh (Malla):**

Definición: Es un tipo de red inalámbrica en la que varios routers trabajan juntos para proporcionar una cobertura más amplia y estable.

Ejemplo: Si TecmiCorp quisiera mejorar la cobertura WiFi en toda su sede, podría implementar una red Mesh en lugar de depender de un solo router.

- **Protocolo de Enrutamiento:**

Definición: Son reglas que determinan cómo los routers se comunican entre sí para encontrar la mejor ruta para los datos.

Ejemplo: En la red de TecmiCorp, se puede usar un protocolo de enrutamiento dinámico, como OSPF o RIP, para mejorar la comunicación entre sucursales.

- **Proxy:**

Definición: Es un servidor que actúa como intermediario entre los dispositivos de una red y el acceso a Internet, filtrando y gestionando el tráfico.

Ejemplo: TecmiCorp podría utilizar un proxy para bloquear el acceso a sitios web no autorizados desde sus computadoras corporativas.

- **Latencia:**

Definición: Es el tiempo que tarda un paquete de datos en viajar de un punto a otro dentro de una red. Se mide en milisegundos (ms).

Ejemplo: Si la latencia en la comunicación entre la sede principal y las sucursales de TecmiCorp es alta, los empleados experimentarán retrasos al acceder a servidores remotos.

- **Red de Alta Disponibilidad:**

Definición: Es una infraestructura de red diseñada para minimizar el tiempo de inactividad, garantizando que los servicios siempre estén operativos.

Ejemplo: TecmiCorp implementó una red de alta disponibilidad con enlaces redundantes para evitar interrupciones en caso de fallos en el sistema.

- **Red escalable:**

Definición: Se refiere a una red que puede expandirse fácilmente con más dispositivos sin comprometer su rendimiento.

Ejemplo: El diseño de red en TecmiCorp es escalable, lo que permite agregar más computadoras y sucursales sin afectar la conectividad existente.

- **Dirección IP Estática:**

Definición: Es una dirección IP fija asignada manualmente a un dispositivo en la red.

Ejemplo: El router de la sede central de TecmiCorp tiene una dirección IP estática para garantizar una configuración estable en la red.

- **Dirección IP Dinámica:**

Definición: Es una dirección IP que cambia periódicamente y es asignada por un servidor DHCP.

Ejemplo: Las laptops de las sucursales reciben direcciones IP dinámicas, asignadas automáticamente por el router de cada sucursal.

- **Switch Gestionable:**

Definición: Es un switch que permite configuraciones avanzadas, como la creación de VLANs y control del tráfico de red.

Ejemplo: En TecmiCorp se usa un switch gestionable Cisco 2960-24TT para controlar mejor la conectividad de la sede principal.

- **Firewall:**

Definición: Es un sistema de seguridad que controla el tráfico de red, permitiendo o bloqueando conexiones según reglas predefinidas.

Ejemplo: En la sede principal de TecmiCorp, un firewall protege la red contra accesos no autorizados desde Internet.

- **Ancho de Banda:**

Definición: Es la cantidad máxima de datos que pueden transmitirse en una red en un período de tiempo determinado, medido en Mbps o Gbps.

Ejemplo: TecmiCorp contrató un servicio de Internet de 100 Mbps para garantizar que la sede principal tenga suficiente ancho de banda para todas sus operaciones.

- **QoS (Quality of Service):**

Definición: Es una técnica utilizada en redes para priorizar ciertos tipos de tráfico, asegurando que aplicaciones críticas tengan mejor rendimiento.

Ejemplo: Si TecmiCorp usa QoS, puede priorizar el tráfico de videollamadas sobre descargas de archivos, evitando interrupciones en reuniones virtuales.

- **VPN (Virtual Private Network):**

Definición: Es una conexión segura que permite a los empleados acceder a la red corporativa desde ubicaciones remotas.

Ejemplo: Si un empleado de TecmiCorp trabaja desde casa, puede conectarse a la red de la empresa a través de una VPN segura.

BIBLIOGRAFÍA

FS.com. (n.d.). RIP vs OSPF: ¿Cuál es la diferencia?. Recuperado de

<https://www.fs.com/es/blog/rip-vs-ospf-what-is-the-difference-5221.html>

Cisco Networking Academy. (s.f.).

[Cisco Networking Academy](#)

OpenAI. (2024). ChatGPT (modelo GPT-4-turbo) [Asistente de IA].

<https://openai.com/chatgpt>

AUTORES



Alonso Renovato Esparza



Roberto Alejandro Ovalle Garza



Emilio Arturo Rodriguez Veloz



Gael Marroquín Torres



Josue David Murillo Gomez

CONCLUSIÓN

La implementación de la infraestructura de NovaRed para Tecmicorp representa un avance significativo en la seguridad, escalabilidad y eficiencia de la red corporativa. A lo largo del desarrollo de esta tesis, se diseñó una topología de red jerárquica de tres niveles con una arquitectura WAN en estrella, conectando una sede principal con cinco sucursales mediante enrutamiento dinámico RIP. Además, se configuraron servicios críticos como DHCP, DNS, SSH, HTTP y FTP para optimizar la administración de los recursos y garantizar la conectividad entre los distintos nodos de la red.

El diseño de la red no solo permite una mejor gestión del tráfico y segmentación eficiente, sino que también refuerza la seguridad mediante la implementación de protocolos de acceso remoto seguro y monitoreo constante de la infraestructura. La inclusión de servidores dedicados por sucursal y switches bien estructurados minimiza los puntos únicos de falla y mejora la redundancia del sistema.

En términos de pruebas, se verificó la conectividad y el correcto funcionamiento de los servicios implementados, asegurando que la red cumpla con los requisitos operativos de la empresa. Se realizaron simulaciones de tráfico y escenarios de contingencia para evaluar la estabilidad de la infraestructura bajo distintas condiciones de carga.

En conclusión, la infraestructura de NovaRed ofrece una solución robusta y escalable que facilita la administración de la red en un entorno corporativo con múltiples sucursales. Su diseño modular permite futuras expansiones sin comprometer la estabilidad de la red, asegurando así la continuidad operativa de Tecmicorp y optimizando el rendimiento de sus servicios.

Link del video explicativo

[Novared para Tecmicorp](#)