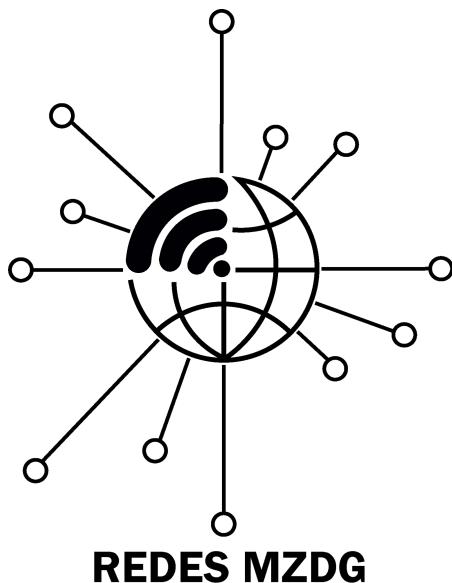


# Proyecto Final

## Propuesta de Topología de Red — TecmiCorp

|                                     |  |
|-------------------------------------|--|
| <b>Materia:</b><br>Gestión de Redes | <b>Maestros:</b><br>Blanca Aracely Aranda Machorro |
| <b>Módulo:</b><br>Semana 7          | <b>Actividad:</b><br>Proyecto final                |
| <b>Fecha:</b> 14 de enero de 2025   |  |



## ÍNDICE

|   |           |
|---|-----------|
| <b>Propuesta de Topología de Red — TecmiCorp.....</b> | <b>0</b>  |
| <b>ÍNDICE.....</b>                                    | <b>1</b>  |
| <b>Resumen.....</b>                                   | <b>3</b>  |
| <b>Introducción.....</b>                              | <b>4</b>  |
| <b>Propuesta de Topología de Red — TecmiCorp.....</b> | <b>5</b>  |
| Alcance.....  | 7         |
| Análisis.....   | 8         |
| Diseño.....   | 9         |
| En general.....                                       | 9         |
| Sede central.....                                     | 10        |
| Sucursales.....                                       | 14        |
| Tabla de equipos y sus propósitos.....                | 16        |
| Desarrollo.....                                       | 24        |
| ISP / MPLS.....                                       | 24        |
| DHCP.....   | 25        |
| Servidor FTP.....                                     | 28        |
| Servidor DNS.....                                     | 29        |
| Servidor WEB.....                                     | 31        |
| Implementación.....                                   | 33        |
| Configuración de comunicaciones.....                  | 33        |
| Wireless:.....  | 33        |
| Cableado:.....  | 35        |
| Seguridad.....  | 40        |
| Redundancia:.....                                     | 40        |
| Usuarios y Administradores:.....                      | 42        |
| Límite de IP's:.....                                  | 43        |
| Recomendaciones de Seguridad para la Topología.....   | 43        |
| Potenciales ataques a la red.....                     | 44        |
| Identificación de amenazas comunes.....               | 46        |
| Medidas de seguridad.....                             | 47        |
| Propuestas para hacer que la red sea confiable.....   | 48        |
| Pruebas y Resultados.....                             | 51        |
| Prueba de ping.....                                   | 51        |
| Pruebas de DNS y FTP.....                             | 54        |
| <b>Anexo:.....</b>                                    | <b>59</b> |
| Configuración de la sede central.....                 | 60        |
| Configuración de las sucursales.....                  | 74        |

|  |            |
|--|------------|
| Intercomunicación entre sede central y sucursales..... | 77         |
| <b>Pruebas.....</b>                                    | <b>92</b>  |
| A través de ping.....                                  | 92         |
| A través de PDU's.....                                 | 93         |
| <b>Glosario de Términos y Condiciones.....</b>         | <b>96</b>  |
| <b>Bibliografía.....</b>                               | <b>97</b>  |
| <b>Autores.....</b>                                    | <b>99</b>  |
| <b>Conclusiones.....</b>                               | <b>102</b> |
| <b>Agradecimientos.....</b>                            | <b>105</b> |

## Resumen

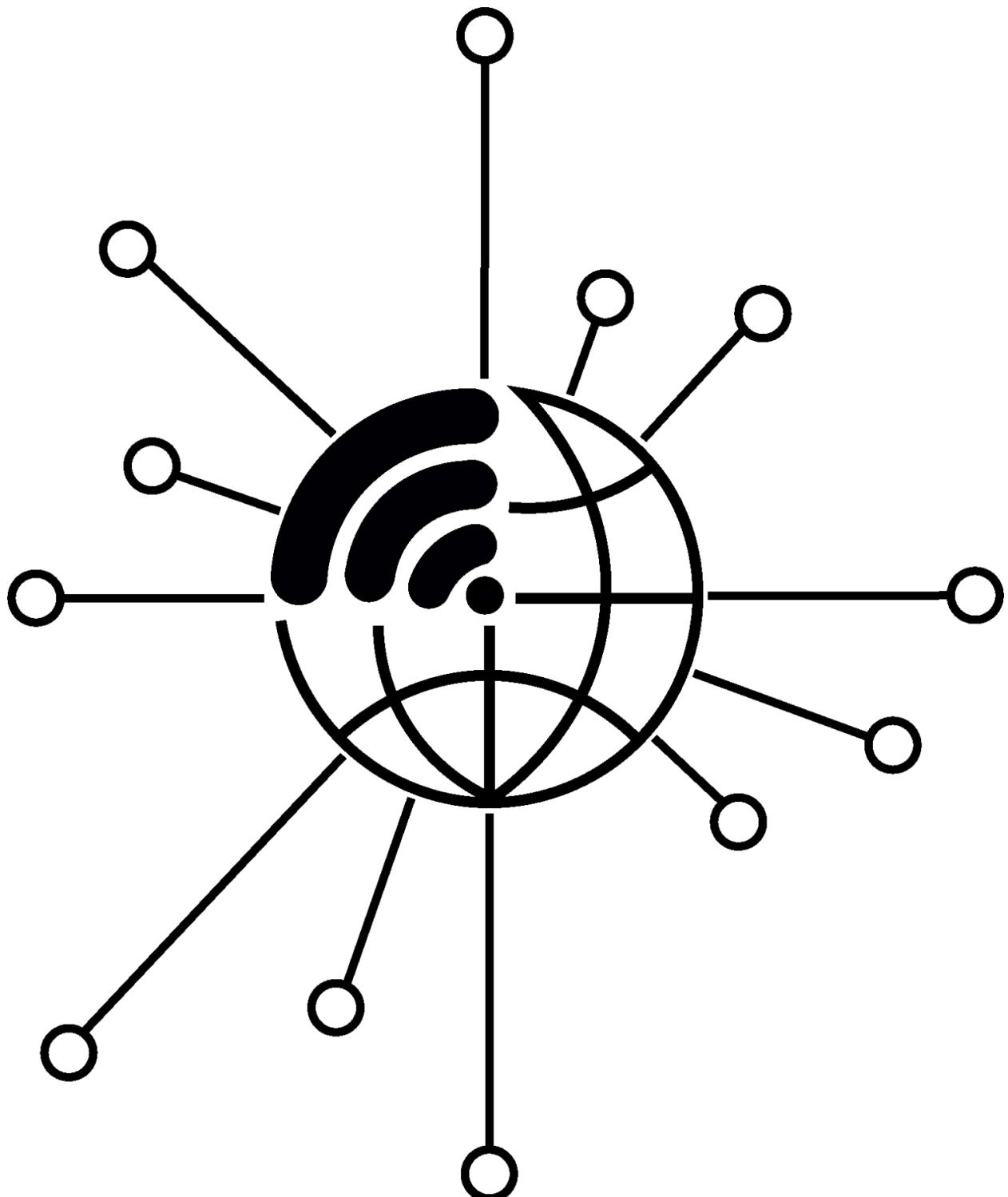
En este documento, se describe el desarrollo de la propuesta de infraestructura de red para la empresa “TecmiCorp”, la cual se especifica que está pasando por una creciente demanda de conectividad, la cual representa un reto para la empresa. Como consultores de redes, se ha diseñado una solución innovadora, segura y escalable mediante el uso de la herramienta de Cisco Packet Tracer, con la cual se simula el correcto funcionamiento de la red. El proyecto se divide en dos fases principales. La primera fase se centra en el diseño y configuración de la red para la sede central y las cinco sucursales con las que cuenta la empresa. En la segunda fase se implementa un servidor FTP a la red diseñada en la fase 1 y se garantiza la estabilidad y protección de la infraestructura. Por medio de este caso de estudio se demuestra aspectos importantes en el proceso del desarrollo de una infraestructura de red como una planificación adecuada, el uso de herramientas clave y la optimización del rendimiento y seguridad de la red.

**Palabras Clave:** *Infraestructura de red, Cisco Packet Tracer, Seguridad de redes, Servidor FTP, Configuración de la red.*

## Introducción

Una pequeña empresa llamada “TecmiCorp”, la cual actualmente se encuentra en expansión, se está enfrentando a un reto donde con su infraestructura actual no le permite satisfacer la demanda de conectividad por parte de sus clientes e incluso de sus mismos colaboradores. Nuestro objetivo es ofrecerle a esta empresa un diseño de infraestructura de red en donde se tenga una sede central y cinco sucursales, cada una con sus respectivos dispositivos. Dicha red deberá ser sólida, segura y escalable, con la capacidad de adaptarse al crecimiento que pueda tener este negocio. La sede central contará con 10 dispositivos finales: 5 equipos de escritorio y 5 laptops; mientras que cada sucursal contará con 1 equipo de escritorio y 3 laptops. Tanto la sede como cada sucursal deberán contar con sus respectivos switches y routers para habilitar el envío de datos entre sucursales y desde y hacia la sede central. Finalmente, la comunicación entre la sede y sucursales debe realizarse de manera inalámbrica. Esto, nuevamente, para asegurar una red sólida, segura y escalable.

## **Propuesta de Topología de Red — TecmiCorp**



# REDES MZDG

## **Alcance**

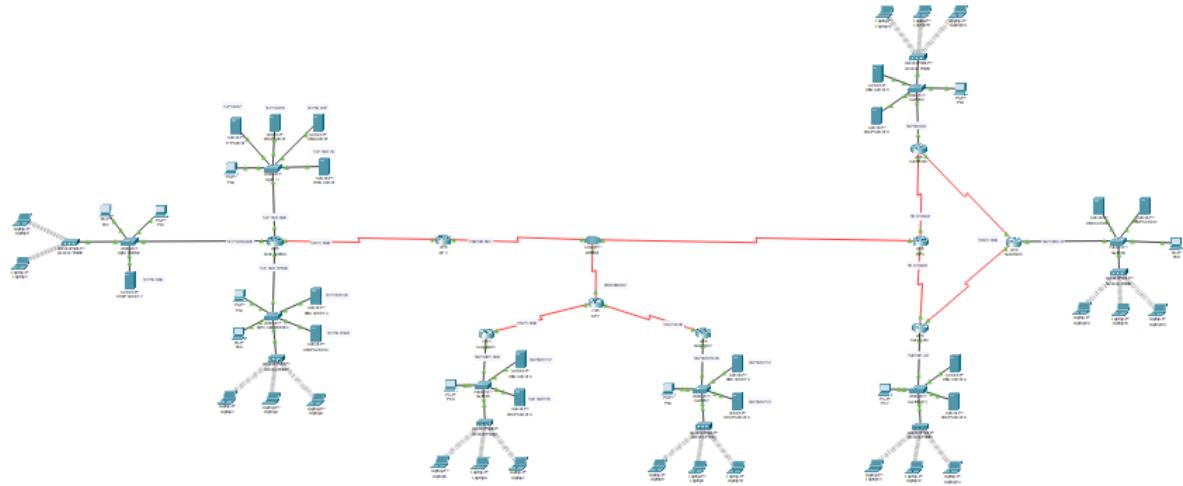
La empresa TecmiCorp, dedicada a la creación, elaboración y distribución de videojuegos. La sede central representa los encargados del marketing y la elaboración y desarrollo de videojuegos, mientras que cada sucursal se encarga de la distribución en cada ciudad. Nuestra investigación e infraestructura de topología de estrella refleja la manera segura y escalable de expandir un negocio a varias sucursales en distintas ciudades y/o estados. Demostramos cómo podemos realizar una intercomunicación entre la sede central y entre cada sucursal. Logramos que haya una cantidad limitada de conexiones para que, al intentar agregar un nuevo dispositivo, su configuración resulte sencilla y sin dificultades. La infraestructura que hemos creado aquí es un ejemplo viable que cualquier empresa puede usar para expandir su negocio sin fallas y con las medidas de seguridad necesarias para salir y enfrentar los retos del mundo moderno.

## Análisis

La topología que usamos para la infraestructura fue la del tipo estrella ya que ésta nos permite seguir interactuando con la propia red en caso de que haya habido un error con un equipo de cómputo. Esta topología es la mejor en nuestro caso ya que hemos previsto las situaciones en donde una sucursal o un equipo deje de funcionar por alguna razón. De esta manera, no comprometerá la red de ninguna manera. La razón del por qué hemos decidido usar una cantidad considerable de sucursales es por el hecho de que, en la vida real, las empresas y compañías están en constante crecimiento y necesitan una manera real y funcional de expandirse. Asimismo, no pueden quedarse con conexiones anticuadas, en donde todo se conectaba únicamente con cableado. Las conexiones modernas requieren de dispositivos tanto conectados como inalámbricos. Nuestra infraestructura demuestra una resolución de estas demandas modernas y cómo una expansión a otras ciudades o estados es posible y de manera segura, correcta y escalable. De la misma manera, nuestra infraestructura demuestra las posibles soluciones en caso de que haya fallos en la red y cómo responder ante amenazas de seguridad comunes y específicas.

## Diseño

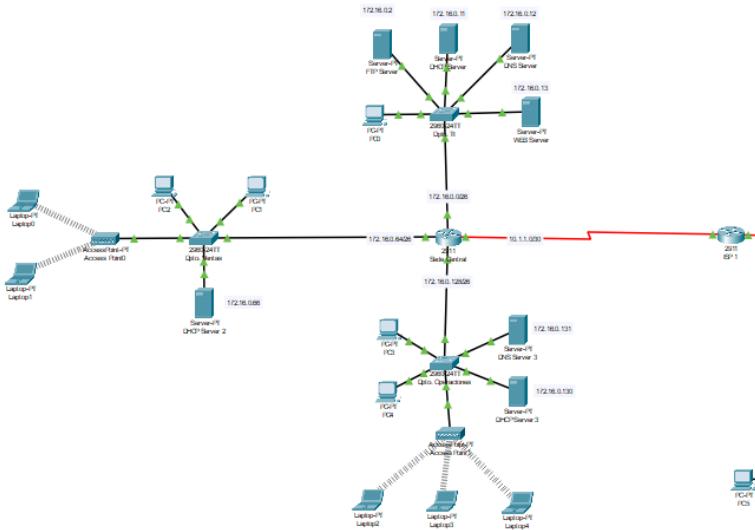
En general



- Según la ubicación de las diferentes “regiones” de nuestra red, estas “regiones” se conectan directamente a una ISP diferente:
  - El router de la sede central se conecta al ISP 1.
  - Los routers de las sucursales 1 y 2 se conectan al ISP 2.
  - Los routers de las sucursales 3 y 5 se conectan al ISP 3.
    - El router de la sucursal 4 no está conectado directamente al ISP, pero sí lo está a los routers de las otras dos sucursales de su “región”. Esto se debe a que, debido a la forma en la que la red fue segmentada, sólo dos routers (sucursales) se pueden conectar directamente al ISP.
    - Para permitirle conexión, la sucursal 4 utiliza enrutamiento dinámico, tomando las mismas rutas que las sucursales 3 y 5.

- Los ISPs tienen múltiples propósitos: además de permitir la conexión entre diferentes “regiones” mediante el internet (representado como una nube en Cisco Packet Tracer), también permite que todo lo que está dentro de una región se pueda comunicar entre sí de forma más rápida.
- Dentro de todas las redes, los PCs, los servidores y los puntos de acceso son conectados mediante cables Ethernet a los switches de sus respectivas zonas (ej. los diferentes departamentos de la sede central o cada sucursal), estos siendo conectados a los routers de sus zonas (sea la sede central en sí o cada sucursal), y finalmente, a los ISPs. Las laptops se conectan de forma inalámbrica a los puntos de acceso.

## Sede central



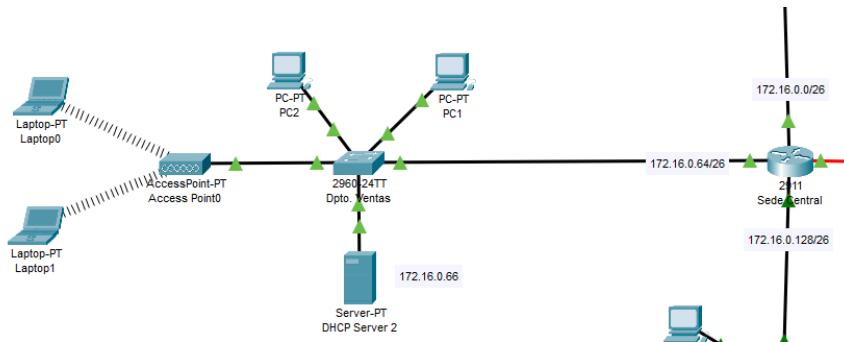
- Usa máscara de subred /24, y luego es segmentada con la máscara /26, lo que resulta en cuatro subredes con 62 direcciones IPv4 disponibles para los hosts

(dos direcciones son usadas para el network y para el broadcast en todas las subredes).

#### Subnets

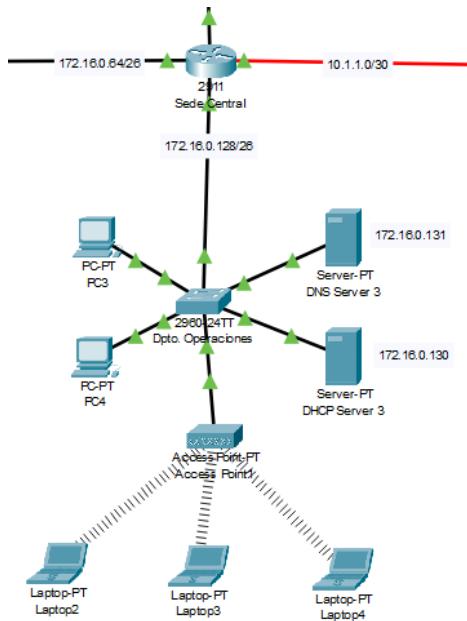
|            |                      |  |
|------------|----------------------|--|
| Netmask:   | 255.255.255.192 = 26 | <b>11111111.11111111.11111111.11 000000</b>                    |
| Wildcard:  | 0.0.0.63             | 00000000.00000000.00000000.00 111111                           |
| Network:   | 172.16.0.0/26        | <b>10101100.00010000.00000000.00 000000</b> ( <b>Class B</b> ) |
| Broadcast: | 172.16.0.63          | 10101100.00010000.00000000.00 111111                           |
| HostMin:   | 172.16.0.1           | 10101100.00010000.00000000.00 000001                           |
| HostMax:   | 172.16.0.62          | 10101100.00010000.00000000.00 111110                           |
| Hosts/Net: | 62                   | (Private Internet)   |
| Network:   | 172.16.0.64/26       | <b>10101100.00010000.00000000.01 000000</b> ( <b>Class B</b> ) |
| Broadcast: | 172.16.0.127         | 10101100.00010000.00000000.01 111111                           |
| HostMin:   | 172.16.0.65          | 10101100.00010000.00000000.01 000001                           |
| HostMax:   | 172.16.0.126         | 10101100.00010000.00000000.01 111110                           |
| Hosts/Net: | 62                   | (Private Internet)   |
| Network:   | 172.16.0.128/26      | <b>10101100.00010000.00000000.10 000000</b> ( <b>Class B</b> ) |
| Broadcast: | 172.16.0.191         | 10101100.00010000.00000000.10 111111                           |
| HostMin:   | 172.16.0.129         | 10101100.00010000.00000000.10 000001                           |
| HostMax:   | 172.16.0.190         | 10101100.00010000.00000000.10 111110                           |
| Hosts/Net: | 62                   | (Private Internet)   |

- Solamente tres de estas subredes son usadas, cada una para un departamento de la sede: una para el de ventas, otra para el de operaciones y otra para el de TI. Estos son representados por los switches, los cuales también están conectados todos al router de la sede central, lo que permite una comunicación más instantánea entre estos.

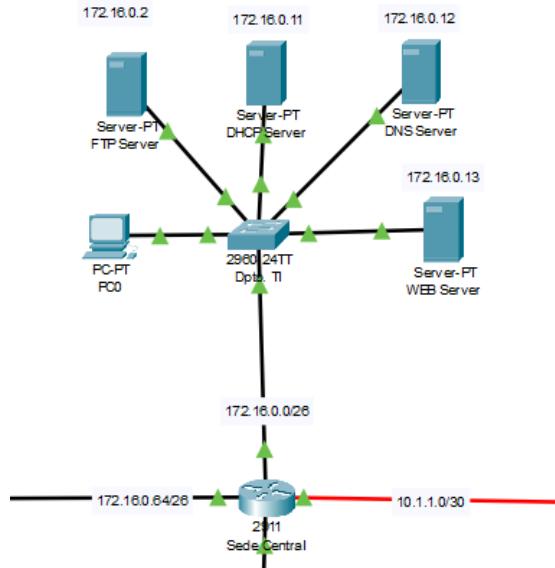


- La subred del departamento de ventas:
  - Contiene dos PCs.
  - Contiene un servidor DHCP.

- Contiene dos laptops.
- Contiene un punto de acceso.



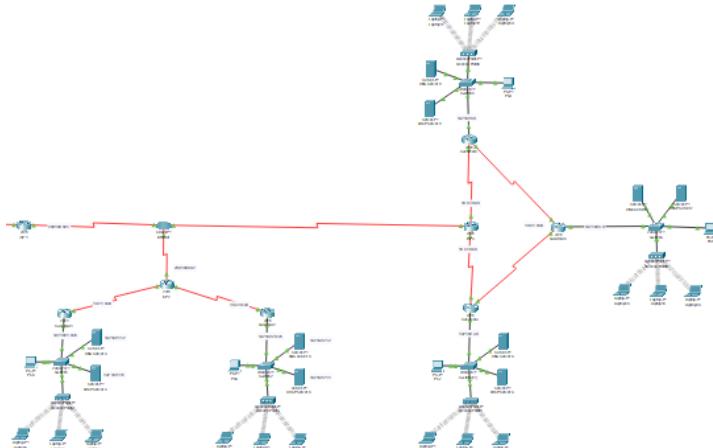
- La subred del departamento de operaciones:
  - Contiene dos PCs.
  - Contiene un servidor DHCP.
  - Contiene un servidor DNS.
  - Contiene dos laptops.
  - Contiene un punto de acceso.



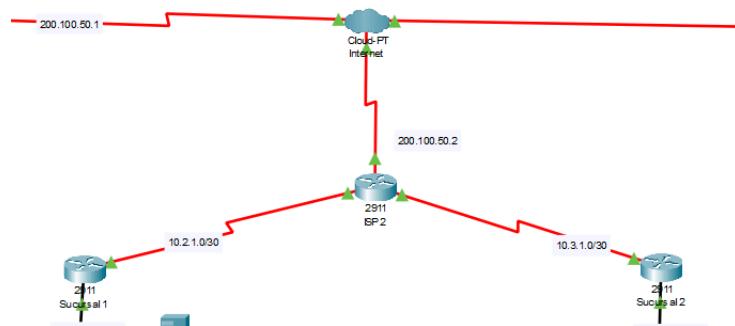
- La subred del departamento de IT:

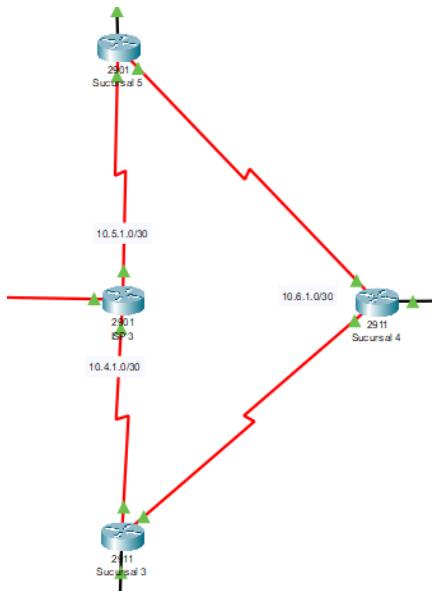
- Contiene una PC.
- Contiene un servidor DHCP.
- Contiene un servidor DNS.
- Contiene un servidor FTP.
- Contiene un servidor WEB.

## Sucursales

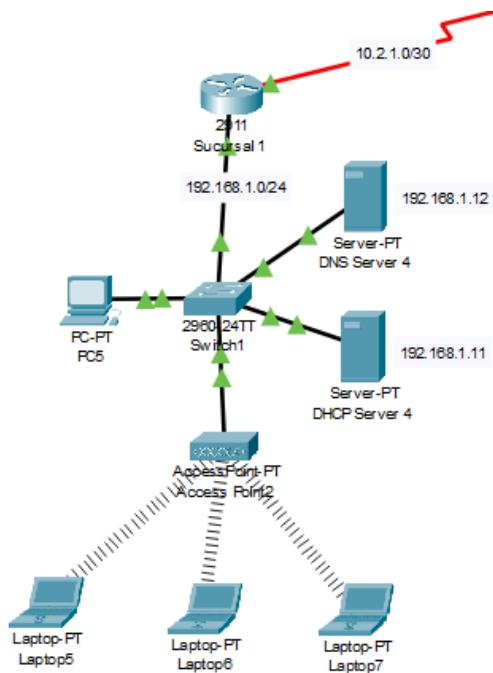


- Los ISPs se segmentan con una máscara de subred /30, dando dos direcciones IP (y por consiguiente, solamente dos conexiones) disponibles. Estas son usadas para conectar las sucursales directamente, estas siendo representadas con routers.





- Todas las sucursales, a excepción de la 4ta, se conectan directamente con los ISPs de sus “regiones” correspondientes: las sucursales 1 y 2 al ISP 2, y las sucursales 3 y 5 al ISP 3.
  - Como se mencionó anteriormente, la sucursal 4 utiliza enrutamiento dinámico para acceder al ISP 3.



- Internamente, todas las subredes:
  - Contienen un switch.
  - Contienen una PC.
  - Contienen dos servidores PT.
  - Contienen tres laptops.
  - Contienen un punto de acceso.

Tabla de equipos y sus propósitos

| Nombre del equipo        | Tipo de equipo | IP          | Tipo de IP | Sede / Sucursal | Dpto. | Propósito   |
|--------------------------|----------------|-------------|------------|-----------------|-------|---|
| Dpto. TI                 | SWITCH 2960    | —           | —          | Sede Central    | TI    | Interconecta los dispositivos dentro de una red local (la LAN de esta sucursal) |
| Servidor WEB - ALFATMC01 | SERVER         | 172.16.0.13 | Estática   | Sede Central    | TI    | Aloja y proporciona la página principal de la compañía                          |

|                             |              |             |          |              |        |  |
|-----------------------------|--------------|-------------|----------|--------------|--------|--|
|                             |              |             |          |              |        | (tecmicorp.com) a los empleados para que accedan mediante un navegador web.  |
| Servidor DNS - ALFATMC02    | SERVER       | 172.16.0.12 | Estática | Sede Central | TI     | El servidor principal el cual traduce la dirección IP a una página (tecmicorp.com) que se usa para gestionar el inventario y los empleados de la compañía. |
| Servidor DHCP - ALFATMC03   | SERVER       | 172.16.0.11 | Estática | Sede Central | TI     | Funciona como el que asigna automáticamente las direcciones IP y otros parámetros de red en este departamento.   |
| Servidor FTP - ALFATMC04    | SERVER       | 172.16.0.2  | ESTÁTICA | Sede Central | TI     | El servidor principal que permite la transferencia de archivos a aquellos equipos con el acceso permitido.   |
| ALFATMC05                   | PC           | 172.16.0.14 | DINÁMICA | Sede Central | TI     | Se encarga de monitorear principalmente la infraestructura de la red.  |
| Servidor DHCP - BETATMC01   | SERVER       | 172.16.0.66 | ESTÁTICA | Sede Central | Ventas | Funciona como el que asigna automáticamente las direcciones IP y otros parámetros de red en este departamento.   |
| Dpto. Ventas                | SWITCH 2960  | —           | —        | Sede Central | Ventas | Interconecta los dispositivos dentro de una red local (la LAN de esta sucursal)  |
| Punto de Acceso - BETATMC02 | Access Point | —           | —        | Sede Central | Ventas | Interconecta los dispositivos de manera inalámbrica  |
| BETATMC03                   | PC           | 172.16.0.68 | DINÁMICA | Sede Central | Ventas | Gestiona las relaciones con distribuidores y retailers   |
| BETATMC04                   | PC           | 172.16.0.69 | DINÁMICA | Sede Central | Ventas | Diseña campañas de preventa y  |

|                              |              |              |          |              |             | lanzamientos   |
|------------------------------|--------------|--------------|----------|--------------|-------------|--|
| BETATMC05                    | LAPTOP       | 172.16.0.71  | DINÁMICA | Sede Central | Ventas      | Analiza el mercado y las tendencias de ventas  |
| BETATMC06                    | LAPTOP       | 172.16.0.70  | DINÁMICA | Sede Central | Ventas      | Atención a clientes y soporte post-venta   |
| Servidor DHCP - GAMMATMC01   | SERVER       | 172.16.0.130 | ESTÁTICA | Sede Central | Operaciones | Funciona como el que asigna automáticamente las direcciones IP y otros parámetros de red en este departamento.                     |
| Servidor DNS - GAMMATMC02    | SERVER       | 172.16.0.131 | ESTÁTICA | Sede Central | Operaciones | Funciona como un servidor de respaldo para aumentar la velocidad al conectarse a la página web de la compañía.                     |
| Punto de Acceso - GAMMATMC01 | Access Point | —            | —        | Sede Central | Operaciones | Interconecta los dispositivos de manera inalámbrica  |
| GAMMATMC04                   | PC           | 172.16.0.133 | DINÁMICA | Sede Central | Operaciones | Administra y monitorea los servidores donde se alojan los juegos online, bases de datos de jugadores y servicios de autenticación. |
| GAMMATMC05                   | PC           | 172.16.0.132 | DINÁMICA | Sede Central | Operaciones | Coordina la producción y envío de copias físicas a tiendas y distribuidores.   |
| GAMMATMC06                   | LAPTOP       | 172.16.0.135 | DINÁMICA | Sede Central | Operaciones | Monitorea el rendimiento del juego en diferentes plataformas   |
| GAMMATMC07                   | LAPTOP       | 172.16.0.134 | DINÁMICA | Sede Central | Operaciones | Coordina pruebas de rendimiento y compatibilidad en servidores   |
| GAMMATMC08                   | LAPTOP       | 172.16.0.136 | DINÁMICA | Sede Central | Operaciones | Desarrolla estrategias contra trampas y hacks en juegos multijugador   |
| Dpto. Operaciones            | SWITCH 2960  | —            | —        | Sede Central | Operaciones | Interconecta los dispositivos dentro   |

|                              |              |              |          |                          |   |   |
|------------------------------|--------------|--------------|----------|--------------------------|---|---|
|                              |              |              |          |                          |   | de una red local (la LAN de esta sucursal)  |
| Sede Central                 | Router 2911  | —            | —        | Sede Central             | — | Se conecta con el ISP y dirige el tráfico de datos, además de permitir la intercomunicación entre distintos dispositivos. |
| ISP 1                        | Router 2911  | —            | —        | Sede Central             | — | Provee el acceso a Internet a estas sucursales.   |
| Internet                     | Cloud—PT     | —            | —        | —                        | — | Simula la conexión WAN de toda la infraestructura, además de permitir la intercomunicación.                               |
| ISP 2                        | Router 2911  | —            | —        | Sucursal 1<br>Sucursal 2 | — | Provee el acceso a Internet a estas sucursales.   |
| Sucursal 1                   | Router 2911  | —            | —        | Sucursal 1               | — | Se conecta con el ISP y dirige el tráfico de datos, además de permitir la intercomunicación entre distintos dispositivos. |
| Servidor DNS - DELTATMC01    | SERVER       | 192.168.1.12 | ESTÁTICA | Sucursal 1               | — | Funciona como un servidor de respaldo para aumentar la velocidad al conectarse a la página web de la compañía.            |
| Servidor DHCP - DELTATMC02   | SERVER       | 192.168.1.11 | ESTÁTICA | Sucursal 1               | — | Funciona como el que asigna automáticamente las direcciones IP y otros parámetros de red en esta sucursal                 |
| Switch Sucursal Delta        | Switch 2960  | —            | —        | Sucursal 1               | — | Interconecta los dispositivos dentro de una red local (la LAN de esta sucursal)   |
| Punto de Acceso - DELTATMC03 | Access Point | —            | —        | Sucursal 1               | — | Interconecta los dispositivos de manera inalámbrica   |

|                             |              |              |          |            |   |   |
|-----------------------------|--------------|--------------|----------|------------|---|---|
| DELTATMC04                  | PC           | 192.168.1.15 | DINÁMICA | Sucursal 1 | — | Se conecta con la central y al servidor FTP. Gestiona a los empleados y al inventario.                                    |
| DELTATMC05                  | LAPTOP       | 192.168.1.16 | DINÁMICA | Sucursal 1 | — | Realiza store procedures en el inventario y efectúa ventas.   |
| DELTATMC06                  | LAPTOP       | 192.168.1.18 | DINÁMICA | Sucursal 1 | — | Realiza store procedures en el inventario y efectúa ventas.   |
| DELTATMC07                  | LAPTOP       | 192.168.1.17 | DINÁMICA | Sucursal 1 | — | Realiza store procedures en el inventario y efectúa ventas.   |
| Sucursal 2                  | Router 2911  | —            | —        | Sucursal 2 | — | Se conecta con el ISP y dirige el tráfico de datos, además de permitir la intercomunicación entre distintos dispositivos. |
| Servidor DNS - EPSITMC01    | SERVER       | 192.168.2.12 | ESTÁTICA | Sucursal 2 | — | Funciona como un servidor de respaldo para aumentar la velocidad al conectarse a la página web de la compañía.            |
| Servidor DHCP - EPSITMC02   | SERVER       | 192.168.2.11 | ESTÁTICA | Sucursal 2 | — | Funciona como el que asigna automáticamente las direcciones IP y otros parámetros de red en esta sucursal                 |
| Switch Sucursal Épsilon     | Switch 2960  | —            | —        | Sucursal 2 | — | Interconecta los dispositivos dentro de una red local (la LAN de esta sucursal)   |
| Punto de Acceso - EPSITMC03 | Access Point | —            | —        | Sucursal 2 | — | Interconecta los dispositivos de manera inalámbrica   |
| EPSITMC04                   | PC           | 192.168.2.15 | DINÁMICA | Sucursal 2 | — | Se conecta con la central y al servidor FTP. Gestiona a los empleados y al inventario.                                    |

|                             |              |              |          |  |   |   |
|-----------------------------|--------------|--------------|----------|--|---|---|
| EPSITMC05                   | LAPTOP       | 192.168.2.18 | DINÁMICA | Sucursal 2                             | — | Realiza store procedures en el inventario y efectúa ventas.   |
| EPSITMC06                   | LAPTOP       | 192.168.2.16 | DINÁMICA | Sucursal 2                             | — | Realiza store procedures en el inventario y efectúa ventas.   |
| EPSITMC07                   | LAPTOP       | 192.168.2.17 | DINÁMICA | Sucursal 2                             | — | Realiza store procedures en el inventario y efectúa ventas.   |
| ISP 3                       | Router 2911  | —            | —        | Sucursal 3<br>Sucursal 4<br>Sucursal 5 | — | Provee el acceso a Internet a estas sucursales.   |
| Sucursal 3                  | Router 2911  | —            | —        | Sucursal 3                             | — | Se conecta con el ISP y dirige el tráfico de datos, además de permitir la intercomunicación entre distintos dispositivos. |
| Servidor DNS - ZETATMC01    | SERVER       | 192.168.3.12 | ESTÁTICA | Sucursal 3                             | — | Funciona como un servidor de respaldo para aumentar la velocidad al conectarse a la página web de la compañía.            |
| Servidor DHCP - ZETATMC02   | SERVER       | 192.168.3.11 | ESTÁTICA | Sucursal 3                             | — | Funciona como el que asigna automáticamente las direcciones IP y otros parámetros de red en esta sucursal                 |
| Switch Sucursal Zeta        | Switch 2960  | —            | —        | Sucursal 3                             | — | Interconecta los dispositivos dentro de una red local (la LAN de esta sucursal)   |
| Punto de Acceso - ZETATMC03 | Access Point | —            | —        | Sucursal 3                             | — | Interconecta los dispositivos de manera inalámbrica   |
| ZETATMC04                   | PC           | 192.168.3.13 | DINÁMICA | Sucursal 3                             | — | Se conecta con la central y al servidor FTP. Gestiona a los empleados y al inventario.                                    |
| ZETATMC05                   | LAPTOP       | 192.168.3.14 | DINÁMICA | Sucursal 3                             | — | Realiza store procedures en el  |

|                            |              |              |          |            |   |   |
|----------------------------|--------------|--------------|----------|------------|---|---|
|                            |              |              |          |            |   | inventario y efectúa ventas.  |
| ZETATMC06                  | LAPTOP       | 192.168.3.16 | DINÁMICA | Sucursal 3 | — | Realiza store procedures en el inventario y efectúa ventas.   |
| ZETATMC07                  | LAPTOP       | 192.168.3.15 | DINÁMICA | Sucursal 3 | — | Realiza store procedures en el inventario y efectúa ventas.   |
| Sucursal 4                 | Router 2911  | —            | —        | Sucursal 4 | — | Se conecta con el ISP y dirige el tráfico de datos, además de permitir la intercomunicación entre distintos dispositivos. |
| Servidor DNS - ETATMC01    | SERVER       | 192.168.4.12 | ESTÁTICA | Sucursal 4 | — | Funciona como un servidor de respaldo para aumentar la velocidad al conectarse a la página web de la compañía.            |
| Servidor DHCP - ETATMC02   | SERVER       | 192.168.4.11 | ESTÁTICA | Sucursal 4 | — | Funciona como el que asigna automáticamente las direcciones IP y otros parámetros de red en esta sucursal                 |
| Switch Sucursal Eta        | Switch 2960  | —            | —        | Sucursal 4 | — | Interconecta los dispositivos dentro de una red local (la LAN de esta sucursal)   |
| Punto de Acceso - ETATMC03 | Access Point | —            | —        | Sucursal 4 | — | Interconecta los dispositivos de manera inalámbrica   |
| ETATMC04                   | PC           | 192.168.4.13 | DINÁMICA | Sucursal 4 | — | Se conecta con la central y al servidor FTP. Gestiona a los empleados y al inventario.                                    |
| ETATMC05                   | LAPTOP       | 192.168.4.14 | DINÁMICA | Sucursal 4 | — | Realiza store procedures en el inventario y efectúa ventas.   |
| ETATMC06                   | LAPTOP       | 192.168.4.15 | DINÁMICA | Sucursal 4 | — | Realiza store procedures en el inventario y efectúa   |

|                              |              |              |          |            |   |   |
|------------------------------|--------------|--------------|----------|------------|---|---|
|                              |              |              |          |            |   | ventas.   |
| ETATMC07                     | LAPTOP       | 192.168.4.16 | DINÁMICA | Sucursal 4 | — | Realiza store procedures en el inventario y efectúa ventas.   |
| Sucursal 5                   | Router 2911  | —            | —        | Sucursal 5 | — | Se conecta con el ISP y dirige el tráfico de datos, además de permitir la intercomunicación entre distintos dispositivos. |
| Servidor DNS - THETATMC01    | SERVER       | 192.168.5.12 | ESTÁTICA | Sucursal 5 | — | Funciona como un servidor de respaldo para aumentar la velocidad al conectarse a la página web de la compañía.            |
| Servidor DHCP - THETATMC02   | SERVER       | 192.168.5.11 | ESTÁTICA | Sucursal 5 | — | Funciona como el que asigna automáticamente las direcciones IP y otros parámetros de red en esta sucursal                 |
| Switch Sucursal Theta        | Switch 2960  | —            | —        | Sucursal 5 | — | Interconecta los dispositivos dentro de una red local (la LAN de esta sucursal)   |
| Punto de Acceso - THETATMC03 | Access Point | —            | —        | Sucursal 5 | — | Interconecta los dispositivos de manera inalámbrica   |
| THETATMC04                   | PC           | 192.168.5.13 | DINÁMICA | Sucursal 5 | — | Se conecta con la central y al servidor FTP. Gestiona a los empleados y al inventario.                                    |
| THETATMC05                   | LAPTOP       | 192.168.5.14 | DINÁMICA | Sucursal 5 | — | Realiza store procedures en el inventario y efectúa ventas.   |
| THETATMC06                   | LAPTOP       | 192.168.5.16 | DINÁMICA | Sucursal 5 | — | Realiza store procedures en el inventario y efectúa ventas.   |
| THETATMC07                   | LAPTOP       | 192.168.5.15 | DINÁMICA | Sucursal 5 | — | Realiza store procedures en el inventario y efectúa ventas.   |

## Desarrollo

### ISP / MPLS

La conmutación de etiquetas multiprotocolo, MPLS por sus siglas en inglés, es un protocolo de transporte de datos basado en la utilización de etiquetas en una red de telecomunicaciones. Este protocolo funciona entre la capa de enlace de datos y la capa de red del modelo OSI.

La llegada del MPLS reemplazó la ya obsoleta tecnología de Frame Relay, al brindar mayor fiabilidad y mayor rendimiento al transportar datos a alta velocidad y voz digital en una sola conexión. Otro de los beneficios de este protocolo es el de reducir los costos de transporte mediante una mayor eficiencia de red.

En nuestra solución implementamos este servicio por medio de un ISP, quien se encarga de gestionar la red MPLS y brinda un enlace a cada sucursal. El motivo detrás de esta decisión es debido a las ventajas de implementar este servicio a través de un ISP, entre ellas se encuentra una menor inversión inicial, ya que la infraestructura para este servicio es la de nuestro de ISP, el soporte y mantenimiento va incluido en la contratación del servicio, menos tiempo de implementación y garantías de latencia, ancho de banda y disponible.

La única desventaja significativa es que la contratación de este servicio tiene un costo mensual recurrente, sin embargo, es una inversión significativamente menor al de la implementación y mantenimiento de un ISP propio. Tecmicorp se encuentra en un proceso de expansión, lo que se significa que apenas se está consolidando, por lo que la contratación del MPLS es la mejor opción.

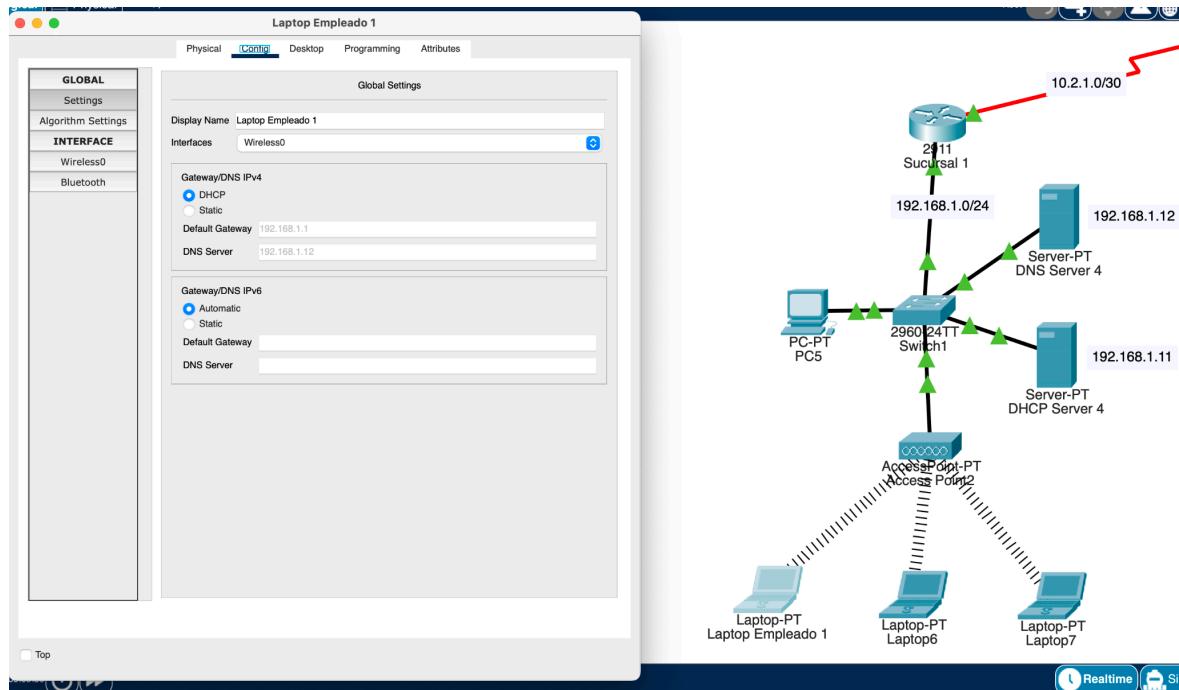
El flujo del tráfico en este servicio sería de la siguiente manera:

- Nuestra sucursal 1 envía un archivo a la sede central.

- El router de la sucursal encapsula el paquete utilizando una etiqueta MPLS y lo envía al router de nuestro ISP.
- El ISP lee la etiqueta del paquete sin necesidad de analizar la dirección IP y le redirecciona al router.
- El ISP al que está conectado nuestra sede central recibe el archivo, elimina la etiqueta de MPLS y lo envía al router de la sede central.
- La sede central recibe el archivo y le envía al dispositivo con la IP correspondiente.

## DHCP

En nuestra infraestructura se configuraron las redes para que, al conectar cualquier dispositivo extra, su configuración sea relativamente sencilla y que los empleados y personas externas a la red, como lo podría ser un consultor, puedan unirse. A diferencia de las redes estáticas, el DHCP nos otorga la capacidad de realizar este proceso de manera dinámica, por lo que al entregar las laptops a los empleados, solamente tienen que unirse a la red Wi-Fi y sin ninguna otra complicación. Ya que hay un host dinámico, los empleados no tienen por qué preocuparse de realizar una configuración manual. Solamente entran a trabajar y continuar con su labor en la empresa.



De la misma manera, el DHCP se ha configurado para que sólo dé un límite de IP's. A consecuencia, esto funciona como una capa de seguridad más ya que, al existir un límite, en caso de que un dispositivo externo se conecte, sabremos que hay una especie de posible invasión y riesgo de seguridad. El monitorear estas direcciones IP dinámicas nos asegura que tenemos un control sobre nuestros dispositivos y nuestros empleados y asegurarnos de que nuestra red siempre está a la vanguardia en cuestiones de rendimiento y seguridad.

**Servidor DHCP de Ventas**

| Physical    Config <b>Services</b> Desktop    Programming    Attributes | <div style="border-bottom: 1px solid #ccc; margin-bottom: 10px;"> <b>DHCP</b> </div> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; vertical-align: top; padding-right: 10px;">           Interface         </td> <td style="width: 30%; text-align: center; padding-right: 10px;">           FastEthernet0         </td> <td style="width: 10%; text-align: center; padding-right: 10px;"> <input checked="" type="radio"/> On         </td> <td style="width: 40%; text-align: right;"> <input type="radio"/> Off         </td> </tr> <tr> <td colspan="2">           Pool Name         </td> <td colspan="2">           serverPool         </td> </tr> <tr> <td colspan="2">           Default Gateway         </td> <td colspan="2">           172.16.0.65         </td> </tr> <tr> <td colspan="2">           DNS Server         </td> <td colspan="2">           172.16.0.12         </td> </tr> <tr> <td colspan="2">           Start IP Address :         </td> <td>           172         </td> <td>           16         </td> </tr> <tr> <td colspan="2">           Subnet Mask:         </td> <td>           255         </td> <td>           255         </td> </tr> <tr> <td colspan="2">           Maximum Number of Users :         </td> <td colspan="2">           15         </td> </tr> <tr> <td colspan="2">           TFTP Server:         </td> <td colspan="2">           0.0.0.0         </td> </tr> <tr> <td colspan="2">           WLC Address:         </td> <td colspan="2">           0.0.0.0         </td> </tr> <tr> <td colspan="2" style="text-align: center;"> <a href="#" style="border: 1px solid #ccc; padding: 2px 10px;">Add</a> </td> <td colspan="2" style="text-align: center;"> <a href="#" style="border: 1px solid #ccc; padding: 2px 10px;">Save</a> </td> <td colspan="2" style="text-align: center;"> <a href="#" style="border: 1px solid #ccc; padding: 2px 10px;">Remove</a> </td> </tr> <tr> <th style="text-align: center; padding: 5px;">Pool Name</th> <th style="text-align: center; padding: 5px;">Default Gateway</th> <th style="text-align: center; padding: 5px;">DNS Server</th> <th style="text-align: center; padding: 5px;">Start IP Address</th> <th style="text-align: center; padding: 5px;">Subnet Mask</th> <th style="text-align: center; padding: 5px;">Max User</th> <th style="text-align: center; padding: 5px;">TFTP Server</th> <th style="text-align: center; padding: 5px;">WLC Address</th> </tr> <tr> <td style="padding: 5px;">serverPool</td> <td style="padding: 5px;">172.16....</td> <td style="padding: 5px;">172.16....</td> <td style="padding: 5px;">172.16....</td> <td style="padding: 5px;">255.255....</td> <td style="padding: 5px;">15</td> <td style="padding: 5px;">0.0.0.0</td> <td style="padding: 5px;">0.0.0.0</td> </tr> </table> | Interface   | FastEthernet0             | <input checked="" type="radio"/> On                                       | <input type="radio"/> Off | Pool Name   |             | serverPool |  | Default Gateway |  | 172.16.0.65 |  | DNS Server |  | 172.16.0.12 |  | Start IP Address : |  | 172 | 16 | Subnet Mask: |  | 255 | 255 | Maximum Number of Users : |  | 15 |  | TFTP Server: |  | 0.0.0.0 |  | WLC Address: |  | 0.0.0.0 |  | <a href="#" style="border: 1px solid #ccc; padding: 2px 10px;">Add</a> |  | <a href="#" style="border: 1px solid #ccc; padding: 2px 10px;">Save</a> |  | <a href="#" style="border: 1px solid #ccc; padding: 2px 10px;">Remove</a> |  | Pool Name | Default Gateway | DNS Server | Start IP Address | Subnet Mask | Max User | TFTP Server | WLC Address | serverPool | 172.16.... | 172.16.... | 172.16.... | 255.255.... | 15 | 0.0.0.0 | 0.0.0.0 |
|---|--|---|---------------------------|---|---------------------------|-------------|-------------|------------|--|-----------------|--|-------------|--|------------|--|-------------|--|--------------------|--|-----|----|--------------|--|-----|-----|---------------------------|--|----|--|--------------|--|---------|--|--------------|--|---------|--|--|--|---|--|---|--|-----------|-----------------|------------|------------------|-------------|----------|-------------|-------------|------------|------------|------------|------------|-------------|----|---------|---------|
| Interface   | FastEthernet0  | <input checked="" type="radio"/> On                                     | <input type="radio"/> Off |   |                           |             |             |            |  |                 |  |             |  |            |  |             |  |                    |  |     |    |              |  |     |     |                           |  |    |  |              |  |         |  |              |  |         |  |  |  |   |  |   |  |           |                 |            |                  |             |          |             |             |            |            |            |            |             |    |         |         |
| Pool Name   |  | serverPool  |                           |   |                           |             |             |            |  |                 |  |             |  |            |  |             |  |                    |  |     |    |              |  |     |     |                           |  |    |  |              |  |         |  |              |  |         |  |  |  |   |  |   |  |           |                 |            |                  |             |          |             |             |            |            |            |            |             |    |         |         |
| Default Gateway   |  | 172.16.0.65   |                           |   |                           |             |             |            |  |                 |  |             |  |            |  |             |  |                    |  |     |    |              |  |     |     |                           |  |    |  |              |  |         |  |              |  |         |  |  |  |   |  |   |  |           |                 |            |                  |             |          |             |             |            |            |            |            |             |    |         |         |
| DNS Server  |  | 172.16.0.12   |                           |   |                           |             |             |            |  |                 |  |             |  |            |  |             |  |                    |  |     |    |              |  |     |     |                           |  |    |  |              |  |         |  |              |  |         |  |  |  |   |  |   |  |           |                 |            |                  |             |          |             |             |            |            |            |            |             |    |         |         |
| Start IP Address :  |  | 172   | 16                        |   |                           |             |             |            |  |                 |  |             |  |            |  |             |  |                    |  |     |    |              |  |     |     |                           |  |    |  |              |  |         |  |              |  |         |  |  |  |   |  |   |  |           |                 |            |                  |             |          |             |             |            |            |            |            |             |    |         |         |
| Subnet Mask:  |  | 255   | 255                       |   |                           |             |             |            |  |                 |  |             |  |            |  |             |  |                    |  |     |    |              |  |     |     |                           |  |    |  |              |  |         |  |              |  |         |  |  |  |   |  |   |  |           |                 |            |                  |             |          |             |             |            |            |            |            |             |    |         |         |
| Maximum Number of Users :   |  | 15  |                           |   |                           |             |             |            |  |                 |  |             |  |            |  |             |  |                    |  |     |    |              |  |     |     |                           |  |    |  |              |  |         |  |              |  |         |  |  |  |   |  |   |  |           |                 |            |                  |             |          |             |             |            |            |            |            |             |    |         |         |
| TFTP Server:  |  | 0.0.0.0   |                           |   |                           |             |             |            |  |                 |  |             |  |            |  |             |  |                    |  |     |    |              |  |     |     |                           |  |    |  |              |  |         |  |              |  |         |  |  |  |   |  |   |  |           |                 |            |                  |             |          |             |             |            |            |            |            |             |    |         |         |
| WLC Address:  |  | 0.0.0.0   |                           |   |                           |             |             |            |  |                 |  |             |  |            |  |             |  |                    |  |     |    |              |  |     |     |                           |  |    |  |              |  |         |  |              |  |         |  |  |  |   |  |   |  |           |                 |            |                  |             |          |             |             |            |            |            |            |             |    |         |         |
| <a href="#" style="border: 1px solid #ccc; padding: 2px 10px;">Add</a>  |  | <a href="#" style="border: 1px solid #ccc; padding: 2px 10px;">Save</a> |                           | <a href="#" style="border: 1px solid #ccc; padding: 2px 10px;">Remove</a> |                           |             |             |            |  |                 |  |             |  |            |  |             |  |                    |  |     |    |              |  |     |     |                           |  |    |  |              |  |         |  |              |  |         |  |  |  |   |  |   |  |           |                 |            |                  |             |          |             |             |            |            |            |            |             |    |         |         |
| Pool Name   | Default Gateway  | DNS Server  | Start IP Address          | Subnet Mask   | Max User                  | TFTP Server | WLC Address |            |  |                 |  |             |  |            |  |             |  |                    |  |     |    |              |  |     |     |                           |  |    |  |              |  |         |  |              |  |         |  |  |  |   |  |   |  |           |                 |            |                  |             |          |             |             |            |            |            |            |             |    |         |         |
| serverPool  | 172.16....   | 172.16....  | 172.16....                | 255.255....   | 15                        | 0.0.0.0     | 0.0.0.0     |            |  |                 |  |             |  |            |  |             |  |                    |  |     |    |              |  |     |     |                           |  |    |  |              |  |         |  |              |  |         |  |  |  |   |  |   |  |           |                 |            |                  |             |          |             |             |            |            |            |            |             |    |         |         |

**Servidor DHCP Sucursal 1**

| Physical   | Config          | <b>Services</b> | Desktop                             | Programming               | Attributes    |             |             |  |  |  |  |  |  |           |               |         |                                     |                           |  |  |  |  |           |            |  |  |  |  |  |  |                 |             |  |  |  |  |  |  |            |              |  |  |  |  |  |  |                    |     |     |   |    |  |  |  |  |              |     |     |     |   |  |  |  |  |                           |    |  |  |  |  |  |  |              |         |  |  |  |  |  |  |              |         |  |  |  |  |  |  |            |  |             |  |  |               |  |  |  |           |                 |            |                  |             |          |             |             |            |            |            |            |            |    |         |         |
|--|-----------------|-----------------|-------------------------------------|---------------------------|---------------|-------------|-------------|--|--|--|--|--|--|-----------|---------------|---------|-------------------------------------|---------------------------|--|--|--|--|-----------|------------|--|--|--|--|--|--|-----------------|-------------|--|--|--|--|--|--|------------|--------------|--|--|--|--|--|--|--------------------|-----|-----|---|----|--|--|--|--|--------------|-----|-----|-----|---|--|--|--|--|---------------------------|----|--|--|--|--|--|--|--------------|---------|--|--|--|--|--|--|--------------|---------|--|--|--|--|--|--|------------|--|-------------|--|--|---------------|--|--|--|-----------|-----------------|------------|------------------|-------------|----------|-------------|-------------|------------|------------|------------|------------|------------|----|---------|---------|
| <table border="1"> <thead> <tr> <th colspan="8">DHCP</th> </tr> <tr> <td>Interface</td> <td>FastEthernet0</td> <td>Service</td> <td><input checked="" type="radio"/> On</td> <td><input type="radio"/> Off</td> <td colspan="4"></td> </tr> </thead> <tbody> <tr> <td>Pool Name</td> <td colspan="7">serverPool</td> </tr> <tr> <td>Default Gateway</td> <td colspan="7">192.168.1.1</td> </tr> <tr> <td>DNS Server</td> <td colspan="7">192.168.1.12</td> </tr> <tr> <td>Start IP Address :</td> <td>192</td> <td>168</td> <td>1</td> <td>15</td> <td colspan="4"></td> </tr> <tr> <td>Subnet Mask:</td> <td>255</td> <td>255</td> <td>255</td> <td>0</td> <td colspan="4"></td> </tr> <tr> <td>Maximum Number of Users :</td> <td colspan="7">20</td> </tr> <tr> <td>TFTP Server:</td> <td colspan="7">0.0.0.0</td> </tr> <tr> <td>WLC Address:</td> <td colspan="7">0.0.0.0</td> </tr> <tr> <td align="center" colspan="2"><b>Add</b></td> <td align="center" colspan="3"><b>Save</b></td> <td align="center" colspan="4"><b>Remove</b></td> </tr> <tr> <th>Pool Name</th> <th>Default Gateway</th> <th>DNS Server</th> <th>Start IP Address</th> <th>Subnet Mask</th> <th>Max User</th> <th>TFTP Server</th> <th>WLC Address</th> </tr> <tr> <td>serverPool</td> <td>192.168...</td> <td>192.168...</td> <td>192.168...</td> <td>255.255...</td> <td>20</td> <td>0.0.0.0</td> <td>0.0.0.0</td> </tr> </tbody> </table> |                 |                 |                                     |                           |               | DHCP        |             |  |  |  |  |  |  | Interface | FastEthernet0 | Service | <input checked="" type="radio"/> On | <input type="radio"/> Off |  |  |  |  | Pool Name | serverPool |  |  |  |  |  |  | Default Gateway | 192.168.1.1 |  |  |  |  |  |  | DNS Server | 192.168.1.12 |  |  |  |  |  |  | Start IP Address : | 192 | 168 | 1 | 15 |  |  |  |  | Subnet Mask: | 255 | 255 | 255 | 0 |  |  |  |  | Maximum Number of Users : | 20 |  |  |  |  |  |  | TFTP Server: | 0.0.0.0 |  |  |  |  |  |  | WLC Address: | 0.0.0.0 |  |  |  |  |  |  | <b>Add</b> |  | <b>Save</b> |  |  | <b>Remove</b> |  |  |  | Pool Name | Default Gateway | DNS Server | Start IP Address | Subnet Mask | Max User | TFTP Server | WLC Address | serverPool | 192.168... | 192.168... | 192.168... | 255.255... | 20 | 0.0.0.0 | 0.0.0.0 |
| DHCP   |                 |                 |                                     |                           |               |             |             |  |  |  |  |  |  |           |               |         |                                     |                           |  |  |  |  |           |            |  |  |  |  |  |  |                 |             |  |  |  |  |  |  |            |              |  |  |  |  |  |  |                    |     |     |   |    |  |  |  |  |              |     |     |     |   |  |  |  |  |                           |    |  |  |  |  |  |  |              |         |  |  |  |  |  |  |              |         |  |  |  |  |  |  |            |  |             |  |  |               |  |  |  |           |                 |            |                  |             |          |             |             |            |            |            |            |            |    |         |         |
| Interface  | FastEthernet0   | Service         | <input checked="" type="radio"/> On | <input type="radio"/> Off |               |             |             |  |  |  |  |  |  |           |               |         |                                     |                           |  |  |  |  |           |            |  |  |  |  |  |  |                 |             |  |  |  |  |  |  |            |              |  |  |  |  |  |  |                    |     |     |   |    |  |  |  |  |              |     |     |     |   |  |  |  |  |                           |    |  |  |  |  |  |  |              |         |  |  |  |  |  |  |              |         |  |  |  |  |  |  |            |  |             |  |  |               |  |  |  |           |                 |            |                  |             |          |             |             |            |            |            |            |            |    |         |         |
| Pool Name  | serverPool      |                 |                                     |                           |               |             |             |  |  |  |  |  |  |           |               |         |                                     |                           |  |  |  |  |           |            |  |  |  |  |  |  |                 |             |  |  |  |  |  |  |            |              |  |  |  |  |  |  |                    |     |     |   |    |  |  |  |  |              |     |     |     |   |  |  |  |  |                           |    |  |  |  |  |  |  |              |         |  |  |  |  |  |  |              |         |  |  |  |  |  |  |            |  |             |  |  |               |  |  |  |           |                 |            |                  |             |          |             |             |            |            |            |            |            |    |         |         |
| Default Gateway  | 192.168.1.1     |                 |                                     |                           |               |             |             |  |  |  |  |  |  |           |               |         |                                     |                           |  |  |  |  |           |            |  |  |  |  |  |  |                 |             |  |  |  |  |  |  |            |              |  |  |  |  |  |  |                    |     |     |   |    |  |  |  |  |              |     |     |     |   |  |  |  |  |                           |    |  |  |  |  |  |  |              |         |  |  |  |  |  |  |              |         |  |  |  |  |  |  |            |  |             |  |  |               |  |  |  |           |                 |            |                  |             |          |             |             |            |            |            |            |            |    |         |         |
| DNS Server   | 192.168.1.12    |                 |                                     |                           |               |             |             |  |  |  |  |  |  |           |               |         |                                     |                           |  |  |  |  |           |            |  |  |  |  |  |  |                 |             |  |  |  |  |  |  |            |              |  |  |  |  |  |  |                    |     |     |   |    |  |  |  |  |              |     |     |     |   |  |  |  |  |                           |    |  |  |  |  |  |  |              |         |  |  |  |  |  |  |              |         |  |  |  |  |  |  |            |  |             |  |  |               |  |  |  |           |                 |            |                  |             |          |             |             |            |            |            |            |            |    |         |         |
| Start IP Address :   | 192             | 168             | 1                                   | 15                        |               |             |             |  |  |  |  |  |  |           |               |         |                                     |                           |  |  |  |  |           |            |  |  |  |  |  |  |                 |             |  |  |  |  |  |  |            |              |  |  |  |  |  |  |                    |     |     |   |    |  |  |  |  |              |     |     |     |   |  |  |  |  |                           |    |  |  |  |  |  |  |              |         |  |  |  |  |  |  |              |         |  |  |  |  |  |  |            |  |             |  |  |               |  |  |  |           |                 |            |                  |             |          |             |             |            |            |            |            |            |    |         |         |
| Subnet Mask:   | 255             | 255             | 255                                 | 0                         |               |             |             |  |  |  |  |  |  |           |               |         |                                     |                           |  |  |  |  |           |            |  |  |  |  |  |  |                 |             |  |  |  |  |  |  |            |              |  |  |  |  |  |  |                    |     |     |   |    |  |  |  |  |              |     |     |     |   |  |  |  |  |                           |    |  |  |  |  |  |  |              |         |  |  |  |  |  |  |              |         |  |  |  |  |  |  |            |  |             |  |  |               |  |  |  |           |                 |            |                  |             |          |             |             |            |            |            |            |            |    |         |         |
| Maximum Number of Users :  | 20              |                 |                                     |                           |               |             |             |  |  |  |  |  |  |           |               |         |                                     |                           |  |  |  |  |           |            |  |  |  |  |  |  |                 |             |  |  |  |  |  |  |            |              |  |  |  |  |  |  |                    |     |     |   |    |  |  |  |  |              |     |     |     |   |  |  |  |  |                           |    |  |  |  |  |  |  |              |         |  |  |  |  |  |  |              |         |  |  |  |  |  |  |            |  |             |  |  |               |  |  |  |           |                 |            |                  |             |          |             |             |            |            |            |            |            |    |         |         |
| TFTP Server:   | 0.0.0.0         |                 |                                     |                           |               |             |             |  |  |  |  |  |  |           |               |         |                                     |                           |  |  |  |  |           |            |  |  |  |  |  |  |                 |             |  |  |  |  |  |  |            |              |  |  |  |  |  |  |                    |     |     |   |    |  |  |  |  |              |     |     |     |   |  |  |  |  |                           |    |  |  |  |  |  |  |              |         |  |  |  |  |  |  |              |         |  |  |  |  |  |  |            |  |             |  |  |               |  |  |  |           |                 |            |                  |             |          |             |             |            |            |            |            |            |    |         |         |
| WLC Address:   | 0.0.0.0         |                 |                                     |                           |               |             |             |  |  |  |  |  |  |           |               |         |                                     |                           |  |  |  |  |           |            |  |  |  |  |  |  |                 |             |  |  |  |  |  |  |            |              |  |  |  |  |  |  |                    |     |     |   |    |  |  |  |  |              |     |     |     |   |  |  |  |  |                           |    |  |  |  |  |  |  |              |         |  |  |  |  |  |  |              |         |  |  |  |  |  |  |            |  |             |  |  |               |  |  |  |           |                 |            |                  |             |          |             |             |            |            |            |            |            |    |         |         |
| <b>Add</b>   |                 | <b>Save</b>     |                                     |                           | <b>Remove</b> |             |             |  |  |  |  |  |  |           |               |         |                                     |                           |  |  |  |  |           |            |  |  |  |  |  |  |                 |             |  |  |  |  |  |  |            |              |  |  |  |  |  |  |                    |     |     |   |    |  |  |  |  |              |     |     |     |   |  |  |  |  |                           |    |  |  |  |  |  |  |              |         |  |  |  |  |  |  |              |         |  |  |  |  |  |  |            |  |             |  |  |               |  |  |  |           |                 |            |                  |             |          |             |             |            |            |            |            |            |    |         |         |
| Pool Name  | Default Gateway | DNS Server      | Start IP Address                    | Subnet Mask               | Max User      | TFTP Server | WLC Address |  |  |  |  |  |  |           |               |         |                                     |                           |  |  |  |  |           |            |  |  |  |  |  |  |                 |             |  |  |  |  |  |  |            |              |  |  |  |  |  |  |                    |     |     |   |    |  |  |  |  |              |     |     |     |   |  |  |  |  |                           |    |  |  |  |  |  |  |              |         |  |  |  |  |  |  |              |         |  |  |  |  |  |  |            |  |             |  |  |               |  |  |  |           |                 |            |                  |             |          |             |             |            |            |            |            |            |    |         |         |
| serverPool   | 192.168...      | 192.168...      | 192.168...                          | 255.255...                | 20            | 0.0.0.0     | 0.0.0.0     |  |  |  |  |  |  |           |               |         |                                     |                           |  |  |  |  |           |            |  |  |  |  |  |  |                 |             |  |  |  |  |  |  |            |              |  |  |  |  |  |  |                    |     |     |   |    |  |  |  |  |              |     |     |     |   |  |  |  |  |                           |    |  |  |  |  |  |  |              |         |  |  |  |  |  |  |              |         |  |  |  |  |  |  |            |  |             |  |  |               |  |  |  |           |                 |            |                  |             |          |             |             |            |            |            |            |            |    |         |         |

Por lo tanto, en cada departamento de la sede central se encuentran un límite máximo de 15 IP's dinámicas; mientras que en cada sucursal hay un límite máximo de 20 IP's dinámicas. Entonces se esperaría que solamente esa cantidad máxima de usuarios sea la que esté laborando y ni un empleado más.

## Servidor FTP

El servidor FTP nos permite implementar un protocolo por el cual podemos realizar transferencia de archivos entre dispositivos de la misma o distinta sucursal y sede. Nuevamente, nos permite usar distintos usuarios y contraseñas que sólo se van otorgar a las

personas que se crean pertinentes, como lo serán empleados con un nivel de acceso un poco mayor y a personas que necesiten acceso a los archivos de la compañía. También, podría surgir el caso en que se vayan a configurar las sucursales y se ocupen archivos que solamente existen en las sedes centrales.

En el siguiente [enlace de video sobre el funcionamiento de FTP](#), demostramos justamente cómo se puede acceder al servidor desde una computadora de una sucursal que está relativamente lejos, la cual incluso podría estar en otra ciudad, estado, o país, y sólo con tener el acceso del usuario y la contraseña que los administradores deseen otorgar.

## Servidor DNS

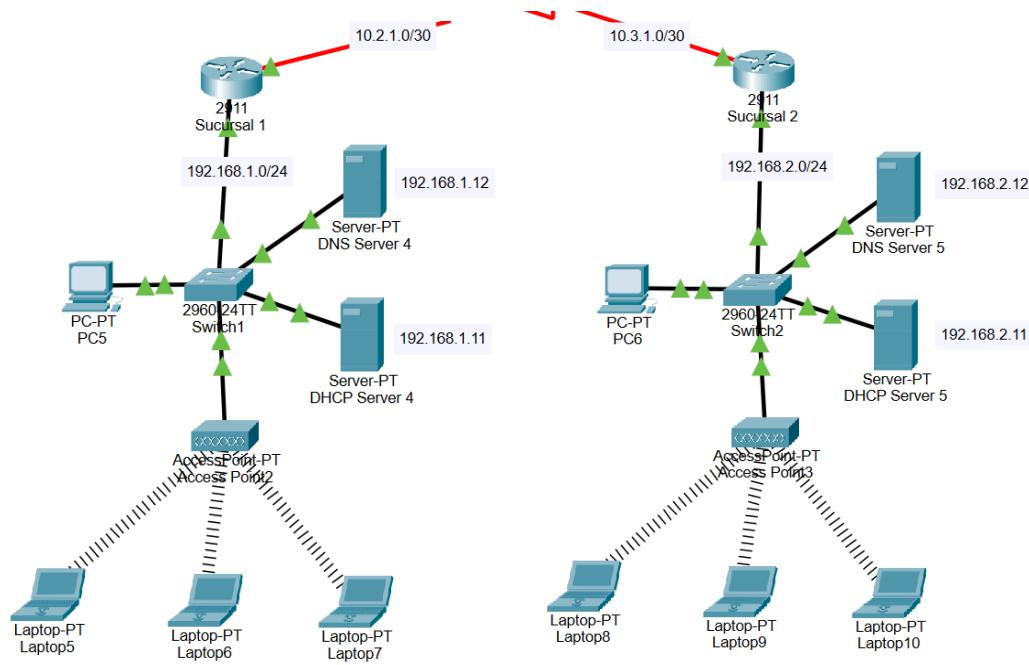
El Servidor DNS (Domain Name System) en esta topología es responsable de la resolución de nombres de dominio dentro de la red. Su función principal es traducir nombres de dominio como [www.ejemplo.com](http://www.ejemplo.com) en direcciones IP que los dispositivos puedan entender y utilizar para la comunicación.

Funciones principales:

- Resolución de nombres: Convierte nombres de dominio en direcciones IP.
- Optimización del tráfico: Reduce la carga en la red al permitir que los dispositivos recuerden respuestas recientes mediante caché.
- Facilita la administración: Permite usar nombres fáciles de recordar en lugar de direcciones IP complicadas.
- Seguridad: Puede configurarse para filtrar accesos no autorizados y evitar ataques como DNS Spoofing.

**Ejemplo:**

Supongamos que un usuario en la red quiere acceder a un servidor web interno escribiendo intranet.empresia.com en su navegador. En lugar de recordar la dirección IP del servidor (por ejemplo, 192.168.1.10), el DNS se encarga de traducir automáticamente el nombre de dominio a la IP correspondiente, permitiendo que la conexión se realice sin complicaciones.



### Servidor WEB

El Servidor WEB en esta topología es el encargado de alojar y servir páginas web a los dispositivos de la red. Su función principal es responder a las solicitudes HTTP y HTTPS de los clientes, proporcionando acceso a contenido web como aplicaciones internas, documentación o sitios corporativos.

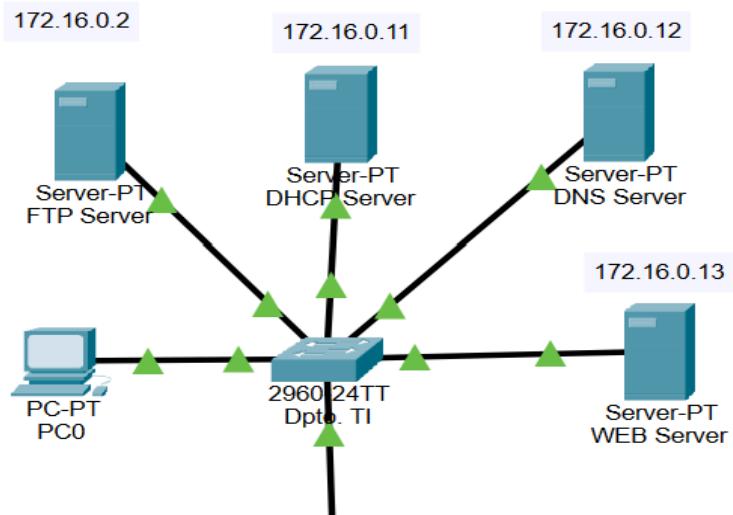
Funciones principales:

- **Almacenamiento de contenido:** Aloja archivos HTML, CSS, JavaScript y otros recursos para páginas web.
- **Procesamiento de solicitudes:** Responde a peticiones de los clientes utilizando protocolos como HTTP/HTTPS.

- **Seguridad:** Puede implementar certificados SSL/TLS para cifrar la comunicación.
- **Integración con bases de datos:** Puede conectarse con servidores de bases de datos para servir contenido dinámico.

Ejemplo:

Un empleado de la empresa necesita acceder a una plataforma interna de gestión. Abre su navegador y escribe [gestión.empresacom](http://gestión.empresacom). El servidor WEB recibe la solicitud, procesa la información y envía la página al usuario, permitiéndole visualizar datos, realizar reportes o interactuar con la plataforma.



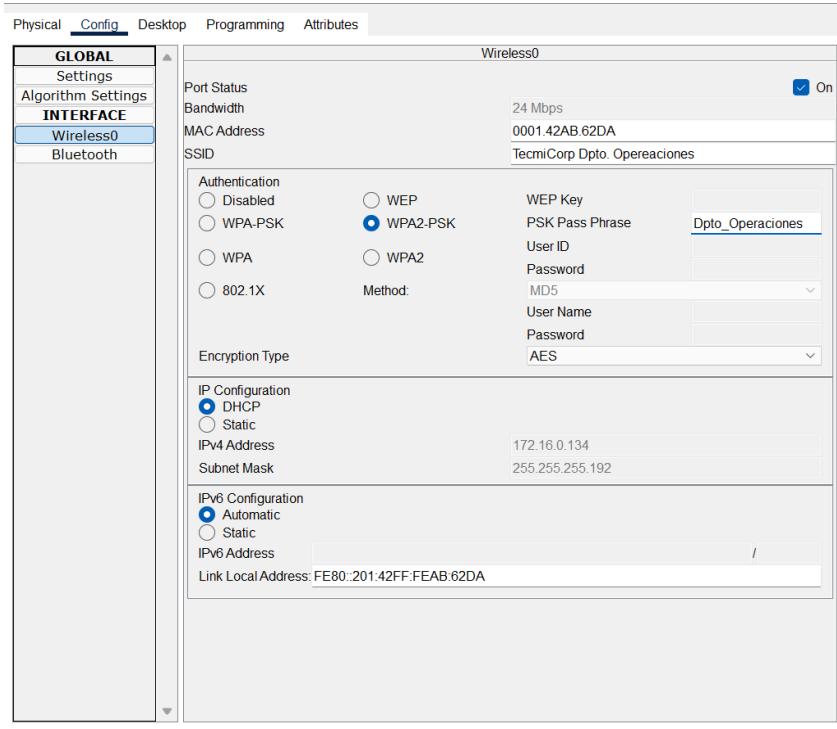
## Implementación

### Configuración de comunicaciones

Wireless:

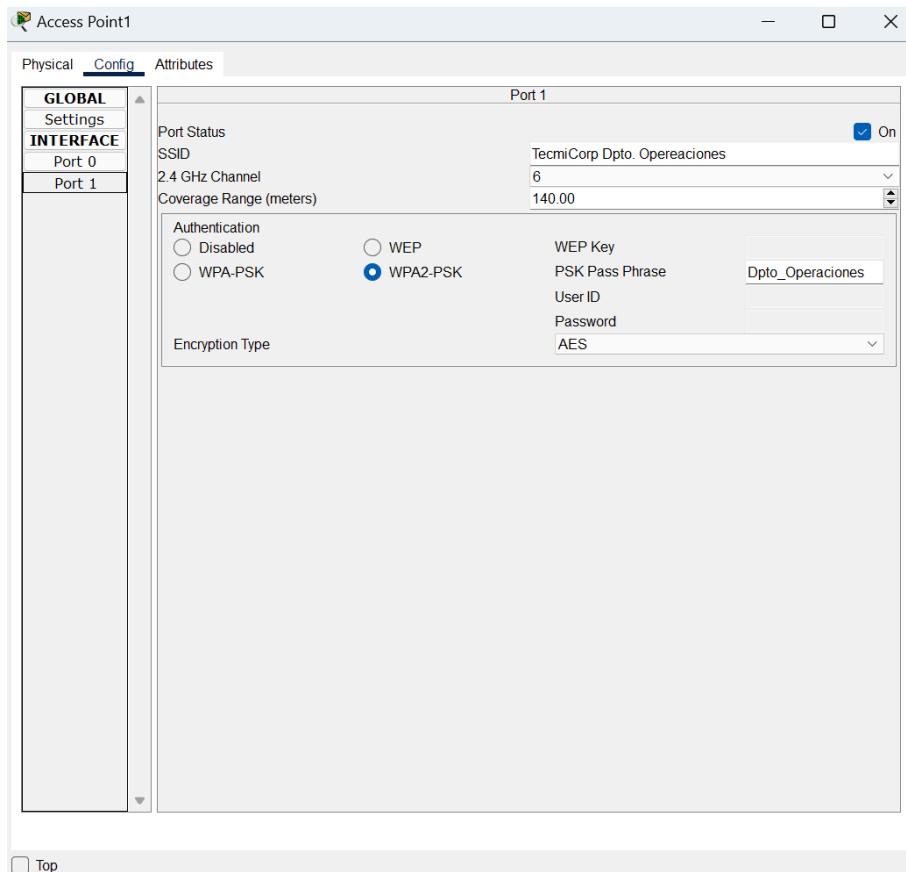
En nuestro proyecto se tomó en cuenta el uso de configuraciones wireless en las laptops de cada departamento/sucursal, ¿Para qué? Al ser las laptops dispositivos portátiles se pensó en el uso del wireless en estas para poder trabajar dentro de la sucursal de manera inalámbrica sin la necesidad de estar forzado a estar fijado en un lugar en específico usando un cable para estar en comunicación.

#### Wireless por departamento/sucursal:



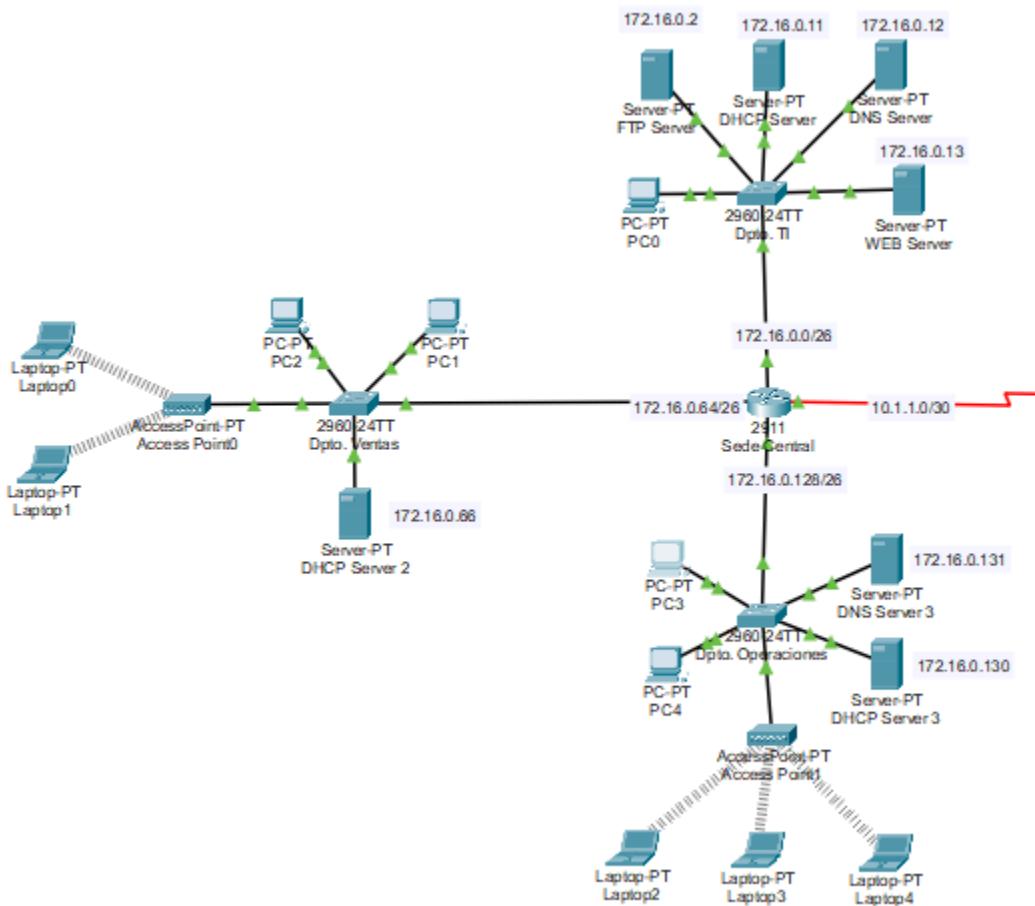
The screenshot shows a software interface for managing network interfaces. The top navigation bar includes tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Config' tab is selected. On the left, a sidebar lists GLOBAL, Settings, Algorithm Settings, INTERFACE, Wireless0 (which is selected and highlighted in blue), and Bluetooth. The main panel displays configuration for 'Wireless0'. Key settings include:

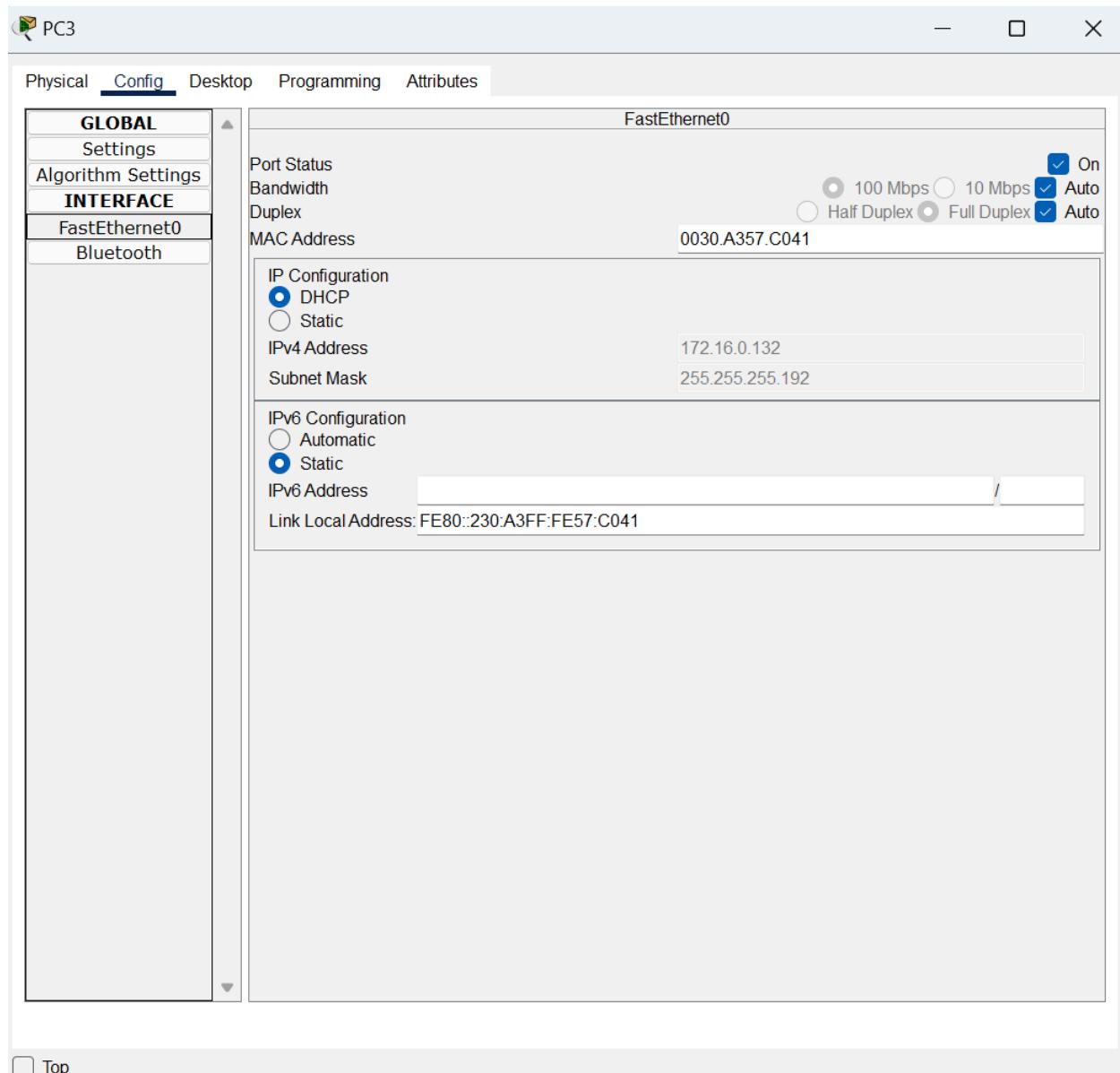
- Port Status:** On (checkbox checked)
- Bandwidth:** 24 Mbps
- MAC Address:** 0001:42AB:62DA
- SSID:** TecmiCorp Dpto. Operaciones
- Authentication:** WPA2-PSK (radio button selected). Other options include Disabled, WEP, WPA, and 802.1X. For WPA2-PSK, fields for PSK Pass Phrase (Dpto\_Operaciones), User ID, Password, Method (MD5), User Name, and Password are present.
- Encryption Type:** AES
- IP Configuration:** DHCP (radio button selected). Other options include Static. Fields for IPv4 Address (172.16.0.134) and Subnet Mask (255.255.255.192) are shown.
- IPv6 Configuration:** Automatic (radio button selected). Other options include Static. A field for IPv6 Address is shown with a placeholder value of /.
- Link Local Address:** FE80::201:42FF:FEAB:62DA

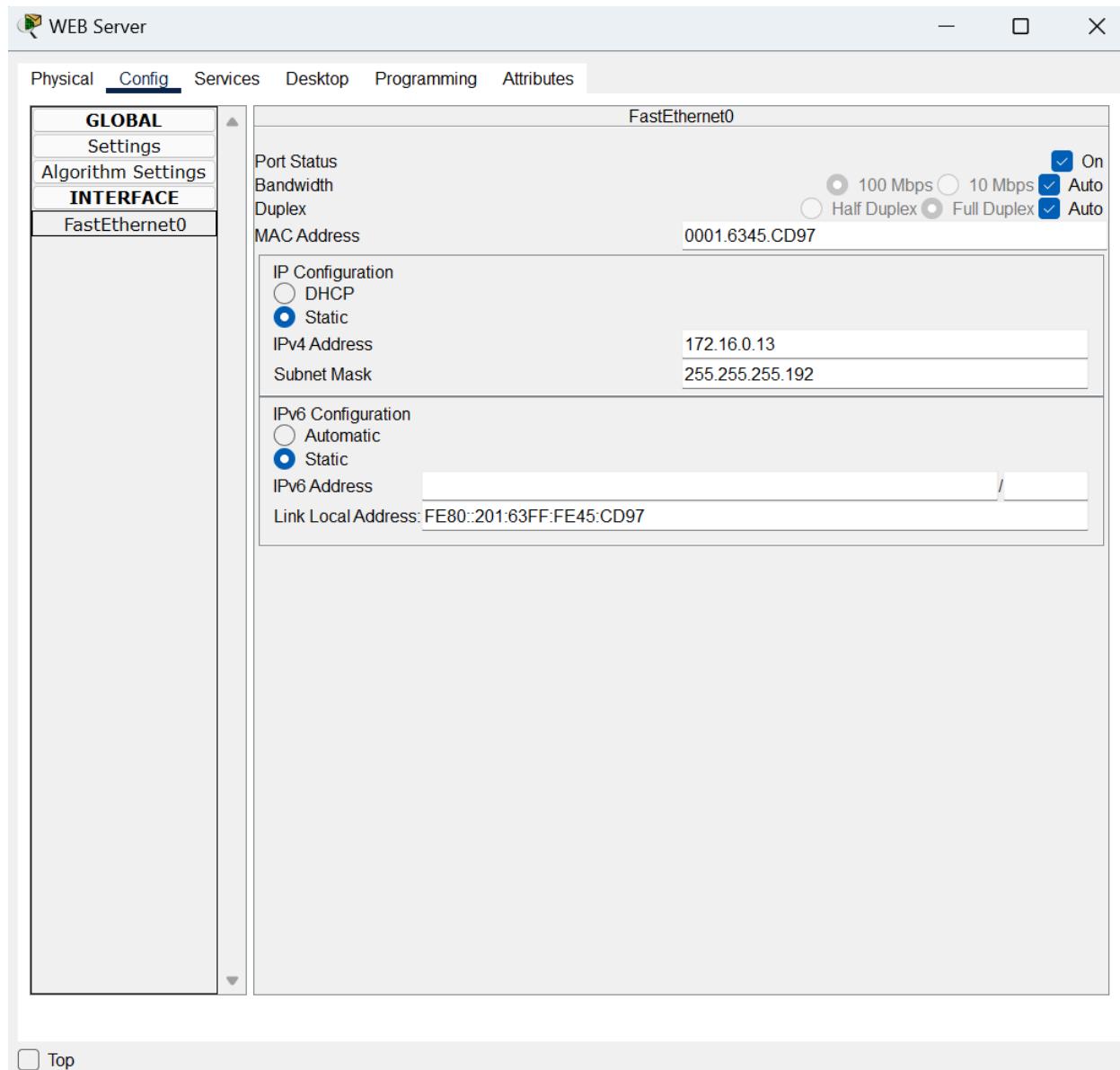


En la configuración de cada laptop se tendrá que especificar su Dirección MAC (que variará por cada laptop) y el SSID al que se estarán conectando (el SSID variará según en la subred que esté). Se activará el DHCP para que se le asigne una ip dinámica y una máscara al wireless de cada pc, así mismo se pondrá en Automático la asignación de ipv6. Los dispositivos que usen wireless al final se conectarán a un access point (que este así mismo se conectará al switch de cada red) el cual será el encargado de evitar interferencias entre dispositivos, dar la cobertura de rango y ser el encargado de llevar a cabo la autentificación de los dispositivos. Sobre la autenticación, para asegurar la seguridad de los dispositivos activamos en el wireless el protocolo WPA2-PSK para evitar hackeos, así mismo configuramos un PSK-Phrase o contraseña de red con la que accederán las laptops.

## Cableado:







Las comunicaciones por cable representan la mayor parte de comunicaciones por red en nuestro proyecto, gracias a estas gran parte de los dispositivos tienen acceso a los demás dispositivos. La topología que se usa en cada sucursal/departamento es la estrella para agilizar las comunicaciones, en este caso haremos énfasis en cómo está armado el cableado. El cableado se basa en conectar cables ethernet en los dispositivos con sus respectivos puertos, los dispositivos como

servidores o computadoras de escritorio usando los puertos fastethernet y para los routers el gigabitEthernet. Una vez conectados los dispositivos usaremos un switch para mantener el orden en el tráfico que derivara de las comunicaciones entre no solo dispositivos cableados sino también de los inalámbricos. A cada puerto se le asignará una ipv4 y una máscara, para las computadoras de escritorio se usar el DHCP para eso pero en los servidores se agregara la ipv4 y la máscara de manera manual.

#### Recomendaciones de seguridad:

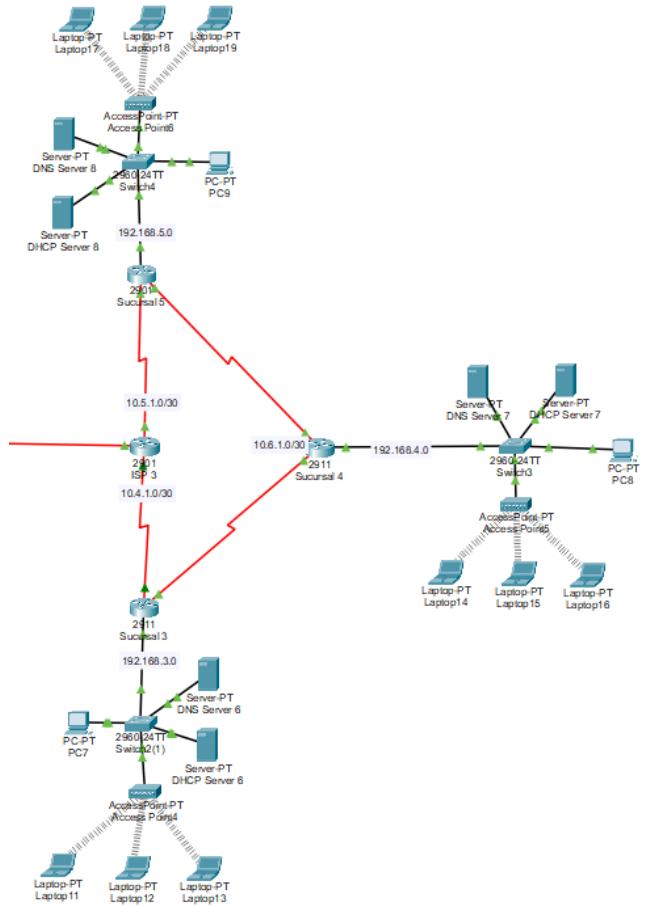
A continuación les mostraremos algunas medidas de seguridad que se sugieren usar a la hora de implementar el cableado y el wireless en nuestras redes. Las acompañaremos con un ejemplo práctico para tener más en claro qué papel desempeñan:

- **Filtrado de Direcciones MAC:** En nuestra red solo queremos admitir los dispositivos de nuestros empleados, al ser la MAC una dirección única por cada dispositivo se puede monitorear a través del switch las MACs de cada dispositivo, cualquier MAC que no se reconozca no se le permitirá el acceso.
- **Ocultar el SSID:** El objetivo es que solo las personas que formen parte de la empresa conozcan el nombre de la red, entonces el nombre del SSID no debe revelar detalles de a qué lugar pertenece para así evitar intrusos intentando conectarse a la red.

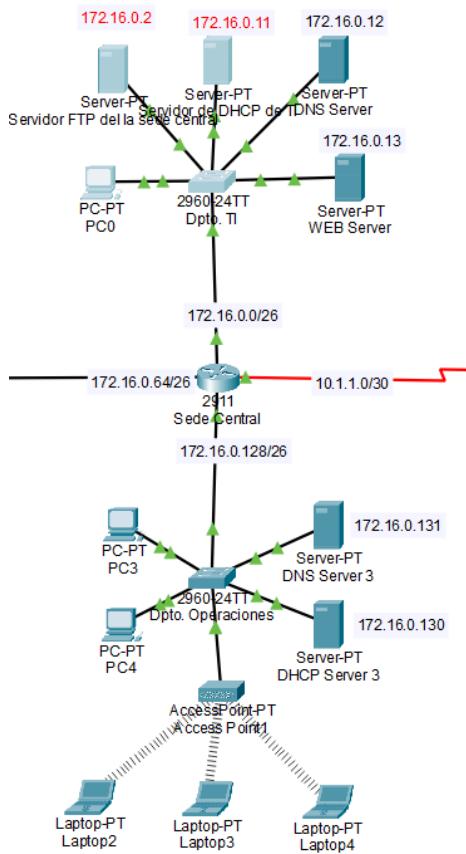
- Habilitar el WPA2-PSK: Todos los empleados deben de ingresar la misma contraseña de red, los que no sepan la contraseña de red, no tendrán acceso a la red.
- Deshabilitar puertos no usados: Los intrusos pueden explotar las vulnerabilidades de nuestra red, ejemplos hay muchos pero uno común sería aprovecharse de los puertos no usados y de ahí conectar un equipo no autorizado. El administrador de red debe deshabilitar los puertos sobrantes.
- Reducir la potencia de emisión: Es importante tener en cuenta el alcance que puede tener la señal, si se quiere evitar que gente fuera del departamento u sucursal tengan posible acceso a la red hay que configurar un correcto alcance.
- Evitar el cableado expuesto: Muchos problemas en las redes son ocasionados por cables dañados o mal conectados, así que es buena práctica tenerlos ocultos para evitar que factores externos puedan dañarlos.

## Seguridad

Redundancia:



Sucursales



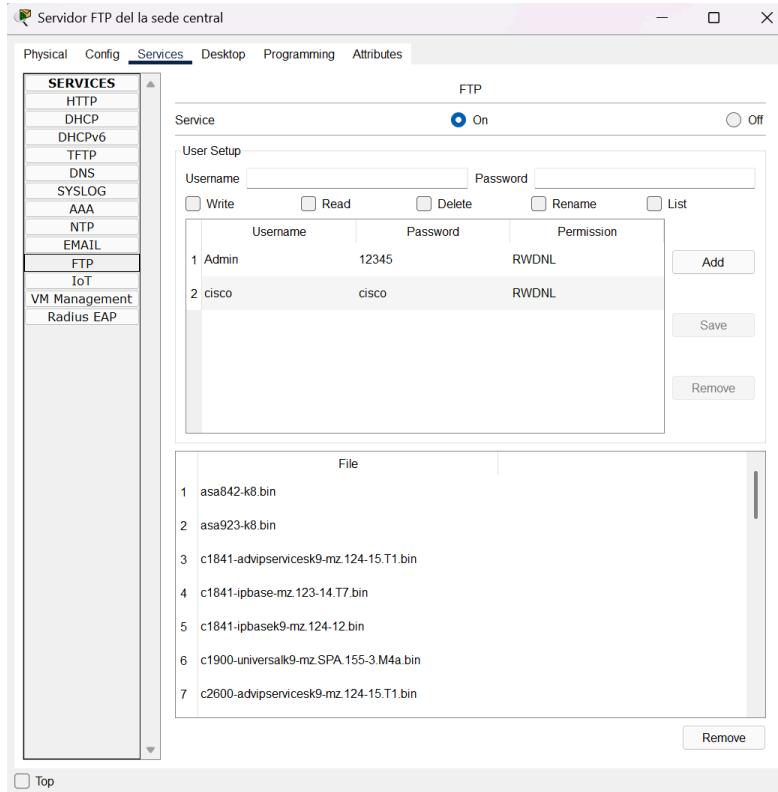
## Sede Central

En nuestra central tenemos en 2 de nuestros departamentos un servidor DNS y en cada sucursal existente tenemos un servidor DNS también, ¿El por qué de esto? Cada uno sirve como un respaldo para en caso del fallo de uno, este no afecte directamente a los demás y no resulte en un gran problema.

Por ejemplo, en caso de que la sucursal de Monterrey se vea afectada, las demás sucursales como, la de Guanajuato o CDMX, no recibirán algo similar, a lo mucho se enteren

de que algo raro pasa en Monterrey, pero no se verán afectados a diferencia de Monterrey en sí.

### Usuarios y Administradores:



Los administradores son los encargados de darles y quitarles a los Usuarios/Empleados cualquier tipo de permisos y también crear cuentas nuevas para los recién ingresados, también vigilan las actividades de los usuarios.

Por ejemplo, un usuario es nuevo, el admin le crea su propia cuenta, otro usuario cometió una infracción, el administrador le quita el permiso para ciertos puestos o proyectos, por ultimo el administrador puede ver un resumen de los usuarios y contraseñas.

Límite de IP's:

Actualmente la red tiene un límite de 15 y 20 IPs gracias a nuestro servicio de DHCP, haciendo que solo puedan acceder a una IP los dispositivos de nuestra compañía, esta medida se ha puesto para aumentar la seguridad y sea más fácil detectar anomalías e intrusos, Ya que al tener pocas IP es mas rápido y fácil tener un registro de quien está conectado lo que hace más notable ver alguien que “no estaba ahí” antes.

Otra razón es para no desperdiciar direcciones IPs ya que no es necesario tener tantas disponibles al ser un servicio dedicado y ahorra costos en la gestión del control de acceso. Por último pero no menos importante es que ayuda mucho al rendimiento de las redes al reducir la cantidad de tráfico en ella, haciendo más eficiente y rápido

#### Recomendaciones de Seguridad para la Topología

**- Recomendamos configurar un firewall** para restringir el acceso a los servidores solo desde direcciones IP autorizadas y aplicar listas de control de acceso (ACLs) para bloquear tráfico no deseado.

**.- Sugerimos segmentar la red** mediante VLANs para separar los servidores de los usuarios y crear una DMZ para los servidores públicos como el Web Server y el DNS Server.

**.- Es importante mantener los servidores actualizados** y utilizar protocolos seguros como HTTPS en lugar de HTTP y SFTP en lugar de FTP. También recomendamos deshabilitar servicios innecesarios para reducir vulnerabilidades.

**.- Recomendamos implementar autenticación multifactor (MFA)** y exigir contraseñas seguras con políticas de caducidad y rotación. Además, es fundamental aplicar el principio de menor privilegio posible a los usuarios.

**.- Sugerimos monitorear la red en tiempo real** utilizando herramientas como SNMP o SIEM y configurar registros de eventos en servidores y dispositivos de red para detectar actividades sospechosas.

**.- Para prevenir ataques externos, recomendamos instalar un IDS/IPS** que detecte y bloquee intentos de intrusión, además de limitar intentos fallidos de autenticación y utilizar VPNs para conexiones remotas seguras.

**.- Es fundamental proteger físicamente los servidores y dispositivos de red,** restringiendo el acceso a personal autorizado. También recomendamos realizar backups periódicos de la configuración y bases de datos en una ubicación segura.

## Potenciales ataques a la red

### 1. Ataques de Configuración de Frame Relay (Spoofing de DLCI)

- **Peligro:** Frame Relay utiliza **DLCI (Data Link Connection Identifiers)** para identificar conexiones. Un atacante podría manipular la configuración de **Frame Relay** o suplantar un router intermedio, redirigiendo tráfico a una máquina no autorizada.
- **Impacto:** Robo de datos, interrupción del servicio entre sucursales y pérdida de control sobre las rutas de comunicación.

**Solución:**

- **Habilitar autenticación** en los routers mediante **CHAP o PAP** en conexiones seriales.
- Configurar **access lists (ACLs)** para filtrar tráfico en cada interfaz serial.
- **Monitorear las tablas de Frame Relay** en los routers con el comando `show frame-relay map`.

**2. Ataques a la Configuración de Rutas Estáticas (Redireccionamiento de Tráfico)**

- **Peligro:** La configuración de **rutas estáticas** en los routers permite intercomunicación, pero si un atacante accede a la configuración del router, podría modificar las rutas **para redirigir todo el tráfico hacia otro destino** (por ejemplo, un router controlado por el atacante).
- **Impacto:**
  - Intercepción del tráfico de todas las sucursales.
  - Desconexión de una o más sucursales de la sede central.
- **Solución:**
  - **Configurar autenticación en los routers** (privilegios de usuario con contraseñas seguras).
  - **Habilitar logging y monitoreo de cambios en la configuración** (`show running-config`).

- **Implementar redundancia con un protocolo dinámico de enrutamiento** (OSPF o EIGRP) en lugar de solo rutas estáticas.

### 3. Ataques de Denegación de Servicio en Enlaces WAN (DoS en la Red de la Nube)

- **Peligro:** Los enlaces **Frame Relay y Serial** dependen de la red WAN. Un atacante podría generar una cantidad excesiva de tráfico o enviar paquetes maliciosos para **saturar los enlaces WAN y hacer que las conexiones entre sucursales fallen.**
- **Impacto:**
  - Lentitud o interrupción total de la comunicación entre sucursales.
  - Fallos en la transmisión de datos entre la sede y las oficinas remotas.
- **Solución:**
  - Configurar **Quality of Service (QoS)** para priorizar tráfico crítico y evitar saturación.
  - Implementar **Access Control Lists (ACLs)** en las interfaces WAN para bloquear tráfico sospechoso.
  - Usar **ICMP Rate Limiting** en los routers para mitigar ataques de ping masivo.

Identificación de amenazas comunes

**Acceso no autorizado a la sede central (Externa):** Como las PC están conectadas por Ethernet y tienen acceso a la sede central, un atacante externo podría intentar acceder a través de ataques como fuerza bruta o explotación de vulnerabilidades en los routers.

**Intercepción de tráfico en la conexión Wi-Fi (Externa):** Las laptops se conectan por Wi-Fi y no tienen acceso a la sede central, pero un atacante podría interceptar tráfico en la red inalámbrica mediante ataques de "Man-in-the-Middle" (MITM).

**Malware en dispositivos internos (Interna):** Un usuario interno podría descargar malware o abrir archivos maliciosos, comprometiendo la seguridad de la red y permitiendo ataques como ransomware.

**Ataques de denegación de servicio (Externa):** Un atacante externo podría saturar los routers con tráfico malicioso para hacer que la red se vuelva inoperable.

**Configuraciones inseguras en switches o routers (Interna):** Si los dispositivos de red no están correctamente configurados, un usuario interno con conocimientos avanzados podría explotar estas configuraciones para obtener acceso no autorizado.

## Medidas de seguridad

**Segmentación de red y VLANs:** Separar la red Wi-Fi de la red cableada mediante VLANs y establecer reglas en los routers para evitar accesos no deseados. Esto prevendría que una laptop comprometida afecte a la sede central.

**Cifrado WPA3 en la red Wi-Fi:** Implementar cifrado WPA3 en los routers para evitar ataques de interceptación en la conexión Wi-Fi y mejorar la seguridad en la autenticación.

**Firewalls y listas de control de acceso (ACLs):** Configurar firewalls en los routers y aplicar ACLs para filtrar tráfico malicioso y permitir únicamente conexiones seguras hacia la sede central.

**Autenticación de múltiples factores (MFA) para acceso remoto:** Implementar autenticación de múltiples factores en las PC con acceso a la sede central, evitando que un atacante pueda comprometer la red solo con credenciales robadas.

**Monitoreo y detección de intrusos (IDS/IPS):** Implementar un sistema de detección y prevención de intrusos (IDS/IPS) en los routers para identificar tráfico sospechoso y prevenir ataques en tiempo real.

Propuestas para hacer que la red sea confiable

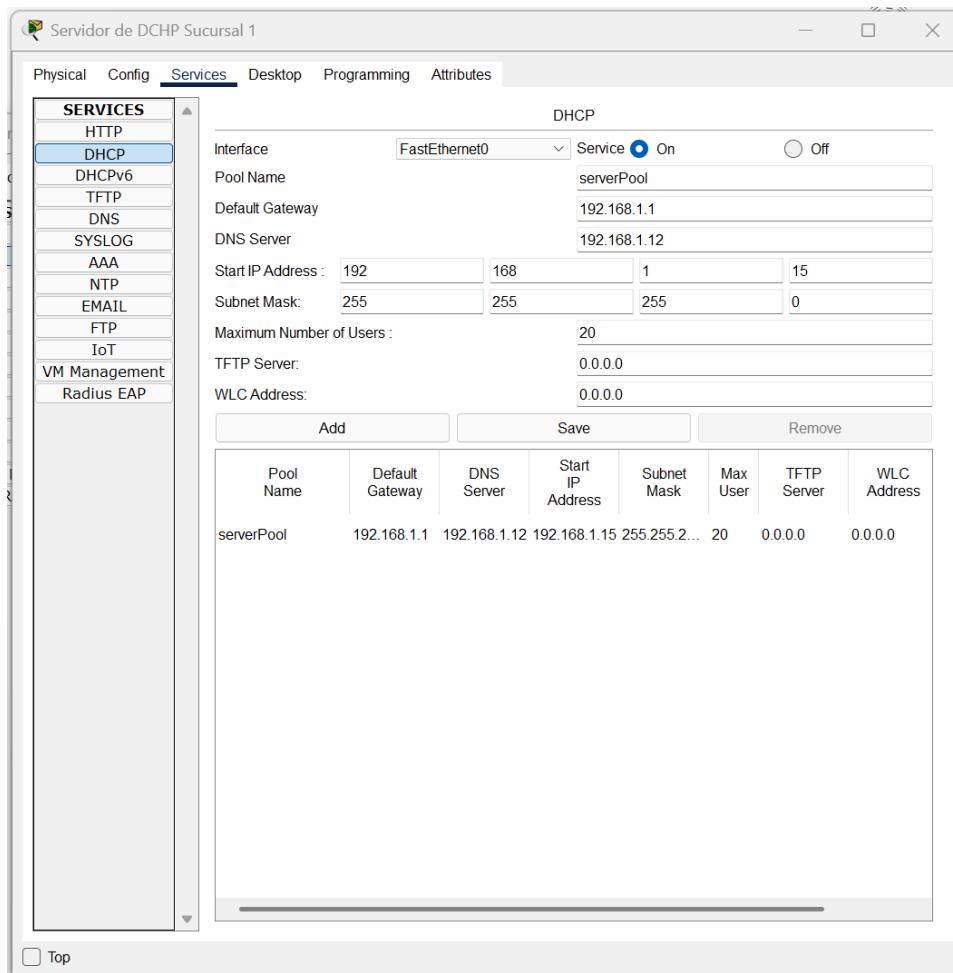
**Redundancia de enlaces:** Las conexiones redundantes permitirían a los elementos de la red el poder tener varias direcciones de conexión. Esto permitiría que, en vez de depender de una sola dirección que, en caso de fallar, pueda causar problemas, podrá usar direcciones alternativas para seguir funcionando apropiadamente. Estos se usarían principalmente en routers, switches, firewalls y servidores, pero también podría extenderse a fuentes de poder, puertos de comunicación, memorias, tableros, UPS, inversores, plantas de CD, entre otros.

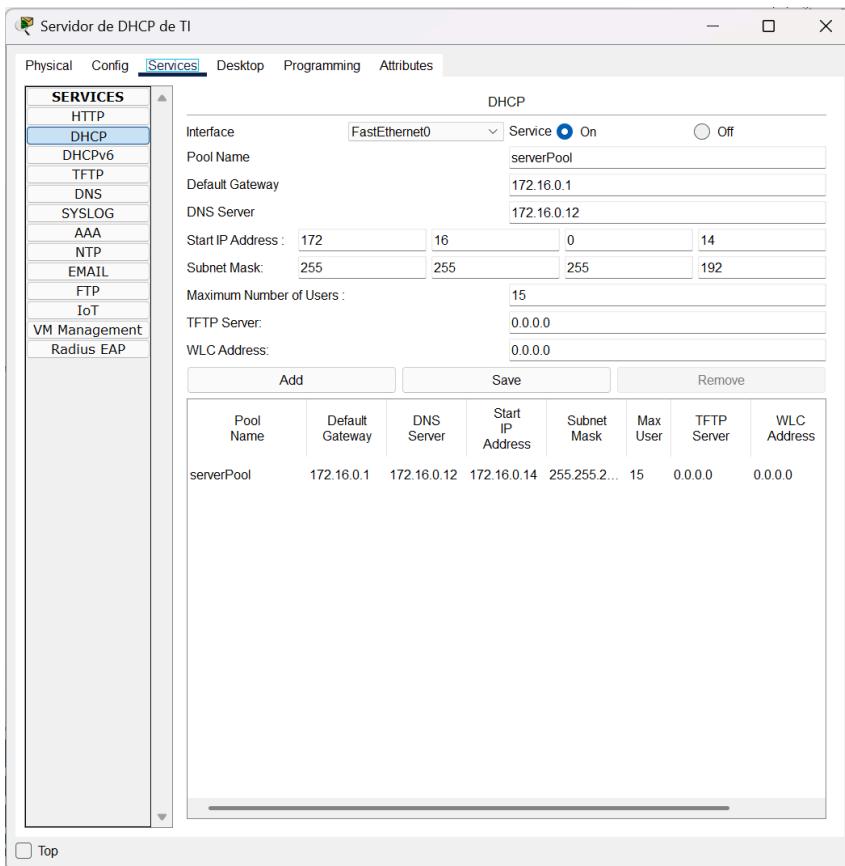
**Balanceo de carga:** Para proteger las bases de datos, se usarían varios servidores para distribuir la carga y así evitar posibles cuellos de botella. Adicionalmente, para poder fortalecer la seguridad de la base de datos y del sitio web, se podrían implementar los protocolos como HSRP o VRRP. En ambos protocolos, hay un router “principal” el cual se usa para las conexiones generalmente, mientras que pueden haber uno o más routers de “respaldo”, los cuales generalmente se activarán si hay un problema con el principal.

**Instanciación de software:** El uso de máquinas virtuales en los servidores podría ayudar a mejorar la tolerancia a fallos de la red. Esto incluiría el uso de routers y firewalls virtuales, los cuales permitirían la aceleración de la conmutación por error (failover), permitiéndole el acceso a los componentes de respaldo; el uso de redes definidas por software

(SDN), las cuales, mediante el uso de APIs, crean una red virtual la cual se comunica con la red física, esencialmente dándole órdenes, y permite mayor flexibilidad y recuperación rápida.

**Segmentación de redes para invitados:** Además de la separación de redes entre los usuarios de diferentes departamentos (en este caso, la red Ethernet de las PCs y la red Wi-Fi de las laptops) que fue mencionada anteriormente, también se recomendaría la segmentación de una red para invitados para así proteger a todos los dispositivos de las redes corporativas.





## Pruebas y Resultados

### Prueba de ping

Pc de departamento TI al servidor

```
Pinging 172.16.0.12 with 32 bytes of data:  
  
Reply from 172.16.0.12: bytes=32 time<1ms TTL=128  
Reply from 172.16.0.12: bytes=32 time<1ms TTL=128  
Reply from 172.16.0.12: bytes=32 time<1ms TTL=128  
Reply from 172.16.0.12: bytes=32 time=9ms TTL=128  
  
Ping statistics for 172.16.0.12:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 9ms, Average = 2ms
```

Usando el comando “ping” a la dirección de la computadora del departamento TI comprobamos que la conexión con el servidor DNS fue exitosa al ver que en los resultados se obtuvo un 0% de pérdida de datos

PC a Laptop en una misma Sucursal

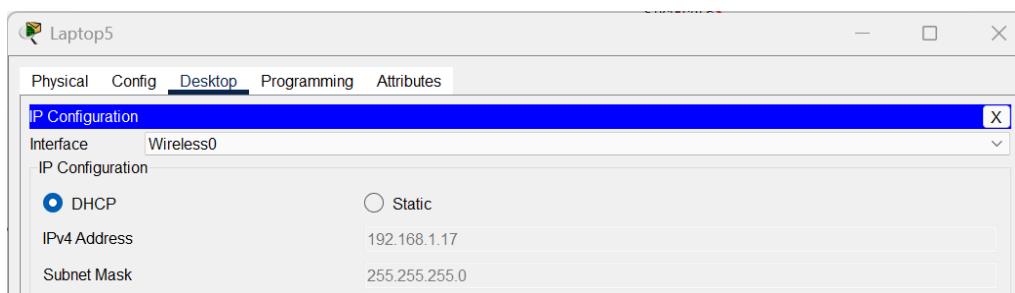
```
c:\>ping 192.168.1.17

Pinging 192.168.1.17 with 32 bytes of data:

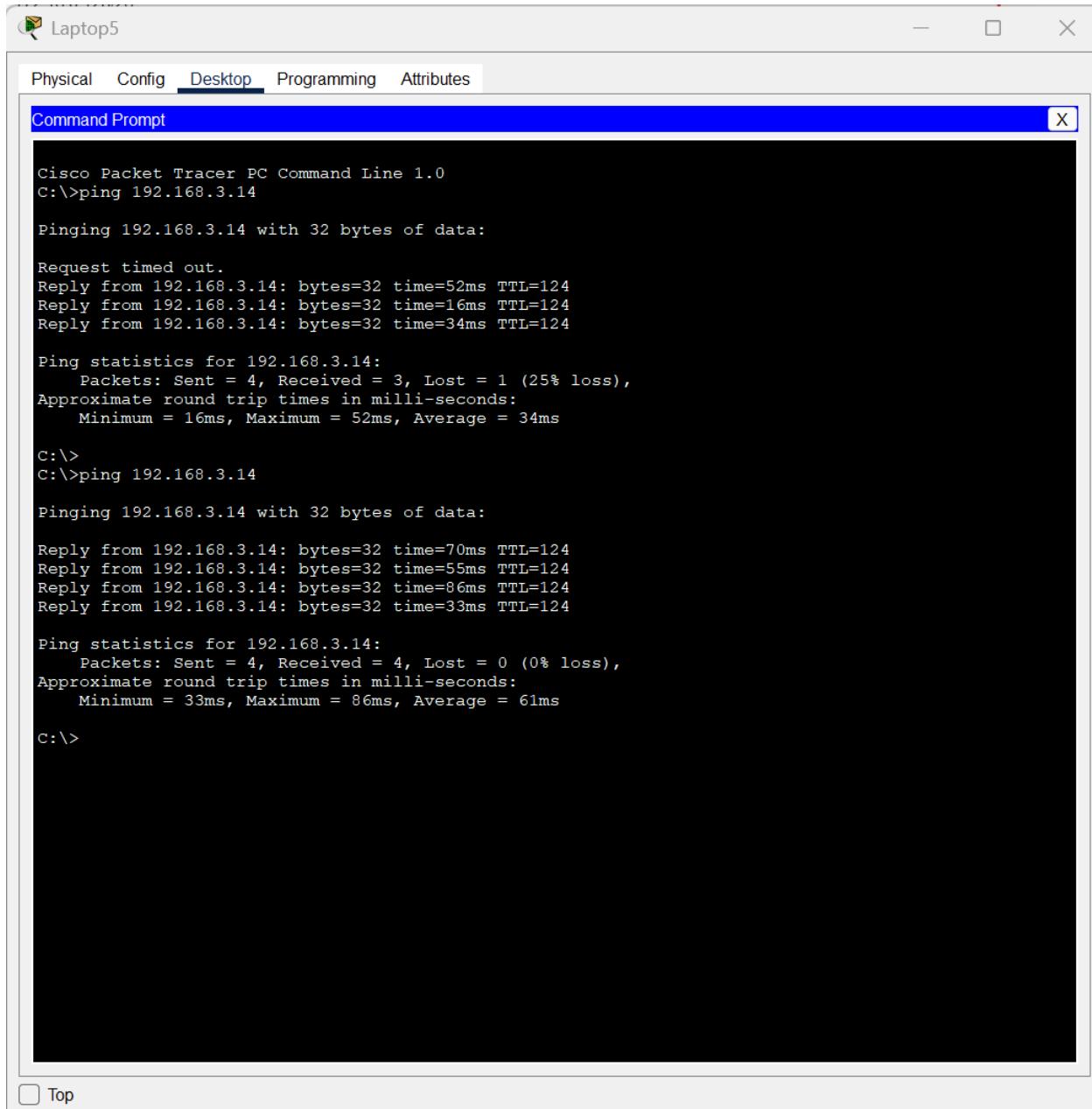
Reply from 192.168.1.17: bytes=32 time=56ms TTL=128
Reply from 192.168.1.17: bytes=32 time=24ms TTL=128
Reply from 192.168.1.17: bytes=32 time=7ms TTL=128
Reply from 192.168.1.17: bytes=32 time=26ms TTL=128

Ping statistics for 192.168.1.17:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 56ms, Average = 28ms

c:\>
```



Desde un PC en la sucursal 1 hacemos ping a una laptop en el mismo sitio, viendo que la conexión es exitosa nuevamente al no haber datos perdidos

Laptop de Sucursal 1 a Sucursal 3

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.14

Pinging 192.168.3.14 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.14: bytes=32 time=52ms TTL=124
Reply from 192.168.3.14: bytes=32 time=16ms TTL=124
Reply from 192.168.3.14: bytes=32 time=34ms TTL=124

Ping statistics for 192.168.3.14:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 52ms, Average = 34ms

C:\>
C:\>ping 192.168.3.14

Pinging 192.168.3.14 with 32 bytes of data:

Reply from 192.168.3.14: bytes=32 time=70ms TTL=124
Reply from 192.168.3.14: bytes=32 time=55ms TTL=124
Reply from 192.168.3.14: bytes=32 time=86ms TTL=124
Reply from 192.168.3.14: bytes=32 time=33ms TTL=124

Ping statistics for 192.168.3.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 33ms, Maximum = 86ms, Average = 61ms

C:\>
```

Desde la laptop 5 hacemos ping con el IPV4 de la laptop 11 dando resultado de 25% de pérdida de datos el primer intento y 0% en el segundo intento, aunque la conexión flaqueó un poco, volvió a la normalidad al rato dando una conexión exitosa

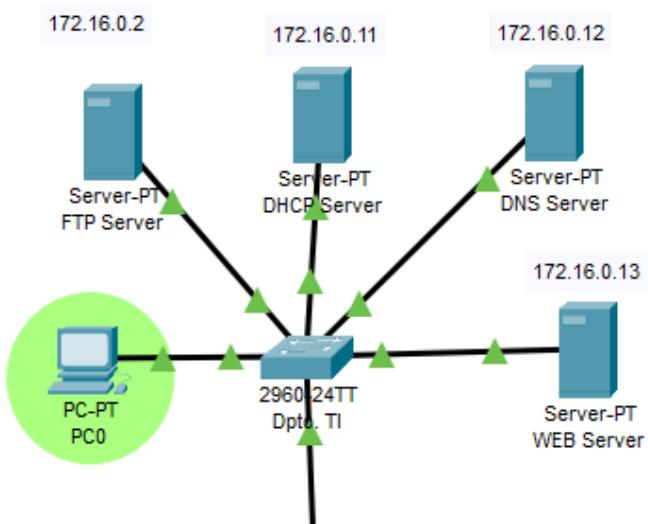
## Pruebas de DNS y FTP

A continuación se adjunta evidencia del correcto funcionamiento de los servicios de DNS y FTP. En cuanto al DNS, cada sucursal tiene su propio servidor DNS con una IP correspondiente a su red LAN, sin embargo el servicio de DNS hace referencia a nuestro servidor WEB localizado en la Sede Central.

El DNS configurado para nuestro servicio web es tecmicorp.com, el cual hace referencia directa a la IP de nuestro servidor web, además se configuró para que funcione incluso con “www.tecmicorp.com”. A continuación se muestra su correcto funcionamiento desde un dispositivo en nuestra sede central, y desde un dispositivo de nuestra sucursal más lejana.

### Funcionamiento en Sede Central:

Se utilizará el siguiente dispositivo:

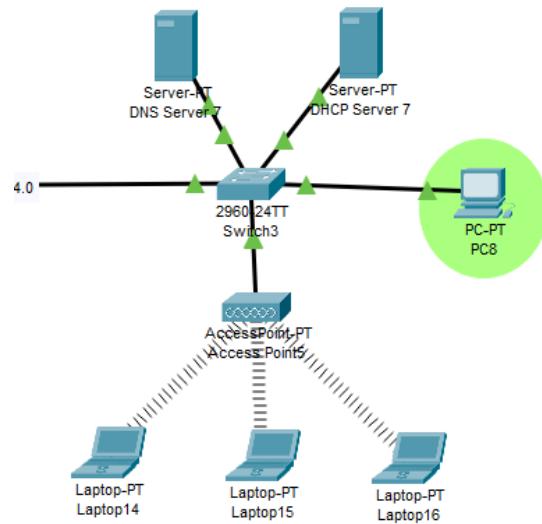


Pruebas utilizando los dos DNS configurados:



## Funcionamiento en Sucursal 4:

Se utilizará el siguiente dispositivo:



Pruebas utilizando los dos DNS configurados:





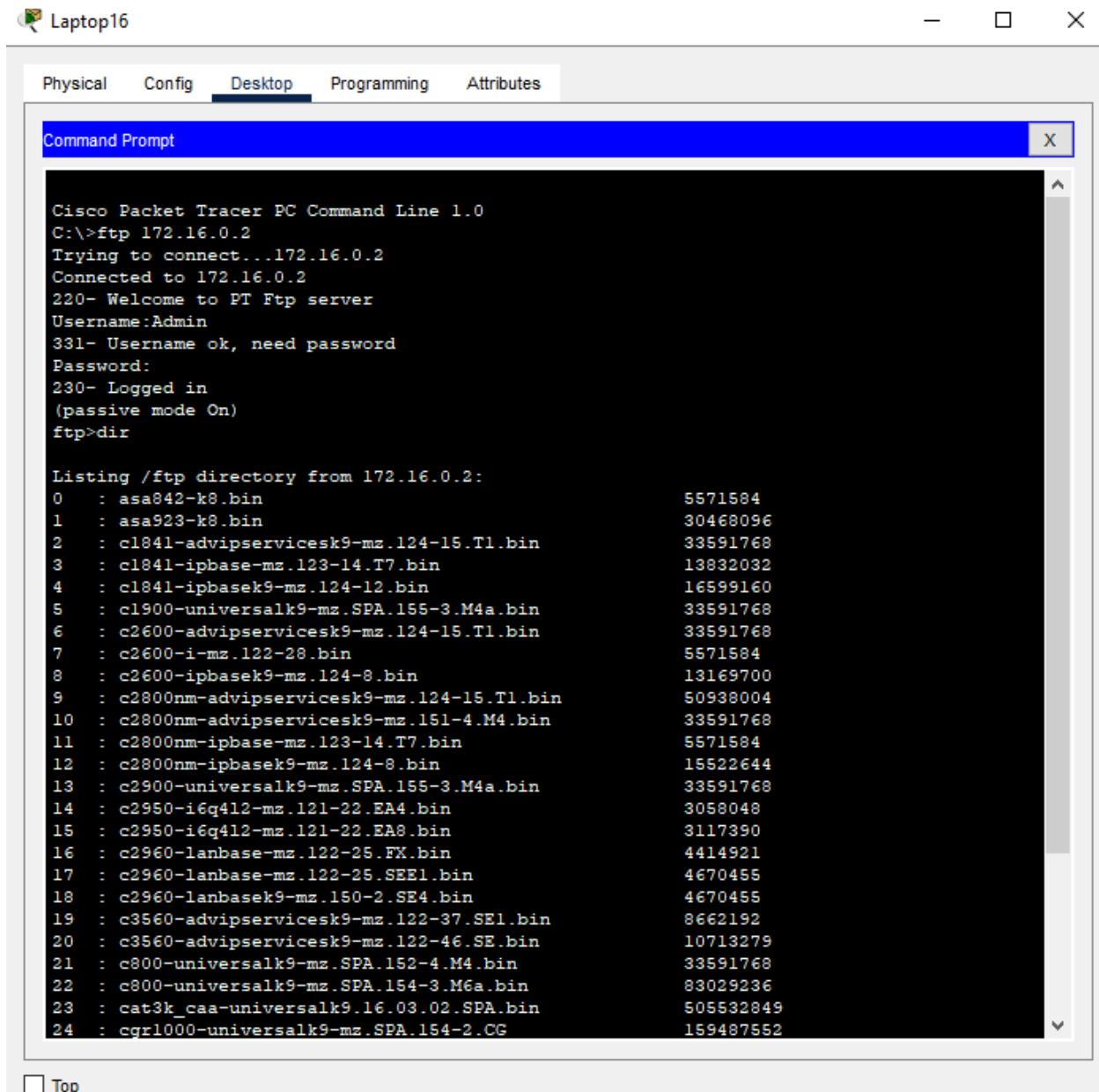
## Página de Administrador

- Sede Central
- Sucursales
- Departamentos
- Usuarios
- Contratos
- Contacto con Redes MGDZ

En cuanto al servicio de FTP solo fue necesario configurar un servidor para toda la red, la manera en la que se puede acceder a este servicio es por medio de un usuario y contraseña que se configuran directamente en el servidor. A continuación mostramos el correcto funcionamiento de este servicio desde nuestro dispositivo más alejado de nuestra sede central.

### Conección a nuestro servidor FTP:

|   | Username | Password | Permission |  |
|---|----------|----------|------------|--|
| 1 | Admin    | 12345    | RWDNL      | <input type="button" value="Add"/>   |
| 2 | Usuario1 | 54321    | R          | <input type="button" value="Save"/><br><input type="button" value="Remove"/> |



Laptop16

Physical Config Desktop Programming Attributes

Command Prompt X

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 172.16.0.2
Trying to connect...172.16.0.2
Connected to 172.16.0.2
220- Welcome to PT Ftp server
Username:Admin
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

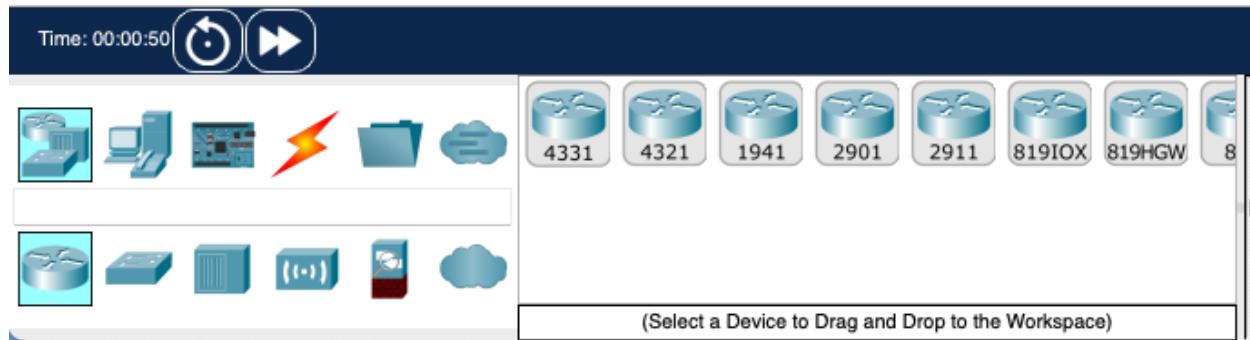
Listing /ftp directory from 172.16.0.2:
0   : asa842-k8.bin                         5571584
1   : asa923-k8.bin                         30468096
2   : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
3   : c1841-ipbasek9-mz.123-14.T7.bin       13832032
4   : c1841-ipbasek9-mz.124-12.bin          16599160
5   : c1900-universalk9-mz.SPA.155-3.M4a.bin 33591768
6   : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
7   : c2600-i-mz.122-28.bin                  5571584
8   : c2600-ipbasek9-mz.124-8.bin           13169700
9   : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
10  : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
11  : c2800nm-ipbasek9-mz.123-14.T7.bin     5571584
12  : c2800nm-ipbasek9-mz.124-8.bin          15522644
13  : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14  : c2950-i6q412-mz.121-22.EA4.bin        3058048
15  : c2950-i6q412-mz.121-22.EA8.bin        3117390
16  : c2960-lanbase-mz.122-25.FX.bin       4414921
17  : c2960-lanbase-mz.122-25.SEE1.bin      4670455
18  : c2960-lanbasek9-mz.150-2.SE4.bin      4670455
19  : c3560-advipservicesk9-mz.122-37.SE1.bin 8662192
20  : c3560-advipservicesk9-mz.122-46.SE.bin 10713279
21  : c800-universalk9-mz.SPA.152-4.M4.bin   33591768
22  : c800-universalk9-mz.SPA.154-3.M6a.bin   83029236
23  : cat3k_caa-universalk9.16.03.02.SPA.bin 505532849
24  : cgr1000-universalk9-mz.SPA.154-2.CG      159487552
```

Top

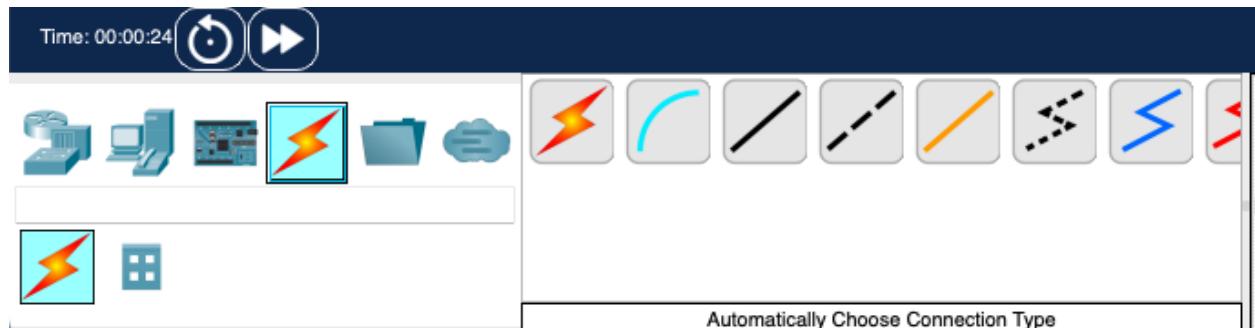
En este caso, se puede observar en nuestro command prompt como pudimos acceder con nuestro usuario admin, y ejecutar un comando que solo puede ejecutar gracias a que tiene los permisos correspondientes.

## Anexo:

A continuación, detallaremos la configuración de la sede central y de las respectivas sucursales. Para esto, necesitamos familiarizarnos con el programa de Cisco Packet Tracer.



Del lado izquierdo inferior, tenemos la sección donde podemos escoger los dispositivos que necesitaremos—en este caso: switches, routers, computadoras y laptops.



De la misma manera, el rayo amarillo-rojo que aparece en la parte de arriba se utiliza para conectar los dispositivos entre sí y transferir archivos entre ellos.



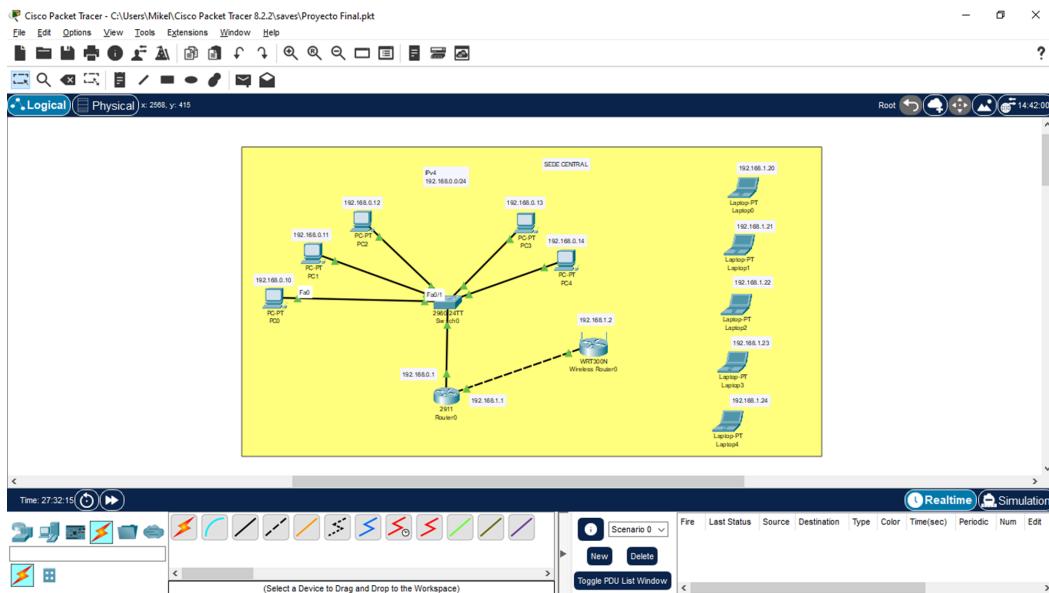
Del lado derecho inferior, tendremos nuestro control donde podremos visualizar si las comunicaciones fueron exitosas “Successful” o si fueron fallidas “Failed”. Habiéndonos familiarizado con esto, podemos continuar con la explicación de cómo conectar cada dispositivo.

### Configuración de la sede central

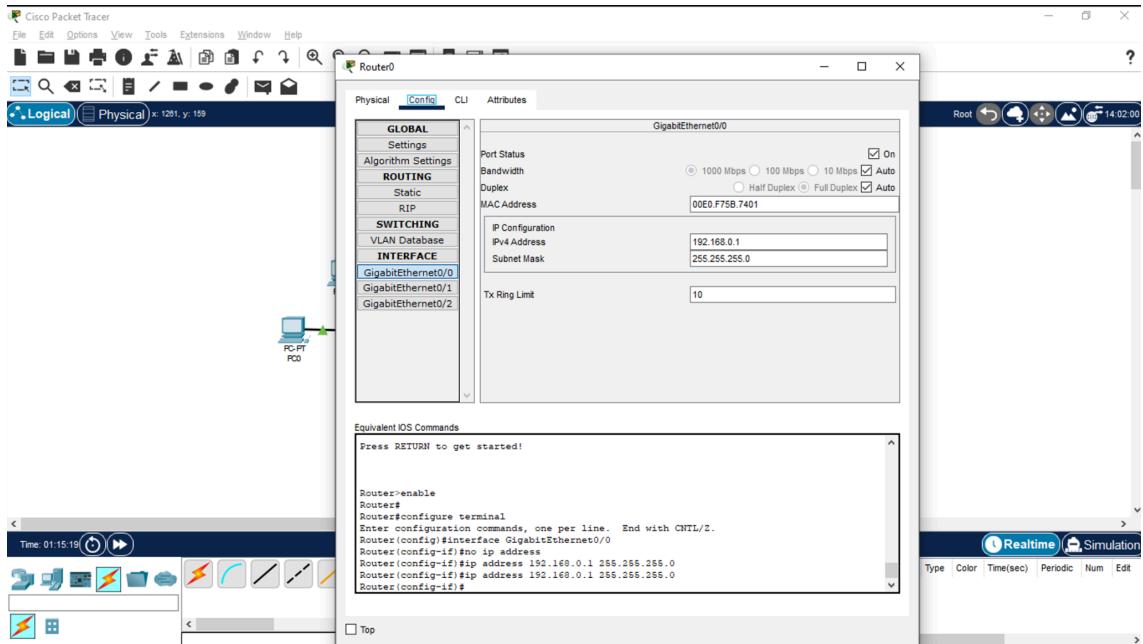
Para esta sede, lo primero que debemos de saber es la cantidad de equipos que vamos a utilizar:

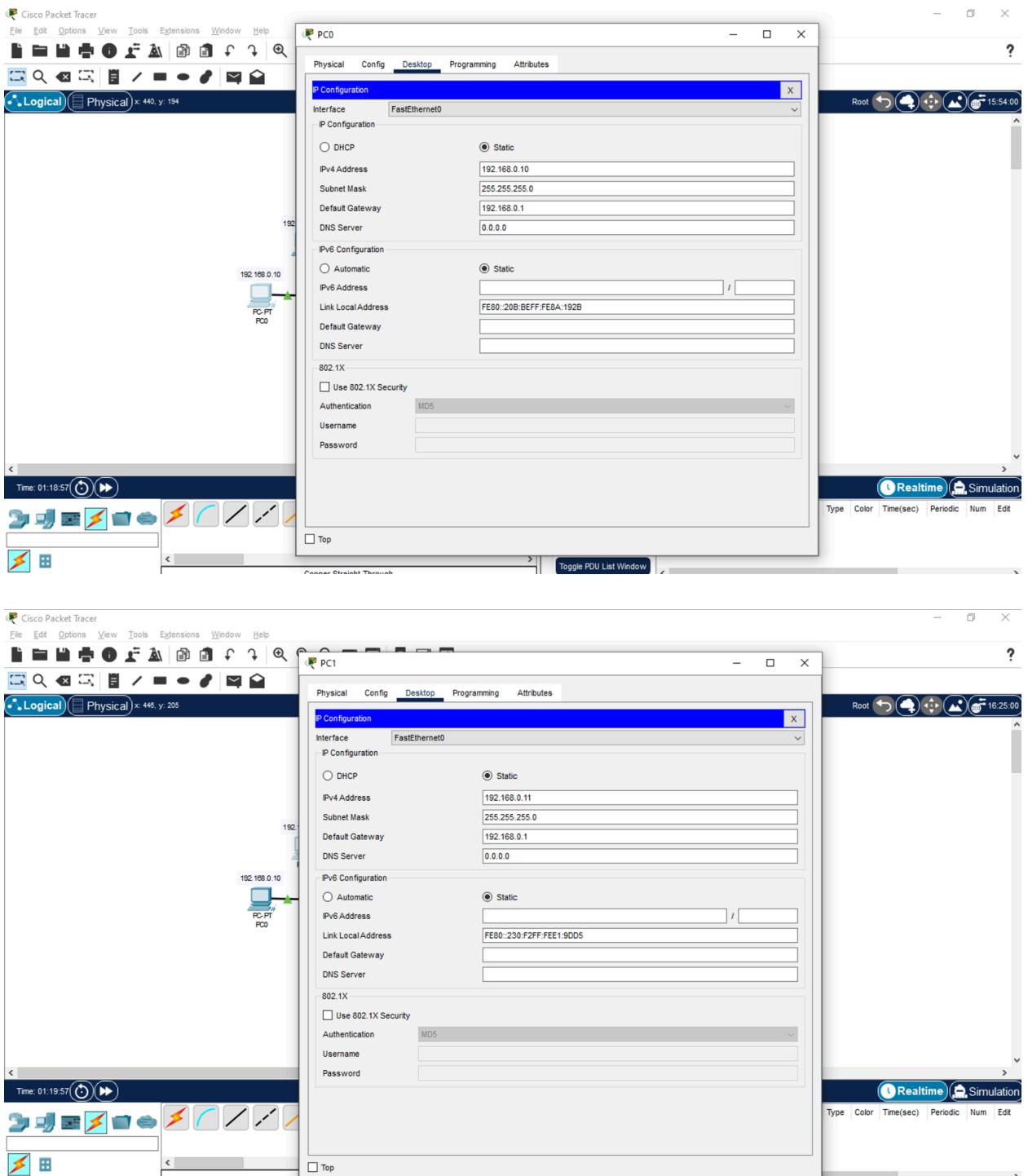
- 5 PC's
- 5 laptops
- 1 router
- 1 switch

Al añadirlos, podemos comenzar con su respectiva configuración. Primero conectamos los dispositivos PC con el switch, mientras que a este lo conectamos con router. En todos los casos, podemos seleccionar el rayo amarillo-rojo, para que la conexión se haga de manera automática, por lo que no tenemos por qué estar buscando el cable en específico.

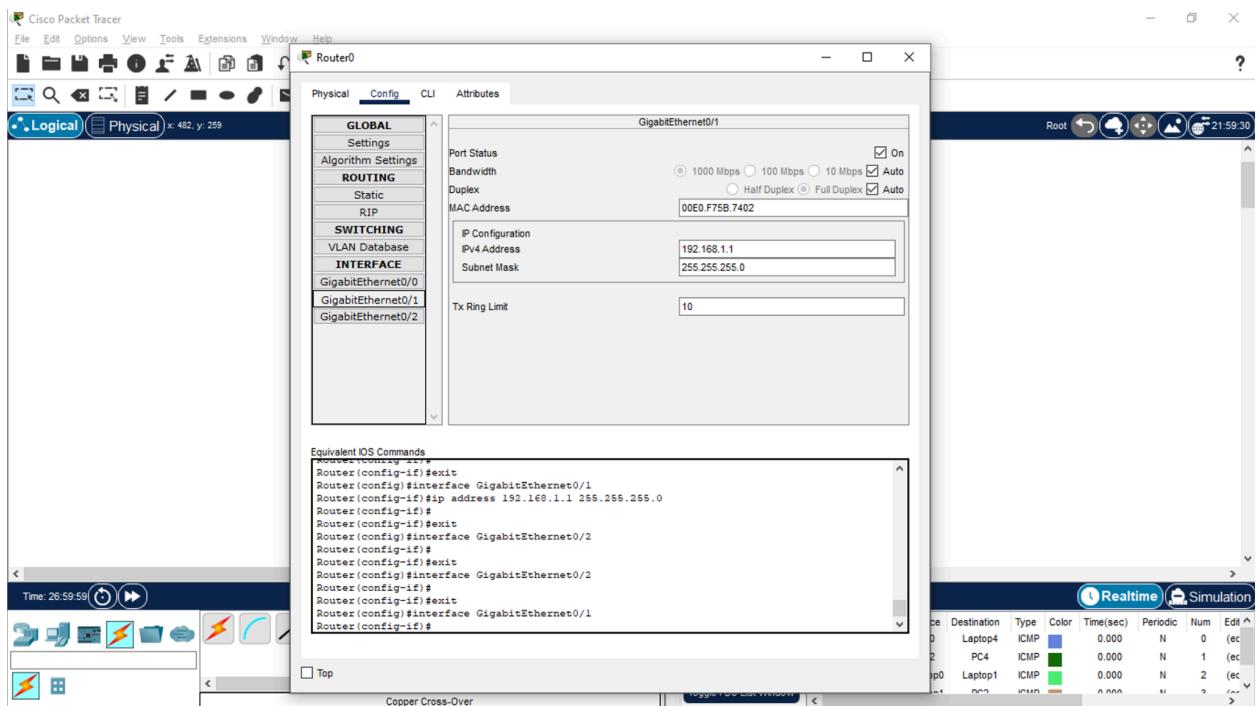


En esta imagen configuramos una laptop en Cisco Packet Tracer para conectarla a una red local. Asignamos una dirección IP fija, una puerta de enlace predeterminada y la conectamos a un switch que permite la comunicación con otros dispositivos de la misma red. Esta configuración asegura que la laptop pueda interactuar correctamente dentro de la red.

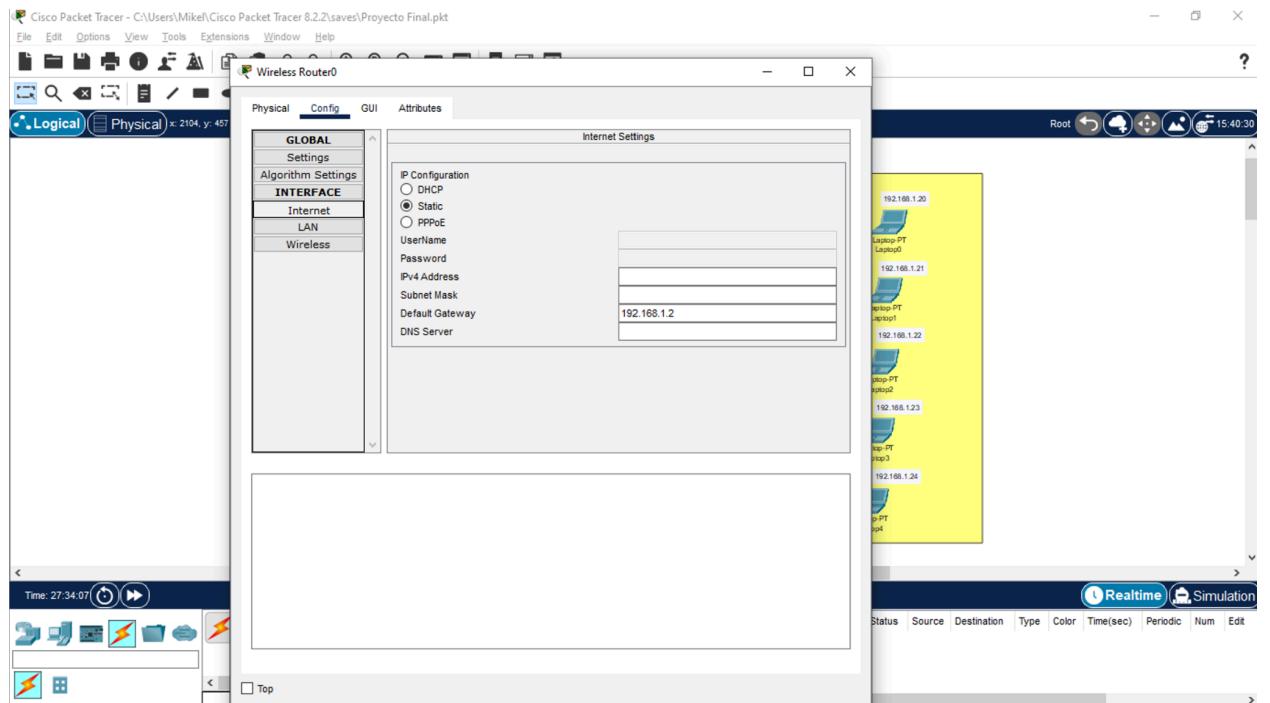




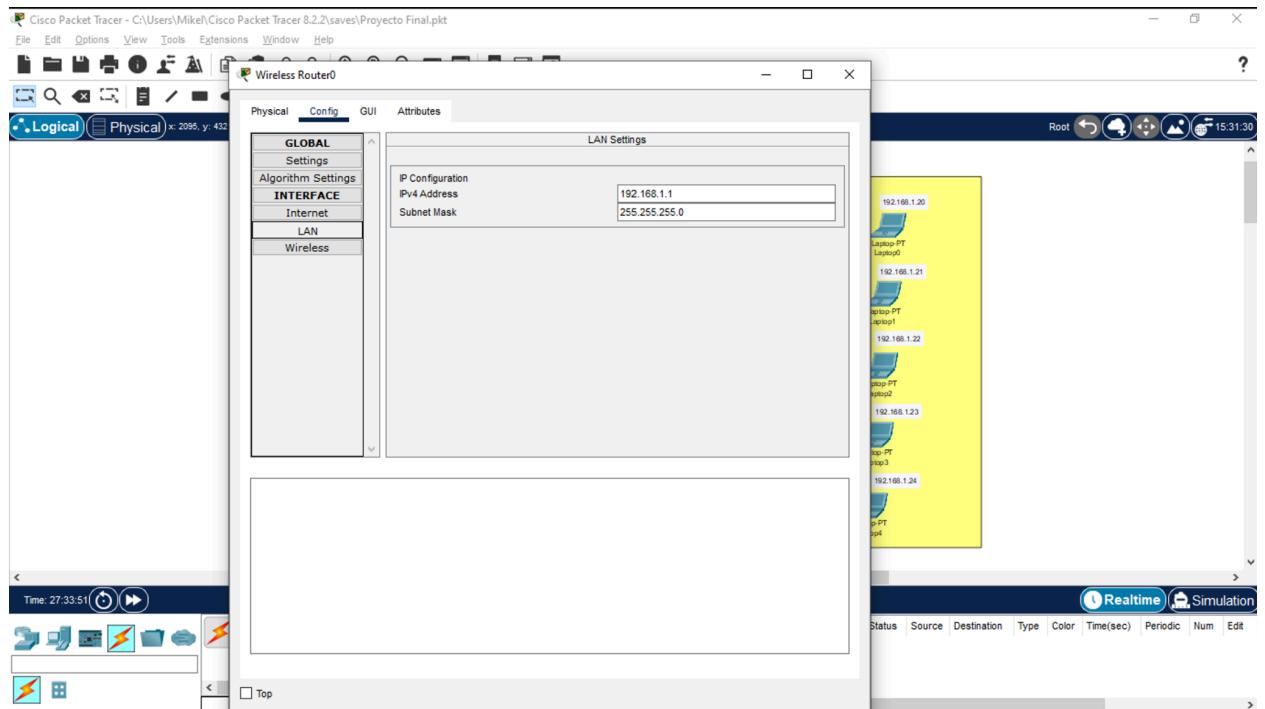
En esta configuración realizada en Cisco Packet Tracer, ajustamos la dirección IPv4 de la PC de forma manual desde la pestaña Desktop > IP Configuration. Se selecciona la opción Static para ingresar los parámetros de red. La dirección IPv4 configurada es 192.168.0.11, con una máscara de subred 255.255.255.0 (clase C estándar). Además, se establece como puerta de enlace predeterminada la dirección 192.168.0.1, correspondiente al router de esta red. El campo del servidor DNS está configurado en 0.0.0.0, indicando que no se ha especificado un servidor DNS.



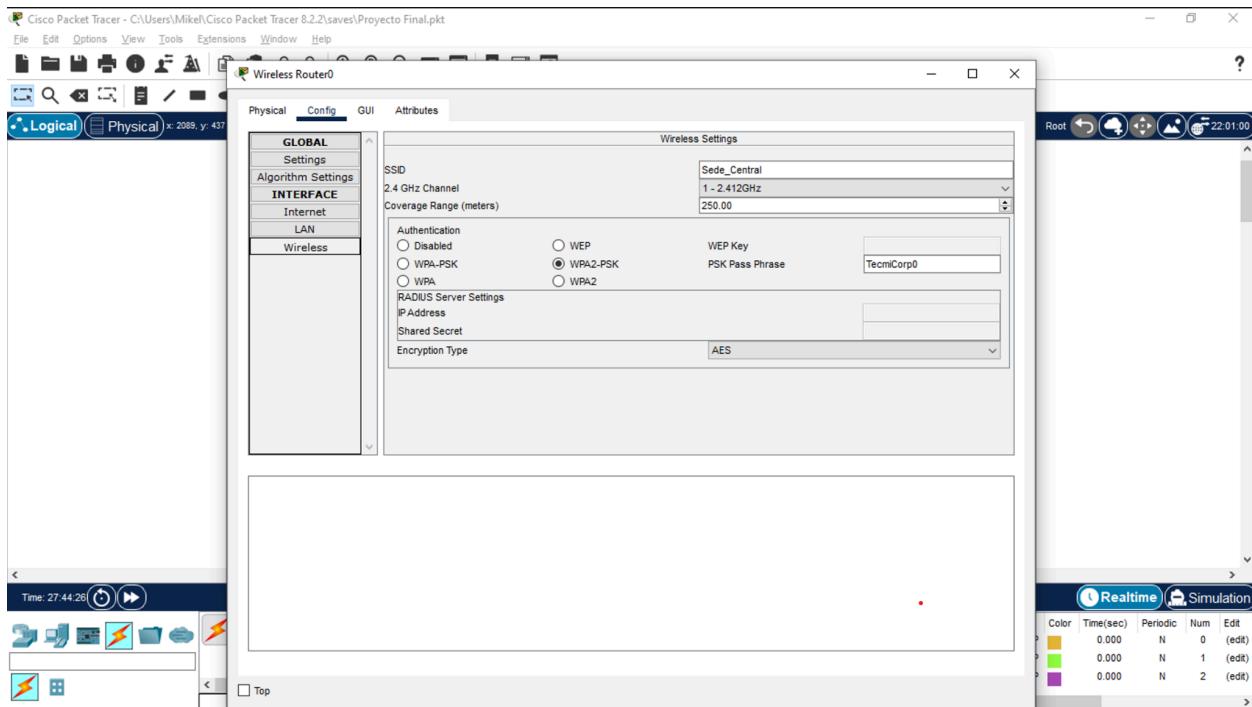
En la primera imagen, se está configurando la interfaz GigabitEthernet0/1 de un router en Cisco Packet Tracer. Se le asigna la dirección IP 192.168.1.1 con máscara de subred 255.255.255.0. El puerto está activado y configurado para funcionar a 1000 Mbps en Full Duplex. Abajo se muestran los comandos equivalentes en la consola del router, que permiten hacer esta configuración de forma manual usando el modo de configuración IOS.



En la imagen estamos configurando la conexión a Internet de un router inalámbrico en Cisco Packet Tracer. En la pestaña "Config", dentro de "Internet", seleccionamos las opciones de configuración IP. Se puede ver que el campo "Default Gateway" está configurado con la dirección "192.168.1.2", pero aún no se han ingresado la dirección IPv4, la máscara de subred ni el servidor DNS. Esto sugiere que estamos en proceso de establecer la configuración de red para que el router pueda conectarse correctamente a Internet y proporcionar acceso a los dispositivos de la red.

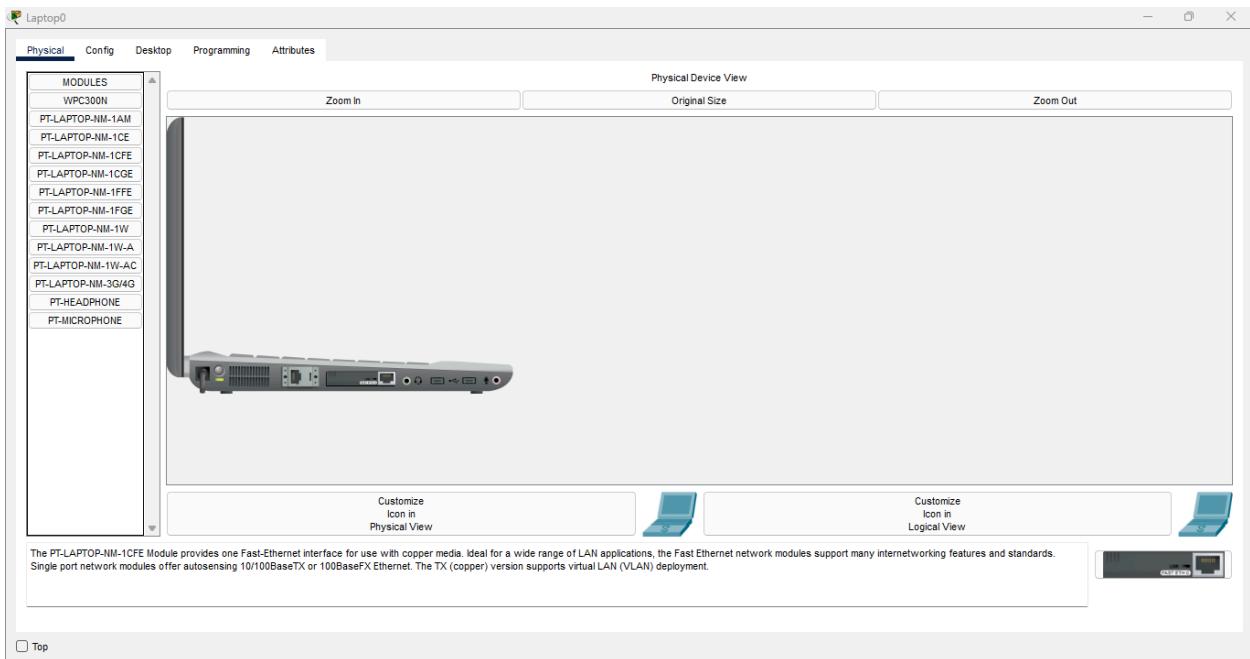


En esta imagen, se está configurando un Wireless Router, específicamente en la parte de LAN Settings. Aquí también se le asigna la dirección IP 192.168.1.1 con la misma máscara de subred 255.255.255.0. Esta configuración define la red interna del router, permitiendo que administre las direcciones IP para los dispositivos conectados, ya sea por Wi-Fi o por cable. Esto asegura que todos los dispositivos de la red puedan comunicarse entre ellos y con el router.

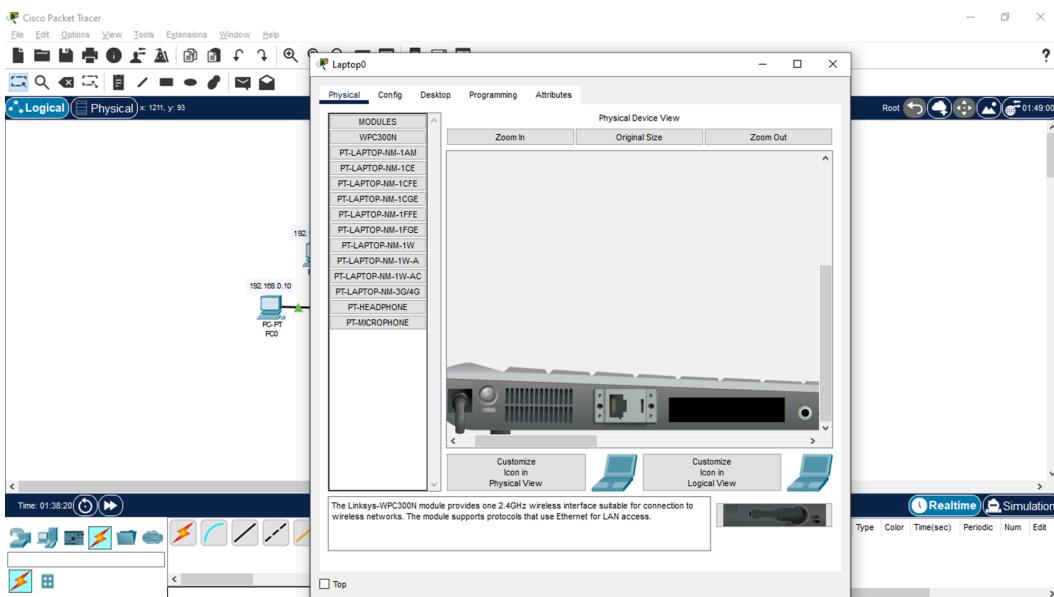


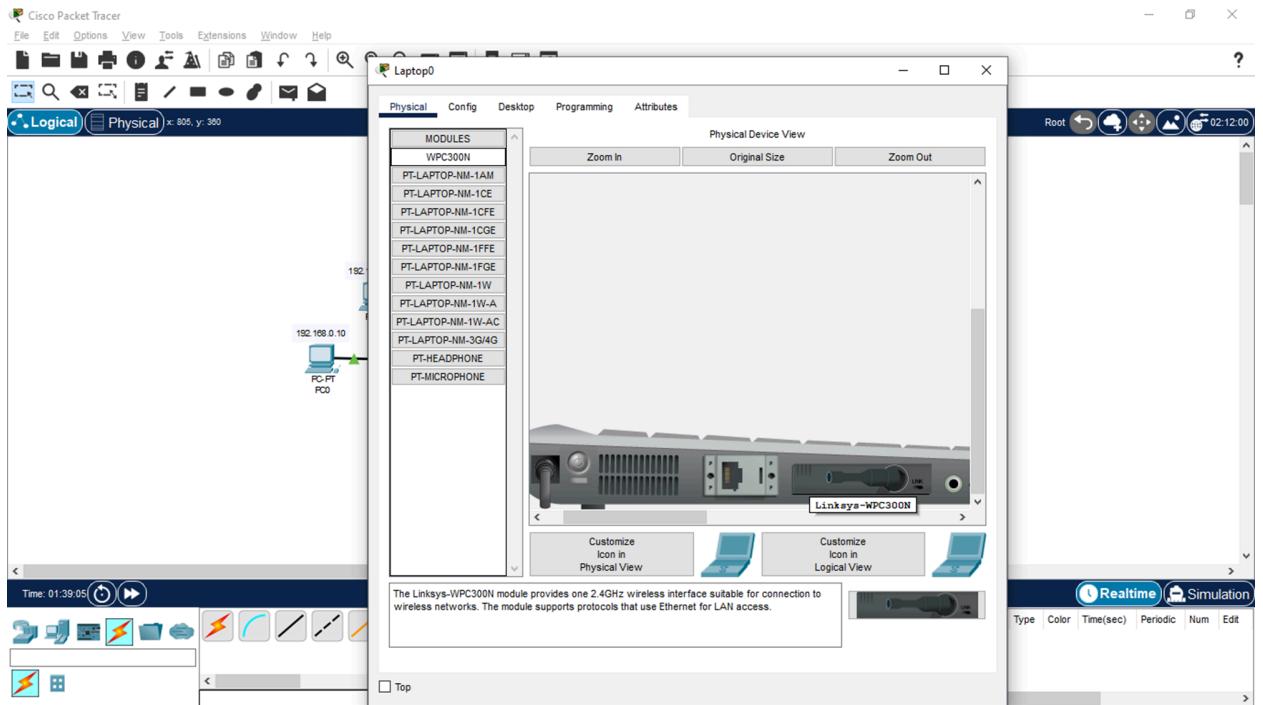
En la imagen estamos configurando un router inalámbrico en Cisco Packet Tracer. En la pestaña "Config", dentro de "Wireless", asignamos el SSID "Sede\_Central", el canal 1 en 2.4 GHz y un rango de 250 metros. Elegimos WPA2-PSK como seguridad, con la clave "TecmiCorp0" y cifrado AES para mayor protección. Esta configuración asegura una conexión segura y estable para los dispositivos.

Una vez hecho todo esto, en todas las laptops, ocupamos abrir la vista física de los dispositivos (pestaña “Physical”). Esto se debe a que, por defecto, las laptops en Cisco Packet Tracer suelen venir con el módulo de la tarjeta de red PT-LAPTOP-NM-1CFE, el cual solamente permite conexión a la red mediante Fast Ethernet, como se puede ver en la siguiente imagen:



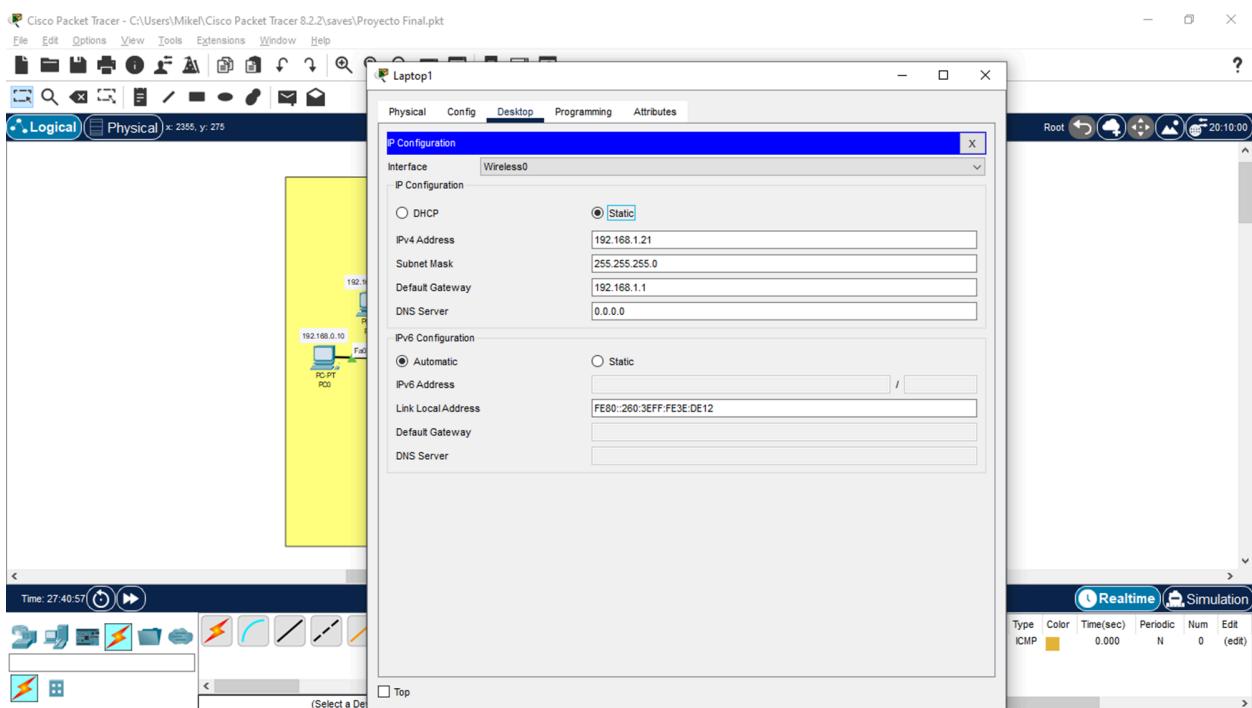
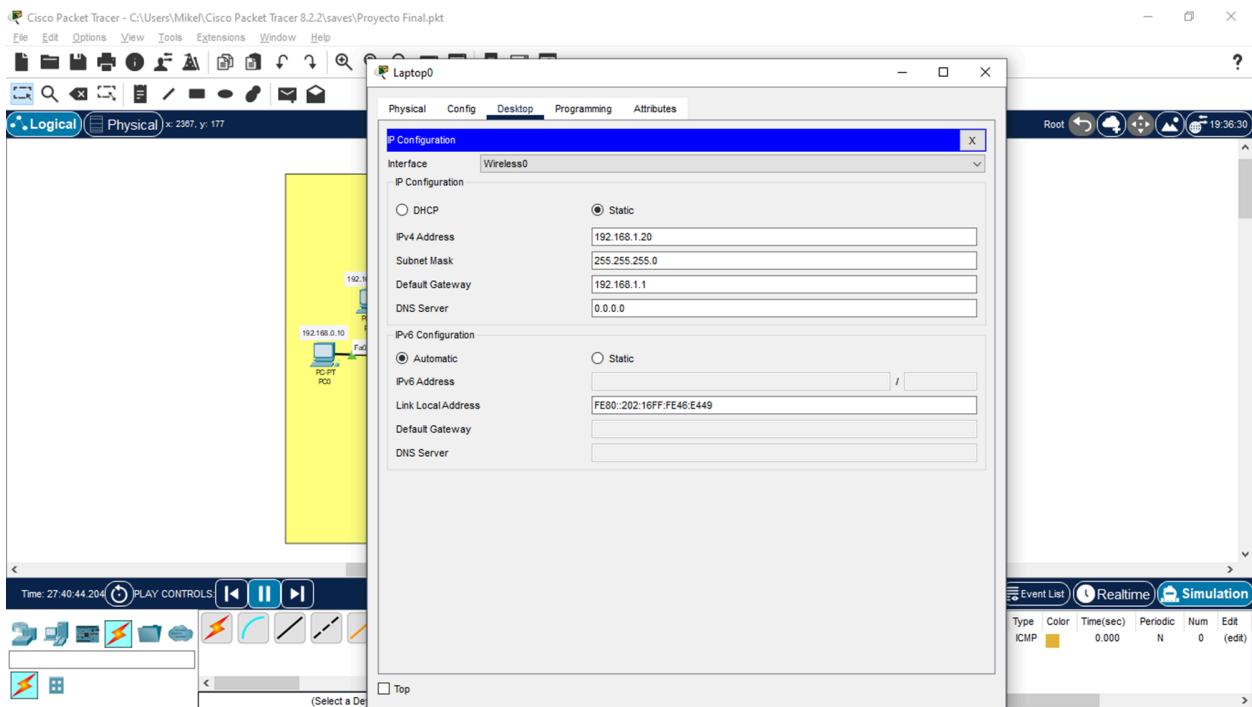
Esto, no obstante, no es lo que ocupamos, ya que nuestro propósito para este proyecto, y debido a eso, vamos a cambiar el módulo de red de cada laptop a el Linksys-WPC300N, ya que este va a permitir la conexión inalámbrica a la red con una velocidad de 2.4 GHz. Para hacer esto, primero ocupamos apagar la laptop (véase el botón con una luz verde), remover el módulo anterior y arrastrar el módulo de la tarjeta de red que queremos al espacio vacío.



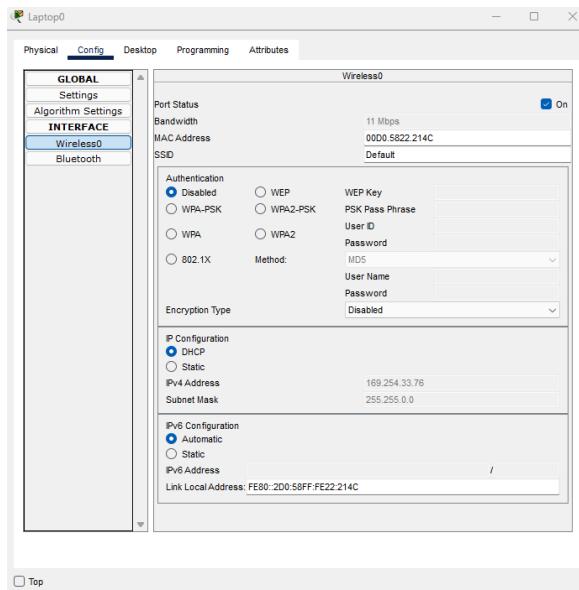


Posteriormente, al igual que con las PCs, debemos asignar direcciones IPv4 a todas las laptops, asegurándonos de que ninguna dirección se repita. Esto se hace haciendo click a Escritorio (Desktop) y luego a Configuración de IP (IP Configuration).

Adicionalmente, ocupamos asignarles máscaras de subred (Subnet Mask) y un gateway por defecto (Default Gateway) a todas las laptops. A diferencia de las direcciones IPv4, estas tienen que ser idénticas en todas las laptops, como se puede ver en las siguientes imágenes:



Finalmente, ocuparemos conectar todas las laptops a la red inalámbrica del router. Para esto, primero ocuparemos abrir una laptop, dirigirnos a Config, y, en la interfaz (Interface), se va a ver por defecto de la siguiente manera:

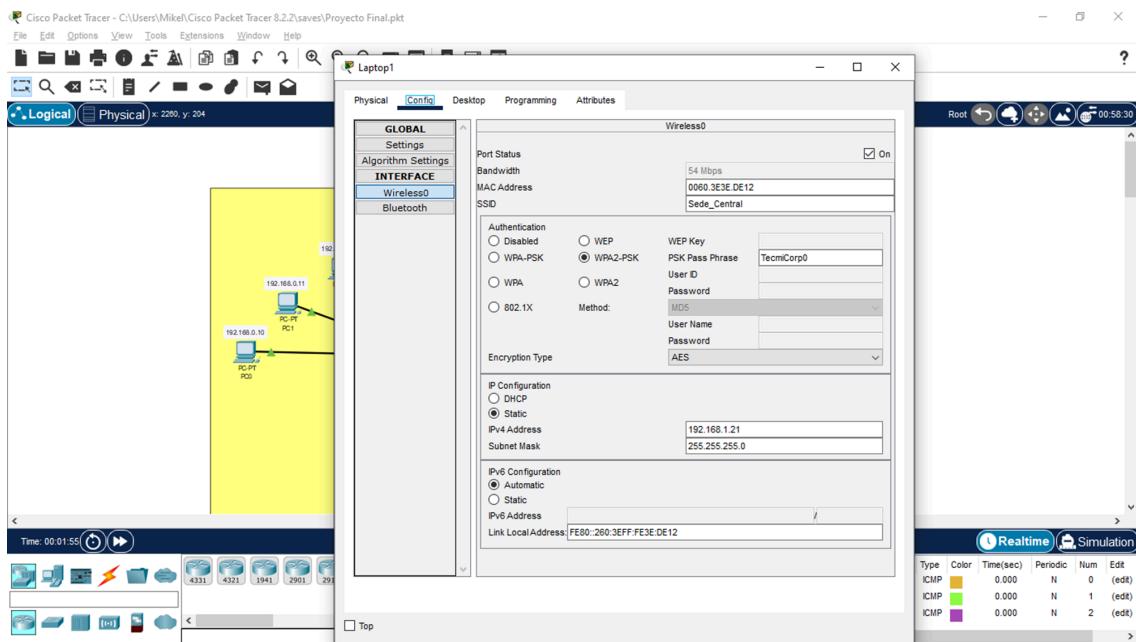
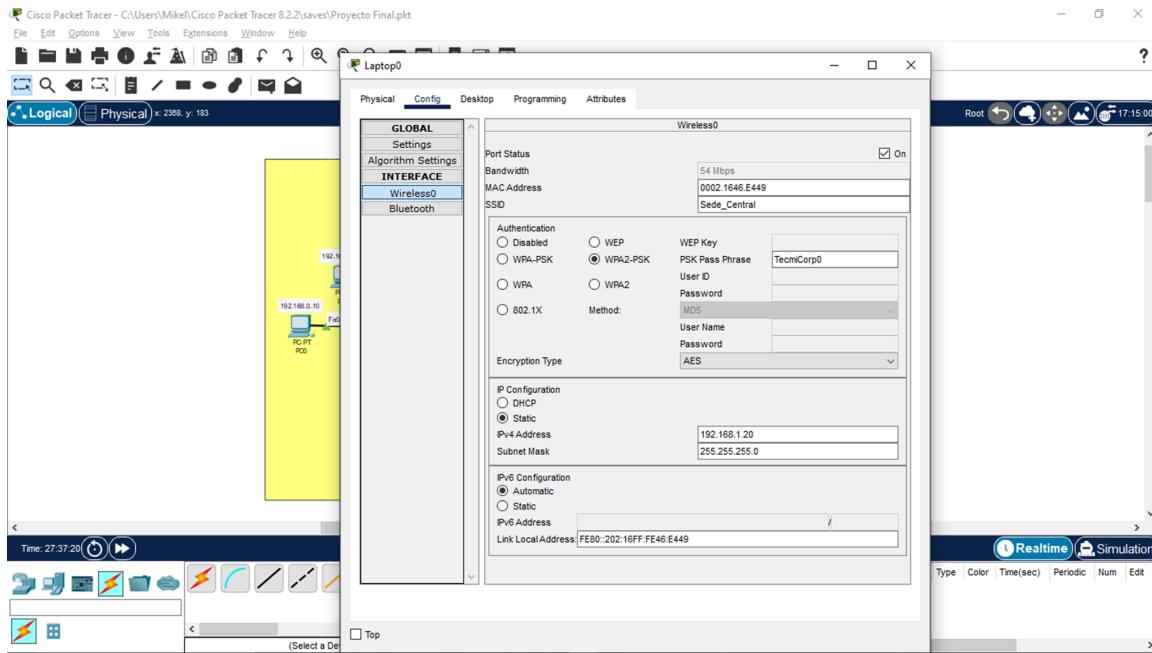


(Nota: esta captura es de un proyecto vacío, y fue tomada solamente para referencia.)

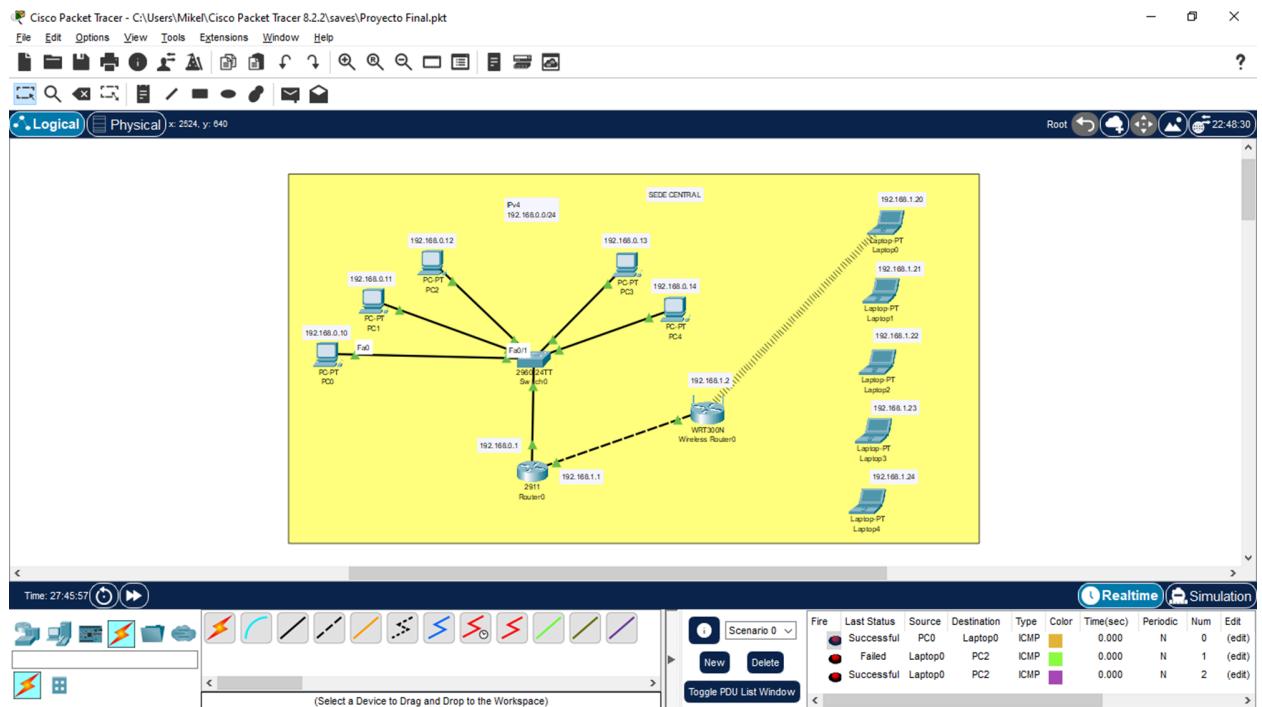
En todas las laptops, las direcciones MAC siempre van a estar asignadas automáticamente, por lo que no es necesario cambiarlas. Lo que va a requerir cambios es:

- El tipo de autenticación: este, por defecto, viene desactivado, por lo que tenemos que cambiarlo para que quede con el del router (en nuestro caso, decidimos seguir el tipo WPA2-PSK, ya que este es el estándar actual generalmente usado en redes SOHO).
- La PSK Pass Phrase: esta es una clave pre-compartida, y es usada por el cliente y por el router para encriptar datos. En nuestro caso, esta es "TecmiCorp0".
- La dirección IPv4 y la máscara de subredes: estas deben ser la misma que le asignaste a cada laptop anteriormente (o la que se asignó automáticamente, en el caso de la máscara de subredes).

Una vez hecho todo esto, las laptops se deberían ver así:



Y las conexiones se deberían de ver así:



## Configuración de las sucursales

En tanto, las sucursales tendrán los siguientes equipos:

- 1 PC
- 3 laptops
- 1 router
- 1 switch

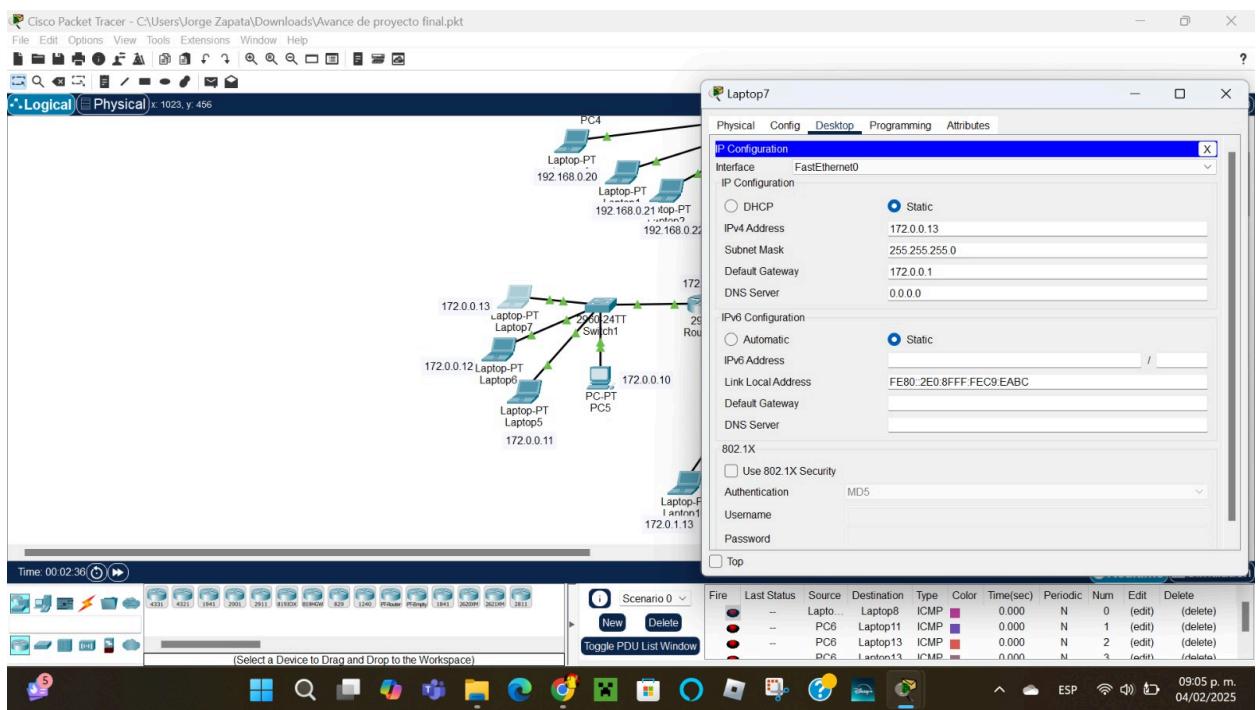


Foto de la “laptop7” de la sucursal 1

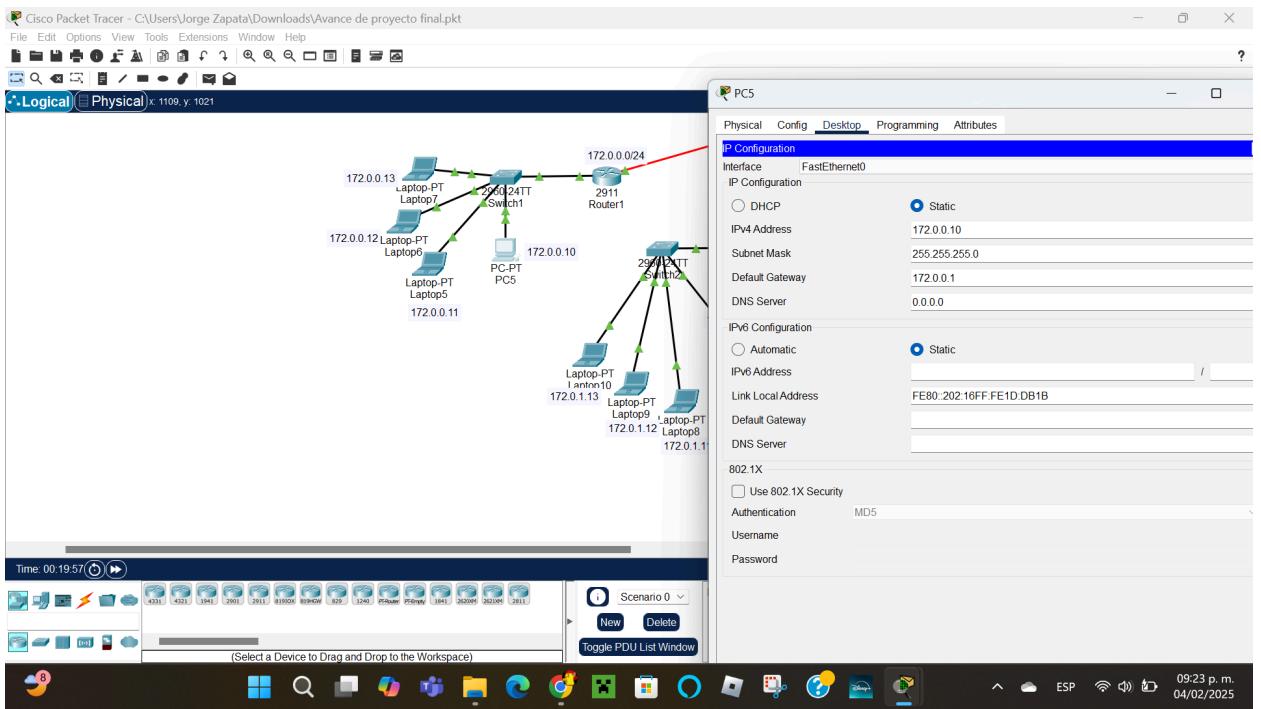


Foto de PC5 de la sucursal 1

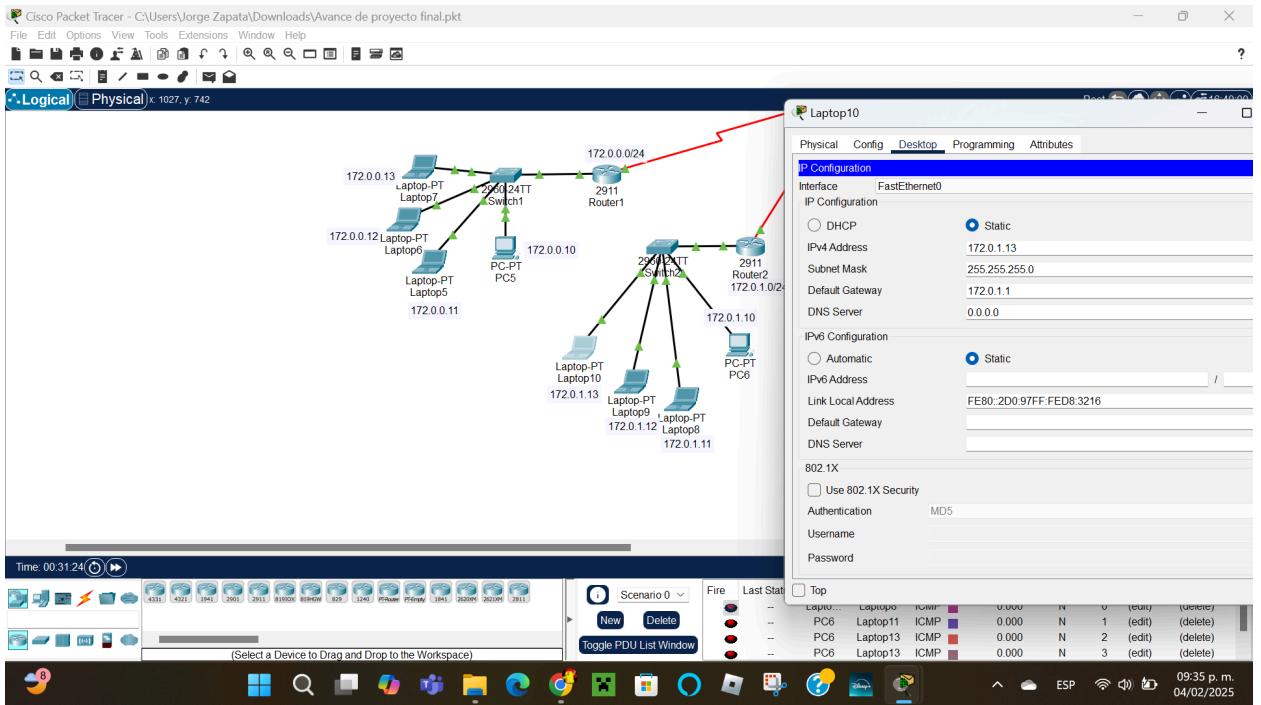
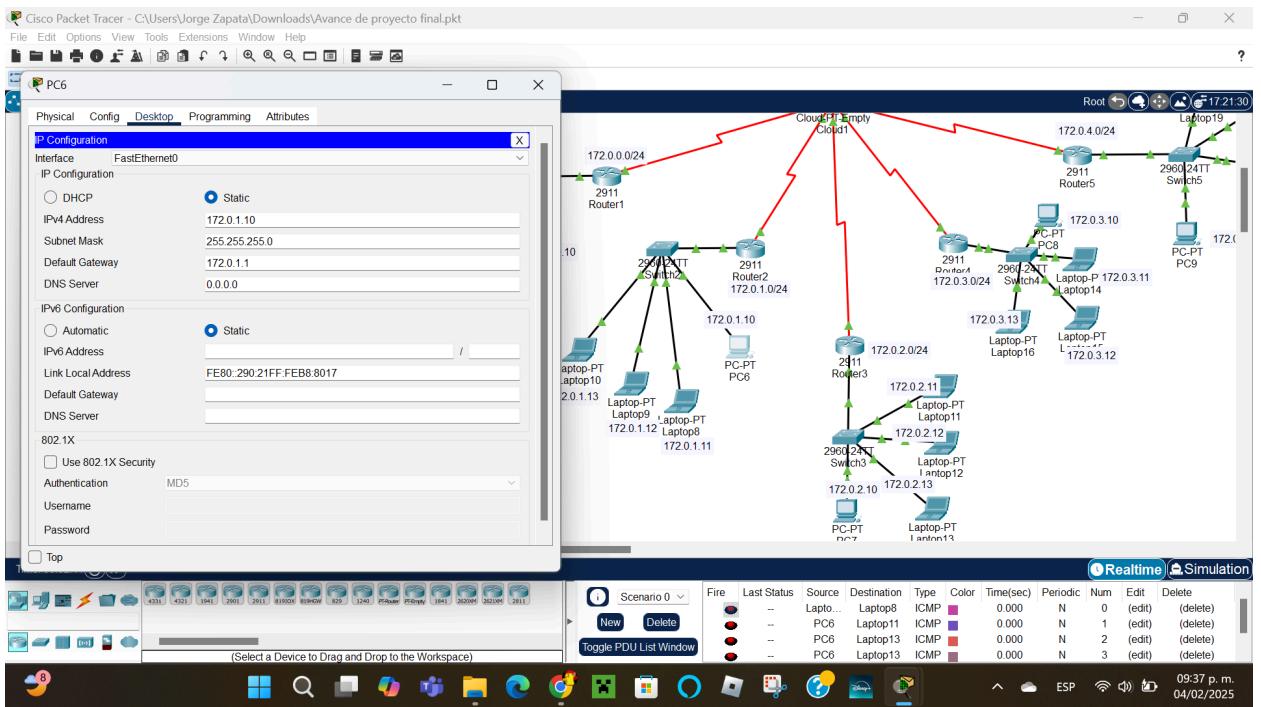


Foto de la laptop10 sucursal 2



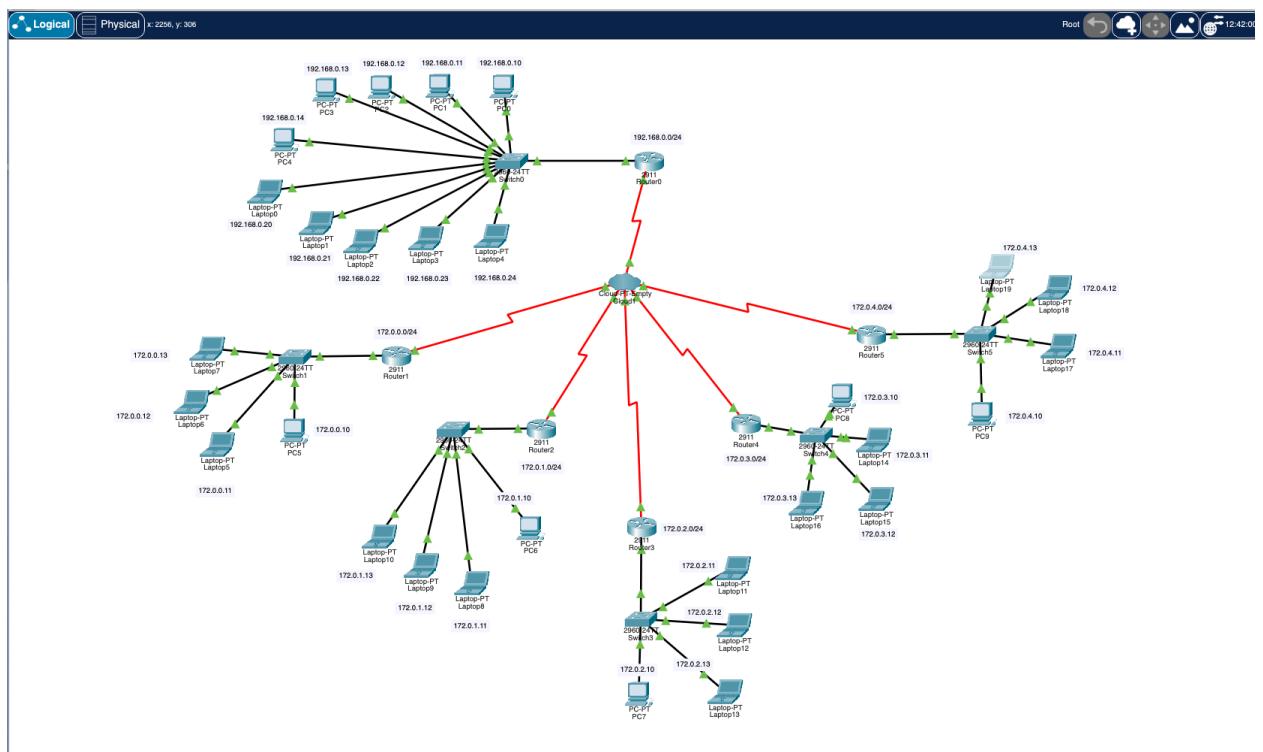
### Foto de la PC6 de la sucursal 2

En estas imágenes los PCs y laptops de cada una de las sucursales estarán conectadas por un cable ethernet al switch, cada dispositivo final contará con una IPV4, una submask y con un default gateway para mandar datos a otras redes. Asimismo todos los dispositivos contarán con la configuración address en modo estático. El switch por otro lado estará conectado con cable ethernet al router para acceder a la red. Esta estructura física será igual para las demás sucursales al igual que la configuración que manejaremos, algo a considerar es que la IP cambia ligeramente en cada sucursal, específicamente el cuarto dígito ejemplo (172.0.0.10, 172.0.0.11) para poder manejar los diferentes tipos de hosts de la área local. Asimismo por cada sucursal también se modificará el tercer dígito de las ips ejemplo (172.0.1.10, 172.0.2.10), para dar a entender que cada dispositivo estará ubicado en subredes diferentes, así se optimizará la administración de la red al no repetir ips. Cabe aclarar que como se puede ver

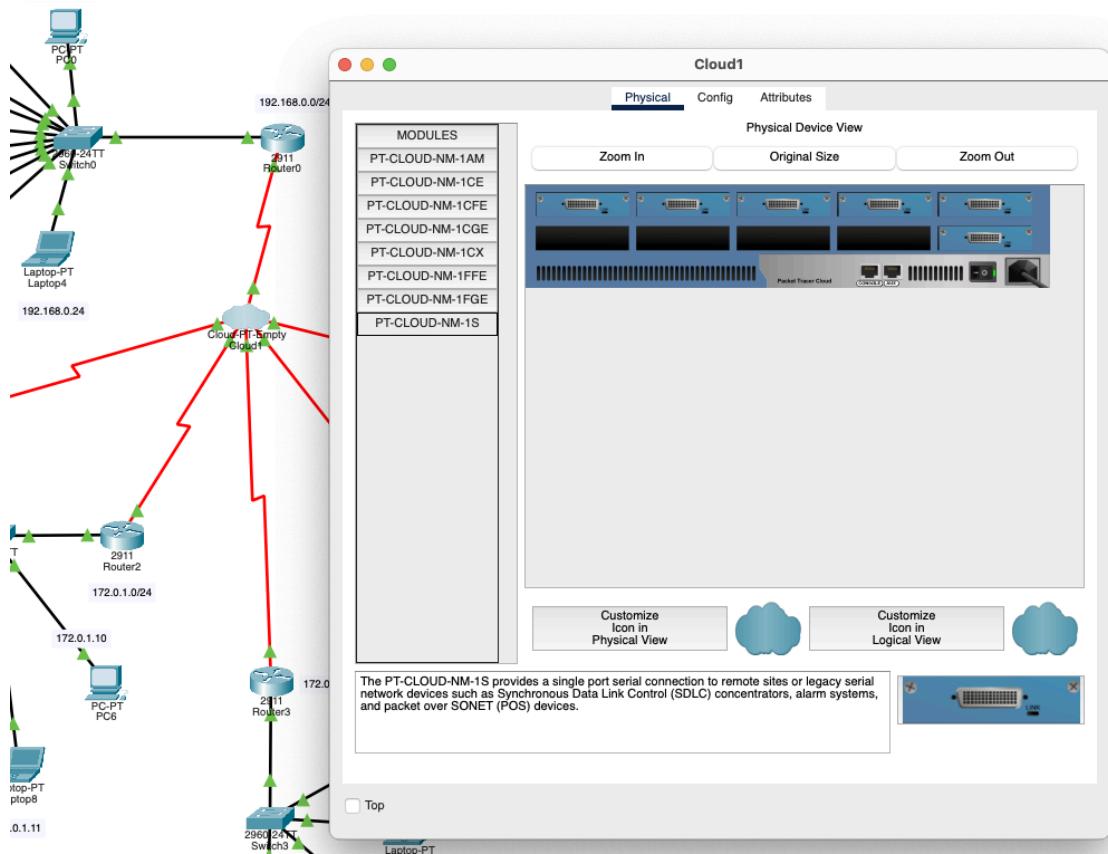
está configurado para solo usar el IPV4 y no el IPV6, utilizando la configuración de predeterminada

## **Intercomunicación entre sede central y sucursales**

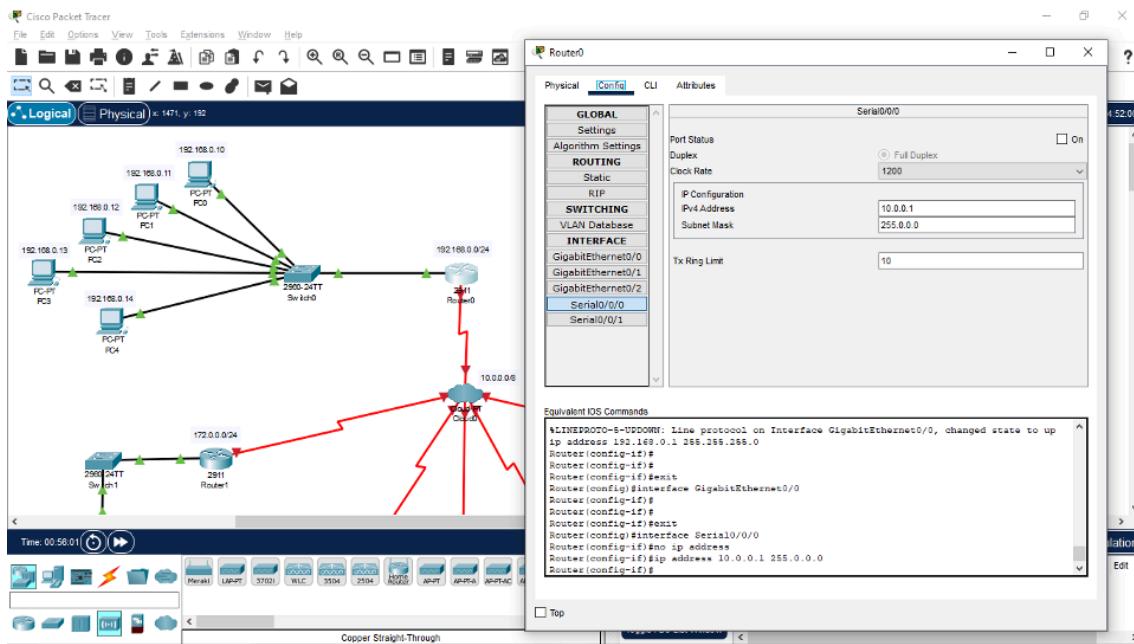
A través de la topología de estrella es como resolveremos la comunicación entre sedes y sucursales. Es necesario recordar que por esto las comunicaciones serían más eficientes, seguras y escalables ya que, si una sucursal se desconectara, las demás y la central seguirían de pie y no habría afectaciones a todo el negocio. Del mismo modo, se podrían agregar más sucursales sin necesidad de alterar toda la infraestructura. En consecuencia, nuestra infraestructura es tanto escalable como segura.



Ahora, como podrá observarse a detalle, todos los routers están conectados a una imagen de una nube, esto representaría el Proveedor de Servicios de Internet (ISP). Por lo que, a pesar de que la comunicación dentro de las mismas sucursales sea a través de un cable, al comunicarse entre ellas lo harían de manera inalámbrica.

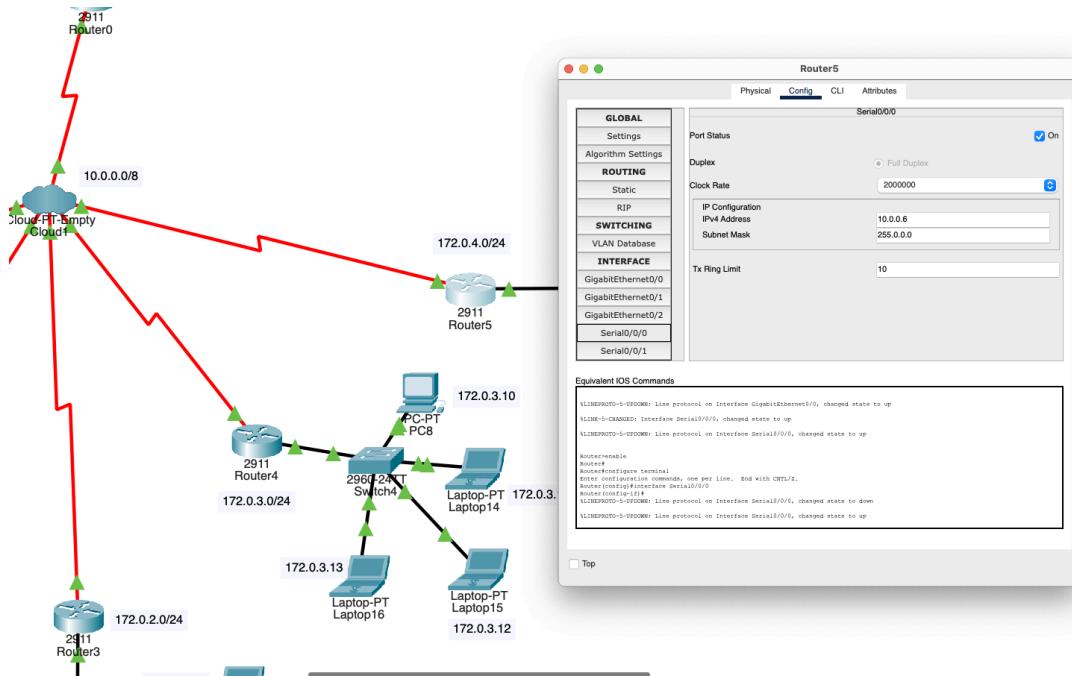


Para ello, primero debemos configurar la nube. Al arrastrar la nube, la conectamos a los routers con un cable Serial DTE e igualmente le vamos añadiendo los módulos tipo PT-CLOUD-NM-15, que en este caso serían seis (1 sede y 5 sucursales). Habiendo hecho eso, podemos proceder a configurar los routers.

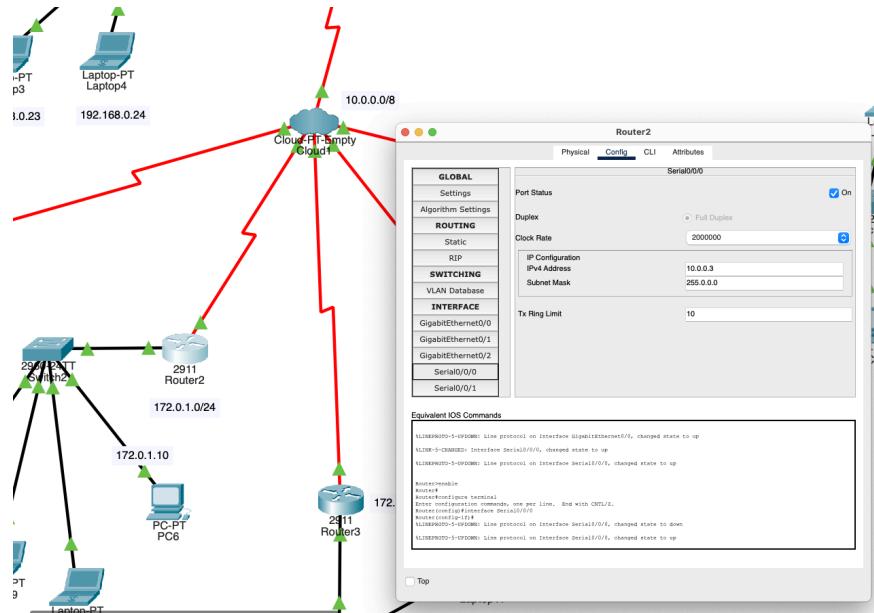


Recordemos que configuramos los puertos GigabitEthernet para habilitar la comunicación dentro de las propias sucursales y sede, pero si deseamos que haya una intercomunicación entre éstas, procederemos a configurar la interface Serial 0/0/0 en la parte de Config al abrir el router. Aquí, en la IPv4, pondremos la dirección, **10.0.0.1**, que se puede observar es perteneciente a la red de la nube; mientras que la submáscara será **255.0.0.0**

Procederemos a realizar lo mismo con todos los routers de cada sucursal

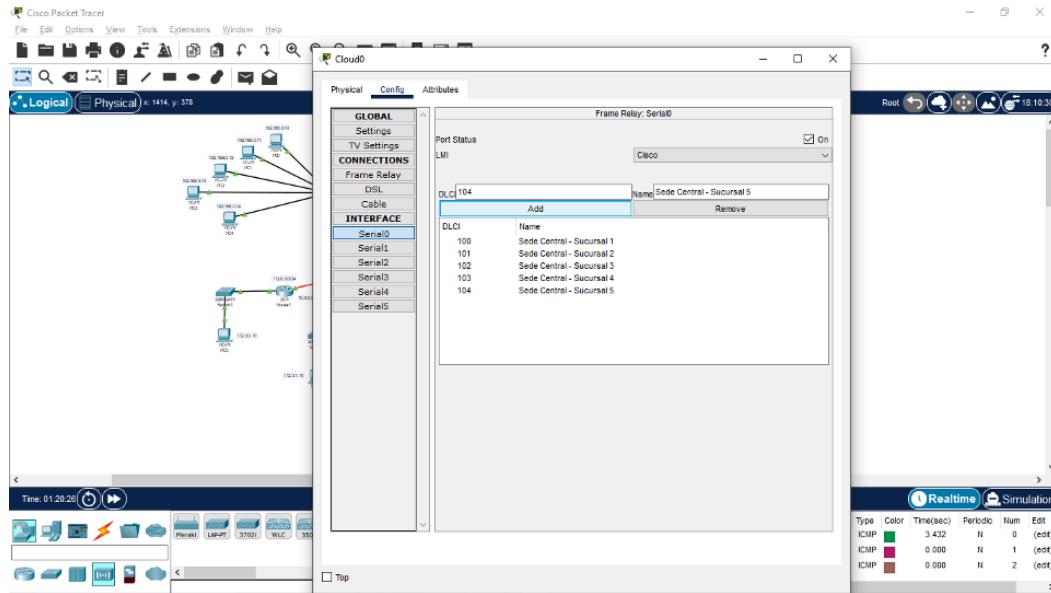


Ejemplo de la sucursal número 2, “Router2”.



Ejemplo de la sucursal número 5, “Router5”.

Ahora, para poder habilitar la comunicación entre las sucursales, debemos realizar lo siguiente. Primero, debemos seleccionar la nube y nos vamos a su interface en configuración. Nos iremos al Serial0, que recordemos que es el puerto donde está conectado nuestra sede central.

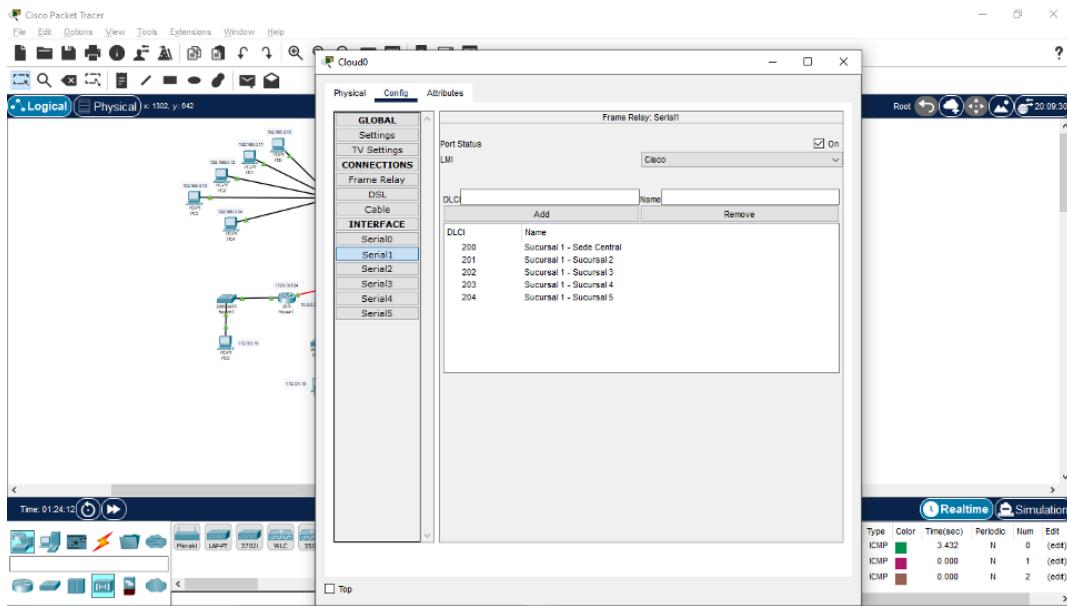


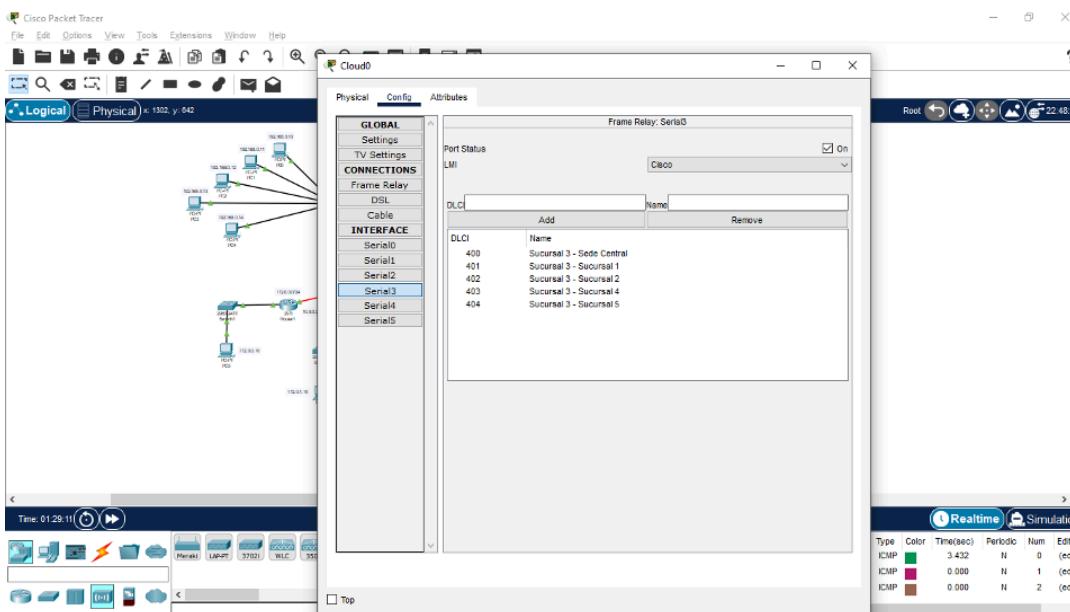
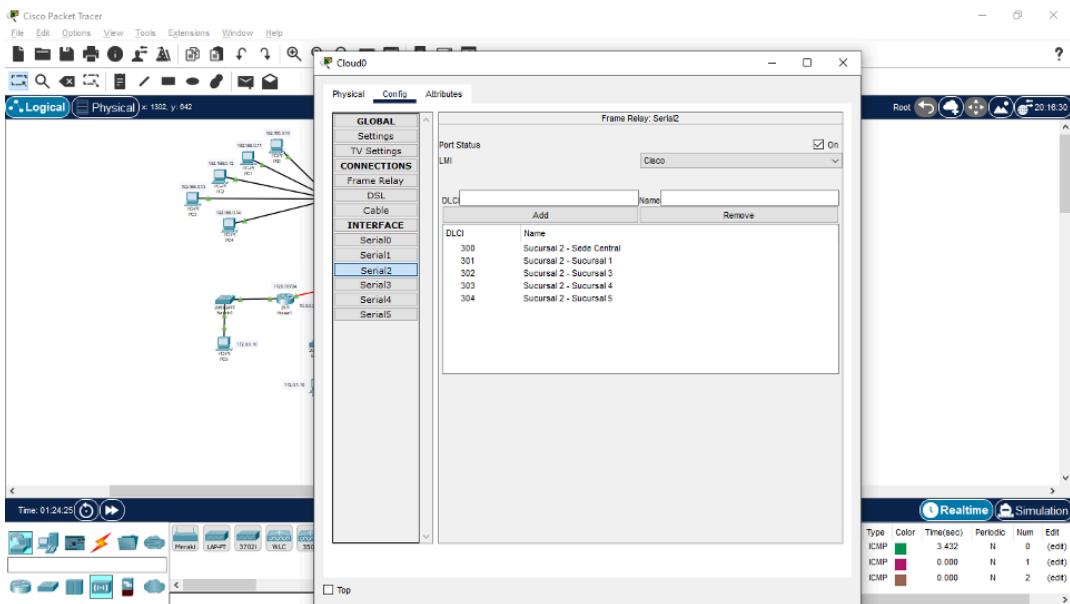
Aquí lo que realizaremos es que en el campo DLCI (el Identificador de Conexión de Datos-Link), pondremos nuestra clave personalizada junto al nombre. En este caso lo decidimos nombrar de la siguiente manera:

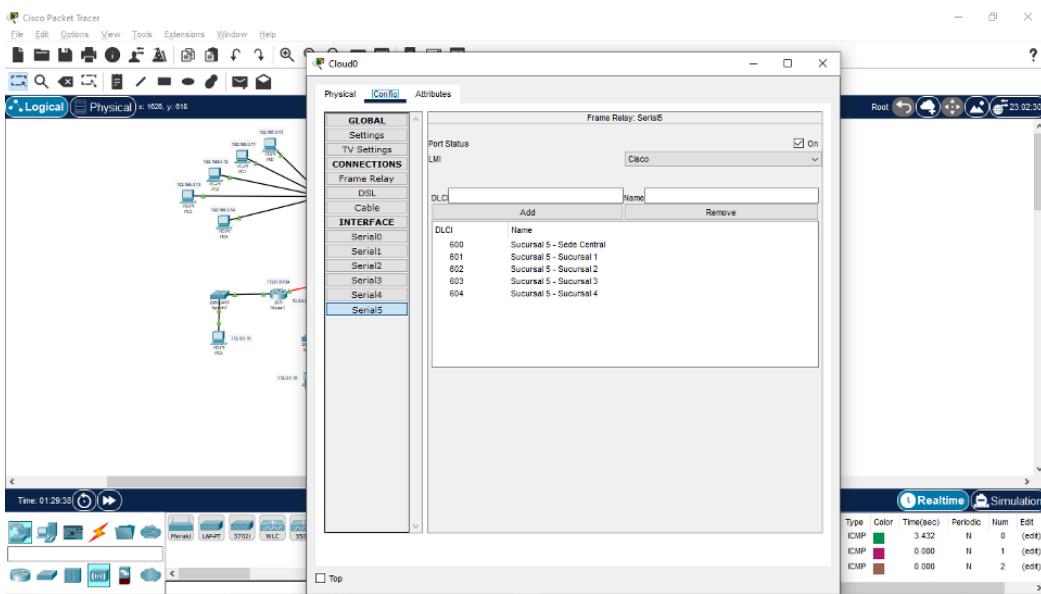
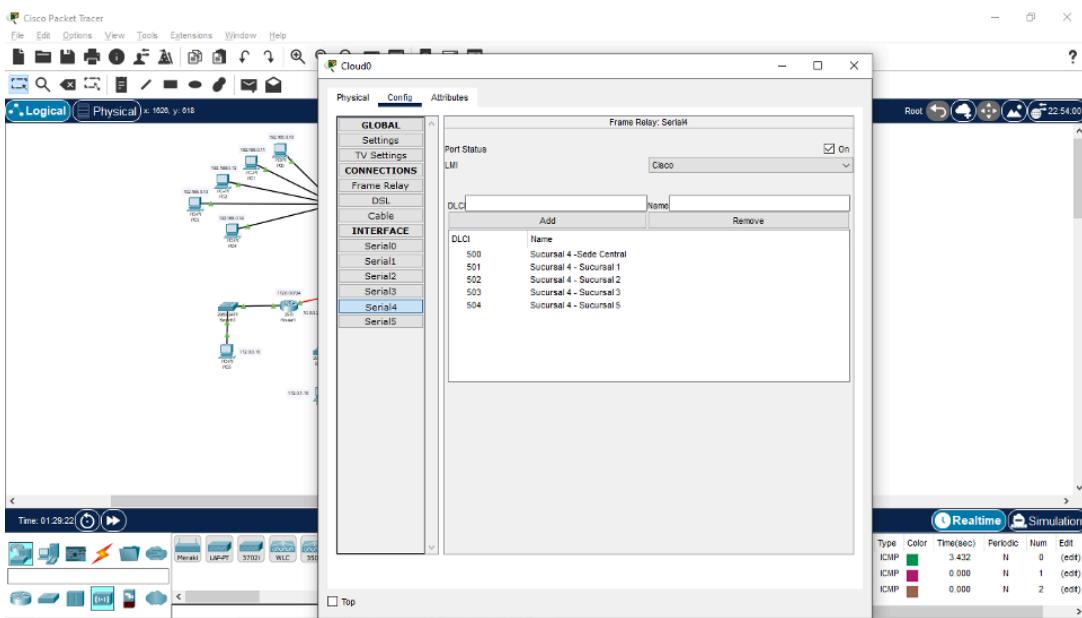
- **100 Sede Central - Sucursal 1:** la cual demuestra la conexión de la sede a la sucursal 1
- **101 Sede Central - Sucursal 2:** la cual demuestra conexión de la sede a la sucursal 2
- **102 Sede Central - Sucursal 3:** la cual demuestra conexión de la sede a la sucursal 3

- **103 Sede Central - Sucursal 4:** la cual demuestra conexión de la sede a la sucursal 4
- **104 Sede Central - Sucursal 5:** la cual demuestra conexión de la sede a la sucursal 5

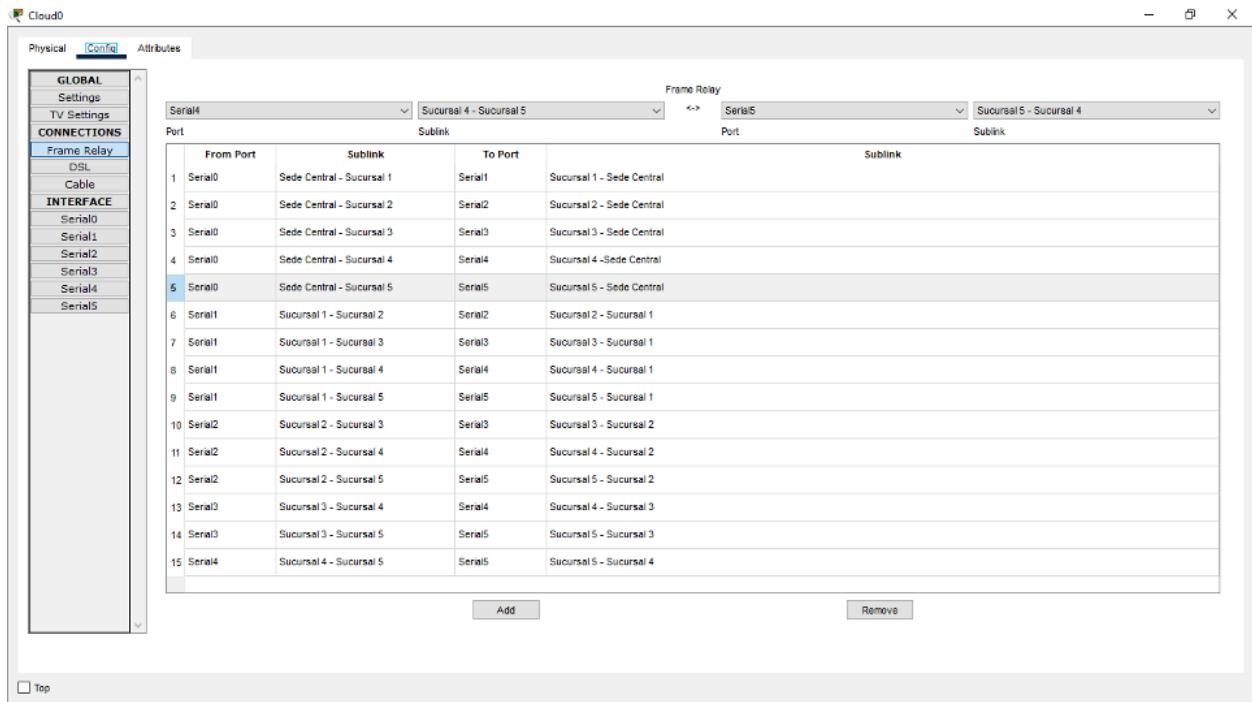
Este proceso, sin embargo, lo tenemos que realizar para cada una de las conexiones—veremos más adelante el porqué. Por lo tanto, nos iremos a cada módulo Serial subsecuente y agregaremos, con la misma nomenclatura, las DLCI que necesitamos.



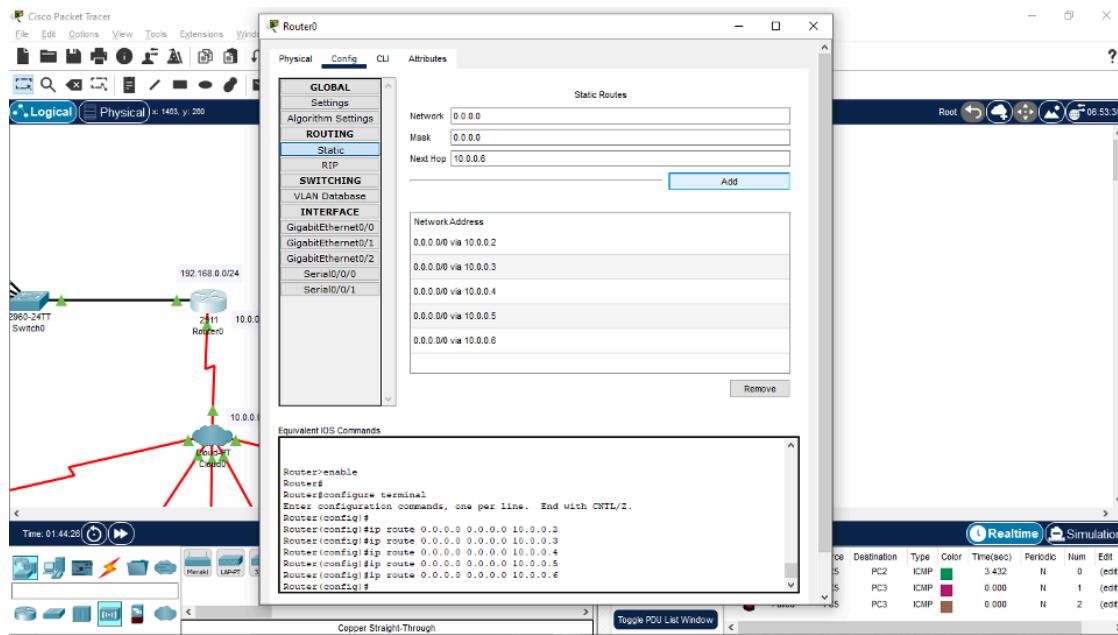




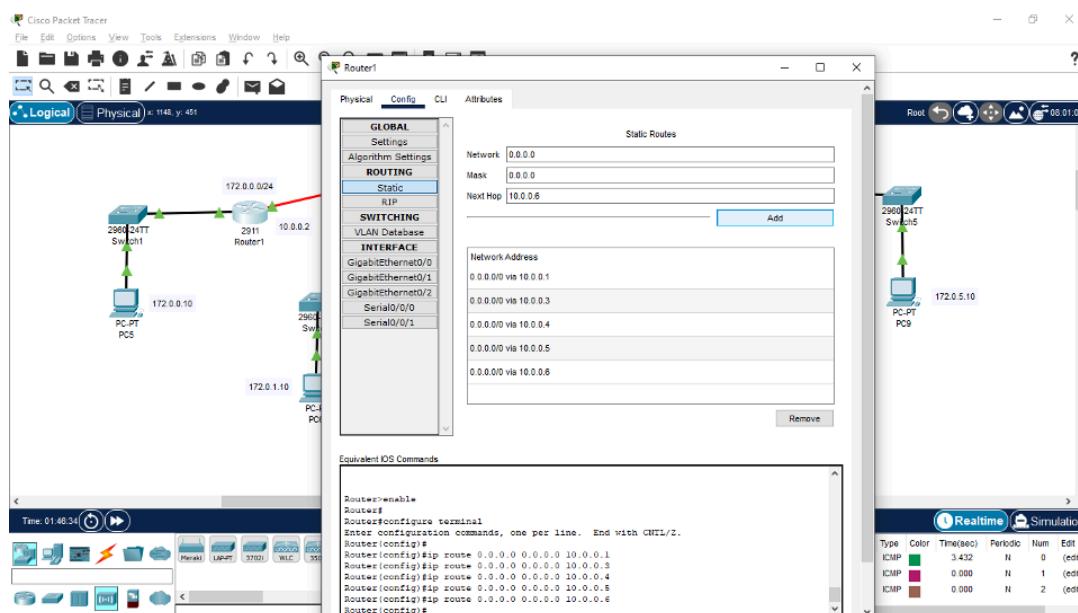
Para ir finalizando, nos iremos a la parte de Connections, donde dice Frame Relay, y pondremos todas las conexiones únicas que existen en nuestra infraestructura. Si bien se sabe, el frame relay es un protocolo que nos permite conectar las redes LAN y las redes WAN. Dicho de otra manera, estamos habilitando que las sucursal 1 se pueda comunicar tanto dentro de ella—una laptop 172.0.0.13 a una PC 172.0.0.10—, como a cualquier otra sucursal.



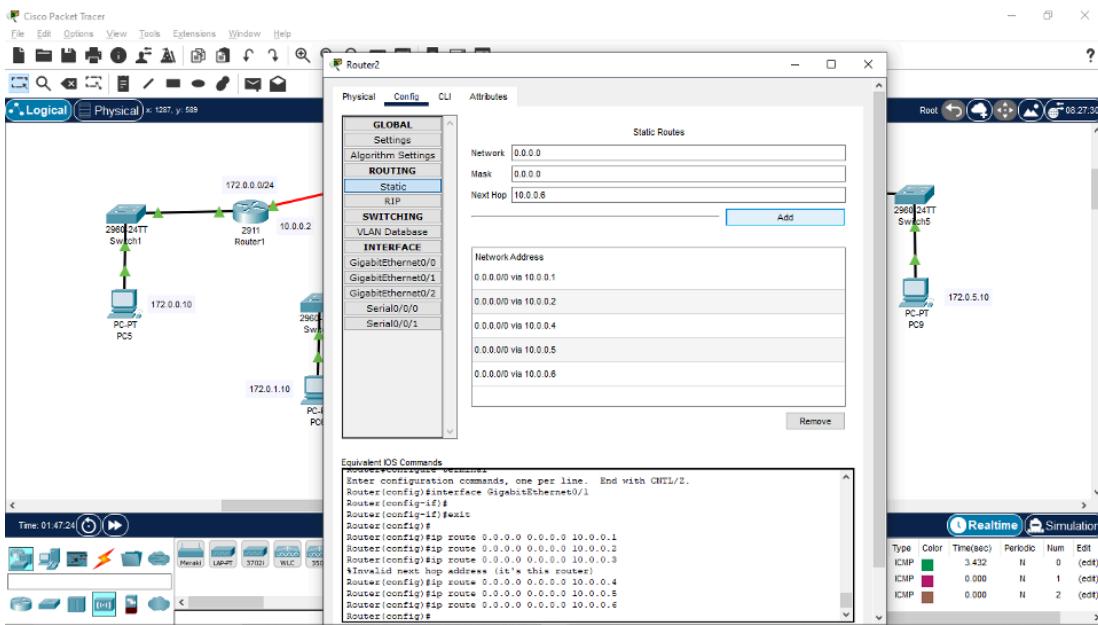
Después de añadirlas a través de esta ventana, observamos que las 15 conexiones únicas están listas para ser implementadas. Sólo nos quedan unos cuantos pasos más. Primero, debemos movernos ahora a cada uno de los routers; empecemos por el de la central. Al abrirlos, en Config, nos iremos a la parte de Routing, y en Static colocaremos la Network como **0.0.0.0**, Mask como **0.0.0.0**, y en Next Hop iremos poniendo **10.0.0.2** (la cual es la conexión a la sucursal 1), y así subsecuentemente hasta llegar a la **10.0.0.6** (la cual es la conexión a la sucursal 5).



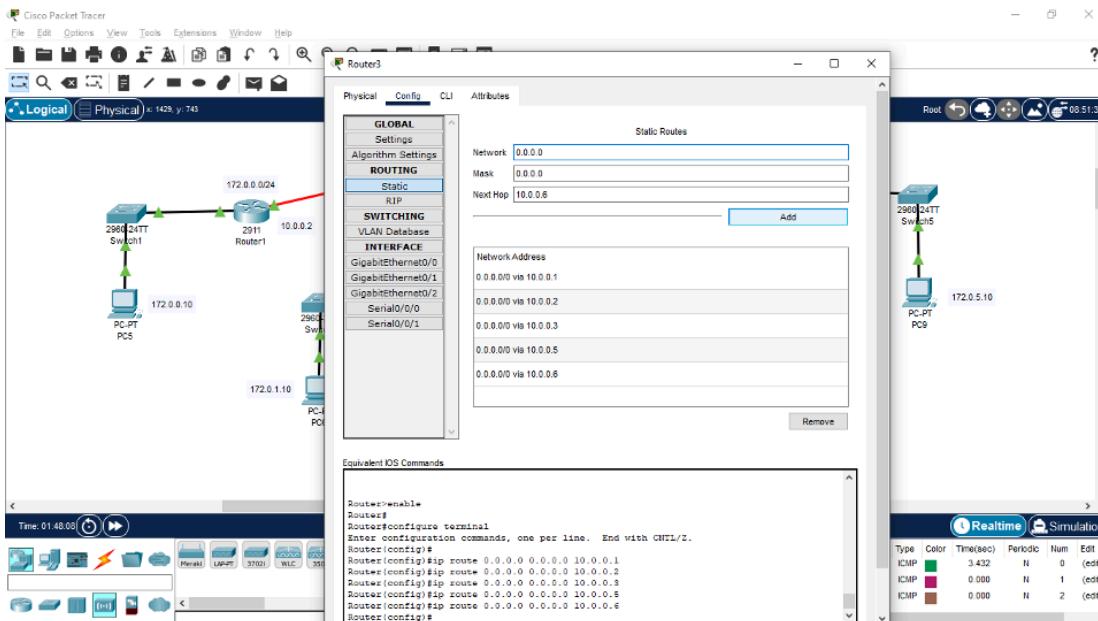
Debemos continuar con los demás routers, por lo que el de la primera sucursal tendrá casi las mismas configuraciones que la de la sede central, con una excepción. Empezaríamos con Next Hop **10.0.0.1** (la dirección de la sede) y no pondríamos la **10.0.0.2**, ya que ésta es la misma dirección de la sucursal 1, y es en ésta donde nos encontramos. Por lo que nuestras direcciones se verían de la siguiente manera, del **0.1** al **0.6**, omitiendo el **0.2**.



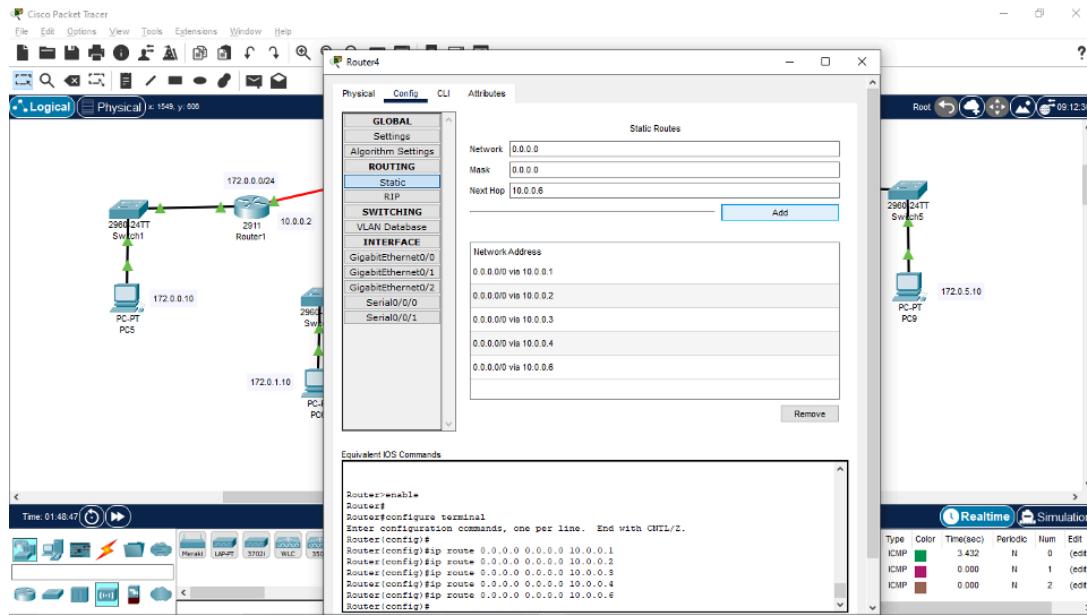
Continuaríamos así con cada router, omitiendo su respectiva terminación.



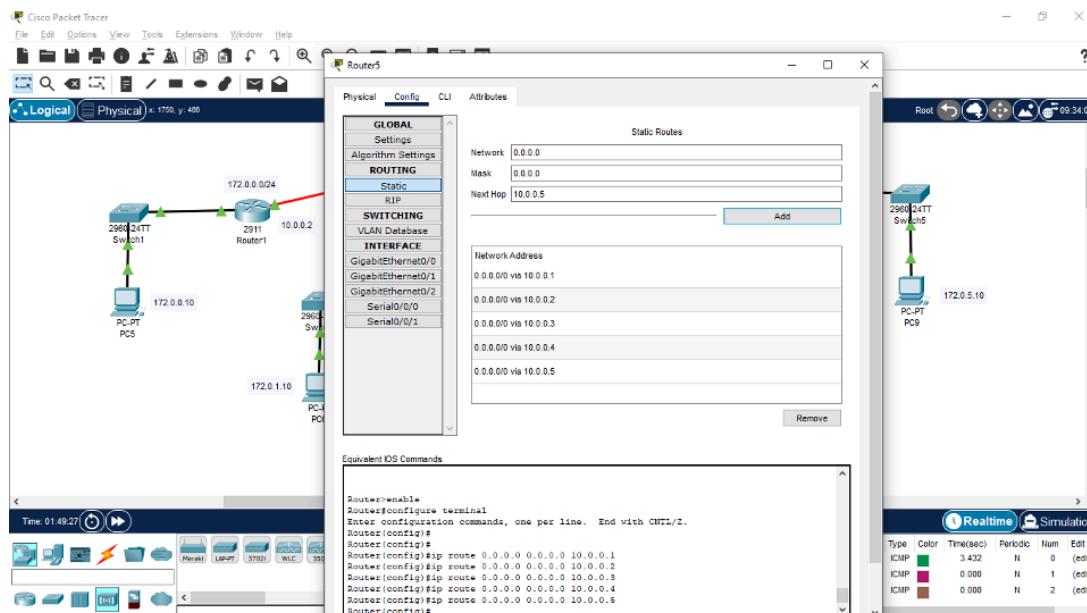
### Omitimos el 0.3 (sucursal 2)



### Omitimos el 0.4 (sucursal 3)

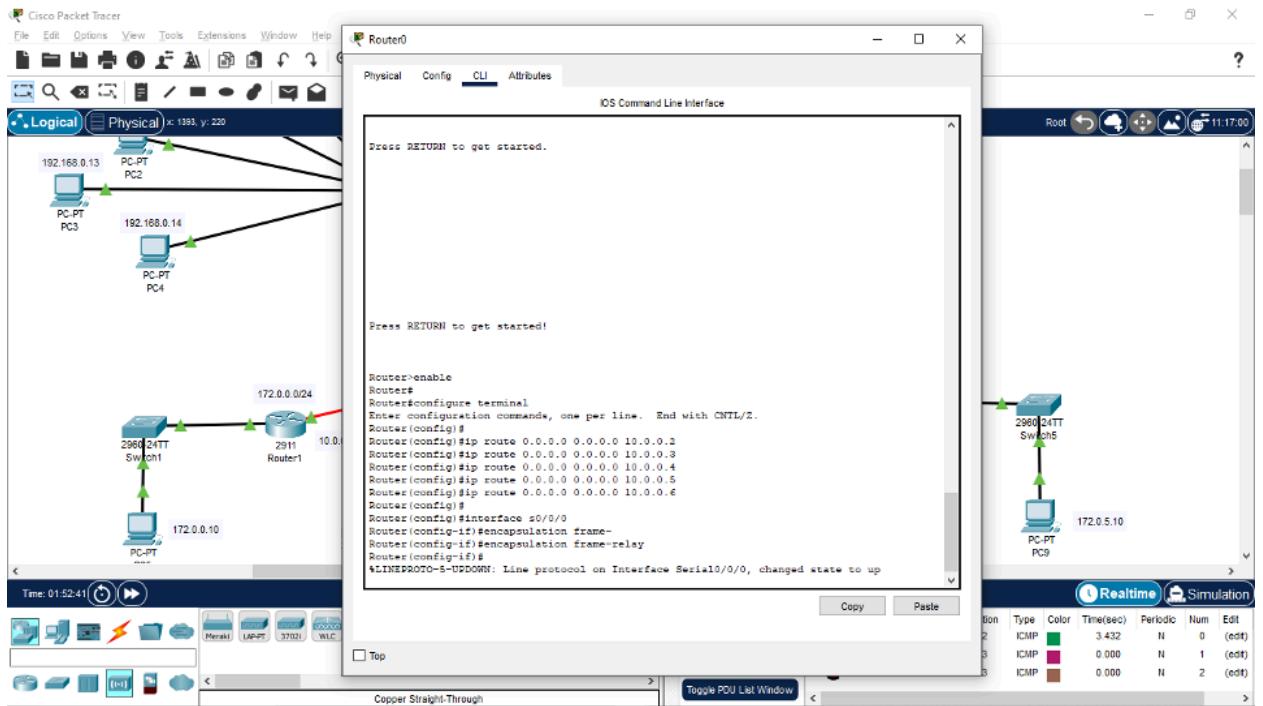


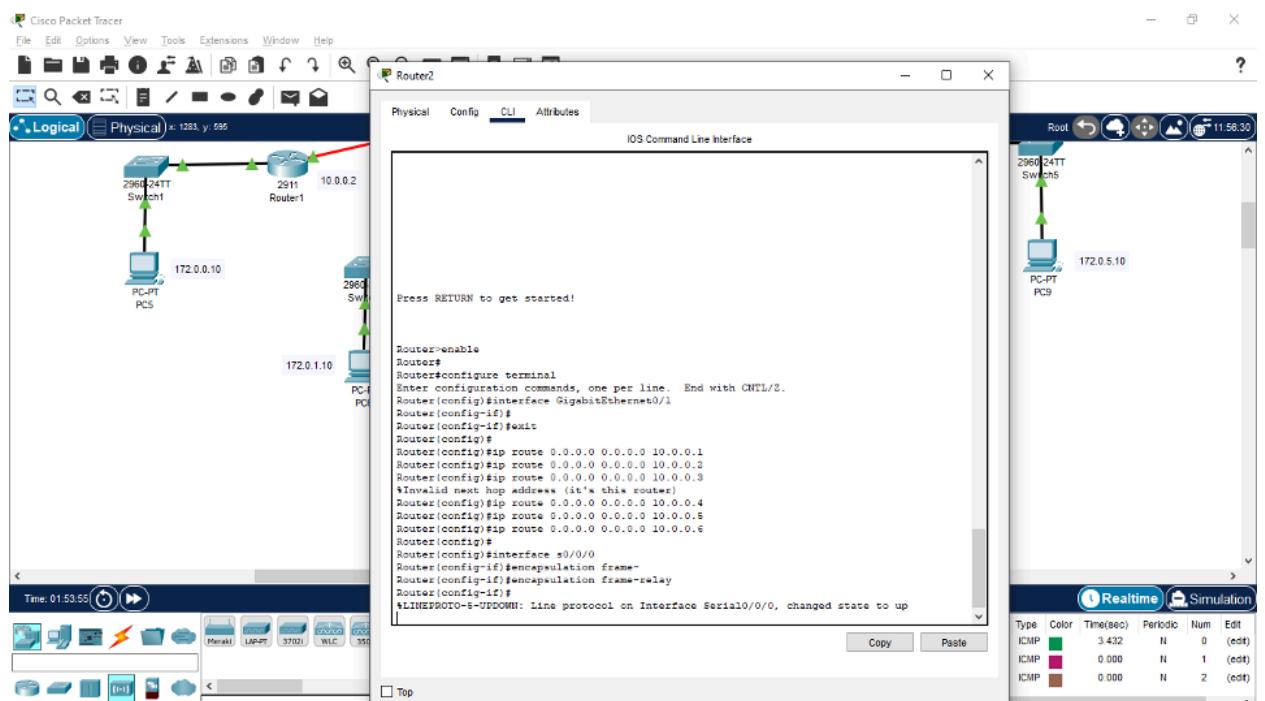
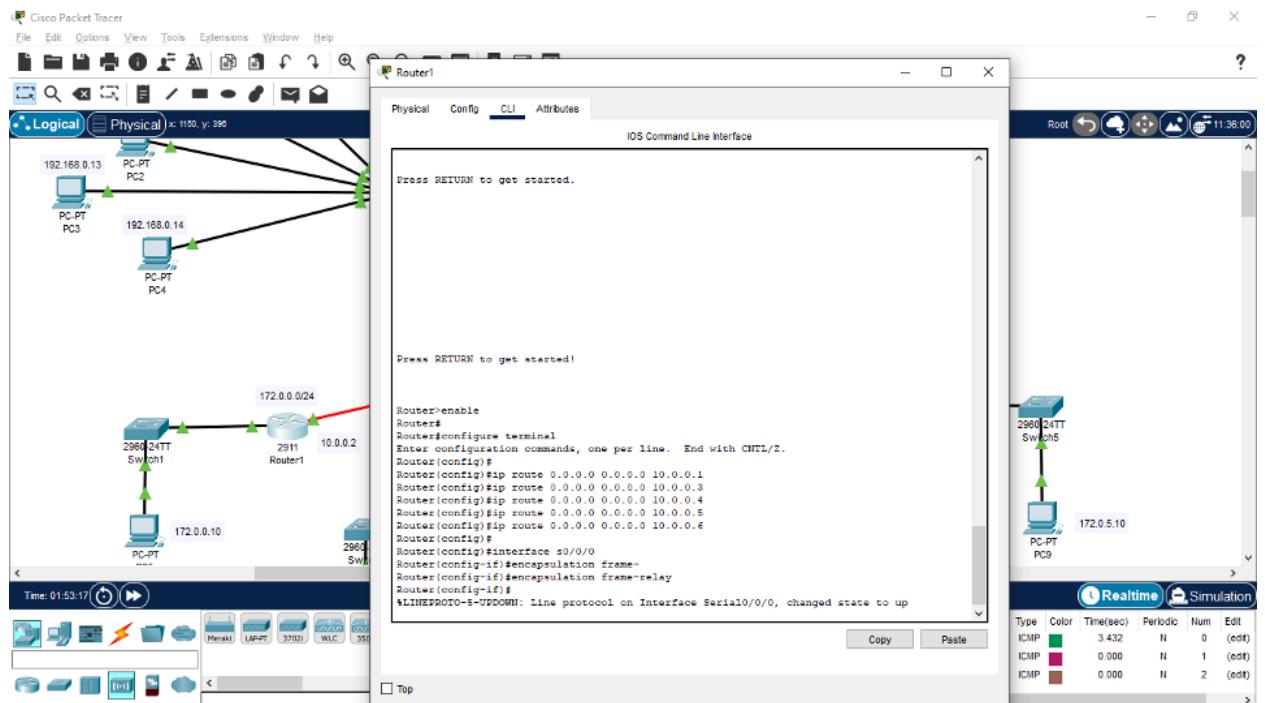
### Omitimos el 0.5 (sucursal 4)

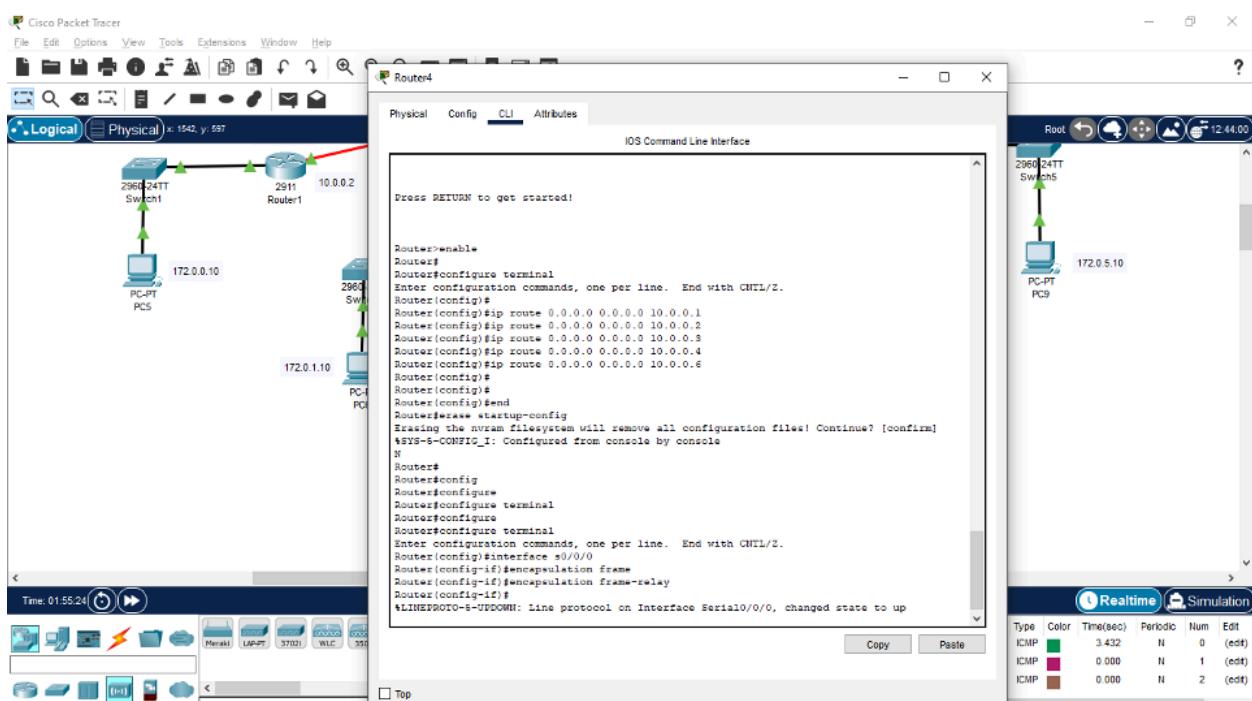
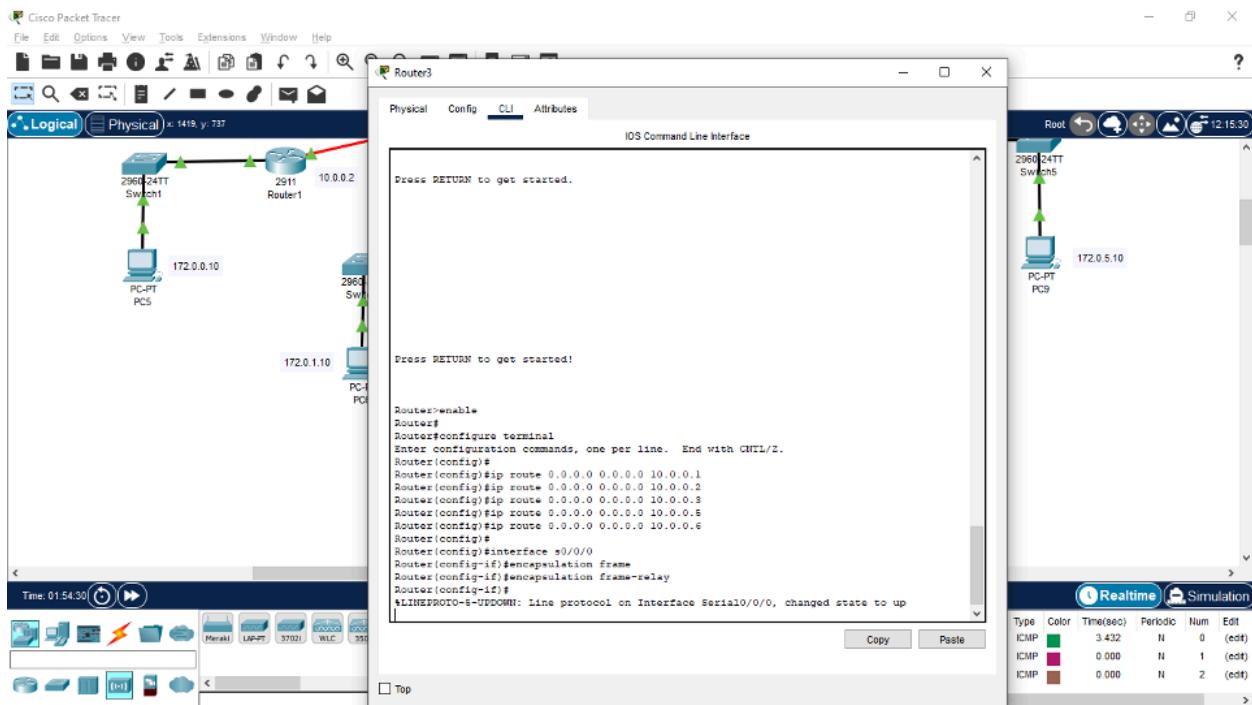


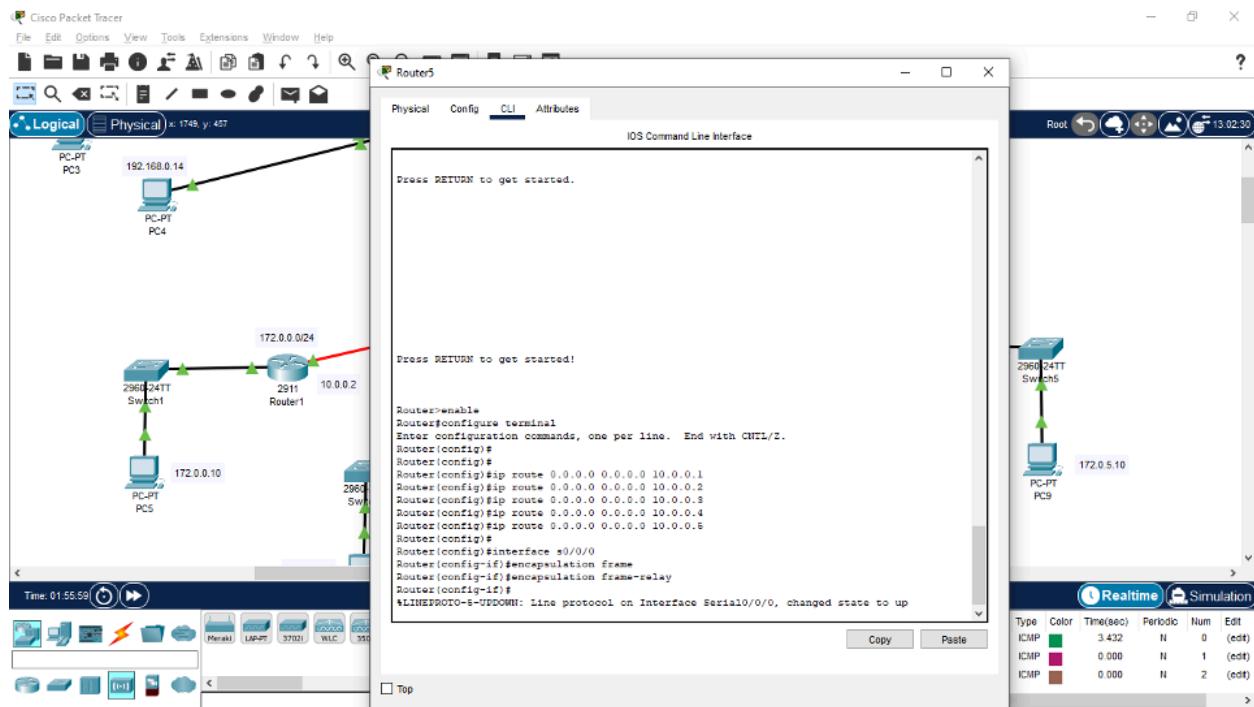
### Omitimos el 0.6 (sucursal 5)

Nuevamente, nos vamos a cada router y en este caso, abrimos su respectivo CLI, en donde pondremos **interface s0/0/0**, para conectarnos a los módulos de la nube. Después encapsulation frame-relay para habilitarlo y que ya, finalmente, pueda existir la comunicación intra e intersucursales.







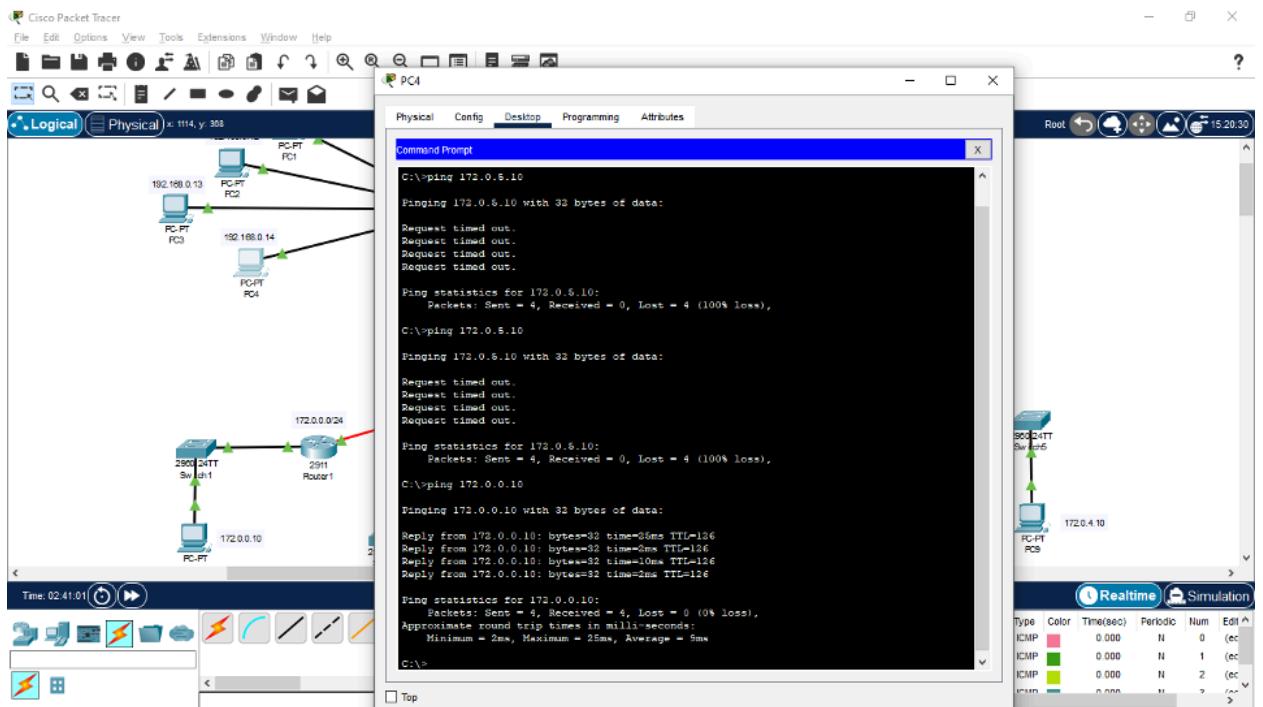


## Pruebas

En esta sección se podrán observar cómo las conexiones, tras hacer las configuraciones antes mencionadas, son exitosas y cómo comprobarlas.

### A través de ping

Para probar si tenemos una conexión exitosa, podemos abrir cualquier dispositivo final—en este caso la PC4 de la sede central—, dirigirnos a Desktop y en Command Prompt escribir **ping** seguido de la dirección IP del dispositivo de destino.



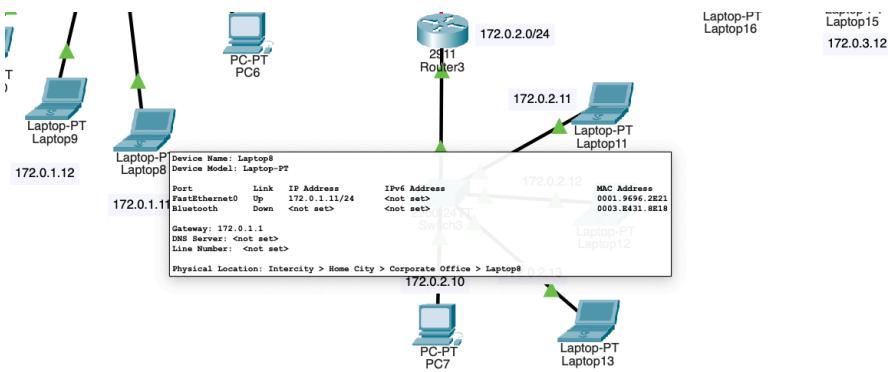
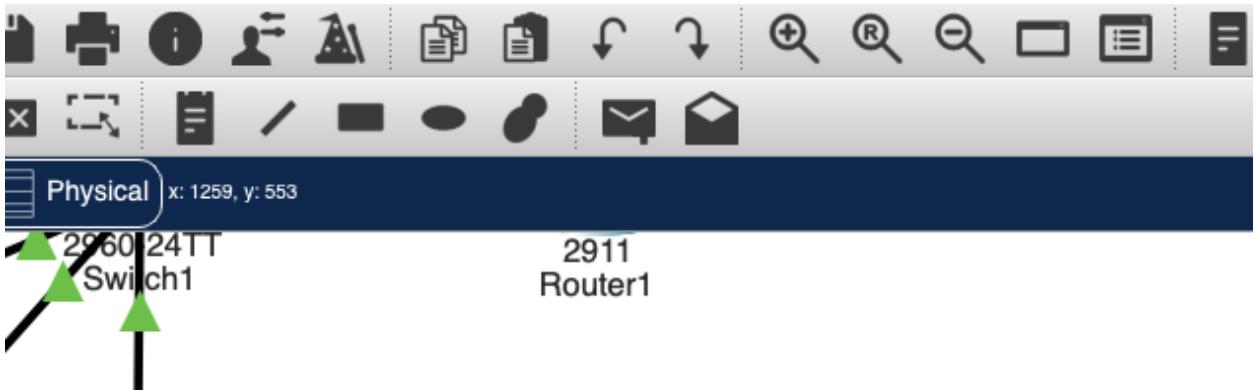
En la imagen de arriba se puede observar cómo al hacer **ping 172.0.5.10** (sucursal 5) desde la PC4 (sede central) dos veces, obtuvimos un **Request timed out**. Lo que significa que no hubo comunicación, pero en la tercera ocasión decidimos hacer un **ping 172.0.0.10** (sucursal 1), vemos cómo nos muestra un **Reply from** y la ping de destino, lo que significa que hubo una comunicación exitosa.

**Nota:** se hizo un ejemplo de **Request timed out** para observar cómo es que una comunicación **no** es exitosa. Las configuraciones están bien hechas en el archivo final.

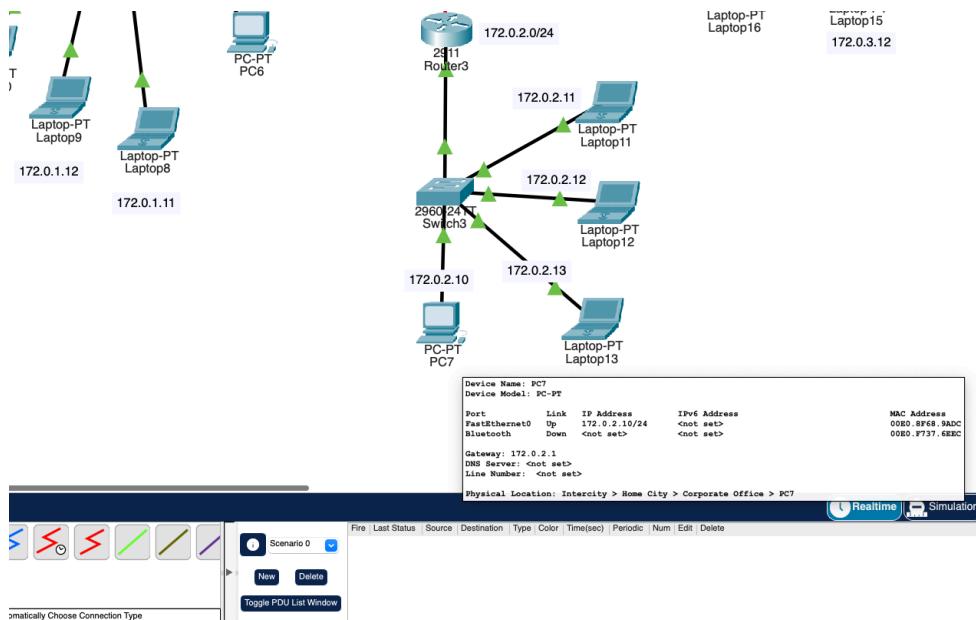
## A través de PDU's

Para lo siguiente, en Cisco, debemos darle clic al sobre cerrado de arriba y seleccionar primero el dispositivo de origen, y luego el dispositivo de destino. Este sobre representa el

envío de paquetes entre dispositivos, y para demostrar la comunicación existente enviamos un paquete de una Laptop de la sucursal 2 a una PC de la sucursal 3.



**Dispositivo origen (Laptop8 - Sucursal 2)**



### Dispositivo destino (PC7 - Sucursal 3)

Obtendremos un Successful, lo cual indica que nuestra comunicación es exitosa. y podemos ver en **Source** y **Destination** los distintos dispositivos a los que se intentó conectar y como todos estos fueron exitosos. Por lo tanto, nuestra infraestructura no sólo es escalable y segura, sino que también funcional y adaptable.

| Fire       | Last Status | Source   | Destination | Type |
|------------|-------------|----------|-------------|------|
| Successful | Laptop8     | PC7      | ICMP        |      |
| Successful | Laptop10    | PC7      | ICMP        |      |
| Successful | PC6         | Laptop13 | ICMP        |      |

## Glosario de Términos y Condiciones

- **DHCP (Dynamic Host Configuration Protocol):** Protocolo de red que asigna automáticamente direcciones IP, puerta de enlace y otros parámetros a los dispositivos de una red, facilitando la configuración y administración sin intervención manual.
- **ISP (Internet Service Provider):** Empresa que ofrece servicios de conexión a Internet, junto con otros servicios como alojamiento web, correo electrónico y telefonía IP, permitiendo que los usuarios accedan y naveguen en la web.
- **IP (Internet Protocol):** Protocolo fundamental para la comunicación en redes, que identifica y direcciona dispositivos mediante direcciones IP únicas, permitiendo el envío y recepción de datos a través de Internet o redes privadas.
- **PNS (Private Network Service):** Servicio que proporciona una conexión segura entre redes privadas, permitiendo la comunicación entre sucursales o dispositivos sin exponer los datos a redes públicas como Internet.
- **MPLS (Multiprotocol Label Switching) / FRAME RELAY:** Tecnologías de telecomunicaciones usadas para la transmisión eficiente de datos en redes. **Frame Relay** es un método antiguo basado en conmutación de paquetes, mientras que MPLS es una tecnología más avanzada que mejora la velocidad y calidad del tráfico en redes empresariales al usar etiquetas para enrutar los datos de manera más eficiente.

## Bibliografía

Barrera, C. (2024, 25 junio). Balanceo de carga de internet: qué es y cómo funciona. *axessnet*.

Recuperado 23 de febrero de 2025, de

<https://axessnet.com/el-balanceo-de-carga-de-red/>

colaboradores de Wikipedia. (2023, 18 octubre). *Virtual router Redundancy Protocol*. Wikipedia,

la Enciclopedia Libre. Recuperado 23 de febrero de 2025, de

[https://es.wikipedia.org/wiki/Virtual\\_Router\\_Redundancy\\_Protocol](https://es.wikipedia.org/wiki/Virtual_Router_Redundancy_Protocol)

*Comprender las funciones y la funcionalidad del HoT Standby Router Protocol*. (2023, 14

septiembre). Cisco. Recuperado 23 de febrero de 2025, de

[https://www.cisco.com/c/es\\_mx/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html](https://www.cisco.com/c/es_mx/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html)

De TechTarget, C. (2021, 16 julio). *Failover o conmutación por error*. ComputerWeekly.es.

Recuperado 23 de febrero de 2025, de

<https://www.computerweekly.com/es/definicion/Failover-o-conmutacion-por-error>

International Business Machines [IBM]. (2021, 17 agosto). *¿Qué es la instancia?* SSPS

Modeler Subscription. Recuperado 23 de febrero de 2025, de

<https://www.ibm.com/docs/es/spss-modeler/saas?topic=node-what-is-instantiation>

Jupamea, A. (2023, 25 enero). *¿Qué es la redundancia y cuál es su importancia?* ENI

Networks. Recuperado 23 de febrero de 2025, de

<https://www.eninetworks.com/que-es-la-redundancia-y-cual-es-su-importancia/>

*¿Qué es una instancia en la computación en la nube? - Explicación de instancias en la nube - AWS.* (s. f.). Amazon Web Services, Inc. Recuperado 23 de febrero de 2025, de

<https://aws.amazon.com/es/what-is/cloud-instances/>

¿Qué son las redes definidas por software (SDN)? (2025, 9 enero). *IBM*. Recuperado 23 de febrero de 2025, de <https://www.ibm.com/mx-es/topics/sdn>

*Speakable content*. (2023, 26 julio). Powernet. Recuperado 23 de febrero de 2025, de <https://www.powernet.es/blog/redundancia-o-conexion-redundante-que-es-y-por-que-es-importante-en-el-sector-it>

Ti, C. (2019, 18 junio). ¿Qué hacer para una red más confiable? - Canales TI 2025. *Canales TI*. Recuperado 23 de febrero de 2025, de

<https://itcomunicacion.com.mx/que-hacer-para-una-red-mas-confiable/>

Zscaler. (s. f.). ¿Qué es la segmentación de red? - Definición y casos prácticos | Zscaler. En *Zscaler*. Recuperado 23 de febrero de 2025, de

<https://www.zscaler.com/es/resources/security-terms-glossary/what-is-network-segmentation>

## Autores



Carlos Adrián del Olmo Cantú



Lars Ewert Morales



Mauricio Gonzalez Gonzalez



Adrián Alonso Jair Morales Márquez



Miguel Omar Muñoz Solis



Jorge Daniel Zapata Oyervides

## Conclusiones

**Mauricio:**

Con este proyecto logramos diseñar y simular una infraestructura de red que cubre las necesidades de TecmiCorp y su crecimiento. A lo largo del proceso, nos dimos cuenta de lo importante que es planificar bien, asegurar la estabilidad y optimizar los recursos para que la red funcione de manera eficiente.

Este trabajo nos dejó claro que una buena infraestructura no solo resuelve los problemas actuales, sino que también debe estar preparada para lo que venga en el futuro. Además, nos permitió aplicar conocimientos clave y entender mejor cómo funciona una red dentro de una empresa.

**Lars Ewert Morales:**

En mi experiencia personal, este proyecto me enseñó la importancia de la organización y de lo impresionante y eficiente que es una empresa bien diseñada como la de nosotros, tener diferentes servidores, routers, módems y dispositivos y poder visualizarlos de forma ordenada me dio una nueva perspectiva en cuanto a organización y configuración.

Definitivamente me gusto mucho trabajar con mis compañeros en este gran proyecto y disfruté mucho aprender todo sobre Cisco Packet Tracer y las maravillas de las redes.

**Carlos del Olmo:**

Siendo honesto, debo admitir que no fuí el principal encargo de la construcción de la red en Cisco Packet Tracer, pero a pesar de eso, pienso que fue una experiencia muy interesante el aprender muy a profundidad durante no solo esta actividad, pero durante todo el curso de

Gestión de Redes sobre cómo funcionan las redes de internet, y la cantidad de detalles que vienen al tener que hacer algo tan simple como abrir un sitio web.

Personalmente, no creo que este ámbito de ingeniería de desarrollo software sea algo que me interese, pero a pesar de eso, el descubrir todo sobre cómo funcionan las redes, como las IPs son repetidas en muchos lugares, como hay una diferencia entre “privadas” y “públicas”, como se crean las subredes mediante la segmentación, entre otros datos, se me hizo muy interesante para mí, y ahora tengo una admiración por la gente que se encarga de cuidar que las redes funcionen.

**Jorge Zapata:**

Durante la realización del proyecto aprendí lo realmente importante que es tener conocimientos de redes en la industria, ya que su correcta implementación son fundamentales para sacar adelante redes empresariales.

Temas tan amplios como la asignación de ipv4, ipv6 y submáscaras de red en los dispositivos, tipos de comunicaciones(blueooth, wireless, por cableado etc...), protocolos de red, diferencias entre ips públicas y privadas, manejo de CLIs junto con el uso de sus comandos básicos, hasta conocimientos amplios en ciberseguridad para salvaguardar la información de nuestros dispositivos en la red. Todo estos conocimientos fueron gracias en parte a la plataforma cisco packet tracer que me dio la oportunidad de simular de manera muy precisa el poder crear y configurar redes con una amplia variedad de dispositivos para probar.

En lo personal no me veo siendo un profesional en esta rama de la ingeniería, pero sin duda sé que durante mi estancia profesional como desarrollador de software voy a aplicar todo lo enseñado en este certificado para mejorar la calidad de mi trabajo.

**Jair Morales:**

Gracias a la plataforma de Cisco Packet Tracer fue que profundicé en cómo las redes funcionan. Ya había estado metiéndome un poco en el tema debido a que poseemos en mi hogar personal una serie de dispositivos en malla, de thread, e inteligentes, entonces tuve que realizar mi mini investigación para cada uno de estos dispositivos.

Al inicio, cuando empezamos, me parecía frustrante todo lo que se tenía que configurar para simular una conexión de la vida real, como cuando me conecto desde mi laptop al Wi-Fi. Sin embargo, esto mismo me ha hecho apreciar la facilidad de los dispositivos modernos, y cómo nos ayudan a no realizar estas tareas que, más que tediosas, pueden terminar siendo contraproducentes para nuestra privacidad en línea.

En sí, me agració mucho la forma en que usamos, actividad tras actividad, el Cisco Packet Tracer. A pesar de sus limitaciones y tardanza, considero que es una buena manera de introducirse al tema de gestión de redes.

**Miguel Muñoz:**

Este proyecto me fue de mucha ayuda para tener un primer acercamiento a lo que es ser un consultor de red y de cómo se desarrolla una red empresarial desde cero utilizando protocolos y tecnologías diferentes a los vistos en clase. Verdaderamente abrió mi panorama de lo que son las redes, y he de decir que me gusto mucho trabajar con redes, diseñarlas y probarlas, haciéndome considerar especializarme más en este campo de la tecnología.

Fue un reto desarrollar nuestra topología, sin embargo no puedo negar que fue un reto que disfruté mucho el poder solucionar en conjunto con mi equipo de trabajo quienes me ayudaron de manera clave a lo largo de este proyecto.

## Agradecimientos

Agradecemos a la Universidad Tecmilenio, quien nos brindó las herramientas y recursos necesarios para poder llevar a cabo el desarrollo de este proyecto. Además de agradecer el apoyo de los ingenieros Pamela Sandoval, Gilberto Lopez y Omar Muñoz por el apoyo que nos brindaron al resolver nuestras dudas de nuestra red, al igual que el de brindarnos mas contexto de cómo se diseña una red en el mundo profesional, lo que nos permitió que nuestra arquitectura fuera coherente y lo más cercano a la realidad.