



Universidad Nacional Autónoma de México
Facultad de Ingeniería



Carrera: Ingeniería en Computación

Curso: Redes de datos seguras

Proyecto final

Profesor: M.C. MARIA JAQUELINA LOPEZ BARRIENTOS

Alumno:

Crisantos Martínez Diego Jair

327029264

Fecha de entrega: 23-04-2023

Semestre: 2023-2

Contenido

Introducción	3
Análisis y diseño	4
Desarrollo	6
a) Haga las consideraciones necesarias a fin de determinar el número de nodos a instalar en cada piso del edificio. Explique y justifique las necesidades identificadas.	6
b) Especifique cuántos de esos nodos se utilizarán para la instalación de equipos WiFi, porqué es necesaria su consideración, en dónde serán instalados, con qué tipo de antena, alcance, cobertura y número de usuarios.	7
c) Determine el segmento de red privado a utilizar y realice el esquema de direccionamiento VLSM, identificando para cada subred: IP de segmento de red, IP de broadcast, rango de IPs útiles, máscara de subred.	8
d) Realice la elección de los dispositivos de interconexión y los medios de transmisión, justificando en todo momento la elección realizada.	10
e) Implemente seguridad en los routers configurando las contraseñas de acceso: acceso al modo privilegiado, consola, VTY, y coloque nombre a cada dispositivo y el mensaje del día.	12
f) Configure las interfaces de los dispositivos con los parámetros de red y al menos una computadora de cada Subred con los parámetros de red correspondientes.	14
g) La red organizacional de la empresa debe contar con:	17
a. Servidor de correo: configure una cuenta de correo de manera que se pueda establecer la comunicación mediante este servicio entre todos los usuarios.	17
b. Servidor DHCP: configure el servidor a fin de que todos los hosts cuenten con este servicio.	18
c. Servidor web y servidor DNS: el servidor web debe presentar la página de la empresa con el nombre que usted elija y dentro de ésta su nombre propio completo.	20
h) Argumentar la importancia del uso de normas y estándares. Mencionando de manera puntual cada una de las normas y de los estándares involucrados en el proyecto para la habilitación de la infraestructura, la configuración de la red y su seguridad.	22
i) Estimar el costo del proyecto y presentar un análisis costo-beneficio del mismo.	24
j) REALICE UNA INVESTIGACIÓN DEL IMPACTO AMBIENTAL QUE SE GENERA POR LA INFRAESTRUCTURA TECNOLÓGICA QUE IMPLICA LA INSTALACIÓN DE UNA RED DE DATOS.	31
Conclusiones	33
Diagrama de Gantt	34
Bibliografía:	34

Introducción

En la era digital actual, las redes de comunicación desempeñan un papel crucial en la interconexión de dispositivos y el intercambio eficiente de información. El desarrollo y la simulación de una red son fundamentales para comprender su funcionamiento, optimizar su rendimiento y garantizar su fiabilidad. Este proyecto tiene como objetivo crear y simular una red con el propósito de explorar y analizar sus capacidades, así como su impacto en la comunicación y la eficiencia operativa.

En este proyecto, nos sumergimos en el emocionante mundo de la creación y simulación de redes, utilizando herramientas y tecnologías avanzadas. Nuestro enfoque se centra en diseñar una red que cumpla con los requisitos específicos y que sea capaz de gestionar las demandas de comunicación de manera efectiva.

La simulación de la red nos permite evaluar y analizar su rendimiento en diferentes escenarios y cargas de trabajo. Exploraremos aspectos como la latencia, el ancho de banda, la capacidad de conmutación y la tolerancia a fallos. Al realizar estas simulaciones, obtendremos una visión más clara de cómo se comporta la red en situaciones reales y podremos identificar áreas de mejora y optimización.

Además, este proyecto nos permitirá comprender el impacto de la red en otros aspectos, como la seguridad de la información y la protección de datos. Analizaremos las vulnerabilidades potenciales y las medidas de seguridad necesarias para proteger la red y los dispositivos conectados.

A través de esta investigación y simulación, esperamos obtener conocimientos valiosos sobre el diseño, implementación y gestión de redes eficientes y confiables. Estos hallazgos nos permitirán tomar decisiones informadas para mejorar la infraestructura de red existente y explorar soluciones innovadoras para abordar los desafíos futuros.

Objetivos

1. Determinar el número de nodos a instalar en cada piso del edificio, considerando las necesidades específicas de comunicación y conectividad en cada área.
2. Especificar la cantidad de nodos que se utilizarán para la instalación de equipos WiFi, justificando la necesidad de su consideración, determinando su ubicación, tipo de antena, alcance, cobertura y número de usuarios atendidos.
3. Definir el segmento de red privado a utilizar y realizar el esquema de direccionamiento VLSM, identificando para cada subred la dirección IP de segmento de red, dirección IP de broadcast, rango de direcciones IP útiles y máscara de subred correspondiente.

4. Seleccionar los dispositivos de interconexión y los medios de transmisión adecuados, justificando la elección realizada en función de los requerimientos de la red y la infraestructura existente.
5. Configurar la seguridad en los routers mediante la implementación de contraseñas de acceso para el modo privilegiado, consola y VTY, además de asignar nombres a cada dispositivo y configurar el mensaje del día.
6. Configurar las interfaces de los dispositivos de red con los parámetros de red correspondientes, incluyendo al menos una computadora de cada subred con su respectiva configuración de red.
7. Establecer los servicios esenciales de la red organizacional, como un servidor de correo electrónico, servidor DHCP, servidor web y servidor DNS, con configuraciones adecuadas y personalizadas según las necesidades de la empresa.
8. Argumentar la importancia del uso de normas y estándares en el proyecto, identificando de manera puntual las normas y estándares involucrados en la habilitación de la infraestructura, configuración de red y seguridad.
9. Estimar el costo del proyecto y realizar un análisis costo-beneficio que evalúe los beneficios obtenidos frente a los costos de implementación y mantenimiento de la red.
10. Realizar una investigación exhaustiva sobre el impacto ambiental generado por la infraestructura tecnológica relacionada con la instalación de una red de datos, identificando los posibles efectos negativos y proponiendo medidas de mitigación y buenas prácticas ambientales.

Estos objetivos guiarán el desarrollo del proyecto, permitiendo abordar aspectos clave relacionados con el diseño, implementación y gestión de la red, así como la consideración del impacto ambiental y la aplicación de normas y estándares relevantes.

Análisis y diseño

En primer lugar, se requiere llevar a cabo el diseño de la red de acuerdo con los planos de la infraestructura proporcionados. Es importante considerar las necesidades de los usuarios, en este caso, los miembros de la empresa. Además, se debe tener en cuenta la implementación de estándares de cableado estructurado para garantizar una comunicación eficiente y segura. Esta tarea se puede realizar mediante software de creación de diagramas o mediante la impresión física de los planos y su posterior escaneo, se recomienda el uso de un software para facilitar la modificación de estos en caso de que se requieran cambios.

A continuación, antes de realizar cualquier simulación, resulta crucial diseñar las subredes que estarán presentes en la empresa. Esto permitirá obtener una visión

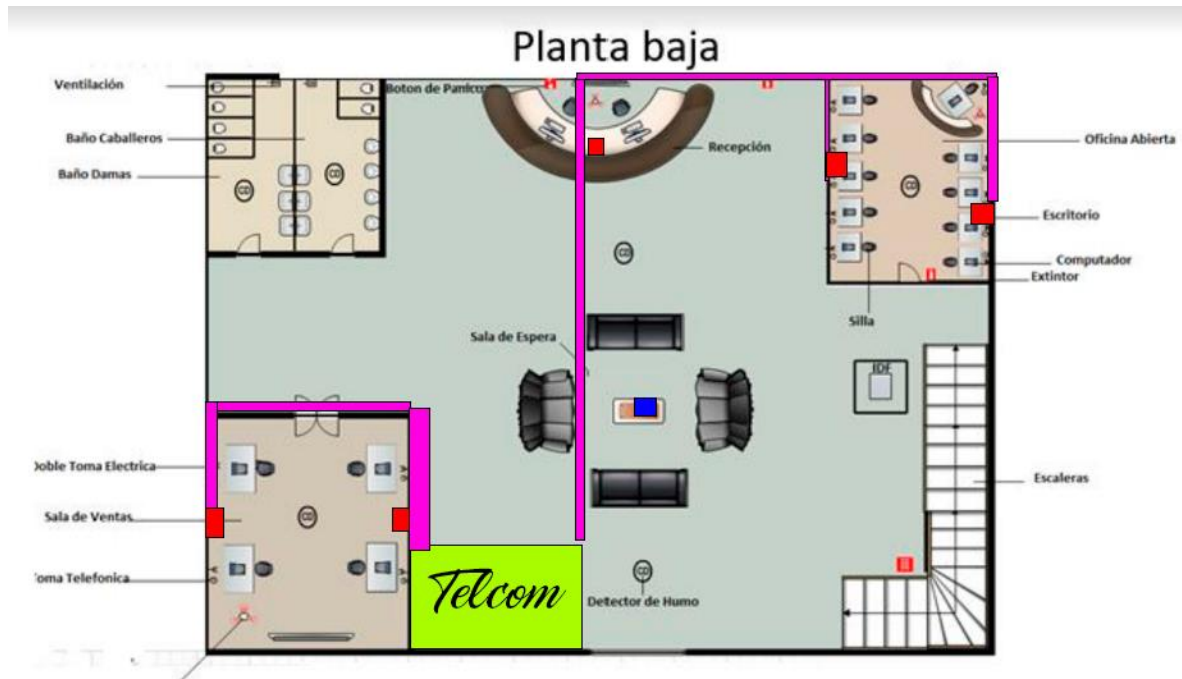
detallada de los usuarios en cada sección y los dispositivos que se utilizarán. Se recomienda utilizar la técnica de VLSM como se vio en clase ya que esta nos permite realizar mas subredes y desperdiciar menos host , ya sea calculando manualmente las direcciones o utilizando herramientas en línea.

Para llevar a cabo la siguiente etapa, es necesario adquirir conocimientos sobre el funcionamiento del software Cisco Packet Tracer. Esto permitirá simular la red, los servicios disponibles en la empresa, así como configuraciones de seguridad y funcionamiento de los dispositivos involucrados. Para facilitar el aprendizaje de este software, se sugiere consultar vídeos disponibles en la plataforma de YouTube y descargar la versión gratuita desde el sitio oficial de Cisco.

Finalmente, para asegurar que el trabajo realizado cumple con los estándares y normas pertinentes, es esencial realizar un análisis exhaustivo de las etapas del desarrollo en las que se aplicaron. Asimismo, es necesario tener en cuenta el costo del proyecto, incluyendo los materiales y equipos a utilizar, así como el consumo de energía. Esto permitirá llevar a cabo una investigación sobre el impacto ambiental asociado con la infraestructura implementada. Se recomienda utilizar software de hojas de cálculo, como Excel, y consultar fuentes confiables para realizar esta tarea.

Desarrollo

- a) Haga las consideraciones necesarias a fin de determinar el número de nodos a instalar en cada piso del edificio. Explique y justifique las necesidades identificadas.



Dentro de la planta, una de las ubicaciones más importantes es el cuarto de telecomunicaciones, el cual se encuentra adyacente a la parte izquierda. Esta elección se debe a que, según el diagrama, no es factible ubicarlo en la parte derecha debido a la presencia de escaleras, y tampoco en la parte izquierda debido a la presencia de los baños.

En relación a la canalización, se ha marcado de color rosa y se ha asegurado de no pasar cerca de los baños, con el objetivo de evitar que la humedad pueda afectarla de alguna manera.

En cuanto a nuestra oficina abierta, se ha identificado la necesidad de conectar un total de 10 equipos. Para esto, se utilizarán rosetas tanto en un extremo como en el lado opuesto, tal como se indica en la imagen y están marcadas en color rojo.

En el caso de la sala de ventas, se requerirá la conexión de 4 equipos. Para lograr esto, se utilizarán dos rosetas, una ubicada en el lado derecho y otra en el lado izquierdo.

Por último, en la zona de recepción, se prevé la conexión de 2 equipos. Para esto, se utilizará únicamente una roseta, lo cual será suficiente para llevar a cabo dicha

conexión.



En los demás pisos, se pueden observar diferentes áreas donde se requerirá conectividad:

En el cuarto de diseño gráfico, se utilizará un total de 8 hosts, los cuales se distribuirán en 2 rosetas: una ubicada en la parte superior y otra en la parte inferior del cuarto.

En el área de la gerencia, se necesitarán 3 conexiones que se realizarán mediante nodos ubicados en la parte superior.

En la zona de recepción, únicamente se requerirá una conexión para un equipo, por lo que solo se dejará esa conexión en dicho lugar.

En la sala de juntas, se prevé contar con 10 conexiones por medio de cable. Para ello, se instalarán 2 rosetas que permitirán realizar las conexiones necesarias.

Esas son las distribuciones de conexiones y rosetas propuestas para cada área en la segunda planta.

b) Especifique cuántos de esos nodos se utilizarán para la instalación de equipos WiFi, porque es necesaria su consideración, en dónde serán instalados, con qué tipo de antena, alcance, cobertura y número de usuarios.

En la planta baja, se prevé contar con un único nodo de conexión WiFi que estará ubicado en la sala de espera. Este nodo permitirá el acceso a la red, pero con ciertas limitaciones para evitar que cualquier persona pueda acceder completamente a la

red privada de la empresa. Se han reservado un total de 30 conexiones para este nodo.

En los demás pisos, se instalará un nodo de conexión WiFi en la sala de juntas, lo cual permitirá que varias personas puedan conectar sus dispositivos, especialmente dispositivos móviles, durante las reuniones. Se han asignado un total de 20 conexiones para este nodo.

Además, se instalará otro nodo de conexión WiFi en la área de gerencia, considerando la presencia de un proyector en esa ubicación. Esto permitirá utilizar de manera eficiente el proyector y facilitar la conexión de dispositivos relacionados con el Internet de las cosas. Se han destinado 15 conexiones para este nodo.



Finalmente, para la conexión en el jardín, se optará únicamente por una conexión WiFi. Se han destinado un total de 30 conexiones para esta área. El nodo de conexión WiFi se ubicará en la parte media inferior del jardín, con el objetivo de garantizar que la conexión se extienda de manera efectiva y cubra la mayor parte de este espacio. De esta manera, se busca proporcionar conectividad inalámbrica para que los usuarios puedan acceder a la red en el jardín de forma cómoda y conveniente.

Estas son las distribuciones de los nodos de conexión WiFi y el número de conexiones asignadas para cada área.

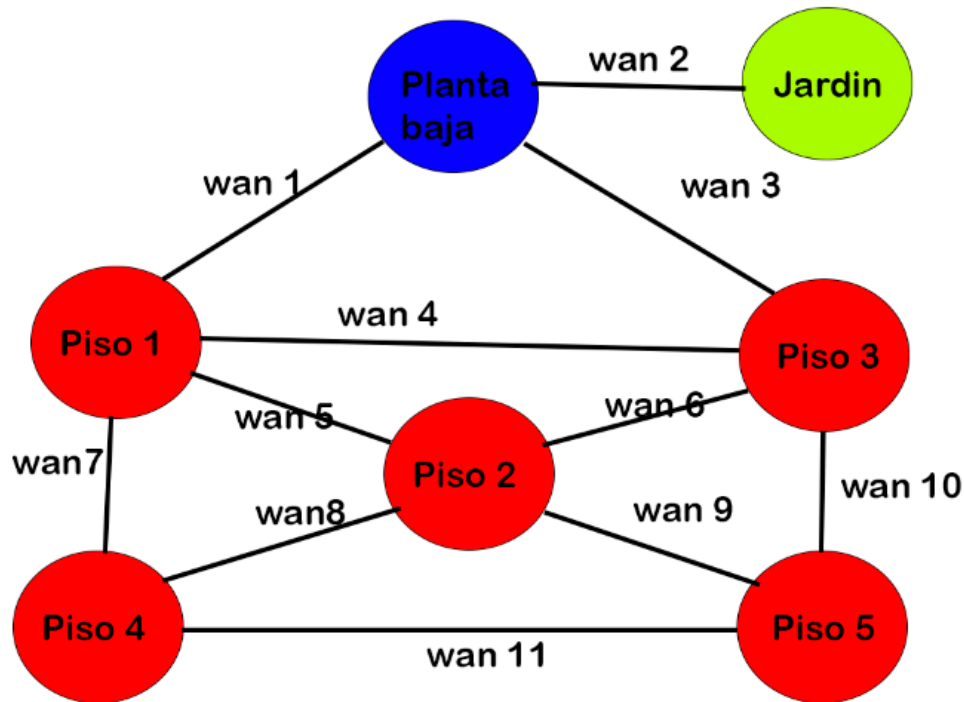
- c) Determine el segmento de red privado a utilizar y realice el esquema de direccionamiento VLSM, identificando para cada subred: IP de segmento de red, IP de broadcast, rango de IPs útiles, máscara de subred.

Una vez realizado el análisis anterior, podemos proceder a calcular la cantidad de subredes que se crearán y el número de hosts en cada una. La distribución quedaría de la siguiente forma:

180.180.0.0

Subred	Segmento	Mascara	Rango	Broadcast
Planta baja 46 host	180.180.0.0/26	255.255.255.192	180.180.0.1- 180.180.0.62	180.180.0.63
Piso 1 57 host	180.180.0.64/26	255.255.255.192	180.180.0.65- 180.180.0.126	180.180.0.127
Piso 2 57 host	180.180.0.128/26	255.255.255.192	180.180.0.129- 180.180.0.190	180.180.0.191
Piso 3 57 host	180.180.0.192/26	255.255.255.192	180.180.0.193- 180.180.0.254	180.180.0.255
Piso 4 57 host	180.180.1.0/26	255.255.255.192	180.180.1.1- 180.180.1.62	180.180.1.63
Piso 5 57 host	180.180.1.64/26	255.255.255.192	180.180.1.65- 180.180.1.126	180.180.1.127
Jardín 30 host	180.180.1.128/27	255.255.255.224	180.180.1.129- 180.180.1.158	180.180.1.159
Wan 1 2 host	180.180.1.160/30	255.255.255.252	180.180.1.161- 180.180.1.162	180.180.1.163
Wan 2 2 host	180.180.1.164/30	255.255.255.252	180.180.1.165- 180.180.1.166	180.180.1.167
Wan 3 2 host	180.180.1.168/30	255.255.255.252	180.180.1.169- 180.180.1.170	180.180.1.171
Wan 4 2 host	180.180.1.172/30	255.255.255.252	180.180.1.173- 180.180.1.174	180.180.1.175
Wan 5 2 host	180.180.1.176/30	255.255.255.252	180.180.1.177- 180.180.1.178	180.180.1.179
Wan 6 2 host	180.180.1.180/30	255.255.255.252	180.180.1.181- 180.180.1.182	180.180.1.183
Wan 7 2 host	180.180.1.184/30	255.255.255.252	180.180.1.185- 180.180.1.186	180.180.1.187
Wan 8 2 host	180.180.1.188/30	255.255.255.252	180.180.1.189- 180.180.1.190	180.180.1.191
Wan 9 2 host	180.180.1.192/30	255.255.255.252	180.180.1.193- 180.180.1.194	180.180.1.195
Wan 10 2 host	180.180.1.196/30	255.255.255.252	180.180.1.197- 180.180.1.198	180.180.1.199
Wan 11 2 host	180.180.1.200/30	255.255.255.252	180.180.1.201- 180.180.1.202	180.180.1.203

- d) Realice la elección de los dispositivos de interconexión y los medios de transmisión, justificando en todo momento la elección realizada.



Como podemos ver, para poder establecer la conexión en el edificio, se ha optado por utilizar una topología de tipo malla. Esta elección se debe a la necesidad de garantizar la continuidad de la red incluso en caso de que alguna de las WAN (Wide Area Network) presente alguna falla. De esta manera, se asegura que la conexión entre todos los pisos se mantenga activa mientras se resuelve cualquier problema que pueda surgir.

En cuanto a los elementos presentes en cada piso, se han considerado los siguientes:

- **Switch:** Los switches desempeñan un papel fundamental en la red, ya que se encargan de la distribución eficiente de los datos entre los diferentes dispositivos conectados. Permiten la interconexión de múltiples equipos en cada piso y garantizan una comunicación fluida y segura.
- **Router:** Los routers son dispositivos esenciales para la conectividad en una red. Su función principal consiste en dirigir el tráfico de datos entre diferentes redes, asegurando que los paquetes de información lleguen a su destino de manera eficiente. En cada piso, los routers desempeñarán un papel clave en la comunicación entre las subredes y en la interconexión con la WAN.

- Access point: El access point se encarga de establecer una red WiFi en el área de cobertura, brindando a los usuarios la capacidad de acceder a los recursos y servicios de la red de manera inalámbrica. Esto permite una mayor flexibilidad y movilidad, ya que los usuarios pueden conectarse y utilizar la red desde cualquier lugar dentro del alcance del access point.
- Equipo final: En cada piso, se encuentran los equipos finales, que pueden ser computadoras u otros dispositivos capaces de conectarse a una red. Estos dispositivos son los puntos de acceso y uso de la red por parte de los usuarios. A través de ellos, se accede a los recursos y servicios disponibles en la red, permitiendo la comunicación, el intercambio de datos y el acceso a información relevante.

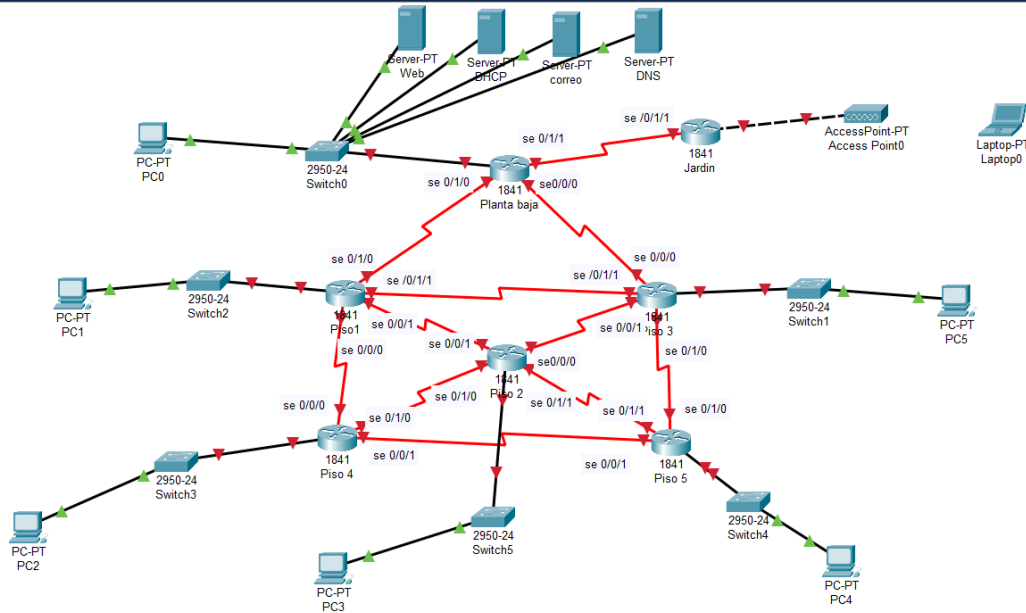
En resumen, la infraestructura de cada piso incluye switches para la distribución de datos, routers para dirigir el tráfico entre redes y equipos finales que actúan como puntos de acceso y uso de la red por parte de los usuarios. Esta combinación de elementos permite establecer una red sólida y eficiente en cada nivel del edificio.

Por otro lado, en el cuarto de telecomunicaciones ubicado en la planta inferior, además de los dispositivos previamente mencionados, encontramos una variedad de elementos esenciales que cumplen funciones específicas para administrar la red. Estos elementos adicionales incluyen:

- Servidor de correo: El servidor de correo despliega un papel fundamental en el manejo y distribución eficiente de los correos electrónicos en la red. Permite gestionar y almacenar los mensajes de correo electrónico, así como asegurar su entrega y recepción de manera segura y confiable.
- Servidor DHCP: El servidor DHCP (Dynamic Host Configuration Protocol) se encarga de asignar y administrar las direcciones IP automáticamente a los dispositivos que se conectan a la red. Proporciona una configuración dinámica de red, lo que simplifica y agiliza la administración de la asignación de direcciones IP en el entorno.
- Servidor web: El servidor web es responsable de alojar y entregar páginas web y otros contenidos a los clientes que solicitan acceso a través de internet. Permite que los usuarios accedan a aplicaciones web, sitios web y servicios disponibles en la red de forma segura y eficiente.
- Servidor DNS: El servidor DNS (Domain Name System) desempeña un papel clave en la resolución de nombres de dominio a direcciones IP correspondientes. Proporciona la capacidad de traducir nombres de dominio legibles para los humanos en direcciones IP numéricas, permitiendo así la navegación y comunicación efectiva en la red.

Estos elementos adicionales presentes en el cuarto de telecomunicaciones, como el servidor de correo, servidor DHCP, servidor web y servidor DNS, se encargan de mejorar y optimizar la administración de la red, brindando servicios esenciales que

En consecuencia, la configuración de la conexión en el entorno de Cisco debería quedar estructurada de la manera siguiente:



Para implementar seguridad en los routers configurando las contraseñas de acceso y asignando nombres a cada dispositivo y mensaje del día, sigue estos pasos:

1. **Accede al router:** Conéctate al router a través de una conexión de consola o mediante una conexión de red utilizando un software de administración de redes como PuTTY o Tera Term.
2. **Acceso al modo privilegiado:** Configura una contraseña para acceder al modo privilegiado (también conocido como modo EXEC). Esto te permitirá realizar cambios de configuración más avanzados en el router. Ingresa al modo de configuración global escribiendo el siguiente comando:

```
Router>enable
Router#
```

Luego, ingresa el siguiente comando para establecer una contraseña para el modo privilegiado:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable secret baja
Router(config)#
```

3. Acceso a la consola: Configura una contraseña para acceder a la consola del router. Esto proporcionará una capa adicional de seguridad para el acceso físico al dispositivo. Utiliza el siguiente comando para acceder a la configuración de la línea de consola:

```
Router(config)#line console 0
Router(config-line)#password baja
Router(config-line)#login
Router(config-line)#
```

4. Acceso VTY (Virtual Teletype): Configura una contraseña para el acceso remoto al router a través de VTY, que se utiliza para conexiones Telnet o SSH. Utiliza los siguientes comandos para acceder a la configuración de las líneas VTY:

```
Router(config-line)#line vty 0 4
Router(config-line)#password baja
Router(config-line)#login
Router(config-line)#
```

5. Asignar nombre a cada dispositivo y mensaje del día: Puedes asignar un nombre a cada dispositivo y configurar un mensaje del día que se mostrará al acceder al router. Utiliza los siguientes comandos para realizar estas configuraciones:

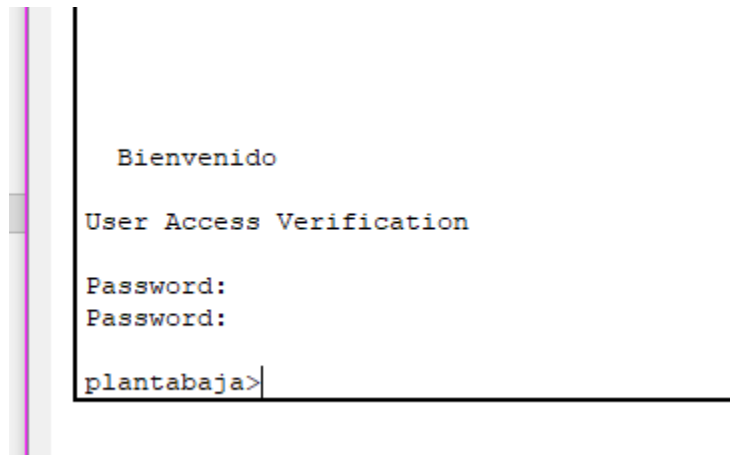
```
Router(config-line)#hostname plantabaja
plantabaja(config)#banner motd #  Bienvenido #
plantabaja(config)#
```

6. Guardar la configuración: Finalmente, asegúrate de guardar la configuración realizada en la memoria del router para que persista después de reinicios. Utiliza el siguiente comando:

```
plantabaja(config)#end
plantabaja#
%SYS-5-CONFIG_I: Configured from console by console

plantabaja#write memory
Building configuration...
[OK]
plantabaja#
```

7. Por ultimo ingresamos al router para verificar que este solicita la contraseña y muestra el mensaje bienvenido:



El mismo procedimiento se llevó a cabo en cada uno de los otros 6 routers, por lo tanto, aquí se presentan las contraseñas correspondientes:

Router	Contraseña
Planta baja	baja
Piso 1	piso1
Piso 2	piso2
Piso 3	piso3
Piso 4	piso4
Piso 5	piso5
Jardín	jardin

- f) Configure las interfaces de los dispositivos con los parámetros de red y al menos una computadora de cada Subred con los parámetros de red correspondientes.

Para comenzar la configuración de cada router, se debe establecer la conexión FastEthernet, la cual nos permitirá determinar a qué subred pertenece cada router. El proceso de configuración se realiza de la siguiente manera:

```

plantabaja>enable
Password:
plantabaja#confi
plantabaja#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
plantabaja(config)# interface ethernet 0/0
%Invalid interface type and number
plantabaja(config)# interface ethernet0/0
%Invalid interface type and number
plantabaja(config)# interface fastethernet0/0
plantabaja(config-if)#ip address 180.180.0.1 255.255.255.192
plantabaja(config-if)#no shutdown

plantabaja(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
exit
plantabaja(config)#exit
plantabaja#
%SYS-5-CONFIG_I: Configured from console by console

plantabaja#

```

Donde una vez realizado lo podemos confirmar si nos vamos a la configuración del router y verificamos la ip address que este contiene:

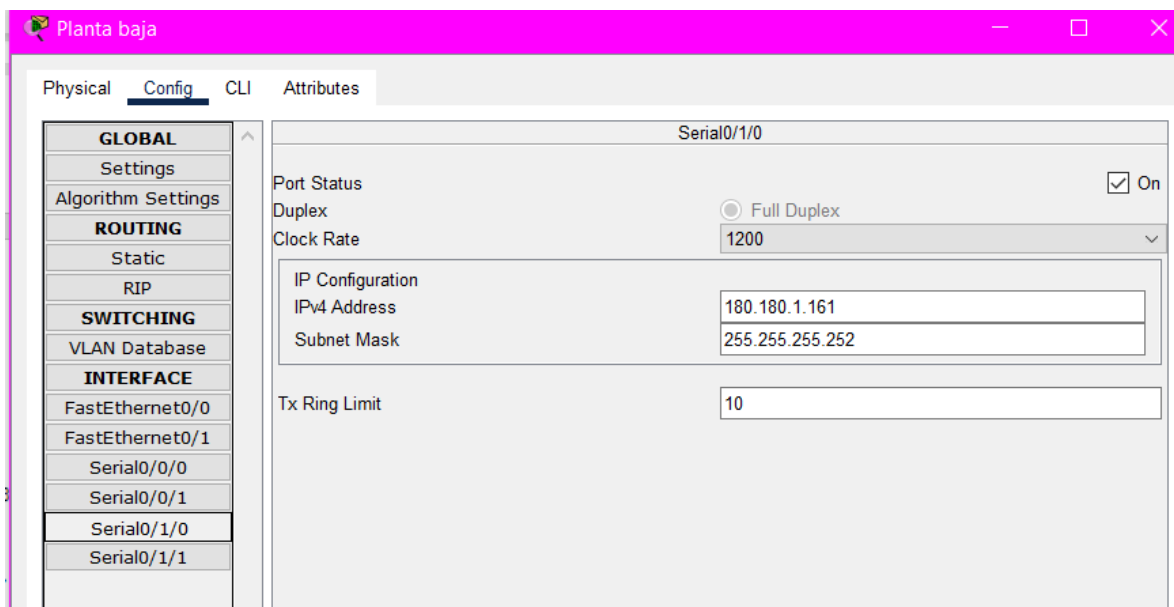
FastEthernet0/0	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	0001.634E.0301
IP Configuration	
IPv4 Address	180.180.0.1
Subnet Mask	255.255.255.192
Tx Ring Limit	10

Para determinar la conexión y la interfaz WAN correspondientes a cada serial, debemos realizar una observación detallada del diagrama presentado al inicio. Para lograr esto, podemos emplear el siguiente código. Mediante su ejecución, podremos obtener la información necesaria acerca de a qué serial está conectado cada dispositivo y qué interfaz WAN se muestra en el diagrama. Esta secuencia de instrucciones nos permitirá realizar cada conexión de forma precisa:


```
plantabaja(config-if)#exit
plantabaja(config)#interface se 0/1/0
plantabaja(config-if)#ip address 180.180.1.161 255.255.255.252
plantabaja(config-if)#no shutdown

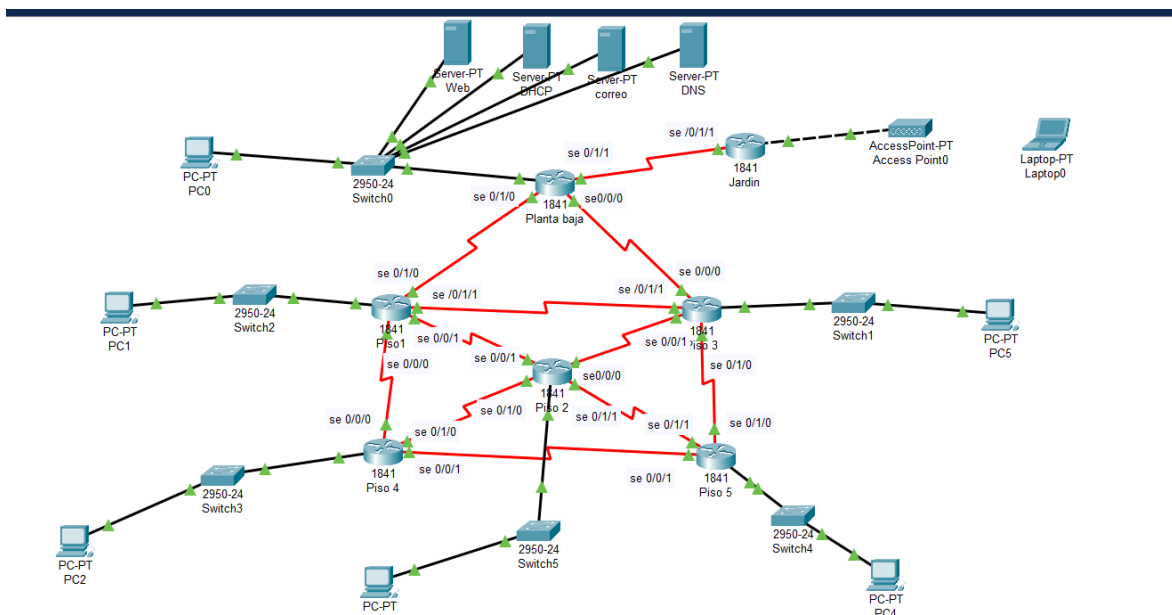
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
plantabaja(config-if)#exit
plantabaja(config)#exit
plantabaja#
%SYS-5-CONFIG_I: Configured from console by console
```

Una vez realizado esto podemos confirmarlo como en la conexión ethernet nos vamos al apartado de la conexión serial configurada y debe aparecer la ip configurada:



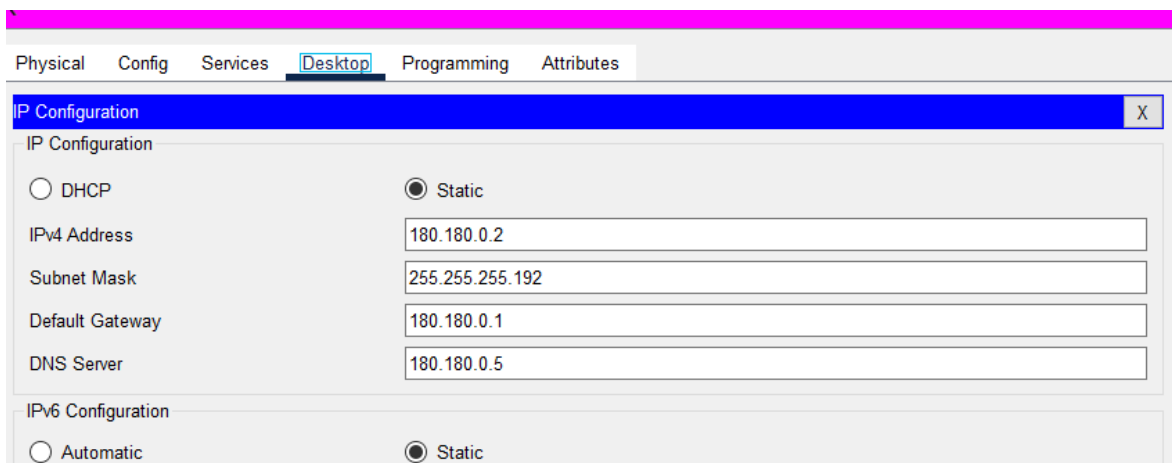
Después de llevar a cabo el proceso mencionado anteriormente, al observar el sistema en la interfaz de Cisco, notamos un cambio significativo en las conexiones. En lugar de los triángulos rojos que solían indicar problemas o desconexiones, ahora nos encontramos con que los triángulos son de color verde.

Este cambio en el color de los triángulos es un indicador positivo, ya que nos muestra que todas las conexiones están funcionando correctamente. El color verde sugiere que las conexiones están estables y en buen estado, lo que nos brinda confianza en el funcionamiento adecuado del sistema.



- g) La red organizacional de la empresa debe contar con:
- Servidor de correo: configure una cuenta de correo de manera que se pueda establecer la comunicación mediante este servicio entre todos los usuarios.

El servidor de correo se configura ingresando una ip como estática en este caso será 180.180.0.2



Después, se accede a la pestaña de servicios y se selecciona la opción de correo electrónico. En esta sección, se procede a comprobar si los servicios de SMTP y POP3 están activados. También se introduce el dominio de la empresa, excluyendo el uso de "www", y se hace clic en la opción "Establecer" para guardar los cambios. Por último, en la sección de configuración de usuarios, se ingresan los nombres de usuario y sus respectivas contraseñas. La secuencia de pasos para llevar a cabo esta configuración es la siguiente:

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL**
- FTP
- IoT
- VM Management

EMAIL

SMTP Service ☒ ON ☐ OFF

POP3 Service ☒ ON ☐ OFF

Domain Name:

User Setup

User Password

*Ambos usuarios creados tienen como contraseña 1234

b. Servidor DHCP: configure el servidor a fin de que todos los hosts cuenten con este servicio.

El servidor DHCP se configura ingresando una ip como estática en este caso será 180.180.0.3

Physical Config Services **Desktop** Programming Attributes

IP Configuration [X]

IP Configuration

☐ DHCP ☒ Static

IPv4 Address

Subnet Mask

Default Gateway

DNS Server

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Para llevar a cabo la configuración del servicio DHCP, es necesario acceder a la pestaña de servicios y seleccionar la opción DHCP. En esta sección, habilitaremos el servicio y configuraremos el "Pool Name" como "serverPool" estableciéndolo en 0, ya que esto ayuda a prevenir posibles fallas. Una vez realizados estos cambios, guardamos el pool y procedemos a crear los necesarios para cada subred.

Para cada router en el sistema, debemos ingresar su dirección de Gateway, la dirección DNS del servidor previamente configurado, la dirección desde la cual comenzará a asignar direcciones DHCP, la máscara de red correspondiente al segmento y el número máximo de usuarios permitidos. Una vez ingresados estos

datos, los añadimos haciendo clic en "Agregar" (Add). De esta manera, el resultado obtenido sería el siguiente:

Para finalizar, es necesario configurar cada router para que pueda recibir paquetes DHCP. Esto se logra mediante el uso del siguiente comando:

The screenshot shows the DHCP configuration interface. The left sidebar lists various services, with DHCP selected. The main configuration area is titled 'DHCP' and shows settings for the 'FastEthernet0' interface. The 'Service' is set to 'On'. The configuration fields include:

- Interface: FastEthernet0
- Service: On
- Pool Name: piso5
- Default Gateway: 180.180.1.65
- DNS Server: 180.180.0.5
- Start IP Address: 180.180.1.66
- Subnet Mask: 255.255.255.192
- Maximum Number of Users: 57
- TFTP Server: 0.0.0.0
- WLC Address: 0.0.0.0

Below the configuration fields is a table showing the configuration for multiple pools:

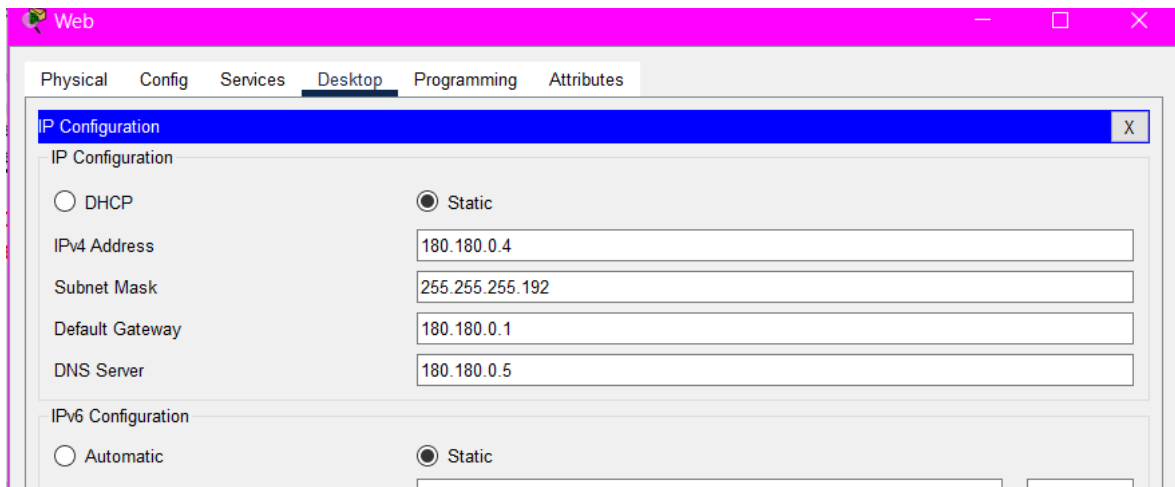
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
piso5	180.180.1.65	180.180.0.5	180.180.1.66	255.255.255.192	57	0.0.0.0	0.0.0.0
piso4	180.180.1.1	180.180.0.5	180.180.1.2	255.255.255.192	57	0.0.0.0	0.0.0.0
piso3	180.180.0.1	180.180.0.5	180.180.0.2	255.255.255.192	57	0.0.0.0	0.0.0.0
piso2	180.180.0.1	180.180.0.5	180.180.0.2	255.255.255.192	57	0.0.0.0	0.0.0.0
piso1	180.180.0.65	180.180.0.5	180.180.0.66	255.255.255.192	57	0.0.0.0	0.0.0.0
jardin	180.180.1.1	180.180.0.5	180.180.1.2	255.255.255.192	30	0.0.0.0	0.0.0.0
plantabaja	180.180.0.1	180.180.0.5	180.180.0.2	255.255.255.192	46	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	180.180.0.0	255.255.255.192	512	0.0.0.0	0.0.0.0

Para finalizar, es necesario configurar cada router para que pueda recibir paquetes DHCP. Esto se logra mediante el uso del siguiente comando:

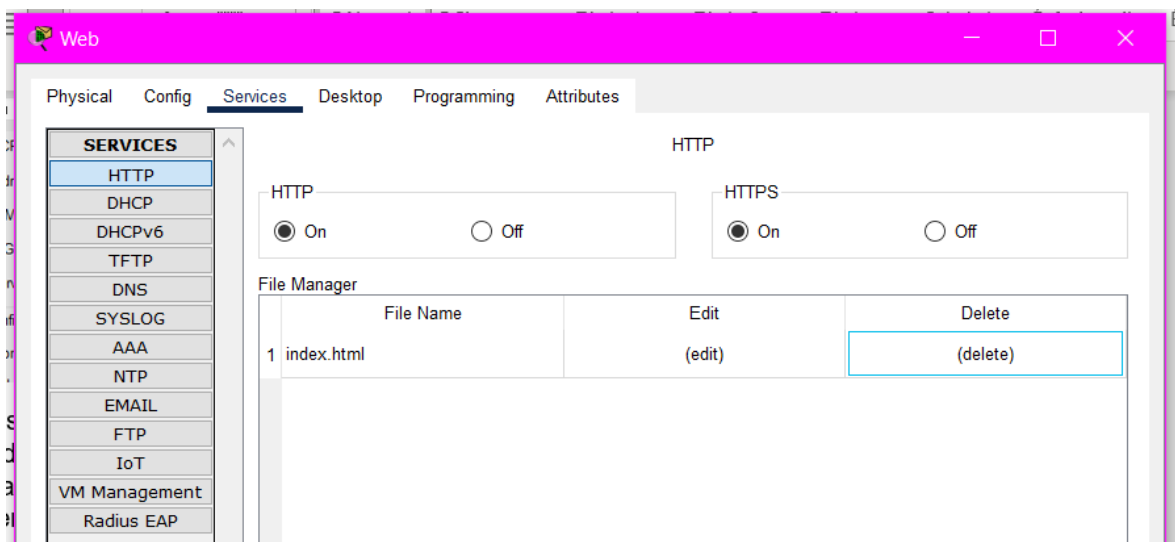
```
plantabaja(config)#interface fa 0/0
plantabaja(config-if)#ip helper-address 180.180.0.3
plantabaja(config-if)#
```

c. Servidor web y servidor DNS: el servidor web debe presentar la página de la empresa con el nombre que usted elija y dentro de ésta su nombre propio completo.

El servidor web se configura ingresando una ip como estática en este caso será 180.180.0.4



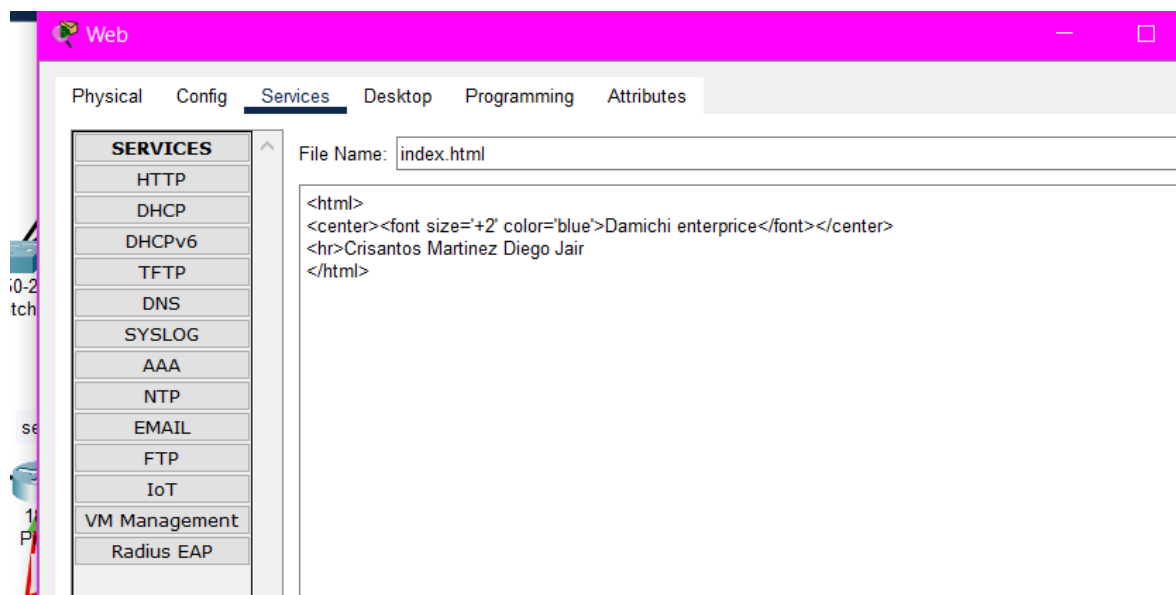
Después, accedemos a la pestaña de servicios y seleccionamos la opción HTTP. Dentro de esta sección, verificamos que tanto las opciones de HTTP como HTTPS estén habilitadas. A continuación, nos dirigimos a la sección de File Manager, donde procedemos a eliminar todos los archivos, excepto el archivo "index.html", ya que este será utilizado para configurar la página web. La configuración mencionada anteriormente se presenta a continuación:



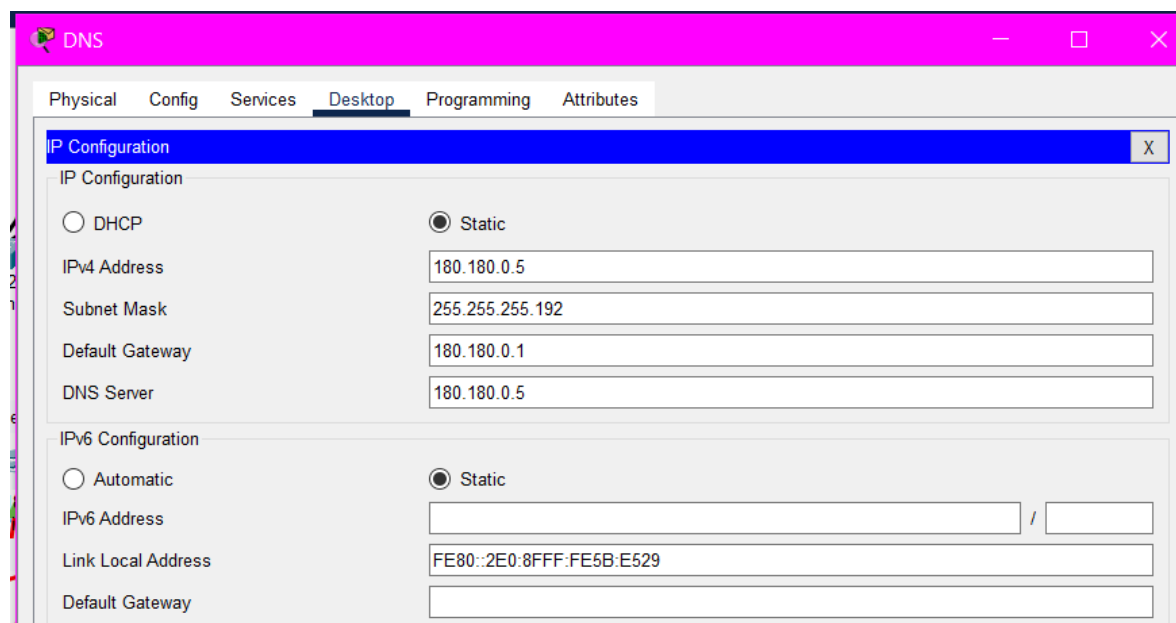
Para finalizar, abrimos el archivo "index.html" haciendo clic en el enlace de edición correspondiente. A partir de ahí, procedemos a configurar la página web según

nuestras preferencias. En este caso particular, se ha establecido el nombre de la empresa como título y el nombre del alumno como contenido.

El contenido del archivo "index.html" se muestra a continuación:



El servidor DNS se configura ingresando una ip como estática en este caso será 180.180.0.5

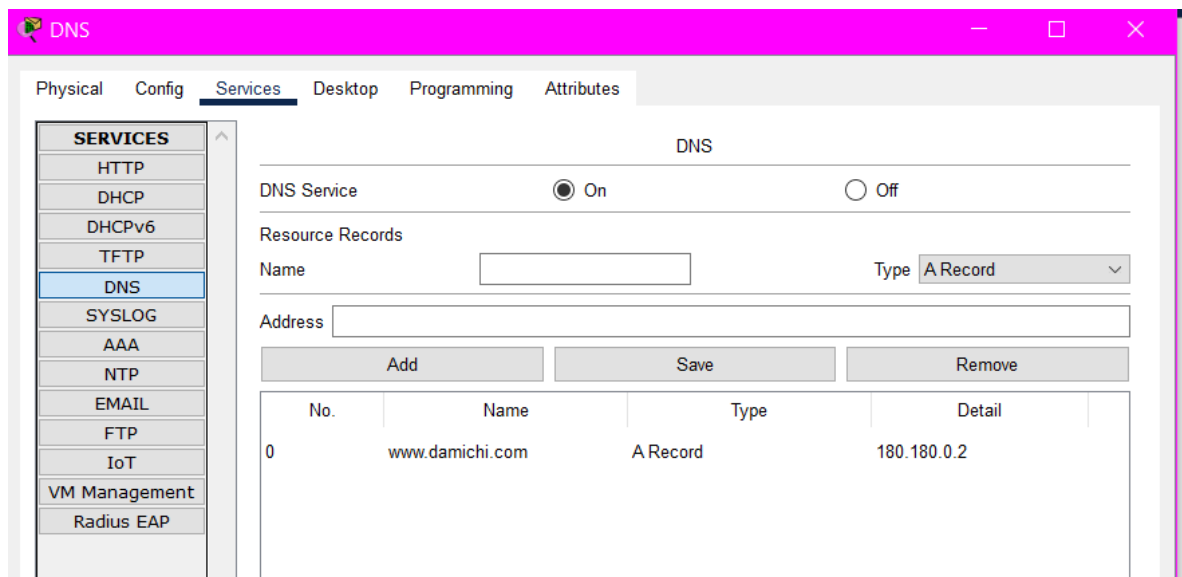


Para agregar el dominio, debemos acceder a la pestaña de servicios y seleccionar la opción DNS. Dentro de esta sección, encendemos el servicio DNS. Luego, procedemos a agregar el nombre del dominio y la dirección IP donde se encuentra alojado el servidor web. En este caso, la dirección IP utilizada será 190.168.0.3.

La configuración mencionada se muestra a continuación:

1. Accede a la pestaña "Services".
2. Selecciona la opción DNS.
3. Habilita el servicio DNS si aún no está encendido.
4. Ingresa el nombre del dominio en la configuración correspondiente.
5. Agrega la dirección IP del servidor web (190.168.0.2) en la configuración del DNS.

Con esta configuración, el DNS asociará el nombre de dominio especificado con la dirección IP del servidor web, lo que permitirá acceder al sitio web utilizando el nombre de dominio en lugar de la dirección IP directamente.



- h) Argumentar la importancia del uso de normas y estándares. Mencionando de manera puntual cada una de las normas y de los estándares involucrados en el proyecto para la habilitación de la infraestructura, la configuración de la red y su seguridad.

El uso de normas y estándares es fundamental en cualquier proyecto que implique la creación y simulación de una red de infraestructura, configuración y seguridad. Estas normas y estándares proporcionan pautas y directrices reconocidas a nivel mundial para garantizar la interoperabilidad, la compatibilidad, la seguridad y la eficiencia de las redes.

En el contexto de la habilitación de la infraestructura, las normas y estándares juegan un papel crucial en el diseño y la implementación de la red. Algunas normas y estándares relevantes pueden incluir:

1. Norma IEEE 802.3: Esta norma define los estándares para la tecnología Ethernet, que es ampliamente utilizada para la transmisión de datos en redes locales. Establece especificaciones para los cables, conectores y protocolos utilizados en la red.
2. Norma IEEE 802.11: Esta norma se refiere a los estándares de Wi-Fi, que son esenciales para el establecimiento de redes inalámbricas. Define las especificaciones para la comunicación inalámbrica de área local y garantiza la interoperabilidad entre los dispositivos compatibles con Wi-Fi.
3. Norma TIA/EIA-568: Esta norma establece los estándares para el cableado estructurado en redes de telecomunicaciones. Proporciona directrices para la instalación y el rendimiento de los cables, conectores y tomas de telecomunicaciones.

En cuanto a la configuración de la red, existen estándares y protocolos específicos que ayudan a garantizar un funcionamiento óptimo y una administración eficiente de la red. Algunos ejemplos incluyen:

1. Protocolo TCP/IP: Este conjunto de protocolos es ampliamente utilizado en Internet y redes locales. Define cómo los datos se envían, direccionan y reciben a través de la red, permitiendo la comunicación entre dispositivos.
2. Estándar SNMP (Simple Network Management Protocol): Este estándar facilita la administración y supervisión de los dispositivos de red. Permite a los administradores recopilar información y realizar acciones de gestión en los dispositivos de la red.
3. Protocolo DHCP (Dynamic Host Configuration Protocol): Este protocolo permite asignar automáticamente direcciones IP a los dispositivos en una red. Simplifica la configuración de red al eliminar la necesidad de configurar manualmente cada dispositivo con una dirección IP única.

En lo que respecta a la seguridad de la red, existen varias normas y estándares que ayudan a proteger la información y prevenir ataques. Algunos de ellos son:

1. Norma ISO/IEC 27001: Esta norma establece los requisitos para la gestión de la seguridad de la información. Proporciona un marco de trabajo para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información.
2. Estándar IEEE 802.1X: Este estándar define un mecanismo de autenticación de red basado en puertos. Ayuda a garantizar que solo los dispositivos y usuarios autorizados puedan acceder a la red.
3. Estándar WPA2 (Wi-Fi Protected Access 2): Este estándar de seguridad se utiliza en redes Wi-Fi para proteger la comunicación inalámbrica. Proporciona cifrado de datos y autenticación para prevenir el acceso no autorizado.

Como conclusión el uso de normas y estándares en proyectos de creación y simulación de redes de infraestructura, configuración y seguridad es crucial para garantizar la interoperabilidad, la compatibilidad, la eficiencia y la seguridad de la red. Algunas normas y estándares relevantes incluyen IEEE 802.3 y IEEE 802.11 para la habilitación de la infraestructura, TIA/EIA-568 para el cableado estructurado, TCP/IP, SNMP y DHCP para la configuración de la red, e ISO/IEC 27001, IEEE 802.1X y WPA2 para la seguridad de la red. Estas normas y estándares proporcionan directrices reconocidas a nivel mundial que ayudan a garantizar el éxito y la fiabilidad de los proyectos de redes.

- i) Estimar el costo del proyecto y presentar un análisis costo-beneficio del mismo.

Materiales:

- 7

routers:

Cómputo (Hardware) > Redes > Router > MX68-HW



Router Cisco Meraki con Firewall MX68, Inalámbrico, 450 Mbit/s, 10x RJ-45, 1x USB 2.0

SKU: MX68-HW



★★★★★ 1 opinión | 0 preguntas

\$14,369.00

en 6 x \$2,394.83
a meses sin intereses

Costo de envío: \$99.00

Calcular fecha de entrega

En existencia

☐ Comparar

- 1 +

Guardar en favoritos

Agregar al carrito

$$14369 \times 7 = 100,583$$

- 7

switch

16

puertos

:



Switch PoE+ de 16 puertos gigabit ethernet L2 no administrable, S1900-16TP, 16 puertos PoE+@135W, metálico, sin ventilador, de sobremesa/montado en rack Hot #132532

Switch Gigabit Ethernet PoE+ plug-and-play con función MDI/MDIX automática para SOHO y pymes

MXN\$2,885

2K vendidos | 12 comentarios | 28 preguntas

FS P/N: S1900-16TP

299 en almacén US. Recibe tu pedido el 19 de jun., 2023

162 en almacén global. Recibe tu pedido el 22 de jun., 2023

76 en tránsito. Recibe tu pedido el 07 de jul., 2023

Ver más disponibilidad de almacén

Enviar a México

Envío gratuito por UPS Ground®


$$2885 \times 7 = 20195$$

• 4

servidores:

Cómputo (Hardware) > Servidores > Servidores > 7D8KA00ALA

Lenovo



Oferta

Servidor Lenovo ThinkSystem ST50 V2, Intel Xeon E-2324G 3.10, 16GB DDR4, 2TB HDD, 3.5", SATA III, Torre (4U) - no Sistema Operativo Instalado

SKU: 7D8KA00ALA

★★★★★ 1 opinión | 0 preguntas

-18% Ahorra \$3,886.00

~~\$22,095.00~~
\$18,209.00
en 6 x \$3,034.83
a meses sin intereses

Costo de envío: \$159.00
Calcular fecha de entrega

¡Sólo quedan 5 pzas.!

☐ Comparar

- 1 +

$$18209 \times 4 = 72836$$

• 22

rosetas

4

nodos:

Electrónicos > Equipos de Audio y Hi-Fi > Accesorios > Distribución > Placas de Pared




Placa de pared Ethernet de 4 puertos, placa de pared Cat 6 hembra-hembra compatible con dispositivos Ethernet Cat7/6/6e/5/5e, color azul

Marca: Phizli

★★★★★ 1,679 calificaciones

\$305⁵¹

+ \$83.79 de envío.

 Pagos y Seguridad

 30 días de devolución sin costo

 Enviado por Amazon

Tamaño:
Cat6-4port

Marca: Phizli
Color: Blanco

$$305 \times 22 = 6710$$



1 paquete de placa de pared Ethernet Cat6 de 2 puertos RJ45 de red hembra a hembra Keystone acoplador de pared, color azul

★★★★★ 19

\$204⁹²

- 14 roseta 2 nodos: Recíbelo el **miércoles, 21 de junio**
204 x 14= 2856



VCE Placa de pared Ethernet de 1
Puerto RJ45 CAT6 Keystone Jack en
Línea Hembra a Hembra en Listado
UL - Blanco 2 Unidades

★★★★★ ~ 1,446

\$329⁹⁹

- 10 roseta 1 nodo:
 $329 \times 5 = 1645$



LinkedPro PROCAT6 Bobina de Cable, Cat6, Color Azul, 1000 Feet

★★★★★ ~ 89

\$1,495⁰⁰ Típico: \$1,661.74

Ahorra 5 % [Solicítala ahora](#)

Recíbelo entre **jueves, 15 de junio** y **miércoles, 21 de junio**

Envío GRATIS en pedidos elegibles

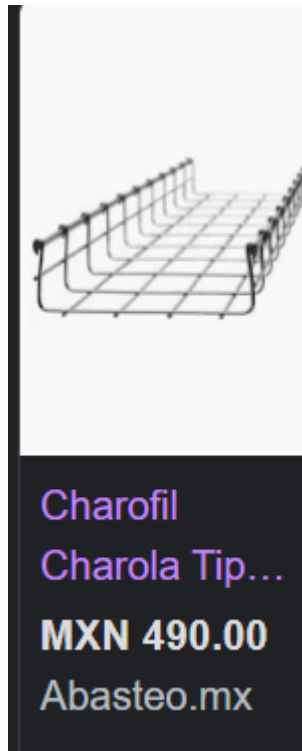
- Bobina de cable cat 6e: 1495
- Canaleta de 2mts: $465 \times 10 = 4650$



Alritz Kit de pista de cables, conducto de pista de cableado de ranura abierta de 138 pulgadas con sistema de gestión de cables de cubierta par...

★★★★★ ~ 655

- Escalerilla 3mts: $490 \times 10 = 4900$



Charofil
Charola Tip...
MXN 490.00
Abasteo.mx

OFERTA



[Access Point TP-Link
Gigabit Ethernet de
Banda Dual EAP225,...](#)
MXN 1,179.00 ~~MXN 1,42...~~
Abasteo.mx

- 3 aps: 1179 x3= 3537

Sumando todo nos da un costo total de 219 407 pesos mexicanos únicamente en material. Por lo que el costo total agregando nuestra ganancia sería de **270 000** pesos mexicanos.

j) REALICE UNA INVESTIGACIÓN DEL IMPACTO AMBIENTAL QUE SE GENERA POR LA INFRAESTRUCTURA TECNOLÓGICA QUE IMPLICA LA INSTALACIÓN DE UNA RED DE DATOS.

La infraestructura tecnológica, en particular la instalación de redes de datos, tiene un impacto ambiental significativo. A continuación, se detallan algunos aspectos clave del impacto ambiental relacionado con la infraestructura tecnológica:

1. Consumo de energía: Los dispositivos de red, como servidores, conmutadores, enrutadores y equipos de almacenamiento, consumen una cantidad considerable de energía eléctrica. Este consumo puede tener un impacto en la emisión de gases de efecto invernadero y contribuir al cambio climático.
2. Uso de recursos naturales: La fabricación de componentes de infraestructura tecnológica implica la extracción de recursos naturales, como minerales, metales y materiales plásticos. La extracción y procesamiento de estos recursos pueden tener consecuencias ambientales negativas, como la degradación del suelo, la contaminación del agua y la destrucción de ecosistemas.
3. Generación de residuos electrónicos: Con el tiempo, los equipos de red se vuelven obsoletos y requieren ser reemplazados o actualizados. Esto genera una gran cantidad de residuos electrónicos, como cables, tarjetas de circuitos impresos y dispositivos de red. El manejo inadecuado de estos residuos puede resultar en la liberación de sustancias tóxicas al medio ambiente y causar contaminación del suelo y del agua.
4. Refrigeración y gestión térmica: Los centros de datos y las salas de servidores requieren una refrigeración adecuada para mantener los equipos funcionando correctamente. Esto implica el uso de sistemas de aire acondicionado y refrigeración, que consumen grandes cantidades de energía y pueden tener un impacto significativo en las emisiones de gases de efecto invernadero.
5. Huella de carbono: La infraestructura tecnológica contribuye a la huella de carbono de una organización debido al consumo de energía y las emisiones asociadas. Esto incluye las emisiones de CO₂ provenientes de la generación de electricidad utilizada para alimentar los dispositivos de red y los sistemas de enfriamiento.

Para mitigar el impacto ambiental de la infraestructura tecnológica, se pueden tomar diversas medidas:

1. Eficiencia energética: Utilizar dispositivos de red con mayor eficiencia energética, como servidores y equipos de red con certificación energética, y optimizar la gestión del consumo de energía en los centros de datos.
2. Virtualización y consolidación: Consolidar los servicios y aplicaciones en menos servidores físicos mediante la virtualización, lo que reduce el consumo de energía y los requerimientos de hardware.
3. Reciclaje y disposición adecuada de residuos electrónicos: Implementar programas de reciclaje y garantizar que los residuos electrónicos se gestionen de manera adecuada, cumpliendo con las regulaciones ambientales y evitando la contaminación.
4. Uso de energías renovables: Transicionar hacia fuentes de energía renovable para alimentar los centros de datos y la infraestructura tecnológica, lo que reduciría las emisiones de gases de efecto invernadero.
5. Diseño eficiente de centros de datos: Construir centros de datos con diseños eficientes en términos de energía y refrigeración, utilizando tecnologías como enfriamiento por agua.
6. Agotamiento de recursos hídricos: La infraestructura tecnológica, especialmente los centros de datos, requiere grandes cantidades de agua para la refrigeración y otros fines operativos. El uso intensivo de agua puede agotar los recursos hídricos locales, especialmente en áreas propensas a la escasez de agua.
7. Contaminación electromagnética: Las redes de datos generan campos electromagnéticos que pueden tener efectos negativos en la salud humana y la vida silvestre. Si bien los estándares y regulaciones están en vigor para mitigar este impacto, es importante tenerlo en cuenta al diseñar y ubicar la infraestructura tecnológica.
8. Impacto durante la fase de construcción: La construcción de infraestructura tecnológica, como centros de datos o torres de comunicación, puede implicar la deforestación de áreas naturales, la alteración de ecosistemas y la generación de residuos de construcción. Es necesario minimizar y mitigar estos impactos durante la fase de construcción.
9. Ciclo de vida de los equipos: Además del impacto ambiental durante la fase de instalación y operación, es importante considerar el ciclo de vida completo de los equipos de infraestructura tecnológica. Esto incluye la extracción de materiales, la fabricación, el transporte y la eliminación adecuada de los equipos al final de su vida útil.
10. Conciencia y educación ambiental: Fomentar la conciencia y la educación ambiental entre los usuarios y operadores de la infraestructura tecnológica

puede ayudar a promover prácticas más sostenibles y responsables. Esto incluye medidas como la optimización del uso de recursos, la adopción de políticas de reducción de residuos y el fomento de la responsabilidad ambiental en todas las etapas del proyecto.

Es importante destacar que la adopción de prácticas sostenibles y la consideración del impacto ambiental en la infraestructura tecnológica no solo son beneficiosas para el medio ambiente, sino también para la eficiencia operativa y la reducción de costos a largo plazo.

Conclusiones

En conclusión, el proyecto de diseño de la red, realizado de manera individual, ha sido un logro destacable que demuestra habilidad técnica y capacidad de autogestión. A lo largo del proceso, se ha llevado a cabo un análisis exhaustivo de los requisitos y se ha desarrollado un diseño eficiente y funcional que cumple con las necesidades establecidas.

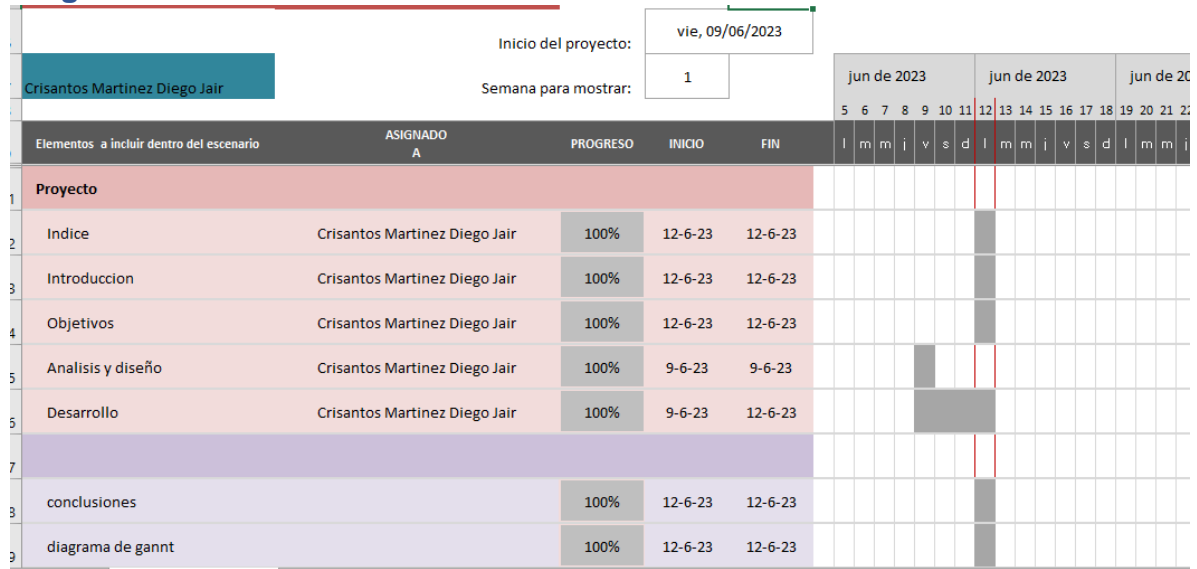
El diseñador ha demostrado un profundo conocimiento en el ámbito de las redes, implementando soluciones que optimizan el rendimiento, la seguridad y la escalabilidad de la red. Se han tenido en cuenta diversos factores, como la topología de red, el ancho de banda requerido y los mecanismos de seguridad, para garantizar el funcionamiento adecuado y confiable de la red.

Además, se ha prestado especial atención a la seguridad de la red, implementando medidas de protección y políticas de acceso que salvaguardan la integridad y confidencialidad de los datos. Esto refleja un compromiso con la privacidad y la protección de la información, aspectos cruciales en cualquier diseño de red.

El trabajo individual ha permitido una toma de decisiones ágil y una implementación eficiente, sin necesidad de coordinación o dependencia de otros miembros del equipo. Esto ha permitido una mayor autonomía y una ejecución más rápida del proyecto.

El proyecto de diseño de la red, realizado, ha sido un éxito al lograr implementar una infraestructura sólida y eficiente que cumple con los requisitos establecidos. El diseñador ha demostrado habilidades técnicas sobresalientes y capacidad para tomar decisiones acertadas en todos los aspectos clave del proyecto. Este logro individual refleja una destacable autogestión y competencia profesional en el ámbito de las redes.

Diagrama de Gantt



Bibliografía:

¿Cuánto contamina internet? (2019, febrero 20). National Geographic.

<https://www.nationalgeographic.es/medio-ambiente/2019/02/cuanto-contamina-internet>

La transmisión por Internet genera gran contaminación. (2020, octubre

15). *Gaceta UNAM*. <https://www.gaceta.unam.mx/la-transmision-por-internet-genera-gran-contaminacion/>

Sepúlveda, M. (2017, noviembre 18). Configuración de DHCP, DNS Web Server en

Cisco Packet Tracer - Aprende a configurar estos servicios en

eClassVirtual. *eClassVirtual - Cursos Cisco en línea*.

<https://eclassvirtual.com/configuracion-servidor-dhcp-dns-web-packet-tracer/>

Walton, A. (2020, junio 23). *Enrutamiento Estático y Dinámico*. CCNA desde Cero. <https://ccnadesdecero.es/enrutamiento-estatico-y-dinamico/>

(S/f). Arcgis.com. Recuperado el 13 de junio de 2023, de <https://pro.arcgis.com/es/pro-app/latest/help/data/utility-network/network-rules.htm#:~:text=Las%20reglas%20de%20red%20establecen,y%20tipos%20de%20activos%20espec%C3%ADficos.>