

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Proyecto Final

Administración de redes

Grupo: 2

Fecha entrega: 24/noviembre/2023

Alumnos:

Cornejo Aguilar Clara Luz 316218423

Crisantos Martínez Diego Jair 3170290264

Profesor

Ing. Magdalena Reyes Granados

Indice

Introducción.....	3
Objetivo.....	3
Justificación	3
Desarrollo y pruebas	4
Pagina web y dns	8
Servidor correo y conexión inalámbrica.....	10
Seguridad SSH	13
Prueba de conectividad voz ip	15
Hardware y software.....	15
Cotización	20
Diagrama de Gant.....	21
Seguridad física y lógica	21
Ataque	22
Impacto ambiental.....	25
Conclusión	27
Referencias	27

Introducción

Actualmente las redes de datos son de gran importancia ya que nos mantienen conectados en todo momento, tanto en nuestras vidas diarias como en la industria. Asegurar que estas redes sean eficientes y confiables se vuelve crucial, ya que su tamaño puede ser enorme.

Para lograr esto en nuestro proyecto, vamos a implementar redundancia, que es tener un plan B para asegurarnos que la red siga en pie, aunque algo salga mal.

En el ámbito de las redes de datos, las direcciones IP desempeñan un papel crucial al identificar de manera única cada dispositivo en la red. Esta tarea, sin embargo, puede volverse compleja y desafiante cuando lidiamos con redes de gran tamaño. En este contexto, surge la Máscara de Subred de Longitud Variable (VLSM) como una solución a esta tarea. A diferencia de la asignación estándar de direcciones, VLSM nos concede flexibilidad para diseñar subredes con dimensiones variables, evitando así el desperdicio de direcciones y optimizando la gestión de la red.

Para llevar a cabo este proceso de diseño y configuración de la red, usaremos el software Cisco Packet Tracer Student. Este entorno de simulación nos otorga la capacidad de simular y evaluar nuestra red antes de su implementación real.

Una vez implementada nuestra red en Cisco Packet Tracer crearemos escenarios en donde someteremos a nuestra red a condiciones que pueden ocurrir en la vida real, lo cual nos asegurará el correcto funcionamiento de la esta.

Objetivo

El objetivo de este proyecto es desarrollar una propuesta para una red empresarial, abordando de manera estratégica los elementos clave de planeación, organización, integración, dirección y control en el establecimiento de una red de voz y datos. La propuesta se centrará en la eficiencia operativa y la seguridad, tanto física como lógica, para garantizar el correcto funcionamiento de la red. Se buscará la optimización de recursos y la implementación de medidas proactivas para prevenir y mitigar posibles amenazas.

Justificación

Se eligió la topología en estrella triangular con tres routers. Esta topología tiene varias ventajas sobre otras topologías, como la redundancia y la tolerancia a fallos, la menor latencia, la facilidad de administración, la distribución eficiente del tráfico y la escalabilidad.

Las principales ventajas de la topología en estrella triangular son:

- **Redundancia y tolerancia a fallos:** Si uno de los routers falla, la comunicación aún puede fluir a través de los otros dos routers. Esto garantiza una mayor tolerancia a fallos y una menor interrupción del servicio en caso de problemas en uno de los routers. Además, la redundancia no solo se limita a los routers individuales, sino que se extiende al diseño

general de la topología en estrella triangular. La colocación de los routers asegura múltiples caminos para la transmisión de datos, permitiendo que la red mantenga su funcionalidad. Esto también disminuye la vulnerabilidad de la red ante eventos imprevistos, asegurando un nivel óptimo de servicio en todo momento.

- Menor latencia: La distancia entre los routers suele ser más corta, lo que reduce el tiempo necesario para que los datos se muevan de un extremo a otro de la red. Actualmente, la velocidad de transmisión es crucial para el correcto funcionamiento de la red, ya que la demanda de ancho de banda continúa aumentando exponencialmente y la transferencia de datos cada vez es más voluminosa. En un entorno empresarial, la eficiencia en la velocidad de transmisión no solo influye en la respuesta instantánea de las aplicaciones y servicios, sino que también se convierte en un factor determinante para la productividad y la satisfacción del usuario.
- Facilidad de administración: La topología en estrella triangular es relativamente sencilla de administrar, ya que solo implica tres routers interconectados. En el sector empresarial se busca que las redes cumplan con los requerimientos estipulados con el menor de los elementos posibles para economizar su costo.
- Distribución eficiente del tráfico: Cada router está conectado directamente a los otros dos, lo que facilita el enrutamiento y la gestión del tráfico. Esta característica contribuye a optimizar el rendimiento general de la red, asegurando una distribución eficiente de los datos y evitando posibles cuellos de botella.
- Escalabilidad: La topología en estrella triangular es escalable, lo que significa que puedes agregar más routers a la red de manera sencilla y eficiente si es necesario. Esto es necesario en el sector empresarial ya siempre existirá una necesidad de crecer la infraestructura de red a medida que las necesidades de la empresa crecen.

Desarrollo y pruebas

Red de datos ethernet, servicio de telefonía VoIP (física y lógica) y wifi para cada área.

-Área A: Vigilancia y Administrativa(100nodos).

-Áreas B: Informática, Telemática, Videoconferencias y Capacitación(220nodos)

.-Áreas C: Soporte técnico (60nodos).

-ID de Red que va a utilizar es: 191.2.0.0.

- Ordenamos de mayor a menor:
 1. B:220
 2. A:100
 3. C:60

Nota: en el caso del segmento para vozip se va a dejar la misma cantidad que se ocupan de nodos para cada área

- Para la subred B:

$2^8 - 2 = 256 - 2 = 254$ por lo tanto el id es 191.2.0.0 con mascara 255.255.255.0

- Para la subred voz1:

$2^8 - 2 = 256 - 2 = 254$ por lo tanto el id es 191.2.1.0 con mascara 255.255.255.0

- Para la subred A:

$2^7 - 2 = 128 - 2 = 126$ por lo tanto el id es 191.2.2.0 con mascara 255.255.255.128

- Para la subred voz2:

$2^7 - 2 = 128 - 2 = 126$ por lo tanto el id es 191.2.2.128 con mascara 255.255.255.128

- Para la subred C:

$2^6 - 2 = 64 - 2 = 62$ por lo tanto el id es 191.2.3.0 con mascara 255.255.255.192

- Para la subred voz3:

$2^6 - 2 = 64 - 2 = 62$ por lo tanto el id es 191.2.3.64 con mascara 255.255.255.192

- Para la subred WAN1:

$2^2 - 2 = 4 - 2 = 2$ por lo tanto el id es 191.2.3.128 con mascara 255.255.255.252

- Para la subred WAN2:

$2^2 - 2 = 4 - 2 = 2$ por lo tanto el id es 191.2.3.132 con mascara 255.255.255.252

- Para la subred WAN3:

$2^2 - 2 = 4 - 2 = 2$ por lo tanto el id es 191.2.3.136 con mascara 255.255.255.252

Subred	ID	Rango	Mascara	Broadcast	Ospf
B:220	191.2.0.0	191.2.0.1- 191.2.0.254	255.255.255.0	191.2.0.255	0.0.0.255
A:100	191.2.1.0	191.2.1.1- 191.2.1.126	255.255.255.128	191.2.1.127	0.0.0.127
C:60	191.2.1.128	191.2.1.129- 191.2.1.190	255.255.255.192	191.2.1.191	0.0.0.63
WAN 1	191.2.1.192	191.2.1.193- 191.2.1.194	255.255.255.252	191.2.1.195	0.0.0.3
WAN 2	191.2.1.196	191.2.1.197- 191.2.1.198	255.255.255.252	191.2.1.199	0.0.0.3
WAN 3	191.2.1.200	191.2.1.201- 191.2.1.202	255.255.255.252	191.2.1.203	0.0.0.3

- Envío de paquetes para observar el correcto funcionamiento de la topología con la correcta comunicación entre las distintas subredes.

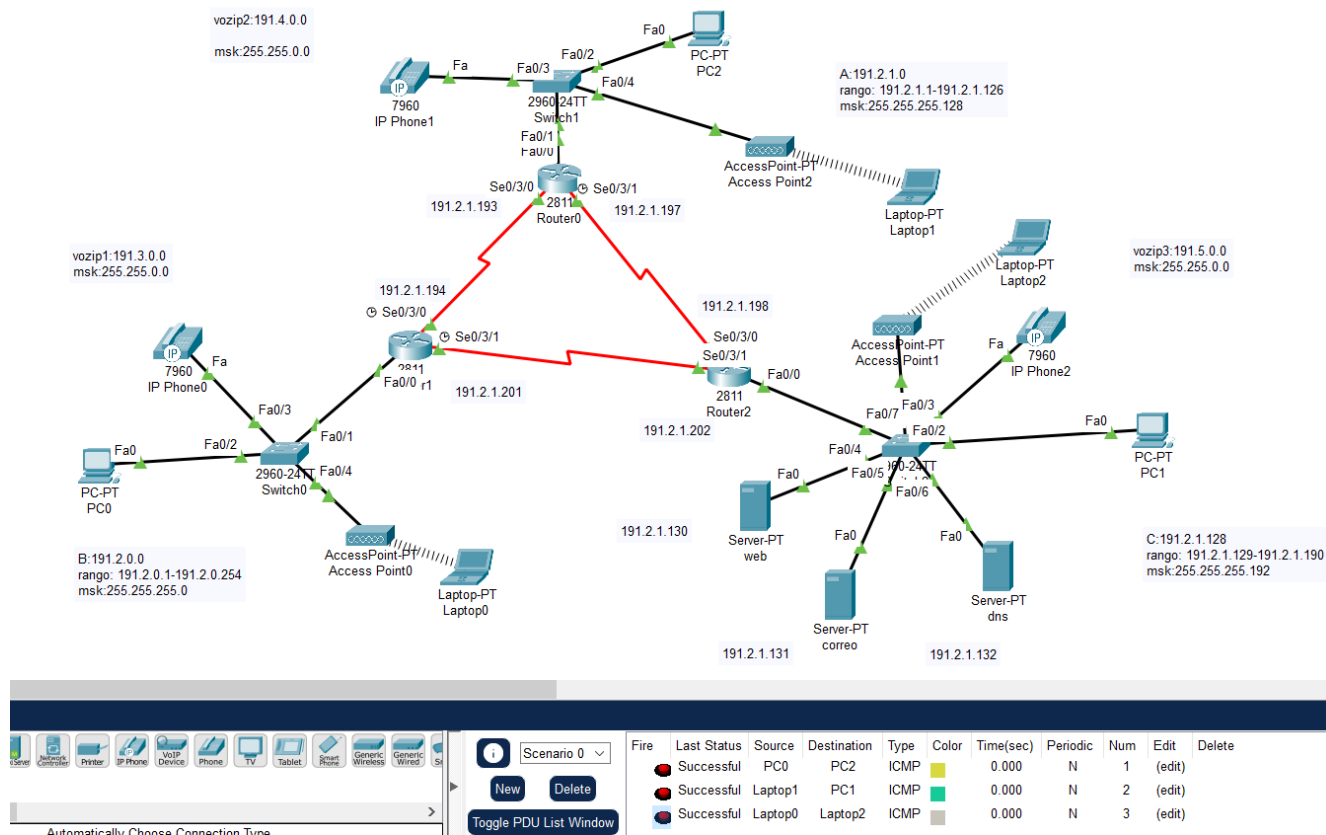


Imagen 1. Red simulada en Cisco Packet Tracer

- La configuración de la red se llevo acabo creando vlans ya que nuestra telefonía ip funciona dentro del mismo switch y router, dichas vlan se llaman:
 - 10, dato1
 - 20, voz1
 - 30, dato2
 - 40, voz2
 - 50, dato3
 - 60, voz3
- Posteriormente se selecciono indico que interfaz pertenecería a cada vlan, siendo las de datos para las computadoras, ap, servidores y las de voz para los teléfonos. Es importante poner la interfaz del router en modo trunk para que permita el paso de los múltiples datos de las vlan.
- Se creo también el DHCP tanto para datos como para voz y se indico dentro del router cuales serian los Gateway para cada vlan.
- Por ultimo se configuro el servicio de voz ip donde se crearon las extensiones
 - 1111
 - 2222
 - 3333
- La parte mas importante aquí esta dentro de los siguientes comandos:
- Router (config)#dial-peer voice Id voip

- Router (config)#destination-pattern x...
- Router (config)#session target ipv4:dir_ip
- Donde el id lo deberemos cambiar 2 veces por router uno para configurar la conexión con un teléfono y el otro para el segundo teléfono, en destination-pattern deberemos ser cuidadosos ya que deberemos indicar el inicio de nuestras extensiones ejemplo: mi primer extensión empieza por 11 por lo que deberemos poner 11.. donde los puntos que siguen indica que puede ser cualquier valor. Por ultimo indicaremos la ip donde se encuentra conectada dicha extension.

OSPF

Para configurarlo deberemos ingresar a cada uno de los router usar los siguientes comando donde deberemos poner las subredes que conoce este router.

enable

configure terminal

router ospf <número de proceso>

router-id <ID_del_router>

network <dirección-de-red> <máscara-de-subred> area <número-de-área>

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#do show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    191.2.0.0/16 is variably subnetted, 9 subnets, 5 masks
C       191.2.0.0/24 is directly connected, FastEthernet0/0.10
L       191.2.0.254/32 is directly connected, FastEthernet0/0.10
O       191.2.1.0/25 [110/65] via 191.2.1.193, 02:56:59, Serial0/3/0
O       191.2.1.128/26 [110/129] via 191.2.1.193, 01:43:44, Serial0/3/0
C       191.2.1.192/30 is directly connected, Serial0/3/0
L       191.2.1.194/32 is directly connected, Serial0/3/0
O       191.2.1.196/30 [110/128] via 191.2.1.193, 01:44:55, Serial0/3/0
C       191.2.1.200/30 is directly connected, Serial0/3/1
L       191.2.1.201/32 is directly connected, Serial0/3/1
    191.3.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       191.3.0.0/16 is directly connected, FastEthernet0/0.20
L       191.3.255.254/32 is directly connected, FastEthernet0/0.20
O       191.4.0.0/16 [110/65] via 191.2.1.193, 02:56:59, Serial0/3/0
O       191.5.0.0/16 [110/129] via 191.2.1.193, 01:43:44, Serial0/3/0
```

Imagen 2. Configuraciones en Router

Pagina web y dns

Para Configurar el servidor DNS, 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 191.2.1.132.

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 (191.2.1.130) 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.

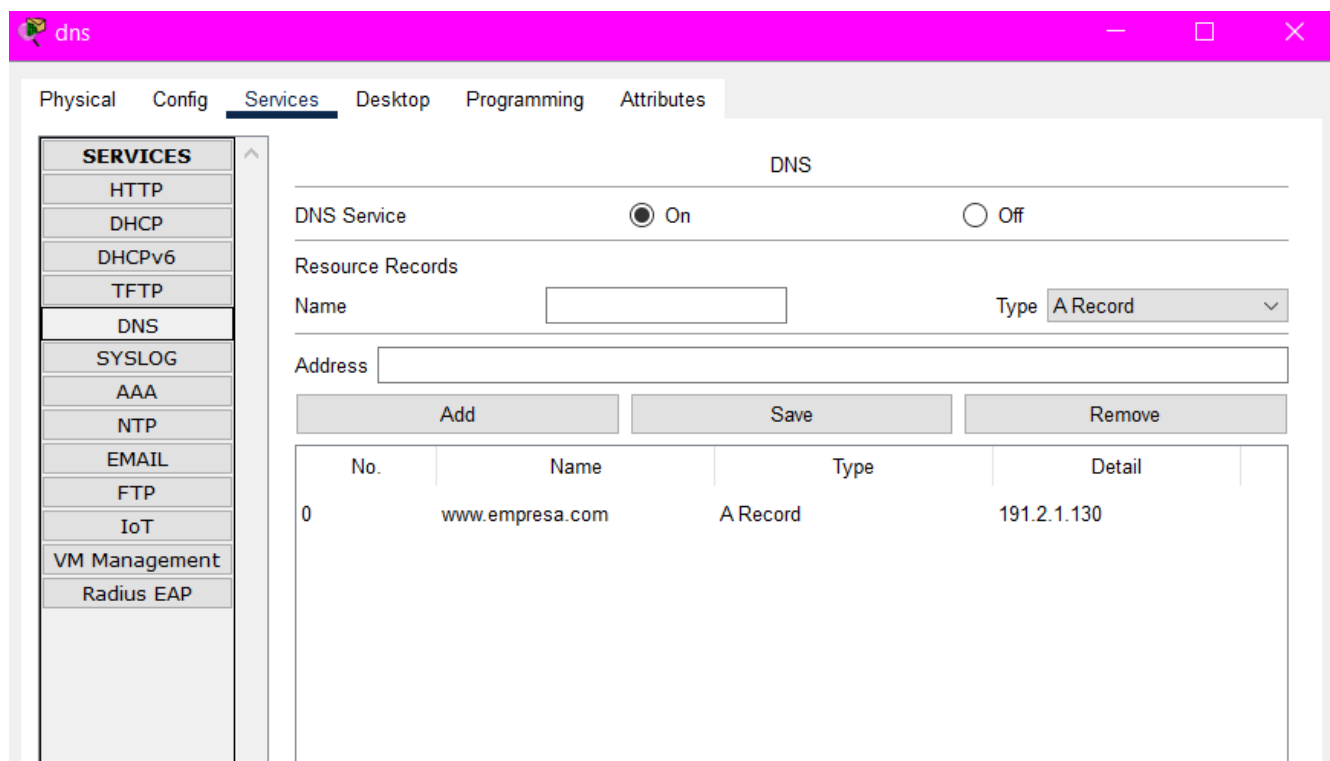


Imagen 3. Configuración DNS

Para el servidor web 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:

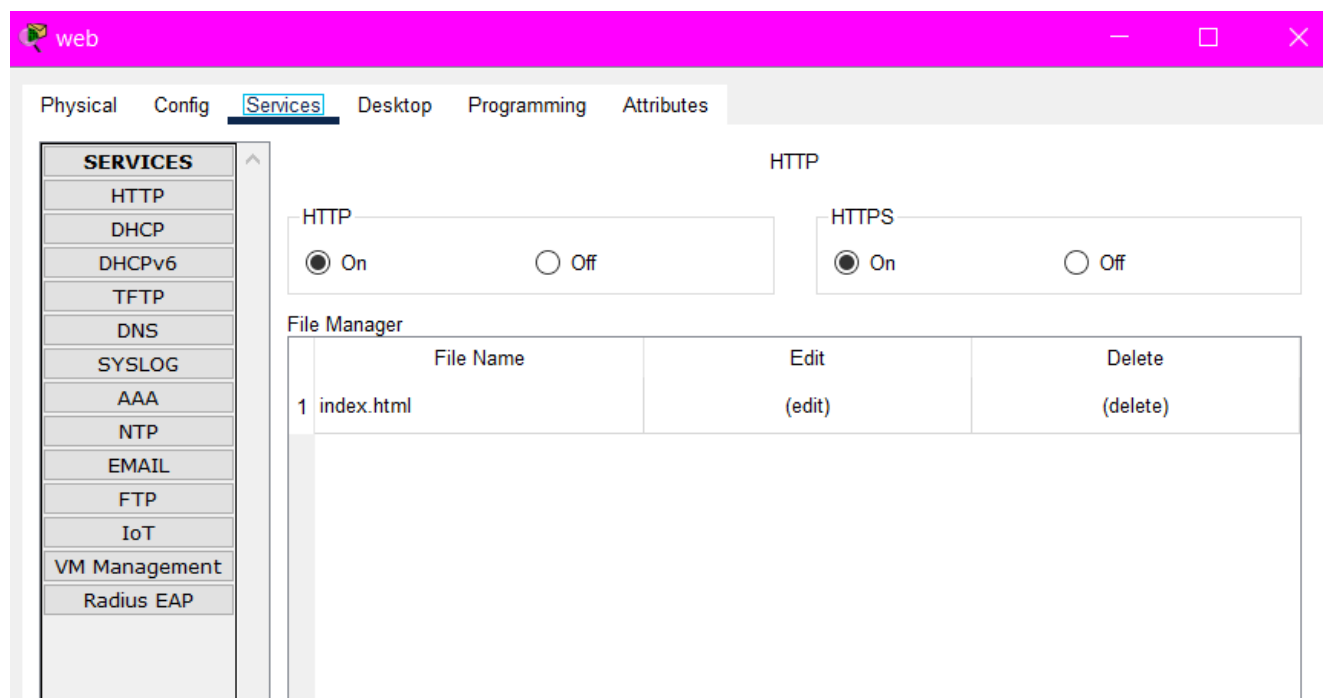


Imagen 4. Configuración página web

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 del proyecto como título y el nombre de los alumnos como contenido.

- Funcionamiento del servidor web que a su vez nos muestra el correcto funcionamiento del servidor dns, la prueba se realizó en dos computadoras distintas para observar que funciona en todas las subredes.



Imagen 5. Página Web mostrada desde PC1



Imagen 6. Página Web mostrada desde PC0

Servidor correo y conexión inalámbrica

El servidor de correo se configura ingresando una ip como estática en este caso será 191.2.1.131

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:

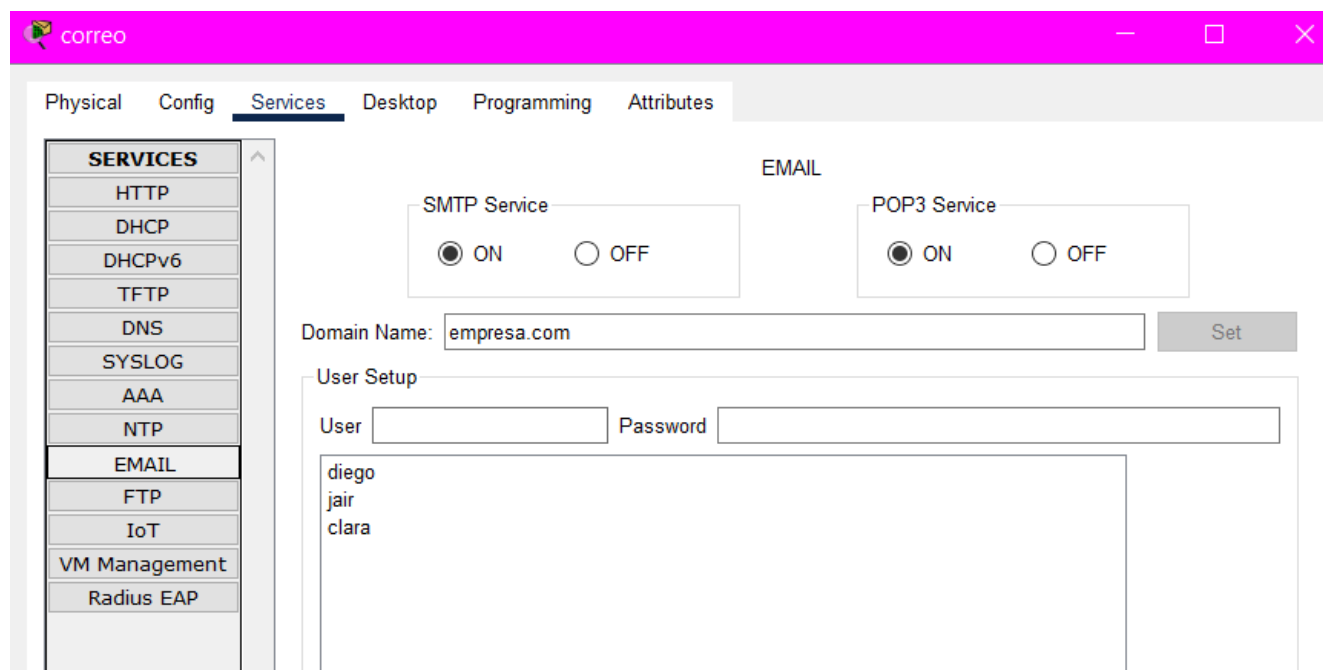


Imagen 7. Configuración de usuarios de correo Electrónico

- Prueba del servidor de correo enviando algunos entre las distintas cuentas que se tienen registradas:
 - Diego@empresa.com pass: 12345
 - Clara@empresa.com pass: 12345
 - Jair@empresa.com pass: 12345

Esta prueba se realizará usando las laptops para también comprobar el correcto funcionamiento de la conexión inalámbrica en cada subred.

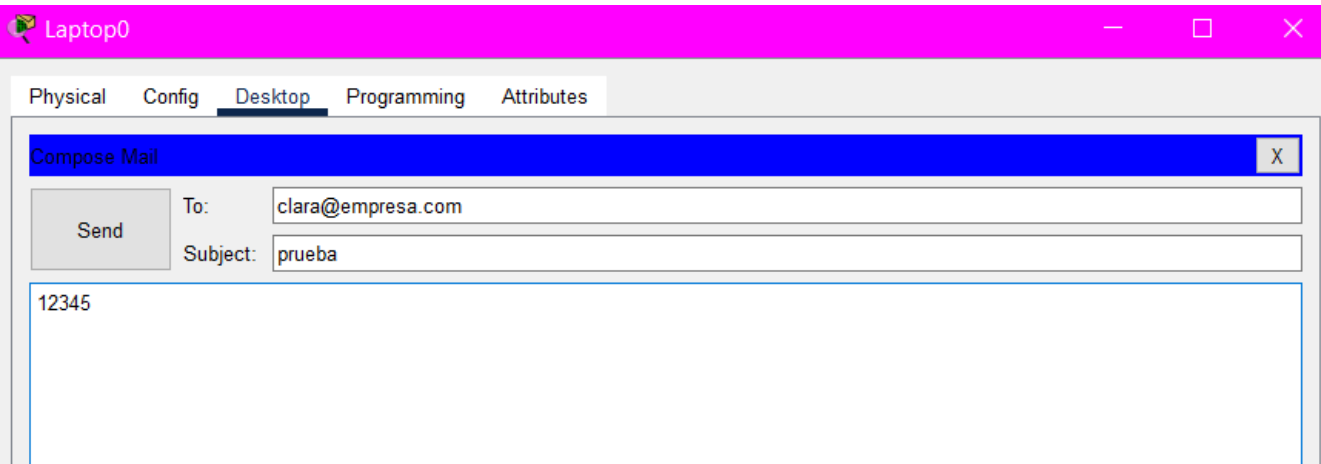


Imagen 8. Probando el correcto funcionamiento de los correo desde Laptop0

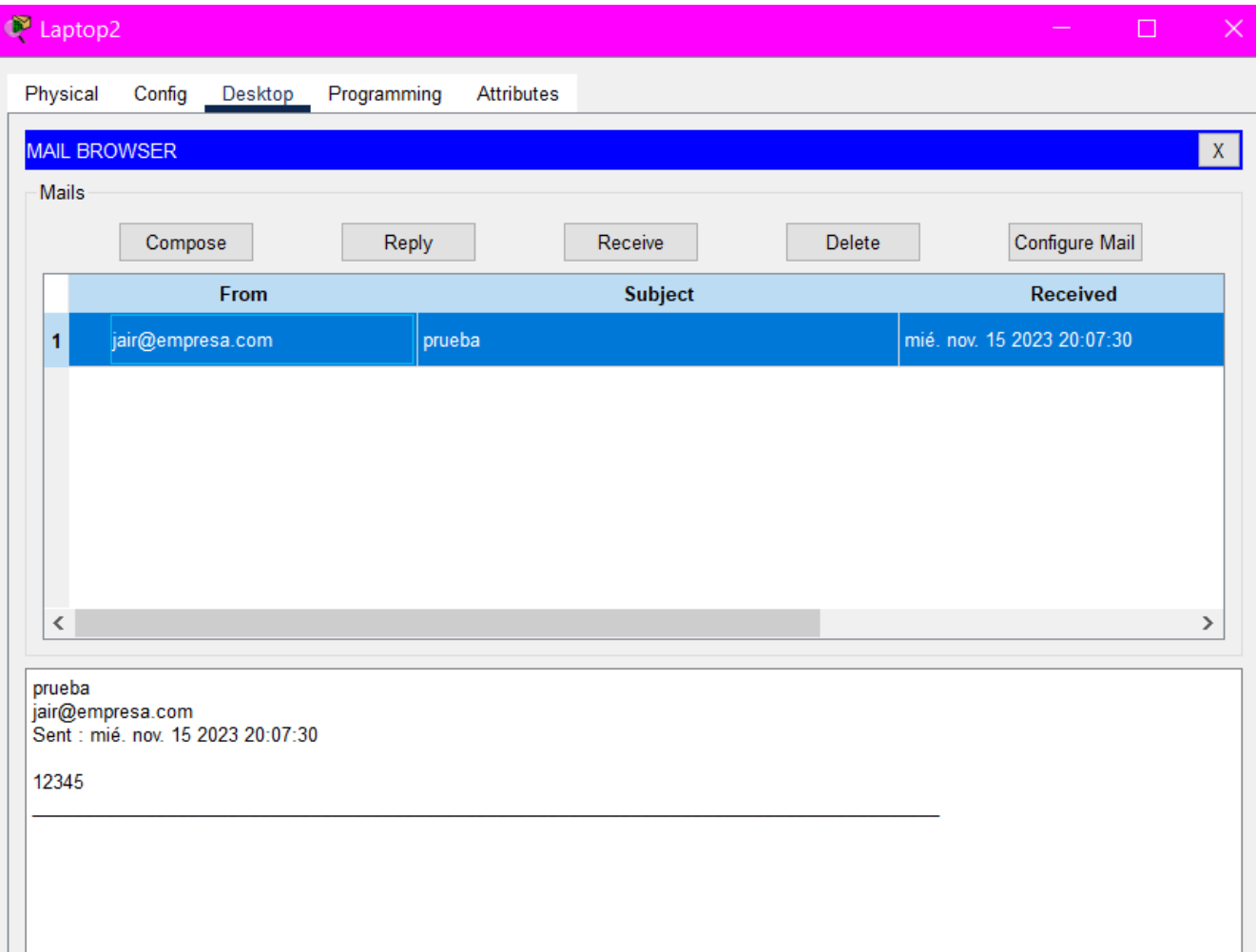


Imagen 9. Probando el correcto funcionamiento de los correo desde Laptop2

Seguridad SSH

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#
```

Imagen 10. Accediendo al router

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

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable secret 1234
Router(config)#
```

Imagen 11. Agregando contraseña en modo privilegiado

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 1234
Router(config-line)#login
Router(config-line)#
```

Imagen 12. Configuración de acceso desde consola

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 1234
Router(config-line)#login
Router(config-line)#
```

Imagen 12. Configuración de contraseña para acceso remoto

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 areal
areal(config)#banner motd # Bienvenido #
areal(config)#
```

Imagen 13. Asignación de nombre

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:

```
areal#
%SYS-5-CONFIG_I: Configured from console by

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

Imagen 14. Guardando la configuración

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

```
Bienvenido

User Access Verification

Password:

areal>enable
Password:
areal#
```

Imagen 15. Verificando solicitud de contraseña

Prueba de conectividad voz ip

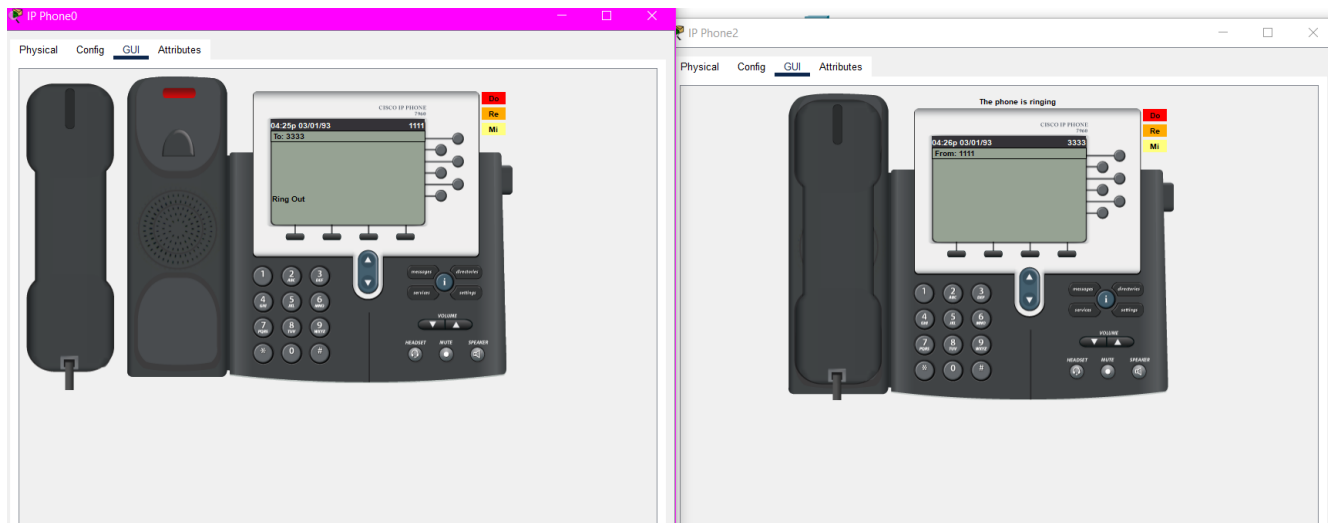


Imagen 16. Realizando llamada por Volp

Hardware y software

- Para los routers que utilizaremos en la red se colocaron, Cisco 2811 Integrated Services Router que es parte de la serie Cisco 2800 Router de Servicios Integrados, que complementa la serie de Routers de Servicios Integrados. Los Routers de Servicios Interados de Cisco Serie 2800 proporciona un gran nivel de rendimiento para ajustarse al crecimiento incluso de grandes negocios. Estos routers nos facilitaran el enrutamiento de datos entre redes, permitiendo la transferencia eficiente de paquetes de un origen a un destino a través de la mejor ruta disponible.

The image displays a Cisco 2811 Integrated Services Router. On the left is a photograph of the physical device, a silver-colored rack-mountable unit. To the right is a product listing with the following details:

Cisco 2811 - Router (0-40 °C, -40-70 °C, 5-95%, 438.2 x 416.6 x 44.5 mm, Alámbrico)

Marca: Cisco

3.6 ★★★★★ 17 calificaciones

\$10,000⁰⁰

Hasta 24 meses de \$586.66 con costo de financiamiento Ver más opciones

Pagos y Seguridad Se puede devolver hasta el Enero 31, 2024

Marca	Cisco
Nombre del modelo	CISCO2811
Frecuencia	63 Hz
Tecnología de conectividad	Ethernet
Peso del producto	14 Libras
Sistema operativo	Cisco IOS

Ver más

Imagen 17. Cisco 2811

- Los switches se eligieron los Cisco Catalyst 2960-24TT, que son switches diseñados para ofrecer conectividad confiable y eficiente en entornos empresariales. Su combinación de puertos 10/100Mbps, capacidades de gestión y seguridad básica lo hace apropiado para una variedad de aplicaciones empresariales como las aplicadas en este proyecto.

[Volver a resultados](#)



CISCO 2960 48-Port Catalyst Switch (WS-C2960S-48FPD-L)

Marca: Cisco

\$15,749⁴⁵

Hasta 24 meses de \$923.96 con costo de financiamiento [Ver más opciones](#)



Pagos y Seguridad



Se puede devolver hasta el Enero 31, 2024



Pasa el mouse encima de la imagen para aplicar zoom

Marca	CISCO
Número de puertos	1
Color	negro
Peso del producto	16 Libras
Voltaje	240 Voltios

Acerca de este artículo

- 740 W PoE Capacidad
- Opcional Cisco flexstack soporte de apilamiento
- 48 puertos Ethernet 10/100/1000 (PoE +

Imagen 18. Cisco 2960

- Electrónicos › Computadoras, Componentes y Accesorios › Servidores

Imagen 19. Cisco Catalyst 9124AX

- Los servidores Cisco UCS S-Series Storage Server nos permitirán cubrir las necesidades de almacenamiento de escala masiva y cargas de trabajo que requieren una capacidad de almacenamiento significativa.

Producto	UCSS-S3260
Descripción del producto	Cisco UCS S3260 Storage Server Base Chassis
Categoría de servicio	A
Precio global en USD	\$27499.57 <div>Alerta de precio</div>
Cantidad mínima	N/A
Cantidad máxima	N/A
Duración	N/A

Imagen 20. Costo Cisco UCS

- Para realizar las llamadas con VoIP se utilizará el Cisco IP Phone 7960 que es un teléfono IP diseñado para su uso en entornos empresariales que utilizan sistemas de telefonía basados en protocolo de Internet (VoIP). Este modelo fue lanzado por Cisco Systems y se ha convertido en un teléfono IP popular y confiable en muchos entornos corporativos.



Teléfono Ip Cisco Serie 7960 Global

\$ 750

en 3 meses sin intereses de \$ 250

Envío gratis

Imagen 20. Cisco IP Phone 7960

- Software para gestión de VoIP Cisco Unified Communications Manager (Unified CM) ofrece un control de llamadas y una administración de sesiones confiable, segura, escalable y manejable.

- Los racks Cisco de la serie R son una solución ideal para entornos críticos que requieren los más altos niveles de confiabilidad, integridad estructural y seguridad. El diseño moderno de la serie ofrece características excepcionales de alimentación, refrigeración y gestión de cables, así como la resistencia y estabilidad necesarias en las actuales envolturas de rack, brindando tranquilidad para los elementos más importantes de la infraestructura.

Racks Cisco de la serie R


Estado	Fin de la venta
Fecha de lanzamiento de la serie	20-DEC-2010
Fecha de fin de la venta	20-NOV-2020
Fecha de fin de soporte	30-NOV-2025
Diagrama	Galería de símbolos de Visio (30 MB .zip file)

Este producto es compatible con Cisco, pero ya no se vende.
Modelos admitidos: Rack Cisco R42610, rack Cisco R42612



Imagen 21. Racks Cisco de la Serie R

- La roseta Cober integra un conector tipo jack dentro de una caja montable en pared color blanco, para colocarla cerca de tus equipos de cómputo, consolas, pantallas o cualquier dispositivo de red, haciendo fácil su conexión o cambio y evitando daños o caídas debido a usar cable en una sola tirada. Contiene un adhesivo de pared para facilitar su instalación.



Nuevo

Roseta Cat 6 Adhesivo Pared
Jack Caja Utp Red RJ45

\$ 50
IVA incluido

[Ver los medios de pago](#)

Envío a todo el país
[Conoce los tiempos y las formas de envío.](#)
[Calcular cuándo llega](#)

Color: **Blanco**

Stock disponible

Cantidad: **1 unidad** (30 disponibles)

Comprar ahora

Agregar al carrito

Imagen 22. Roseta Cat 6

- Cable para redes UTP (Par trenzado sin blindar) de Categoría 6, color azul, con 4 pares calibre 24 AWG, útil para la transmisión de voz y datos a una velocidad de 1 Gbps (Giga bit por segundo).

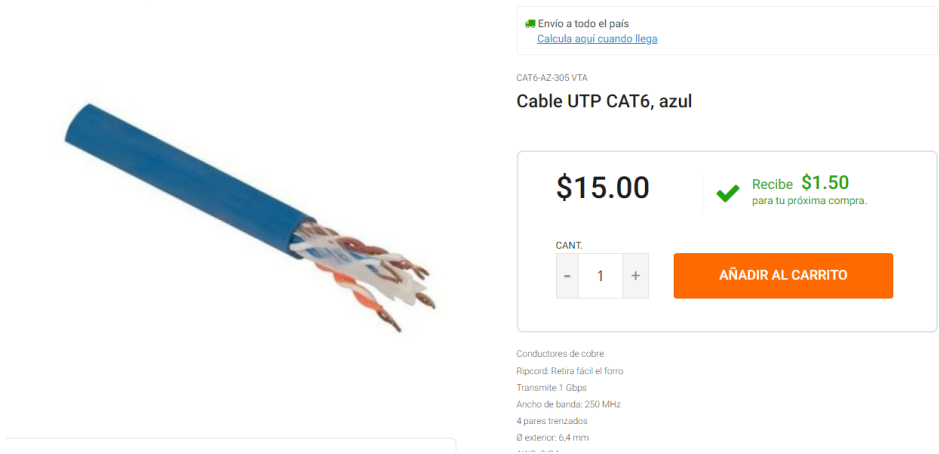


Imagen 23. Cable UTP CAT6

Cotización

Dispositivo	Cantidad	Precio	Total
Router Cisco 2811	3	\$10,000 MX	\$30,000 MX
Switch Cisco Catalyst 2960-24TT	3	\$15,749MX	\$47,247MX
Acces Point Cisco Catalyst 9124AX	3	\$14,402MX	\$43,377MX
Servidores Cisco UCS S-Series Storage Server	3	\$27,499.57MX	\$82,498.71MX
Cisco IP Phone 7960	15	\$750MX	\$11,250MX
Racks Cisco de la serie R	1	\$30,000MX	\$30,000MX
Software para gestión de VoIP Cisco Unified Communications Manager	1	Proveedor Cisco	\$1,500MX mes aprox
Roseta Cober	380	\$50MX	\$19,000MX
Cable para redes UTP	50m/nodo x380 nodos=19,000 m 25,000 m	\$15.00 MXxmetro	\$375,000MX
Contratación del servicio de nuestra empresa que garantiza asistencia.	No aplica	\$1,500MX al mes	
Instalación de la red	56 horas	\$350 MXla hora	\$19,600MX

Capacitación para el uso correcto de la red	16 horas	\$300 MXla hora	\$4800MX
---	----------	-----------------	----------

Total a pagar :\$645,672.71 pesos MX

Pago por servicio mensual: \$3,000 MX

Diagrama de Gant

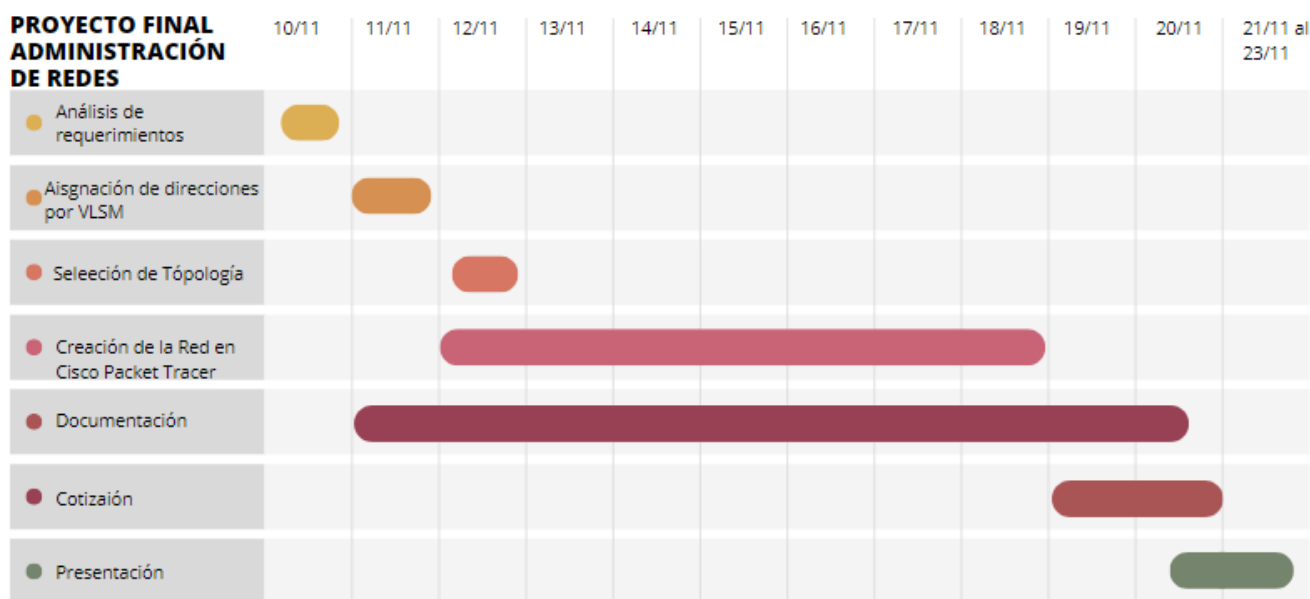


Imagen 23. Diagrama de Gant

Seguridad física y lógica

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.

Ataque

Se decidió simular el ataque de suplantación de dhcp ya que la presencia de un servidor DHCP falso en una red puede tener consecuencias negativas y representar un riesgo de seguridad. El DHCP (Dynamic Host Configuration Protocol) es un protocolo utilizado para asignar direcciones IP y otros parámetros de configuración de red a dispositivos en una red. Aquí hay algunas posibles consecuencias de tener un servidor DHCP falso en tu red:

- Asignación de direcciones IP incorrectas: Un servidor DHCP falso puede asignar direcciones IP que no están autorizadas en la red, lo que puede causar conflictos de direcciones IP y dificultar la comunicación entre dispositivos.
- Ataques de intermediario: Un atacante puede utilizar un servidor DHCP falso para realizar un ataque de intermediario, interceptando el tráfico entre los dispositivos y el servidor DHCP legítimo. Esto podría permitir al atacante realizar ataques de tipo "man-in-the-middle" y espiar o modificar la comunicación entre los dispositivos.
- Denegación de servicio (DoS): Un servidor DHCP falso también podría ser utilizado para realizar ataques de denegación de servicio, saturando la red con solicitudes de asignación de direcciones IP falsas y provocando problemas de conectividad para los dispositivos legítimos.
- Suplantación de identidad: Un servidor DHCP falso podría suplantar la identidad del servidor DHCP legítimo, engañando a los dispositivos para que obtengan configuraciones incorrectas. Esto podría llevar a situaciones en las que los dispositivos se conectan a una red controlada por un atacante.
- Vulnerabilidades en dispositivos: Al proporcionar configuraciones de red falsas, un servidor DHCP falso podría inducir a dispositivos a utilizar configuraciones específicas que podrían ser explotadas para realizar ataques adicionales.

Para protegerte contra este tipo de amenazas, es recomendable implementar medidas de seguridad, como el uso de la autenticación DHCP (por ejemplo, mediante el uso de DHCPv4/IPv6 authentication), la monitorización de la red para detectar servidores DHCP no autorizados y la segmentación de la red para limitar el alcance de posibles ataques. Además, es fundamental utilizar contraseñas seguras y mantener actualizado el software y firmware de los dispositivos de red para mitigar vulnerabilidades conocidas.

Para llevar acabo esto se llevo acabo la configuración de un servidor dhcp falso dentro de nuestra red donde simulamos que por medio de un nodo sin seguridad el atacante se conecto dio de baja nuestro dhcp y conecto uno suyo.

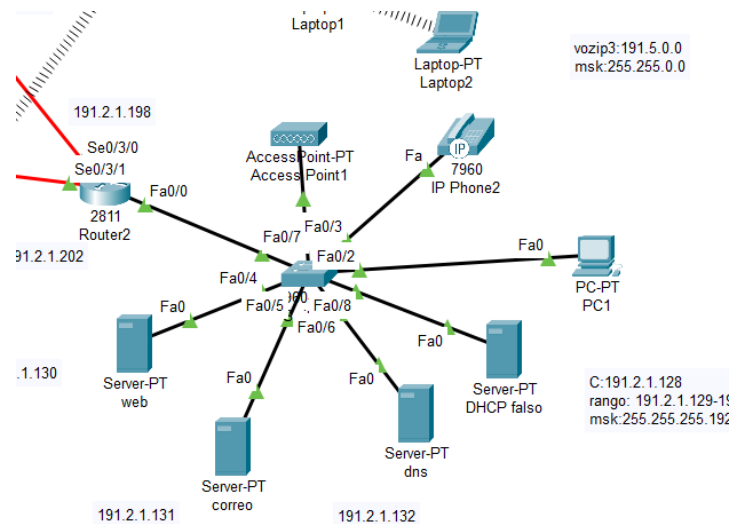


Imagen 24. Servidor falso DHCP

Para poder prevenir esto se hace uso del comando `ip dhcp snooping` el cual es utilizado en switches Cisco para activar la función de DHCP Snooping. DHCP Snooping es una característica de seguridad que protege una red contra ataques relacionados con el protocolo DHCP (Dynamic Host Configuration Protocol). A continuación, se explican las funciones principales de `ip dhcp snooping`:

- **Filtrado de Mensajes DHCP No Autorizados:** DHCP Snooping filtra y descarta los mensajes DHCP no autorizados, es decir, aquellos que provienen de fuentes no confiables. Esto ayuda a prevenir ataques de intermediarios DHCP, donde un dispositivo malicioso intenta proporcionar configuraciones DHCP falsas a otros dispositivos en la red.
- **Registro de Asignaciones DHCP:** DHCP Snooping mantiene un registro (log) de las asignaciones DHCP válidas, incluyendo información sobre las direcciones IP asignadas a dispositivos específicos y las direcciones MAC correspondientes. Este registro es útil para la resolución de problemas y la monitorización de la red.
- **Marcado de Puertos Confiables y No Confiables:** DHCP Snooping permite marcar puertos en el switch como confiables o no confiables. Los puertos confiables son aquellos a través de los cuales se espera que lleguen mensajes DHCP válidos (por ejemplo, conexiones a servidores DHCP), mientras que los puertos no confiables son aquellos a través de los cuales no deberían llegar mensajes DHCP (por ejemplo, puertos de usuario final).
- **Prevención de Ataques de Spoofing:** Al marcar puertos como confiables o no confiables, DHCP Snooping ayuda a prevenir ataques de spoofing, donde un dispositivo malintencionado intenta actuar como un servidor DHCP falso y distribuir configuraciones de red incorrectas.
- **Protección contra Agotamiento de Direcciones IP:** DHCP Snooping puede ayudar a prevenir agotamiento de direcciones IP asignando dinámicamente direcciones IP a

dispositivos legítimos y evitando la asignación de direcciones IP a dispositivos no autorizados.

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp snooping
Switch(config)#int fa0/1
Switch(config-if)#ip dhcp s
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#
```

Imagen 25. DHCP Snooping

Con esto logramos proteger correctamente nuestra red

Impacto ambiental

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.

Conclusión

La ejecución del proyecto nos brindó la oportunidad de poner a prueba todo el conocimiento adquirido en el laboratorio sobre la administración de redes. Comenzamos por proponer una topología que consideramos adecuada para las subredes que estábamos gestionando. Luego, llevamos a cabo la creación de servidores y, aún más crucial, la configuración de contraseñas en nuestros routers. De esta manera, mantuvimos la seguridad en nuestra red, asegurándonos de que no cualquier persona pudiera acceder a ella ni modificar su configuración.

También realizamos consideraciones adicionales que se realiza en la vida real como la cotización si bien este punto puede parecer fácil, el buscar cada producto que se adapte a nuestras necesidades para brindar el mejor de no servicios lleva su debido análisis ya que de esto depende en gran medida el ganar una licitación. Esto no solo fortaleció nuestro conocimiento técnico, sino que también mejoró nuestra capacidad para tomar decisiones informadas en tiempo real, adaptándonos a las circunstancias cambiantes del entorno tecnológico.

Con este proyecto implementamos las necesidades básicas de una red aplicando todo nuestro conocimiento adquirido en la materia y apoyándonos de conocimiento adicional a la carrera.

Referencias

- Forouzan, B. A., Fegan, S. C., & Coombs, C. E. (2015). "Data Communications and Networking" (5th ed.). McGraw-Hill.
- Tanenbaum, A. S., & Wetherall, D. J. (2014). "Computer Networks" (5th ed.). Pearson.
- Moy, J. T. (1998). "OSPF: Anatomy of an Internet Routing Protocol." Addison-Wesley.
- Barrett, D., Silverman, R., & Byrnes, R. (2005). "SSH, The Secure Shell: The Definitive Guide" (2nd ed.). O'Reilly Media
- Ojeda, M. (n.d.). Packet Tracer. https://redesavanzadasiautoms.blogspot.com/2016/06/packet-tracer_16.html
- Cisco Catalyst 2960 Series Switches. (2023, November 14). Cisco. https://www.cisco.com/c/es_mx/support/switches/catalyst-2960-series-switches/series.html
- Cisco Catalyst 9124AX Series Access Points Data Sheet. (2023, March 22). Cisco. <https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/nb-06-cat9124-ser-ap-ds-cte-en.html?oid=dstwls025625>

- Cisco UCS S-Series Storage Servers. (2022, June 6). Cisco.
<https://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-s-series-storage-servers/index.html>
- Product Overview (Version 1.0). (2013, October 18). Cisco.
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/7960g_7940g/sip/1_0/english/administration/guide/ver1_0/overview.html?dtid=osscdc000283#wp1023159
- Cisco Unified Communications Manager. (2023, March 29). Cisco.
https://www.cisco.com/c/es_mx/products/unified-communications/unified-communications-manager-callmanager/index.html?dtid=osscdc000283#~features
- Cisco R42610 Rack Data Sheet. (2016, December 7). Cisco.
https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/r-series-racks/data_sheet_c78-638922.html?dtid=osscdc000283
- Cable UTP CAT6, azul Steren Tienda en Línea. (n.d.). Electrónica Steren México.
<https://www.steren.com.mx/cable-utp-cat6-azul-vta.html>