



**IES FRANCISCO DE GOYA**

**NAVEGANDO EN IPV6**

**DISEÑO E IMPLEMENTACIÓN  
DE LA RED DE EMPRESA DE BILLETES**

**PROYECTO DE FIN DE CICLO  
FORMATIVO**

**SAMANTA MACAS ORDOÑEZ  
Y  
LUIS JIMENEZ CASTILLO**

# Índice

Índice	2
1. Objetivos	4
1.1. Objetivo General	4
1.2. Objetivos Específicos:	4
2. Análisis de Requisitos	5
3. Tecnologías	6
3.1. Tecnología VPN	6
3.2. Cisco Packet Tracer	8
3.3. Sweet Home 3D	9
4.5 Ethernet Channel	9
4. Desarrollo del proyecto	11
4.1. Diseño de Red	11
4.1.1. Descripción	11
4.1.2. Topología de Red	12
4.1.3. Zonas y Segmentación	12
4.1.4. Dispositivos de red y medios de transmisión	13
4.1.5. Medidas de Seguridad	14
4.1.6. Protocolos	15
4.1.6.1. Capa de Aplicación	15
4.1.6.2. Capa de Transporte	16
4.1.6.3. Capa de Red	17
4.1.6.4. Capa de enlace a datos	18
4.1.7. Direcccionamiento IP	21
4.1.8. Esquemas	24
4.1.8.1. Esquema Lógico	25
4.1.8.2. Esquema Físico	26
4.2. Pruebas y funcionamiento de equipos	27
4.2.1. Configuración Zona Desmilitarizada (DMZ)	27
4.2.2. Configuración WEB y DNS	27
4.2.3. Configuración DHCP	29
4.2.4. Configuración de Access-point-PT	37
4.2.5. Configuración de redes virtuales (VLAN)	40
4.2.6. Configuración Ethernet Channel	43
4.2.7. Configuración Tunelización	50
4.2.8. Configuración VPN	54
4.2.9. Listas de control de acceso (ACL)	59
4.3. Implementación de diseño de red	64
4.3.1. Dispositivos Físicos	65

4.3.2. Virtualización de Servidores	75
4.3.2.1. Preparación del entorno y Creación de las máquinas virtuales	77
4.3.2.2. Configuración de recursos para máquinas virtuales:	77
4.3.2.3. Instalación de hipervisor en servidor	78
4.3.2.4. Creación de máquinas virtuales	85
4.3.2.5. Virtualización servidor web y correo :	89
4.3.2.6. Virtualización servidor DHCP, DNS, VPN	91
4.3.3. Software de seguridad	93
4.3.4. FortiClient VPN	94
4.3.5. Presupuesto	96
4.4. Limitaciones	97
4.5. Conclusiones	98
5. Anexo	99
Router-empresa	99
Switch central	104
Switch lateral izquierdo (DRCI)	106
Switch derecho DIS_PD	110
Switch MAD-LOCAL-SERVER	113
6. Bibliografía	124



# 1. Objetivos

## 1.1. Objetivo General

Realizar el diseño de una red corporativa utilizando IPv6 en su totalidad. Tanto nivel de direccionamiento, routing, seguridad, protocolos de aplicación y movilidad.

## 1.2. Objetivos Específicos:

- Establecer una red segura y eficiente que satisfaga las necesidades de comunicación de los diferentes departamentos.
- Establecer políticas y procedimientos de seguridad, incluyendo la gestión de contraseñas, para garantizar el cumplimiento de las políticas de seguridad de la empresa.
- Configurar una conexión VPN para permitir el acceso remoto seguro a los recursos de la red interna.

## 2. Análisis de Requisitos

El presente análisis tiene como objetivo identificar y establecer los requisitos necesarios para el diseño e implementación de la red de la imprenta de billetes la misma que se enfocada en garantizar todas las medidas de seguridad efectivas y aprovechar el uso de IPv6 como protocolo de comunicación en su estructura de red.

Teniendo en consideración los objetivos principales en el que se recoge este proyecto queremos cumplir en todo momento con los estándares de seguridad necesarios para proteger de los recursos de red y la integridad de la información sensible. Es por ello que se deben implementar medidas de seguridad en las diferentes capas del modelo OSI, como firewalls, VLANs, ACLs y autenticación. Además, se configurará una solución de VPN y se implementarán soluciones de protección contra malware y ataques de denegación de servicio. La implementación de IPv6 será prioritaria, aprovechando sus ventajas en términos de dirección IP.

Del mismo modo se requerirá personal capacitado en la configuración y administración de IPv6, estableciendo políticas de asignación de direcciones y llevando un registro actualizado. Además se deben considerar las restricciones de presupuesto, recursos humanos y cumplimiento normativo.

Con estos requisitos y consideraciones, se busca garantizar la seguridad integral de la red de la imprenta de billetes, protegiendo los recursos y la información sensible, y aprovechando las ventajas que ofrece IPv6 en términos de seguridad y rendimiento.

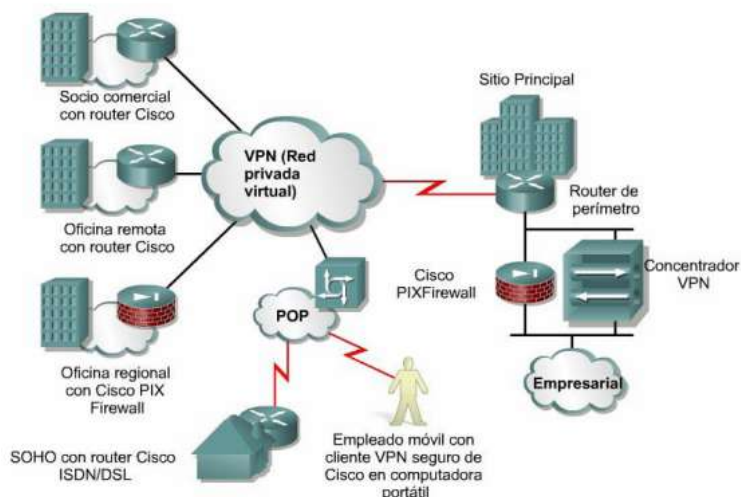
## 3. Tecnologías

### 3.1. Tecnología VPN

Una VPN es una conexión encriptada entre redes privadas a través de una red pública, como Internet. En lugar de utilizar una conexión de Capa 2 dedicada, como una línea arrendada. Una VPN utiliza conexiones virtuales denominadas túneles VPN. Los túneles VPN se enrutan a través de Internet desde la red privada de la empresa al sitio remoto o al host del empleado.

Los siguientes son varios beneficios de usar VPN:

- **Ahorro de costos:** las VPN permiten que las organizaciones usen la Internet global para conectar oficinas remotas, y para conectar usuarios remotos con el sitio corporativo principal. Esto elimina los enlaces WAN dedicados y costosos, y los bancos de módem.
- **Seguridad:** las VPN proporcionan el nivel máximo de seguridad mediante dos protocolos avanzados de cifrado y autenticación que protegen los datos del acceso no autorizado.
- **Escalabilidad:** debido a que las VPN usan la infraestructura de Internet en los ISP y los dispositivos, es fácil agregar nuevos usuarios. Las empresas pueden incrementar ampliamente la capacidad, sin agregar una infraestructura significativa
- **Compatibilidad con la tecnología de banda ancha:** Los proveedores de servicio de banda ancha como DSL y cable soportan la tecnología VPN, lo cual permite que trabajadores móviles y empleados remotos accedan a las redes corporativas utilizando su conexión a internet residencial. Además, las conexiones empresariales de alta velocidad pueden ser una solución rentable para conectar oficinas remotas.



Las VPN se implementan comúnmente de la siguiente manera:

- **VPN de sitio a sitio** - la configuración de VPN se hace en los routers. Los clientes no saben que sus datos están siendo encriptados.
- **VPN Acceso remoto** - El usuario es consciente e inicia la conexión de acceso remoto. Por ejemplo, usar HTTPS en un navegador para conectarse a su banco. Alternativamente, el usuario puede ejecutar software cliente VPN en su host para conectarse y autenticarse con el dispositivo de destino.

De cara a la implementación en nuestro proyecto vamos a configurar una VPN de acceso remoto haciendo uso del protocolo IPsec debido a las especificaciones según los requisitos de la empresa a la hora de la seguridad.

## 3.2. Cisco Packet Tracer

Cisco Packet Tracer es una aplicación de software de simulación de redes basada en eventos discretos. Utiliza una interfaz gráfica de usuario para representar componentes de red y permite a los usuarios diseñar, configurar y solucionar problemas en redes virtuales.

En términos de arquitectura, Packet Tracer utiliza un modelo de cliente-servidor. El componente del servidor se ejecuta como un proceso de fondo que realiza cálculos de simulación y proporciona servicios de red simulados. El componente del cliente es la interfaz gráfica de usuario que permite a los usuarios interactuar con la simulación.

Packet Tracer proporciona una amplia variedad de dispositivos de red que se pueden utilizar en una topología, como routers, switches, servidores, PCs, teléfonos IP y dispositivos inalámbricos. Estos dispositivos están pre configurados con sistemas operativos y características específicas de Cisco, lo que permite a los usuarios aprender y practicar configuraciones y comandos específicos de Cisco.

La herramienta permite a los usuarios crear topologías de red arrastrando y soltando los dispositivos en el área de trabajo. Los usuarios pueden conectar los dispositivos entre sí mediante cables virtuales y configurar las propiedades de los enlaces para simular conexiones físicas.





### 3.3. Sweet Home 3D

Sweet Home 3D es un editor CAD de ingeniería, arquitectura y construcción bajo licencia GNU General Public License para el diseño de los muebles de una vivienda en un plano 2D, y una vista previa en 3D.

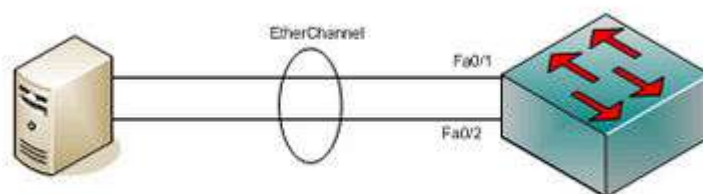



Hemos utilizado esta herramienta para crear una representación más realista de nuestra infraestructura de red empresarial. En ella, se pueden observar distintos dispositivos, como computadoras y armarios de distribución, así como nuestro centro de procesamiento de datos.

### 4.5 Ethernet Channel

Ethernet Channel es una tecnología proporcionada por Cisco que permite combinar múltiples enlaces Ethernet físicos en un solo enlace lógico de alta velocidad. En lugar de utilizar un único enlace Ethernet, EtherChannel permite agrupar varios enlaces en paralelo, lo que resulta en un incremento del ancho de banda y mejora el rendimiento de la red.

La principal ventaja de Ethernet Channel es que proporciona un mayor ancho de banda agregando la capacidad de múltiples enlaces físicos además de redundancia es decir en caso de que uno de los enlaces físicos falle, la comunicación se redirige a través de los enlaces restantes evitando así interrupciones en la conectividad de la red





Además, Ethernet Channel brinda a nivel de enlace. Si uno de los enlaces físicos falla, la comunicación se redirige automáticamente a través de los enlaces restantes, evitando interrupciones en la conectividad de red. Esto proporciona una mayor confiabilidad y continuidad en la infraestructura de red.

A la hora de la implementación tenemos dos protocolos que son LACP Y PAGP

- ❖ **Protocolo de Control de Enlace, LACP:** El protocolo de control de agregación de enlaces (LACP) es un estándar IEEE 802.3ad utilizado en EtherChannel para crear y gestionar canales Ethernet. LACP permite la negociación entre dispositivos de red, lo que resulta en la creación de canales de enlace compartidos que pueden ser activos o pasivos dependiendo de si son iniciados o respondidos por un dispositivo.
- ❖ **Protocolo de Agregación de Puertos, PAgP:** El Protocolo de Agregación de Puertos tiene su origen en el desarrollo no estándar de Cisco y su función principal es facilitar la formación y gestión de EtherChannel. Mediante una estrategia dinámica, PAgP hace posible la integración de varios puertos físicos en un único canal lógico. Este sistema operativo admite dos modos: activo o activamente deseable; ambas opciones permiten iniciar o responder al proceso de generación del canal correspondiente.

Considerando los distintos protocolos disponibles, para la implementación de nuestra red hemos decidido utilizar el **protocolo LACP**. Esta elección se basa en que LACP es un protocolo estándar que es compatible con diversos dispositivos, no solo los de Cisco. Configuraremos dos enlaces físicos, cada uno con una capacidad de 1 Gbps, para formar un canal lógico de 2 Gbps. Esta configuración nos permitirá gestionar un mayor volumen de tráfico de red y mejorar la eficiencia en la transferencia de datos. Nuestro objetivo principal es garantizar una alta disponibilidad y redundancia en la gestión de los datos.

## 4. Desarrollo del proyecto

### 4.1. Diseño de Red

#### 4.1.1. Descripción

La empresa SafeCor pJM, especializada en la impresión de billetes, cuenta con diversos departamentos, como Dirección, Recursos Humanos, Contabilidad, Informática, Diseño y Producción. Además de su sede principal, SafeCorpJM tiene una sucursal en Barcelona que sigue el mismo esquema físico y lógico que la sede central. Para asegurar una comunicación eficiente y segura entre ambas ubicaciones, se requiere la implementación de medidas de seguridad y el uso de protocolos apropiados.

Se propone establecer una arquitectura de red que permita la conexión entre la sede principal y la sucursal en Barcelona utilizando infraestructura de red en IPv4. Para lograr esto, se requiere la implementación de técnicas de migración y protocolos recomendados por el IETF (Internet Engineering Task Force). Algunas de estas técnicas incluyen Dual-stack, Tunnelización y Traducción.

En este caso, se ha decidido utilizar el método de tunnelización para establecer la comunicación entre estas dos redes. La tunnelización de IPv6 sobre IPv4 es un enfoque que permite enviar paquetes IPv6 a través de una infraestructura IPv4 existente. Esto es necesario debido a las diferencias en el formato de las direcciones y las características adicionales de IPv6 en comparación con IPv4. Dado que la implementación de IPv6 aún no es ampliamente adoptada en todo el mundo, la tunnelización proporciona una solución para transportar tráfico IPv6 sobre redes IPv4.

Al implementar la tunnelización, SafeCor pJM puede interconectar las redes IPv6 de ambas ubicaciones a través de la infraestructura basada en IPv4, lo que les permite ofrecer servicios IPv6 sin necesidad de actualizar los conmutadores de la red central.

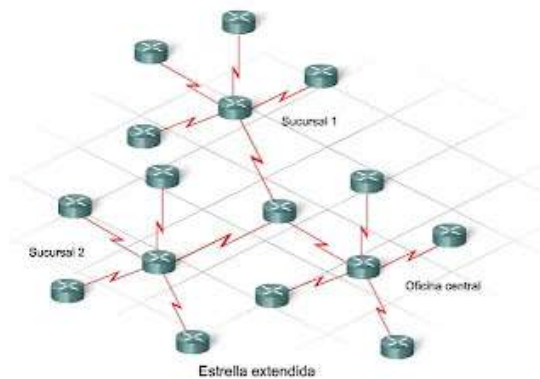
Adicionalmente, se implementarán medidas de seguridad para salvaguardar la integridad y confidencialidad de los datos transmitidos. Esto implica la utilización de VPN para establecer conexiones seguras para los empleados que teletrabajan, a través de redes públicas.

Para ello vamos a implementar el cifrado de datos mediante protocolos como el IPsec (Protocolo de Seguridad de Internet) y la instalación de firewalls para controlar el tráfico de red y prevenir accesos no autorizados.

### 4.1.2. Topología de Red

Teniendo en cuenta las necesidades de la empresa se implementa una **topología en Estrella extendida** ya que permitirá gestionar eficientemente los diferentes departamentos de la empresa.

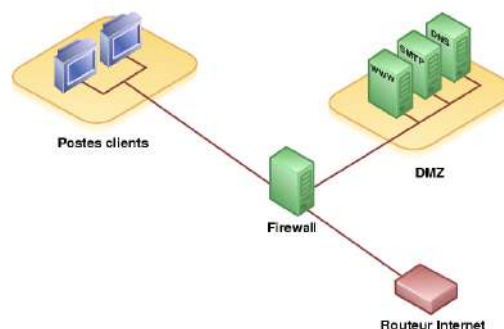
Además proporciona escalabilidad, control de tráfico, gestión centralizada y mejores medidas de seguridad. Su estructura jerárquica facilita la administración y resolución de problemas, lo que la convierte en una opción sólida para redes empresariales de gran envergadura



### 4.1.3. Zonas y Segmentación

En nuestra red, se ha implementado una estructura de zonas y segmentación para optimizar la seguridad y el rendimiento. Algunos aspectos destacados son:

- ❖ Hemos designado un área específica llamada Zona Desmilitarizada (DMZ) para albergar nuestros servidores de correo electrónico, web y DNS. Esta separación garantiza una capa adicional de seguridad al evitar el acceso directo desde Internet a los servidores internos. Los servidores en la DMZ funcionan como puntos de entrada y salida para servicios públicos mientras se mantiene protegida nuestra red interna.



- ❖ Redes de Área Local Virtuales (VLAN): Se han creado varias VLAN para cada departamento dentro de la empresa. Cada VLAN está vinculada a una subred específica en nuestra red LAN. A través de esta segmentación, podemos regular de manera eficiente el tráfico y mantener una gestión centralizada de la seguridad de la red. De esta manera, cada departamento puede establecer sus protocolos únicos en cuanto a acceso y restricciones de red, lo que mejora el rendimiento en general y refuerza las medidas de seguridad en este entorno.

#### 4.1.4. Dispositivos de red y medios de transmisión

Una vez que tenemos claro la topología de red y las diferentes zonas, número de host que habrá comenzamos a desarrollar nuestro esquema de red.

Para este proyecto se requerirían al menos 5 switches capa 2 y un router. Además, se necesitarán uno o dos firewalls y servidores para la zona DMZ.

1. **Router:** El router se encarga de conectar tu red local con Internet. Dirige el tráfico de Internet hacia los dispositivos de la red local y viceversa. Además, puede desempeñar funciones de enrutamiento y gestión del tráfico.
2. **Switch central:** El switch central actúa como el punto central de conexión en la red. Se conecta al router y distribuye la conexión a otros dispositivos de red, como los switches laterales y el firewall. Su tarea principal consiste en enviar datos entre los dispositivos conectados en la red
3. **Switches laterales:** Los switches laterales se conectan al switch central y proporcionan conectividad a los dispositivos de la red local en diferentes áreas o segmentos de la empresa. Estos switches permiten conectar computadoras, impresoras u otros dispositivos en esos segmentos específicos.
4. **Firewall:** El firewall se coloca después del switch central y se encarga de proporcionar seguridad a la red. Su función principal es monitorear y controlar el tráfico de red, permitiendo o bloqueando ciertos tipos de comunicaciones según las reglas de seguridad configuradas. Ayuda a proteger la red y los dispositivos de accesos no autorizados y ataques maliciosos.

5. **Switch de servidores locales:** El otro switch mencionado se conecta al firewall y está destinado a alojar los servidores de la empresa. Este switch proporciona conectividad a los servidores y les permite comunicarse con otros dispositivos en la red.

Esta configuración permite una segmentación de red adecuada y proporciona seguridad a través del firewall.

#### **4.1.5. Medidas de Seguridad**

Las medidas de seguridad se han implementado en varias capas del modelo OSI. Se ha configurado una solución de **VPN** para permitir el acceso remoto seguro a la red interna de la empresa.

La configuración específica de las políticas de seguridad para la simulación se van a realizar en un Router , con ellos vamos a permitir :

##### **❖ Acceso remoto seguro (VPN)**

Se establece una política de redes privadas virtuales empleando el protocolo IPsec con el fin de crear enlaces seguros entre los empleados que teletrabajo permitiendo así una conexión segura a los recursos y red de la empresa.

##### **❖ Control de tráfico entrante y saliente**

Se configuraran reglas y políticas para controlar el el tráfico entrante y saliente de la red de la empresa, para ello se debe tener en cuenta la segmentación que antes habíamos realizado en cuanto a la DMZ y VLAN, siguiendo un esquema generalizado:

#### **DMZ**

- ❖ Configurar reglas para restringir el acceso desde la DMZ hacia la LAN
- ❖ Configurar reglas para permitir el acceso hacia la DMZ desde internet con un nivel de seguridad medio y desde la LAN alto

#### **LAN**

Dentro de la red LAN, se ha implementado una segmentación en 9 subredes virtuales (VLAN), correspondientes a los diferentes departamentos de la empresa. Para garantizar la seguridad en cada una de estas subredes, se han establecido las siguientes reglas:

- ❖ **Permisos de acceso entre subredes departamentales:** Se permite el acceso entre las subredes todos departamentos **excluyendo el wifi-invitados y wifi-empleados**. Esto facilita la comunicación necesaria entre estos departamentos.
- ❖ **Limitación de acceso desde el wifi-clientes:** Los usuarios conectados al wifi-clientes solo tendrán acceso a navegar por Internet y no podrán comunicarse con otros departamentos de la empresa. Esta restricción se implementa para evitar posibles vulnerabilidades o accesos no autorizados desde dispositivos de clientes externos.
- ❖ **Autenticación requerida en wifi-empleados y wifi-invitados:** Tanto el wifi-empleados como el wifi-invitados requerirán una contraseña para acceder a la red de la empresa. Esto garantiza que solo personal autorizado pueda conectarse a la red interna.

#### 4.1.6. Protocolos

Para llevar un correcto registro de los protocolos que se pueden implementar para este diseño de red vamos a agruparlos por capas del modelo OSI.

##### 4.1.6.1. Capa de Aplicación

##### HTTP (Hypertext Transfer Protocol)



Es un protocolo de comunicación que permite las transferencias de información en la World Wide Web a través de archivos, XML, HTML, etc. Permite la comunicación entre un cliente y un servidor web para la solicitud y entrega de recursos

## **DHCPv6 (Dynamic Host Configuration Protocol for IPv6)**

Es un protocolo que permite la asignación automática de direcciones IPv6 y la configuración de parámetros de red en entornos IPv6, simplificando la administración de redes y dispositivos.

## **DNSv6 (Domain Name System for IPv6)**

DNSv6 es una extensión del sistema de nombres de dominio para IPv6. Proporciona resolución de nombres de dominio en entornos de red IPv6. Se utiliza para traducir nombres de dominio legibles para los humanos en direcciones IP numéricas y viceversa.

Con IPv6 y sus direcciones de 128 bits, DNSv6 se hizo necesario para adaptar el sistema de nombres de dominio. Al igual que DNS para IPv4, DNSv6 utiliza registros de recursos como registros A y registros AAAA para almacenar información relacionada con los nombres de dominio y las direcciones IPv6.

DNSv6 desempeña un papel fundamental en la comunicación y enrutamiento de IPv6 en Internet. Permite a los usuarios y aplicaciones acceder a servicios y recursos utilizando nombres de dominio en lugar de direcciones IP largas.

### **4.1.6.2. Capa de Transporte**

En la capa de transporte tenemos dos protocolos el TCP y UDP que en casos diferentes ya vienen configurados en los dispositivos de la red .

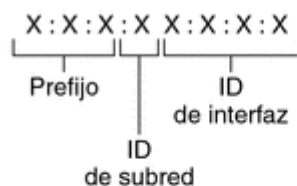
- **TCP:** utiliza un protocolo de enlace de tres vías para establecer la conexión confiable, asegurando que cada segmento que envía la fuente llegue al destino. TCP da soporte a muchas de las aplicaciones más populares de Internet (navegadores, intercambio de ficheros, clientes FTP, etc.) y protocolos de aplicación HTTP, SMTP, SSH y FTP.
- **UDP:** permite el envío de datagramas de forma rápida en redes IP sin establecer previamente una conexión, a diferencia del protocolo TCP, este no garantiza que los mensajes lleguen correctamente. Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida



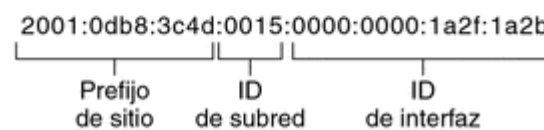
#### 4.1.6.3. Capa de Red

- **IPv6 (Internet Protocol version 6)**

IPv6 es la última versión del protocolo de Internet que proporciona un espacio de direcciones más grande y eficiente que IPv4. Utiliza direcciones de 128 bits en lugar de 32 bits y ofrece mejoras como autoconfiguración de direcciones y soporte nativo para seguridad IPsec. IPv6 facilita la conectividad global, la movilidad y la implementación de nuevas tecnologías como IoT. Las direcciones IPv6 se representan en notación hexadecimal con colons (:). Es esencial para garantizar la comunicación efectiva en un mundo conectado y la compatibilidad con IPv6 es fundamental para el futuro de Internet.



Ejemplo:



- **ICMPv6 (Internet Control Message Protocol for IPv6)**

ICMPv6 es el protocolo de control y diagnóstico utilizado en redes IPv6. Proporciona funciones clave como descubrimiento de vecinos, autoconfiguración sin estado, redireccionamiento y detección de errores. ICMPv6 permite la resolución de direcciones, asignación automática de direcciones, mejora del enrutamiento y notificación de problemas en la comunicación IPv6. Es esencial para la gestión y el control del tráfico en redes IPv6.

- **RIP (Protocolo de Información de Enrutamiento)**

El Protocolo RIP para IPv6 es un protocolo de enrutamiento dinámico que utiliza vectores de distancia y métricas de "saltos" para intercambiar información de enrutamiento entre routers en redes IPv6. Emplea temporizadores, división de horizontes y permite la redistribución de rutas para facilitar el enrutamiento eficiente en la red.

- **OSPF (El Protocolo de Estado de Enlace Abierto)**

OSPF es un protocolo de enrutamiento utilizado en redes IP que ayuda a los routers a intercambiar información y encontrar las mejores rutas para enviar datos. Funciona en áreas lógicas dentro de la red y utiliza mensajes para compartir detalles sobre los enlaces y subredes.

OSPF calcula rutas óptimas utilizando un algoritmo especial y se adapta rápidamente a cambios en la red, como enlaces caídos o nuevos enlaces. Esto asegura que la red pueda encontrar la mejor ruta disponible en todo momento.

Además, OSPF ofrece opciones de seguridad para proteger las actualizaciones de enrutamiento y garantizar que solo los dispositivos autorizados puedan participar en la red.

#### 4.1.6.4. Capa de enlace a datos

- **IEEE 802.1Q**

El protocolo IEEE 802.1Q, también conocido como Dot1q, es un estándar de redes que posibilita la implementación de redes de área local virtual VLAN en redes Ethernet.

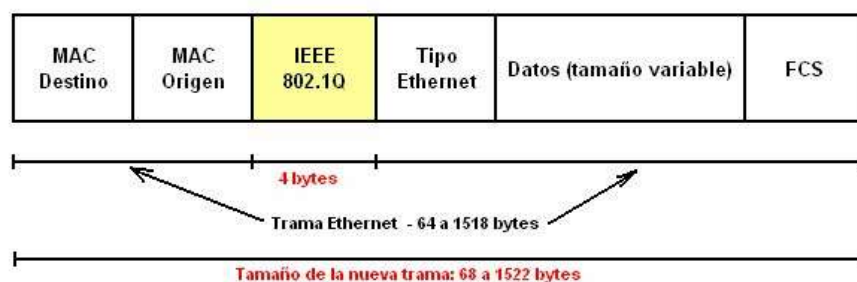
Su función principal es etiquetar las tramas Ethernet para indicar su pertenencia a una VLAN específica. Este protocolo establece las directrices que los puentes y conmutadores deben seguir para gestionar adecuadamente estas tramas etiquetadas.

Cada trama debe ser identificable como parte de una sola VLAN, y en caso de que una trama no contenga una etiqueta VLAN, se asume que pertenece a la VLAN nativa.

**Formato de la trama:**

802.1Q en realidad no encapsula la trama original sino que añade 4 bytes al encabezado Ethernet original. El valor del campo EtherType se cambia a 0x8100 para señalar el cambio en el formato de la trama.

ESTRUCTURA DE LA TRAMA IEEE 802.1Q



## Tipos de puerto en los switches

Existen dos tipos de puertos:

- **Puertos de acceso:** Se conectan las estaciones directamente. Mapean el puerto a una VLAN programada. Cuando entra una trama Ethernet se le añade el TAG de 802.1Q. Cuando sale una trama 802.1Q se le quita el TAG, para que llegue a la estación correspondiente con el formato IEEE 802.3 original.
- **Puertos 1Q Trunk:** Se utilizan para conectar Switches entre si y que pase el tráfico de diferentes VLANs a través de ellos. Las tramas que le llegan y que salen llevan el Tag 802.1Q.

- **VTP (VLAN Trunking Protocol)**

Es un protocolo utilizado en redes LAN para administrar VLANs de manera eficiente. Permite la propagación automática de información de VLAN entre switches. Los switches se agrupan en dominios VTP, lo que facilita la configuración centralizada de VLANs. Los switches en modo servidor pueden crear, modificar y eliminar VLANs, mientras que los switches en modo cliente reciben la información del servidor.

VTP utiliza anuncios periódicos para actualizar la información de VLAN, y los switches comparan la versión y el número de revisión para determinar si deben actualizar su configuración.

El protocolo se utiliza en conjunto con enlaces troncales, que permiten la comunicación de VLANs a través de varios switches, maximizando el uso del ancho de banda.

VTP también ofrece funciones de seguridad, como contraseñas de dominio y control de revisiones, para proteger la integridad de la configuración de VLAN.

- **Spanning Tree Protocol (STP)**

El Spanning Tree (STP) es un protocolo de red que evita bucles en topologías de red redundantes. Su función principal es garantizar que haya un solo camino activo entre los dispositivos de red, evitando así la congestión y los bucles que pueden causar pérdida de datos.

STP logra esto al seleccionar un dispositivo raíz en la red y calcular los caminos más cortos desde ese dispositivo a todos los demás dispositivos. Luego, STP bloquea los caminos redundantes para evitar bucles. Si ocurre una falla en el camino activo, STP rápidamente encuentra una ruta alternativa y desbloquea los puertos correspondientes para mantener la conectividad.

- **IPsec**

IPsec es un protocolo comúnmente utilizado en redes para garantizar la seguridad de las comunicaciones. Se combina frecuentemente con el protocolo de túnel de capa 2, el cual encapsula los paquetes de datos y crea un túnel seguro entre dos puntos de la red, proporcionando una capa adicional de seguridad.

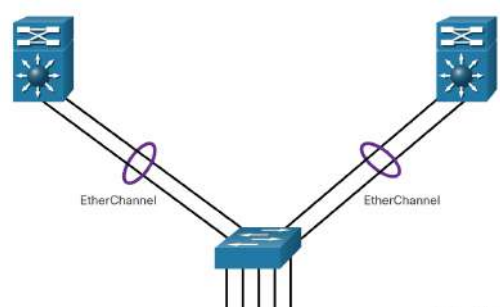
En el contexto de una VPN, el protocolo de túnel de capa 2 establece una conexión virtual entre los dispositivos de origen y destino, brindando seguridad en la comunicación. Al combinarse con IPsec, se obtiene una solución de seguridad sólida. IPsec autentica los dispositivos de la red, verificando su identidad antes de permitir la comunicación, y además cifra los datos transmitidos a través del túnel. Esto garantiza que sólo los dispositivos autorizados puedan acceder a la información y protege los datos contra accesos no autorizados.

La combinación de estos dos protocolos posibilita el establecimiento de conexiones seguras y privadas en una VPN, asegurando la integridad y confidencialidad de la información transmitida a través del túnel.

- **Port Channel o Link Aggregation (LACP)**

Es un estándar de red que permite combinar múltiples enlaces físicos en un único enlace lógico. Su objetivo es incrementar el ancho de banda y mejorar la disponibilidad de la conexión entre dispositivos de red.

Al agrupar enlaces físicos, se crea un enlace lógico con mayor capacidad de transmisión de datos. Esto proporciona un aumento significativo en el rendimiento de la red al permitir la distribución equitativa del tráfico entre los enlaces. Además, en caso de fallas en uno o más enlaces físicos, el tráfico se redirige automáticamente a los enlaces restantes, asegurando la continuidad de la conexión sin interrupciones.



#### **4.1.7. Direccionamiento IP**

Para el direccionamiento IP de la red de la empresa, hemos optado por utilizar direcciones IPv6, partiendo de un prefijo de red 2001:db8:1111::/64, el cual pertenece a una dirección de tipo global. En este enfoque, hemos dejado de lado el uso de direcciones ULA (Unique Local Addresses) para el desarrollo de este ciclo. La razón detrás de esta elección es que los equipos que vamos a implementar en la simulación no admiten NAT (Network Address Translation), lo cual impide la traducción de estas direcciones privadas a direcciones públicas, tal como se hace en IPv4.

Siguiendo esta configuración, hemos creado varias subredes para los diferentes departamentos de la empresa. En el switch de configuración interna, hemos asignado los departamentos de dirección, recursos humanos, contabilidad e informática a las VLANs 10, 20, 30 y 40, respectivamente, ubicados en el lado izquierdo del switch. Por otro lado, en el lado derecho del switch, se encuentran los departamentos de producción y diseño, asignados a las VLANs 50 y 60, respectivamente. Además, hemos configurado enlaces

troncales para permitir la comunicación entre estas VLANs y asegurar la conectividad interna de la red.

## RED LAN SEDE MADRID

Dirección de red : **2001:db8:1111::/64**

Dirección de subredes:

Departamento	ID VLAN	DIRECCIÓN DE RED
Dirección	Vlan 10	2001:db8:1111:10::/64 - 2001:db8:1111:10:3F:FFFF:FFFF:FFFF/ 64
Recursos humanos	Vlan 20	2001:db8:1111:20::/64 - 2001:db8:1111:20:7F:FFFF:FFFF:FFFF/ 64
Contabilidad	Vlan 30	2001:db8:1111:30::/64 -2001:db8:1111:30:BF:FFFF:FFFF:FFFF /64
Informática	Vlan 40	2001:db8:1111:40::/64 - 2001:db8:1111:40:FF:FFFF:FFFF:FFFF/ 64
Producción	Vlan 50	2001:db8:1111:50::/64 - 2001:db8:1111:50:3F:FFFF:FFFF:FFFF/ 64
Diseño	Vlan 60	2001:db8:1111:60::/64 - 2001:db8:1111:60:7F:FFFF:FFFF:FFFF/ 64
Servers Locales	Vlan 90	2001:db8:1111:90::/64- 2001:db8:1111:90:3F:FFFF:FFFF:FFFF/ 64
WIFI-Clientes	vlan 120	2001:db8:1111:120::/64 - 2001:db8:1111:120:3F:FFFF:FFFF:FFF F/64
WIFI-Empleados	vlan 110	2001:db8:1111:110::/64 - 2001:db8:1111:110:3F:FFFF:FFFF:FFFF /64

**EQUIPOS:**

Nombre Equipo	Dirección Ip	Interfaz	Gateway
ROUTER PRINCIPAL	2001:DB8:1111:1::1/64	G0/0/1	-
	2001:DB8:2::1/64	Se0/1/0	INTERNET
	2001:DB8:6::1/64	G0/0/0	-
	2001:DB8:1111:10::1/64	G0/0/1.10	-
	2001:DB8:1111:20::1/64	G0/0/1.20	-
	2001:DB8:1111:30::1/64	G0/0/1.30	-
	2001:DB8:1111:40::1/64	G0/0/1.40	-
	2001:DB8:1111:50::1/64	G0/0/1.50	-
	2001:DB8:1111:60::1/64	G0/0/1.60	-
	2001:DB8:1111:90::1/64	G0/0/1.90	-
	2001:DB8:1111:110::1/64	G0/0/1.110	-
	2001:DB8:1111:120::1/64	G0/0/1.120	
Servidor-web-intranet	2001:DB8:1111:70::10/64	fa0/2	2001:DB8:1111:70::1/64
switch-central		gig3/1	
switch-central		gig2/1	
switch-central		gig1/1	
switch-central		gig6/1	
switch-central		gig7/1	
switch-central		gig8/1	
switch-DRCI		gig0/1	
switch-DRCI		gig0/2	
switch-DRCI		fa0/23	
switch-DRCI		fa0/24	
switch-DIS-PD		gig0/1	
switch-DIS-PD		gig0/2	

Dirección	2001:DB8:1111:10::1-5/64	fa0/11-14	2001:DB8:1111:10::1/64
RRHH	2001:DB8:1111:20::1-5/64	fa0/6-10	2001:DB8:1111:20::1/64
Contabilidad	2001:DB8:1111:30::1-7/64	fa0/2-5	2001:DB8:1111:30::1/64
Informática	2001:DB8:1111:40::1-5/64	fa0/15-19	2001:DB8:1111:40::1/64
Diseño	2001:DB8:1111:50::1-10/64	fa0/17-22	2001:DB8:1111:50::1/64
Producción	2001:DB8:1111:60::1-15/64	fa0/1-16	2001:DB8:1111:60::1/64
WIFI-EMPLEADOS	2001:DB8:1111:110::1-7/64		2001:DB8:1111:110::1/64
WIFI-INVITADOS	2001:DB8:1111:120::1-7/64		2001:DB8:1111:120::1/64

Además se asignan direcciones ip fijas para los servidores :

#### **Servidor-web-intranet**

2001:DB8:1111:90::11/64

#### **Servidor dns**

2001:DB8:1111:90::10/64

#### **Servidor web,dns,**

2001:DB8:6::10/64

### **Empleado Casa**

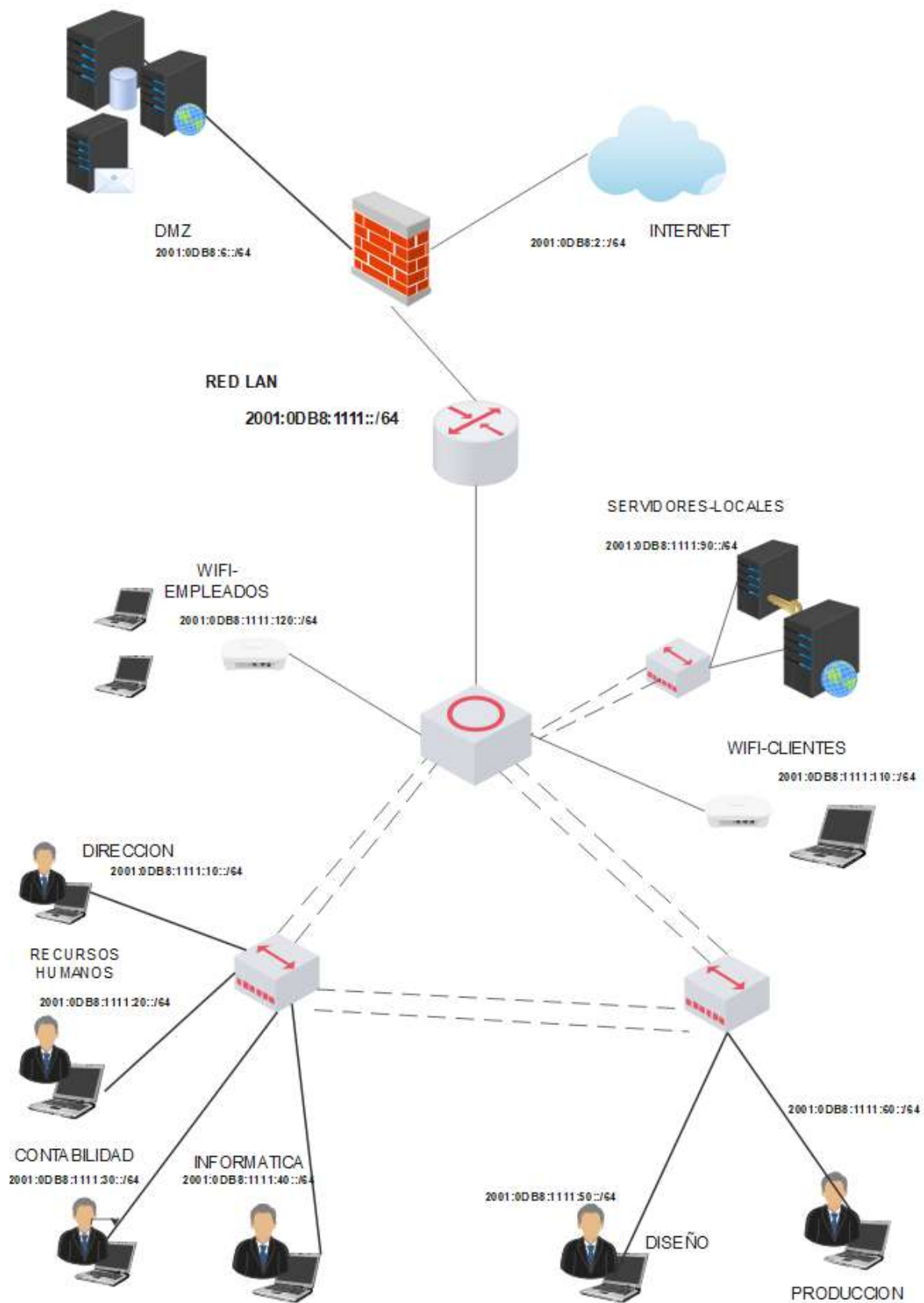
Nombre Equipo	Dirección Ip	Interfaz	Gateway
Router_VPN	2001:0db8:2222::1/64 192.168.1.1	Gig0/0/0	ND 192.168.1.1
	2001:0db8:02::1/64 72.44.20.0/28	Gig0/0/1	ND
Laptop-Empleado	2001:0db8:2222::10/64 192.168.1.10	NIC	2001:0db8:2222::1

### **4.1.8. Esquemas**

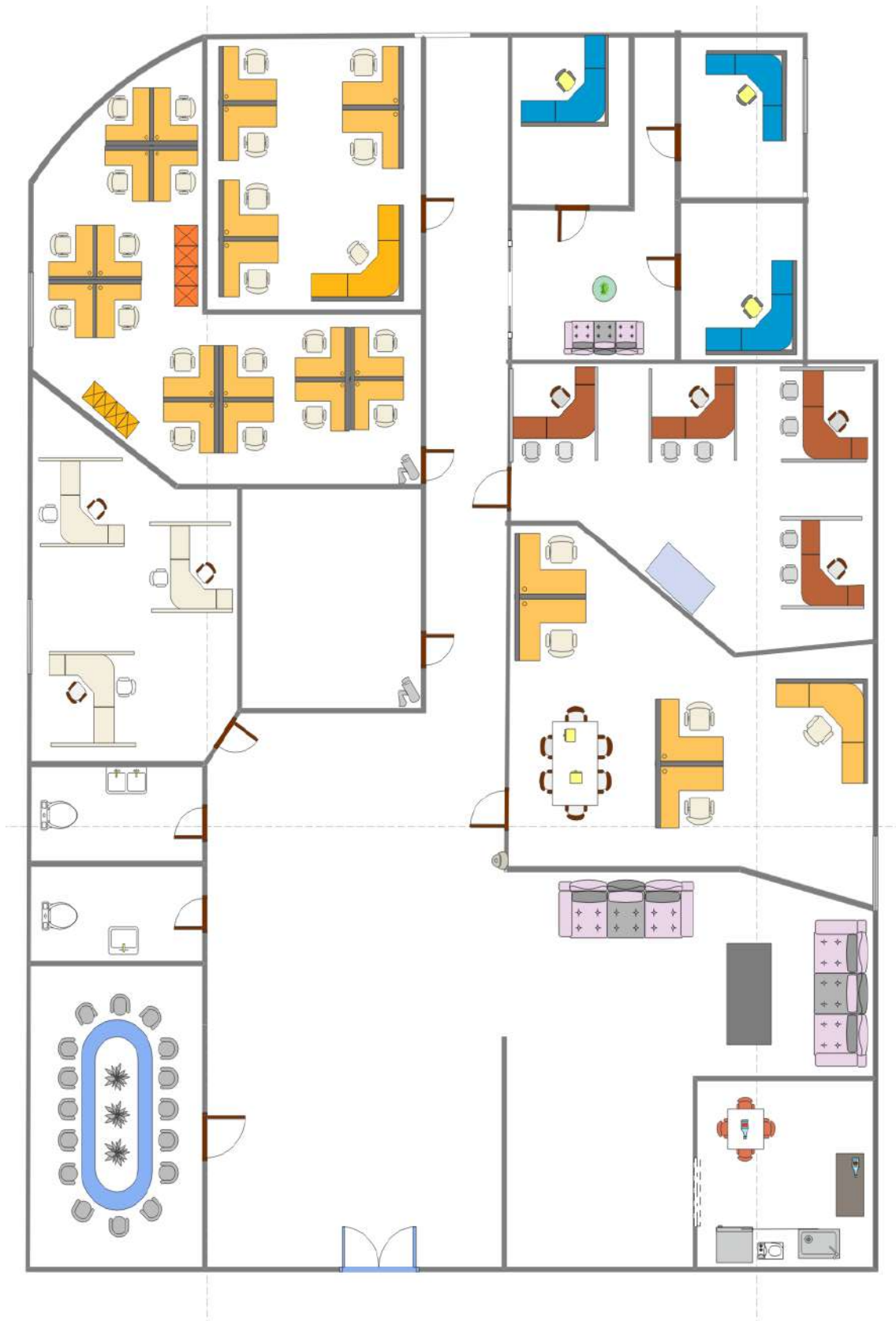
El diseño de la red ha sido visualizado en un diagrama detallado que muestra la interconexión de los diferentes componentes y el flujo del tráfico en la red. Este diagrama facilita la comprensión de la estructura de la red y la ubicación de los dispositivos clave.



#### 4.1.8.1. Esquema Lógico



#### 4.1.8.2. Esquema Físico



## 4.2. Pruebas y funcionamiento de equipos

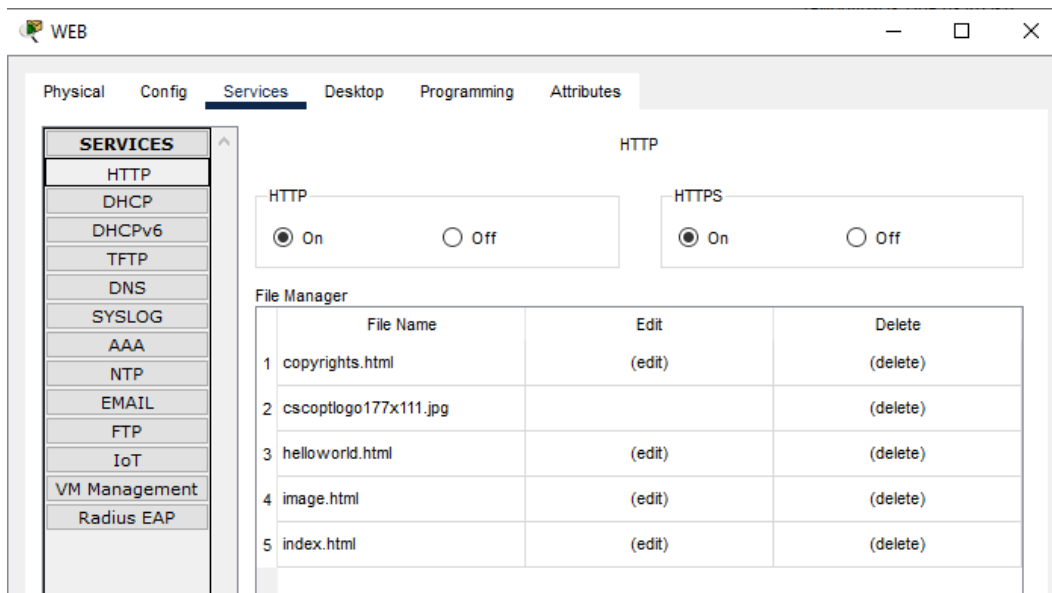
### 4.2.1. Configuración Zona Desmilitarizada (DMZ)

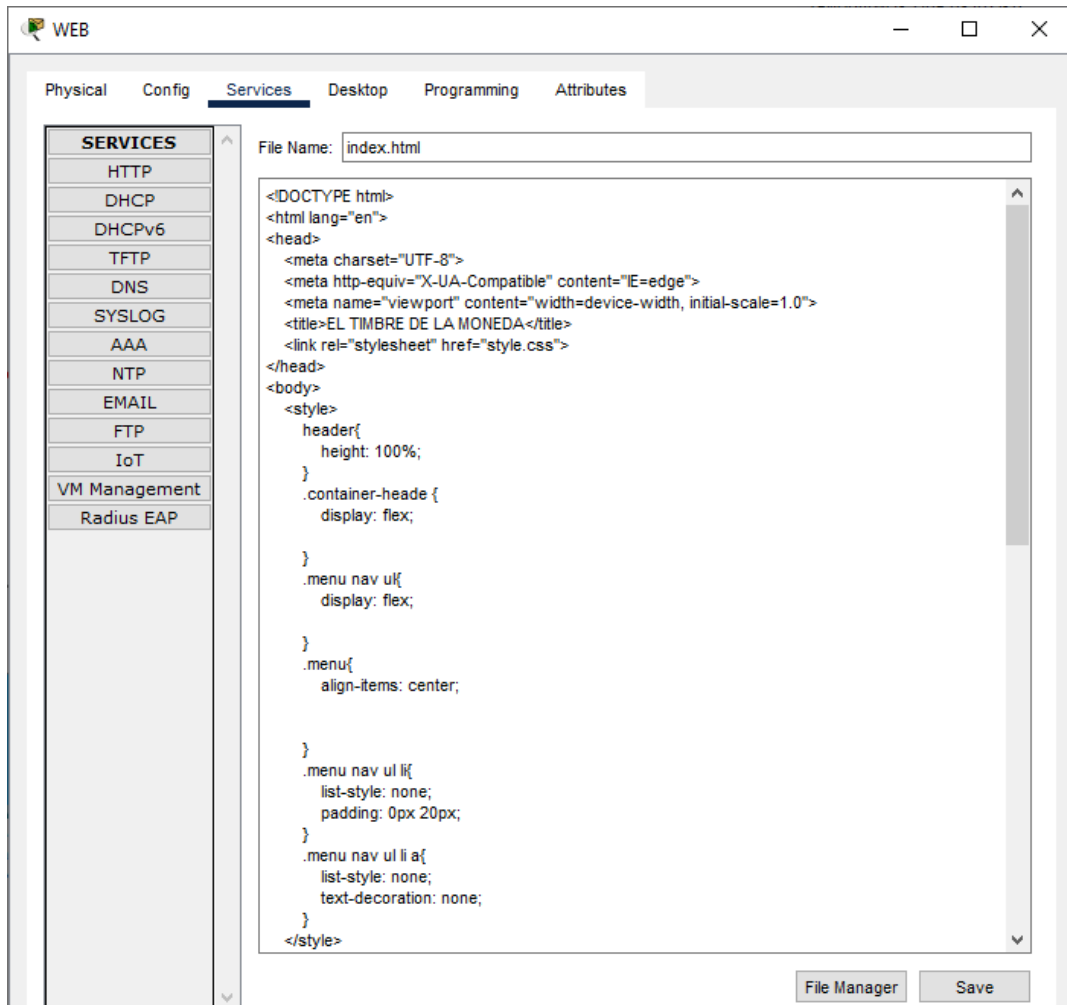
En nuestro caso tenemos incorporado como firewall el router directamente donde solo tenemos que incorporar listas de control con esto tenemos un control mejor de que queremos que entre y que salga de nuestra red LAN

### 4.2.2. Configuración WEB y DNS

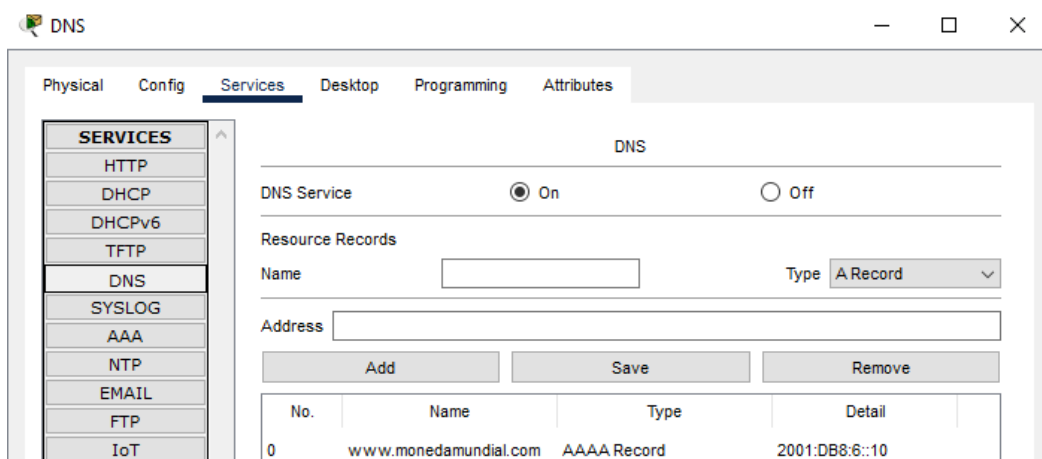
En el servidor web de la DMZ, simplemente debemos activar el servicio HTTP o HTTPS. Luego, incluimos el archivo index.html, que contiene la página web que deseamos mostrar. Dado que solo queremos tener esta página en la DMZ, nos aseguramos de que esté correctamente configurada.

index.html





ahora tenemos que configurar el servidor DNS para que sepa a donde tenemos nuestro servidor web y el nombre de nuestra página web



ahora comprobamos lo que tenemos en la página web en la DMZ que será para el resto del mundo que puede acceder



y en el caso de la página web para la red que sería la *intranet de la empresa*



#### 4.2.3. Configuración DHCP

La configuración del DHCP en el router se divide en diferentes bloques para cada VLAN. Cada bloque tiene la siguiente estructura:

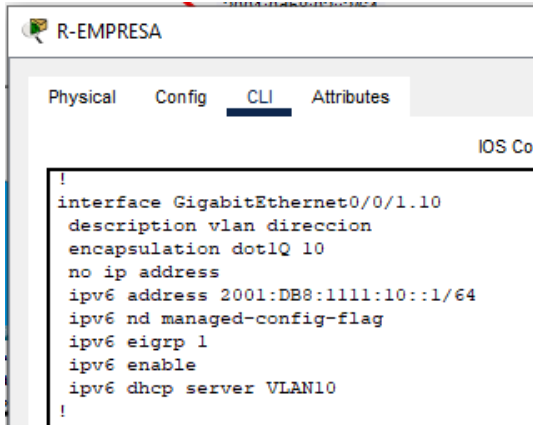
- **ipv6 dhcp pool VLANX:** Define el pool de direcciones para la VLAN X, donde X es el número de la VLAN.
- **address prefix 2001:0db8:1111:X::/64:** Especifica el rango de direcciones IPv6 asignadas a la VLAN X.
- **lifetime 172800 86400:** Establece los tiempos de vigencia (lifetime) de las direcciones asignadas.
- **dns-server 2001:DB8:1111:90::10:** Configura el servidor DNS para la VLAN X.
- **domain-name monedamundial.com:** Establece el nombre de dominio para la VLAN X.

Además de la configuración del DHCP, se han creado subinterfaces vti (interfaz de túnel virtual) para cada VLAN y se les ha asignado el correspondiente pool de direcciones para actuar como servidor DHCP en el router.

Estas subinterfaces vti se han configurado de la siguiente manera:

- **interfaz GigabitEthernet0/0/1.X:** Se han creado subinterfaces vti en el puerto GigabitEthernet0/0/1 para cada VLAN X, donde X representa el número de la VLAN.
- **encapsulation dot1Q X:** Se ha especificado la etiqueta VLAN X en la subinterfaz vti.
- **no ip address:** Se ha eliminado la configuración de dirección IPv4 en las subinterfaces vti.
- **ipv6 address 2001:DB8:1111:X::1/64:** Se ha asignado una dirección IPv6 a la subinterfaz vti para la VLAN X.
- **ipv6 dhcp server VLANX:** Se ha habilitado la funcionalidad de servidor DHCP en la subinterfaz vti para la VLAN X.

Con esta configuración, las subinterfaces vti actúan como servidores DHCP para sus respectivas VLAN, asignando direcciones IPv6 a los dispositivos conectados a esas VLAN. Cada subinterfaz vti tiene su propio pool de direcciones IPv6 definido en la configuración del DHCP.



```
!
interface GigabitEthernet0/0/1.10
description vlan direccion
encapsulation dot1Q 10
no ip address
ipv6 address 2001:DB8:1111:10::1/64
ipv6 nd managed-config-flag
ipv6 eigrp 1
ipv6 enable
ipv6 dhcp server VLAN10
!

interface GigabitEthernet0/0/1.20
description vlan RRHH
encapsulation dot1Q 20
no ip address
ipv6 address 2001:DB8:1111:20::1/64
ipv6 nd managed-config-flag
ipv6 enable
ipv6 dhcp server VLAN20
!
```

```

interface GigabitEthernet0/0/1.20
description vlan RRHH
encapsulation dot1Q 20
no ip address
ipv6 address 2001:DB8:1111:20::1/64
ipv6 nd managed-config-flag
ipv6 enable
ipv6 dhcp server VLAN20
!

interface GigabitEthernet0/0/1.30
description vlan contabilidad
encapsulation dot1Q 30
no ip address
ipv6 address 2001:DB8:1111:30::1/64
ipv6 nd managed-config-flag
ipv6 enable
ipv6 dhcp server VLAN30
!

interface GigabitEthernet0/0/1.40
description vlan informatica
encapsulation dot1Q 40
no ip address
ipv6 address 2001:DB8:1111:40::1/64
ipv6 nd managed-config-flag
ipv6 enable
ipv6 dhcp server VLAN40
!

interface GigabitEthernet0/0/1.50
description vlan disenio
encapsulation dot1Q 50
no ip address
ipv6 address 2001:DB8:1111:50::1/64
ipv6 nd managed-config-flag
ipv6 enable
ipv6 dhcp server VLAN50
!

interface GigabitEthernet0/0/1.60
description vlan produccion
encapsulation dot1Q 60
no ip address
ipv6 address 2001:DB8:1111:60::1/64
ipv6 nd managed-config-flag
ipv6 enable
ipv6 dhcp server VLAN60
!

interface GigabitEthernet0/0/1.90
encapsulation dot1Q 90
no ip address
ipv6 address 2001:DB8:1111:90::1/64
ipv6 nd managed-config-flag
ipv6 enable
!

```

```

interface GigabitEthernet0/0/1.110
description vlan-wifi-empleados
encapsulation dot1Q 110
no ip address
ipv6 address 2001:DB8:1111:110::1/64
ipv6 nd managed-config-flag
ipv6 enable
ipv6 dhcp server VLAN110
!

interface GigabitEthernet0/0/1.120
description vlan-wifi-empleados
encapsulation dot1Q 120
no ip address
ipv6 address 2001:DB8:1111:120::1/64
ipv6 nd managed-config-flag
ipv6 enable
ipv6 dhcp server VLAN120
!

```

Además de la configuración anterior, es importante revisar qué configuración DHCP se ha aplicado en cada subred de las VLAN que se han creado.

```

ipv6 dhcp pool VLAN10
address prefix 2001:0db8:1111:10::/64 lifetime 172800 86400
dns-server 2001:DB8:1111:90::10
domain-name monedamundial.com
!

ipv6 dhcp pool VLAN20
address prefix 2001:0db8:1111:20::/64 lifetime 172800 86400
dns-server 2001:DB8:1111:90::10
domain-name monedamundial.com
!

ipv6 dhcp pool VLAN30
address prefix 2001:0db8:1111:30::/64 lifetime 172800 86400
dns-server 2001:DB8:1111:90::10
domain-name monedamundial.com
!

ipv6 dhcp pool VLAN40
address prefix 2001:0db8:1111:40::/64 lifetime 172800 86400
dns-server 2001:DB8:1111:90::10
domain-name monedamundial.com
!

ipv6 dhcp pool VLAN50
address prefix 2001:0db8:1111:50::/64 lifetime 172800 86400
dns-server 2001:DB8:1111:90::10
domain-name monedamundial.com
!

ipv6 dhcp pool VLAN60
address prefix 2001:0db8:1111:60::/64 lifetime 172800 86400
dns-server 2001:DB8:1111:90::10
domain-name monedamundial.com
!

```



```

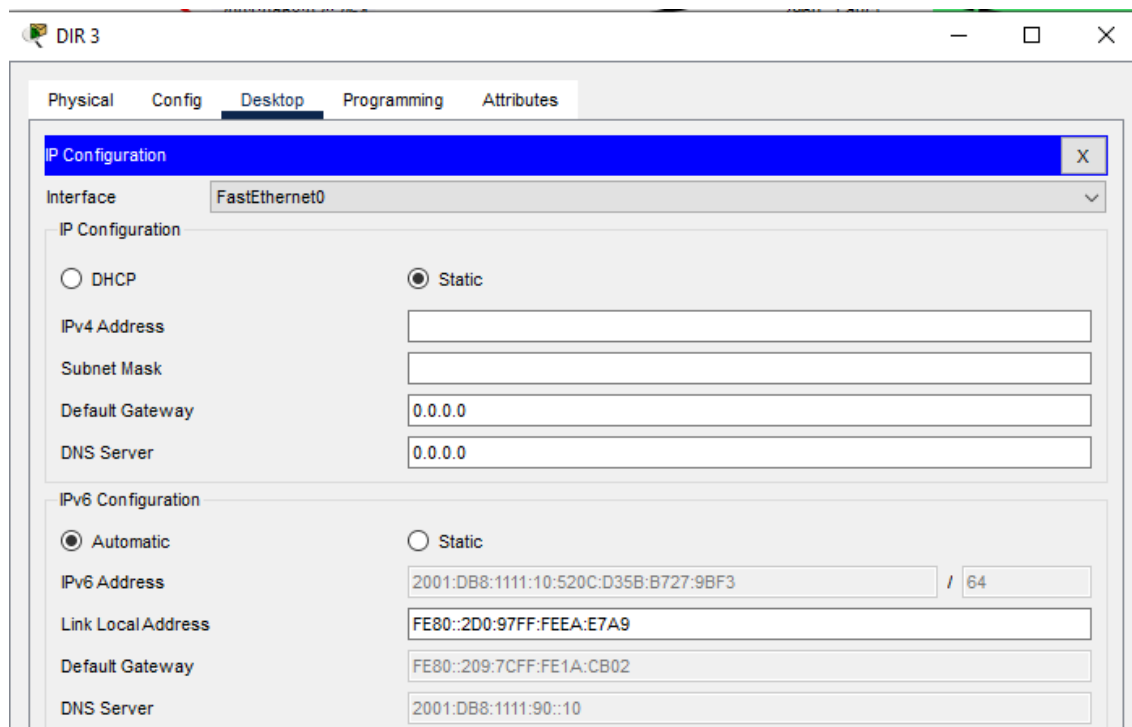
ipv6 dhcp pool VLAN110
 address prefix 2001:0db8:1111:110::/64 lifetime 172800 86400
 dns-server 2001:DB8:1111:90::10
 domain-name monedamundial.com
!

ipv6 dhcp pool VLAN120
 address prefix 2001:0db8:1111:120::/64 lifetime 172800 86400
 dns-server 2001:DB8:1111:90::10
 domain-name monedamundial.com

```

**Para verificar** si los dispositivos en cada departamento tienen una dirección IP asignada, necesitaríamos acceder a cada dispositivo individualmente y verificar su configuración de red.

### Dirección



## Recursos Humanos

RRHH 3

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address

Subnet Mask

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☒ Automatic ☐ Static

IPv6 Address 2001:DB8:1111:20:4308:EF8B:B5C5:A823 / 64

Link Local Address FE80::2D0:FFFF:FE5B:606D

Default Gateway FE80::209:7CFF:FE1A:CB02

DNS Server 2001:DB8:1111:90::10

## Contabilidad

CONT 1

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address

Subnet Mask

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☒ Automatic ☐ Static

IPv6 Address 2001:DB8:1111:30:A2CB:8697:7805:7805 / 64

Link Local Address FE80::201:63FF:FEA6:6162

Default Gateway FE80::209:7CFF:FE1A:CB02

DNS Server 2001:DB8:1111:90::10

## Informática

INF 3

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address

Subnet Mask

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☒ Automatic ☐ Static

IPv6 Address 2001:DB8:1111:40:85E3:3FF9:13C5:522 / 64

Link Local Address FE80::202:17FF:FE4C:67BE

Default Gateway FE80::209:7CFF:FE1A:CB02

DNS Server 2001:DB8:1111:90::10

## Diseño

DISEÑO 4

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address

Subnet Mask

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☒ Automatic ☐ Static

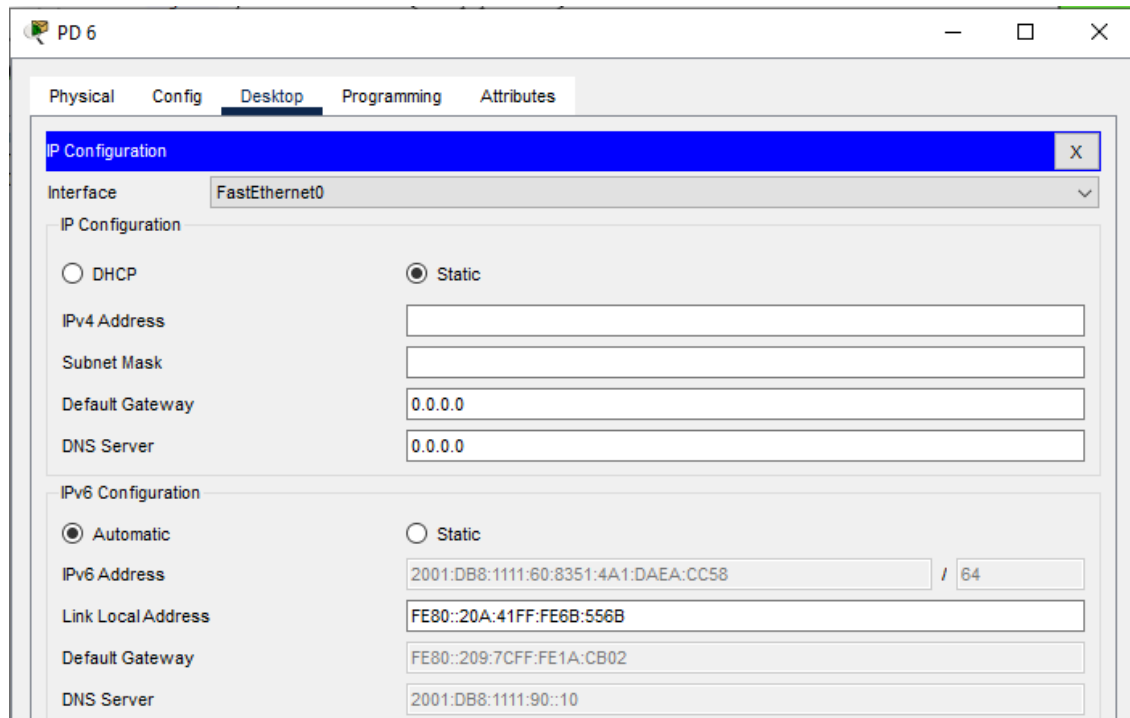
IPv6 Address 2001:DB8:1111:50:84A7:E9C2:BF0C:A17A / 64

Link Local Address FE80::209:7CFF:FECA:D388

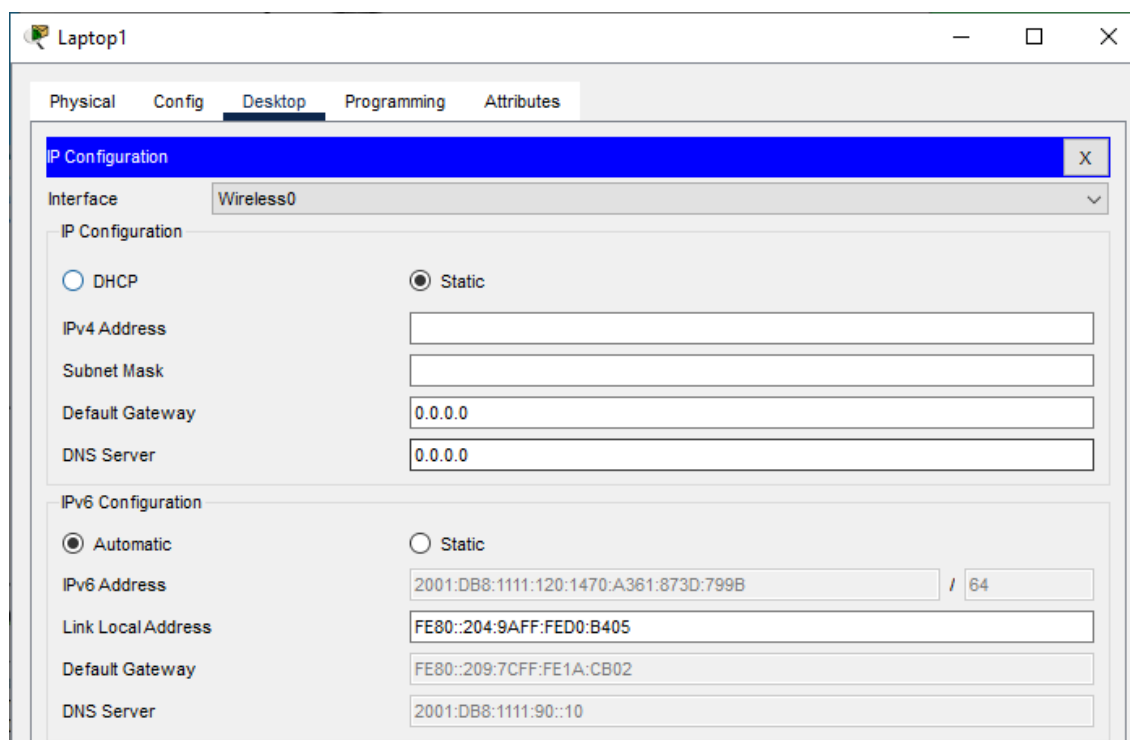
Default Gateway FE80::209:7CFF:FE1A:CB02

DNS Server 2001:DB8:1111:90::10

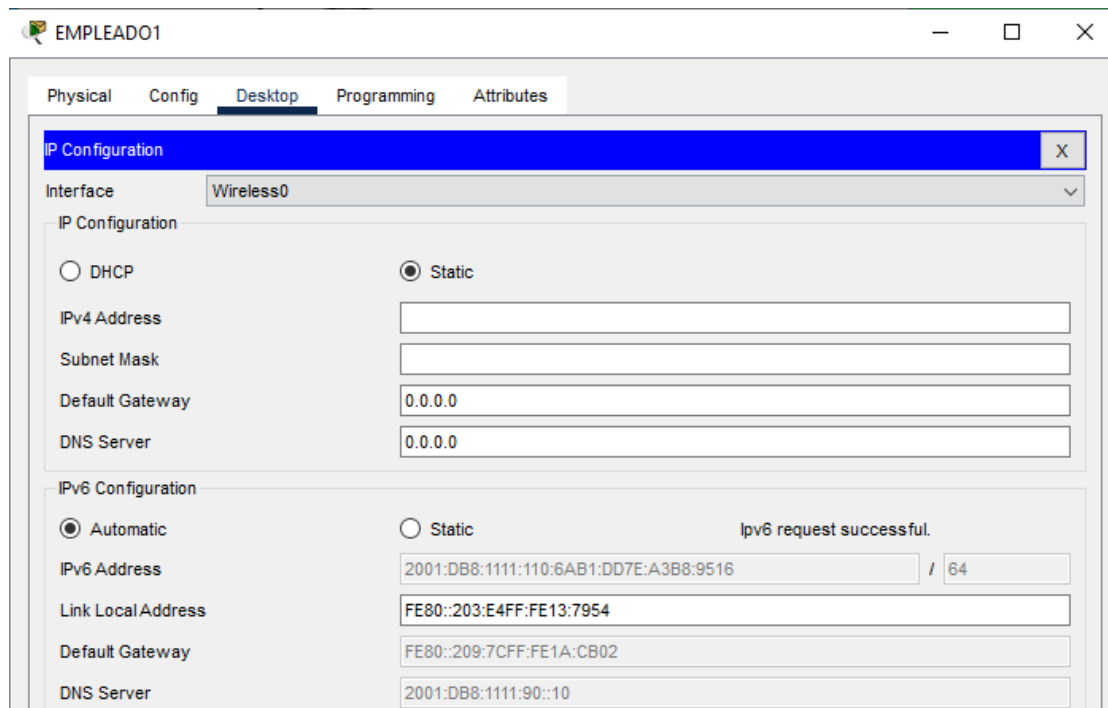
## Producción



## wifi-invitados



## wifi-empleados



### 4.2.4. Configuración de Access-point-PT

Para la configuración del Wi-Fi de empleados e invitados, se han creado dos VLAN correspondientes.

#### **VLAN de Wi-Fi de empleados (VLAN 110):**

- Se ha creado una subinterfaz en el puerto GigabitEthernet0/0/1.110 para la VLAN de Wi-Fi de empleados
- Se ha establecido el encapsulamiento dot1Q para asignar la VLAN 110 a la subinterfaz.
- Se ha habilitado IPv6 en la subinterfaz.
- Se ha configurado el servidor DHCPv6 para la VLAN de Wi-Fi de empleados (VLAN 110).

#### **VLAN de Wi-Fi de invitados (VLAN 120):**

- Se ha creado una subinterfaz en el puerto GigabitEthernet0/0/1.120 para la VLAN de Wi-Fi de empleados.
- Se ha establecido el encapsulamiento dot1Q para asignar la VLAN 120 a la subinterfaz.
- Se ha habilitado IPv6 en la subinterfaz.
- Se ha configurado el servidor DHCPv6 para la VLAN de Wi-Fi de invitados (VLAN 120).

Además, se ha configurado el cifrado **WPA2-PSK** (Wi-Fi Protected Access 2 - Pre-Shared Key) con una contraseña sencilla para ambas redes Wi-Fi de invitados y empleados.

The screenshot shows the 'WIFI-EMPLEADOS' configuration window. The 'Config' tab is active. On the left, under 'INTERFACE', 'Port 1' is selected. The main area shows settings for 'Port 1':

- Port Status: ☒ On
- SSID: WIFI-EMPLEADOS
- 2.4 GHz Channel: 6
- Coverage Range (meters): 140,00
- Authentication: ☒ WPA2-PSK (Other options: Disabled, WEP, WPA-PSK)
- WEP Key: (empty field)
- PSK Pass Phrase: 12345678
- User ID: (empty field)
- Password: (empty field)
- Encryption Type: AES

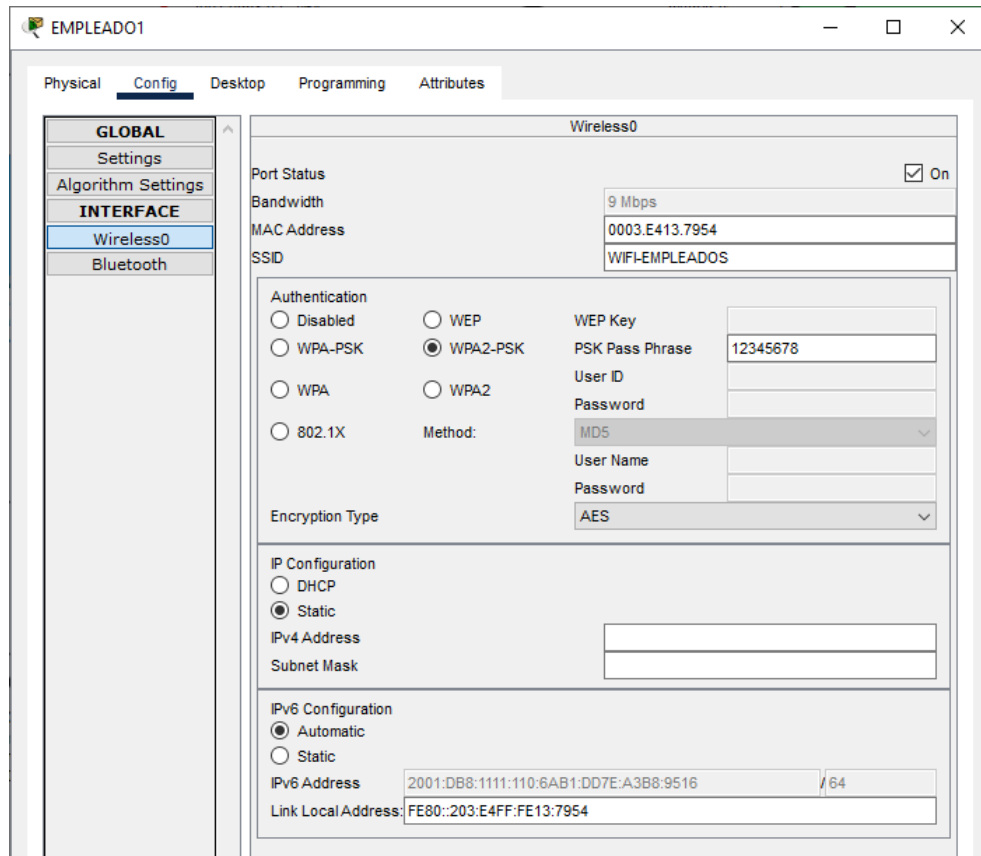
wifi empleados sería lo mismo

The screenshot shows the 'WIFI-CLIENTES' configuration window. The 'Config' tab is active. On the left, under 'INTERFACE', 'Port 1' is selected. The main area shows settings for 'Port 1':

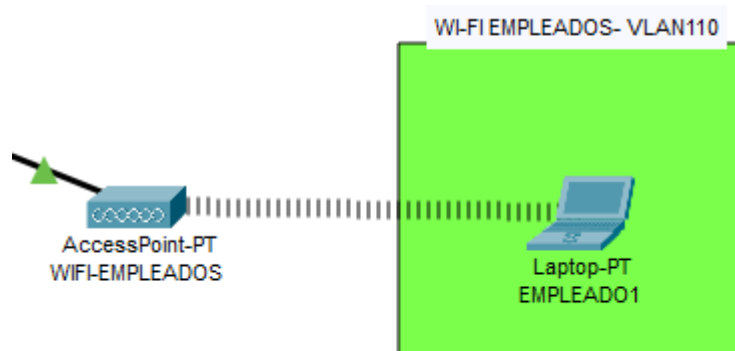
- Port Status: ☒ On
- SSID: WIFI-INVITADOS
- 2.4 GHz Channel: 6
- Coverage Range (meters): 140,00
- Authentication: ☒ WPA2-PSK (Other options: Disabled, WEP, WPA-PSK)
- WEP Key: (empty field)
- PSK Pass Phrase: 12345678
- User ID: (empty field)
- Password: (empty field)
- Encryption Type: AES

## PRUEBAS

Y en el equipo configuramos el SSID el nombre del wifi y introducimos la contraseña del wifi que queremos establecer conexión que es nuestro caso sería WIFI-EMPLEADOS



Se configuran los portátiles añadiéndoles el módulo de acceso inalámbrico a la red y con esto tenemos ya la conexión



#### 4.2.5. Configuración de redes virtuales (VLAN)

En nuestra empresa, hemos implementado la configuración de redes virtuales (VLAN) como parte de nuestras medidas de seguridad para separar y proteger los diferentes departamentos. Cada departamento tiene asignada su propia VLAN, lo que nos permite realizar una gestión más eficiente de nuestra red

A continuación, se detallan las subredes asignadas a cada departamento, junto con las direcciones IP correspondientes:

##### SEDE MADRID

Departamento	ID VLAN	DIRECCIÓN DE RED
Dirección	Vlan 10	2001:db8:1111:10::/64 - 2001:db8:1111:10:3F:FFFF:FFFF:FFFF/64
Recursos humanos	Vlan 20	2001:db8:1111:20::/64 - 2001:db8:1111:20:7F:FFFF:FFFF:FFFF/64
Contabilidad	Vlan 30	2001:db8:1111:30::/64 -2001:db8:1111:30:BF:FFFF:FFFF:FFFF/64
Informática	Vlan 40	2001:db8:1111:40::/64 - 2001:db8:1111:40:FF:FFFF:FFFF:FFFF/64
Producción	Vlan 50	2001:db8:1111:50::/64 - 2001:db8:1111:50:3F:FFFF:FFFF:FFFF/64
Diseño	Vlan 60	2001:db8:1111:60::/64 - 2001:db8:1111:60:7F:FFFF:FFFF:FFFF/64
Servers Locales	Vlan 90	2001:db8:1111:90::/64 - 2001:db8:1111:90:3F:FFFF:FFFF:FFFF/64
WIFI-Clientes	vlan 120	2001:db8:1111:120::/64 - 2001:db8:1111:120:3F:FFFF:FFFF:FFFF/64
WIFI-Empleados	vlan 110	2001:db8:1111:110::/64 - 2001:db8:1111:110:3F:FFFF:FFFF:FFFF/64

Estas subredes se configurarán como subinterfaces virtuales en la interfaz física que conecta el switch principal con el router, estableciendo una conexión troncal.

La distribución de las VLANs en los switches se realizará de la siguiente manera:

- los equipos de los departamentos de dirección, recursos humanos, contabilidad e informática se conectarán **al switch lateral izquierdo**

##### Configuración de interfaces:

- VLAN 10: FastEthernet0/11-14 (modo acceso)
- VLAN 20: FastEthernet0/6-10 (modo acceso)
- VLAN 30: FastEthernet0/2-5 (modo acceso)
- VLAN 40: FastEthernet0/15-19 (modo acceso)



- VLAN 100 (trunk):  
FastEthernet0/23-24 (modo trunk, agrupados en canal 3)  
GigabitEthernet0/1-2 (modo trunk, agrupados en canal 1)

```

Switch>en
Switch#show vlan brief

```

VLAN Name	Status	Ports
1 default	active	Po4, Fa0/1, Fa0/20, Fa0/21 Fa0/22
10 direccion	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14
20 rrhh	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10
30 contabilidad	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5
40 informatica	active	Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19
50 disenio	active	
60 produccion	active	
90 servidores-madrid	active	
100 troncal	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```

Switch#

```

- mientras que los del departamento de producción y diseño se conectarán al **switch lateral derecho**.

### Configuración de interfaces:

VLAN 50:FastEthernet0/17-22 (modo acceso)

VLAN 60:FastEthernet0/1-16 (modo acceso)

VLAN 100 (trunk):

FastEthernet0/23-24 (modo trunk, agrupados en canal 3)

GigabitEthernet0/1-2 (modo trunk, agrupados en canal 2)

DIS-PD

Physical Config CLI Attributes

IOS Command Line Interface

Press RETURN to get started.

Switch>EN  
Switch#SHOW VLAN BRIEF

VLAN	Name	Status	Ports
1	default	active	
10	direccion	active	
20	rrhh	active	
30	contabilidad	active	
40	informatica	active	
50	diseño	active	Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22
60	produccion	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16
90	servidores-madrid	active	
100	troncal	active	
1002	fdi-default	active	
1003	token-ring-default	active	
1004	fdinet-default	active	
1005	trnet-default	active	

Switch#

- El switch principal será el punto central que contendrá todas las VLANs.

SW-CENTRAL-MADRID

Physical Config CLI Attributes

IOS Command Line Interface

SW-CENTRAL-MADRID con0 is now available

Press RETURN to get started.

SW-CENTRAL-MADRID>EN  
SW-CENTRAL-MADRID#SHOW VLAN BRIEF

VLAN	Name	Status	Ports
1	default	active	Gig9/1
10	direccion	active	
20	rrhh	active	
30	contabilidad	active	
40	informatica	active	
50	diseño	active	
60	produccion	active	
90	servidores-madrid	active	
100	troncal	active	
110	wifi-empleados	active	Gig7/1
120	wifi-invitados	active	Gig8/1
1002	fdi-default	active	
1003	token-ring-default	active	
1004	fdinet-default	active	
1005	trnet-default	active	

SW-CENTRAL-MADRID#

Además, se configurarán enlaces troncales desde los switches laterales hacia el switch principal, garantizando así la conectividad interna de la red y permitiendo la comunicación entre las distintas VLANs.

```
SW-CENTRAL-MADRID>EN
SW-CENTRAL-MADRID#SHOW INTERFACES TRUNK
Port      Mode      Encapsulation  Status      Native vlan
-----
Po1       on        802.1q         trunking    100
Po2       on        802.1q         trunking    100
Po4       on        802.1q         trunking    100
Gig0/1    on        802.1q         trunking    100

Port      Vlans allowed on trunk
-----
Po1       10,20,30,40,50,60,90,100
Po2       10,20,30,40,50,60,90,100
Po4       10,20,30,40,50,60,90,100
Gig0/1    1-1005

Port      Vlans allowed and active in management domain
-----
Po1       10,20,30,40,50,60,90,100
Po2       10,20,30,40,50,60,90,100
Po4       10,20,30,40,50,60,90,100
Gig0/1    1,10,20,30,40,50,60,90,100,110,120

Port      Vlans in spanning tree forwarding state and not pruned
-----
Po1       10,20,30,40,50,60,90,100
Po2       10,20,30,40,50,60,90,100
Po4       10,20,30,40,50,60,90,100
Gig0/1    1,10,20,30,40,50,60,90,100,110,120

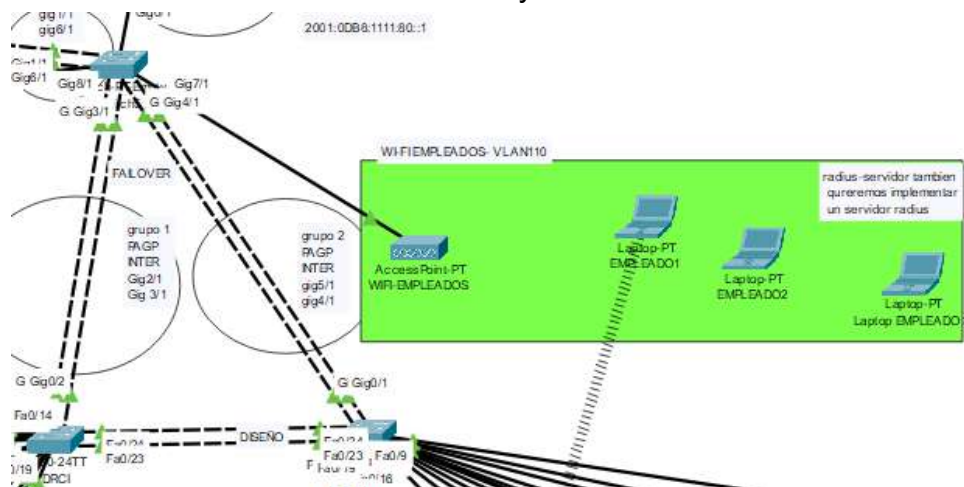
SW-CENTRAL-MADRID#
```

Esta configuración nos permite mantener una segmentación efectiva de nuestra red, mejorando la seguridad y el rendimiento. Al asignar VLANs dedicadas a cada departamento, podemos controlar el tráfico de red de manera más precisa y reducir la posibilidad de accesos no autorizados.

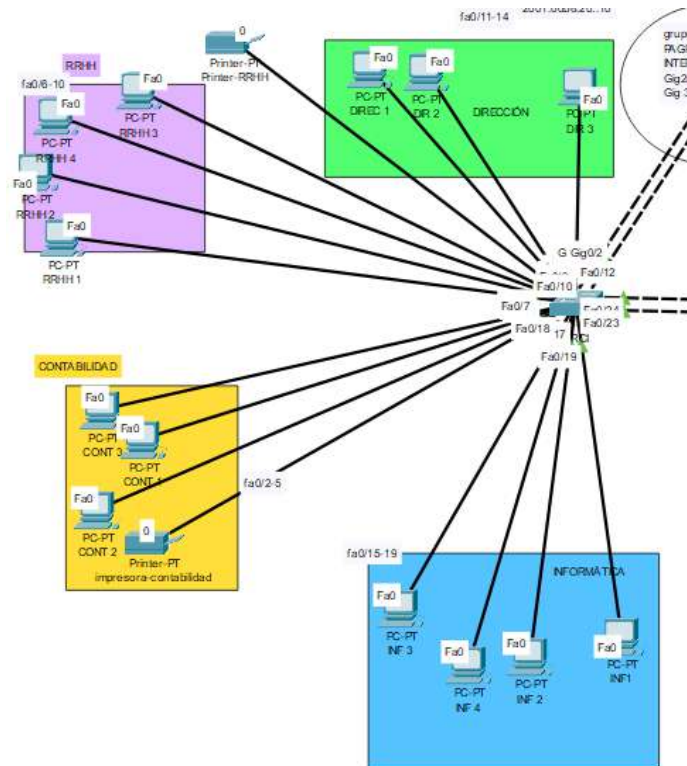
#### 4.2.6. Configuración Ethernet Channel

Para el uso de este protocolo hemos incluido el Ethernet Channel para la redundancia en nuestros switch y el nuevo mecanismo de aumentar el ancho de banda.

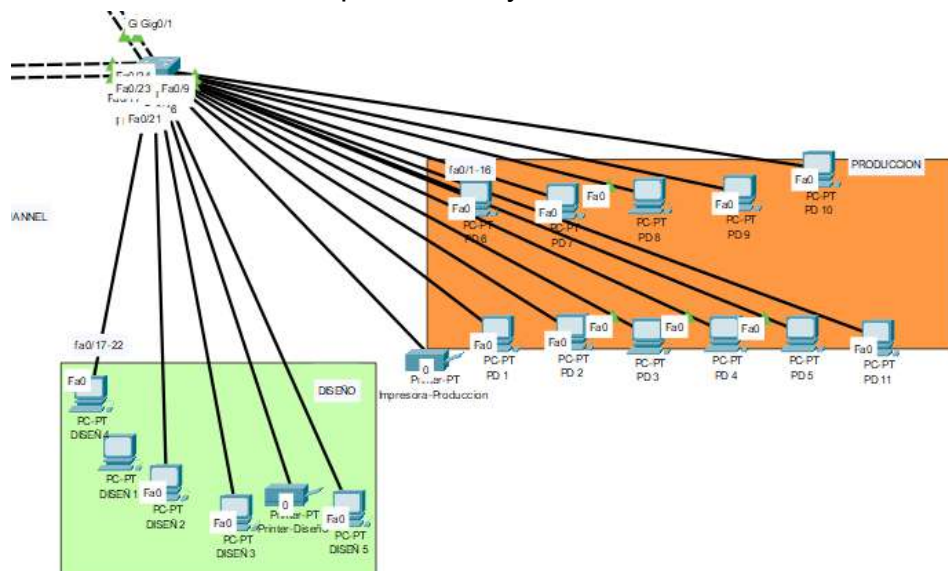
Hemos incluido 4 canales LACP para esta configuración donde tenemos un switch central donde solo esta conectado los switch y ademas el wifi



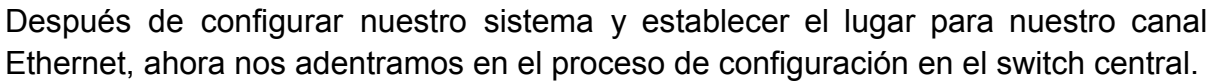
Otro switch donde tenemos los departamentos de dirección,rrhh,contabilidad y informática.



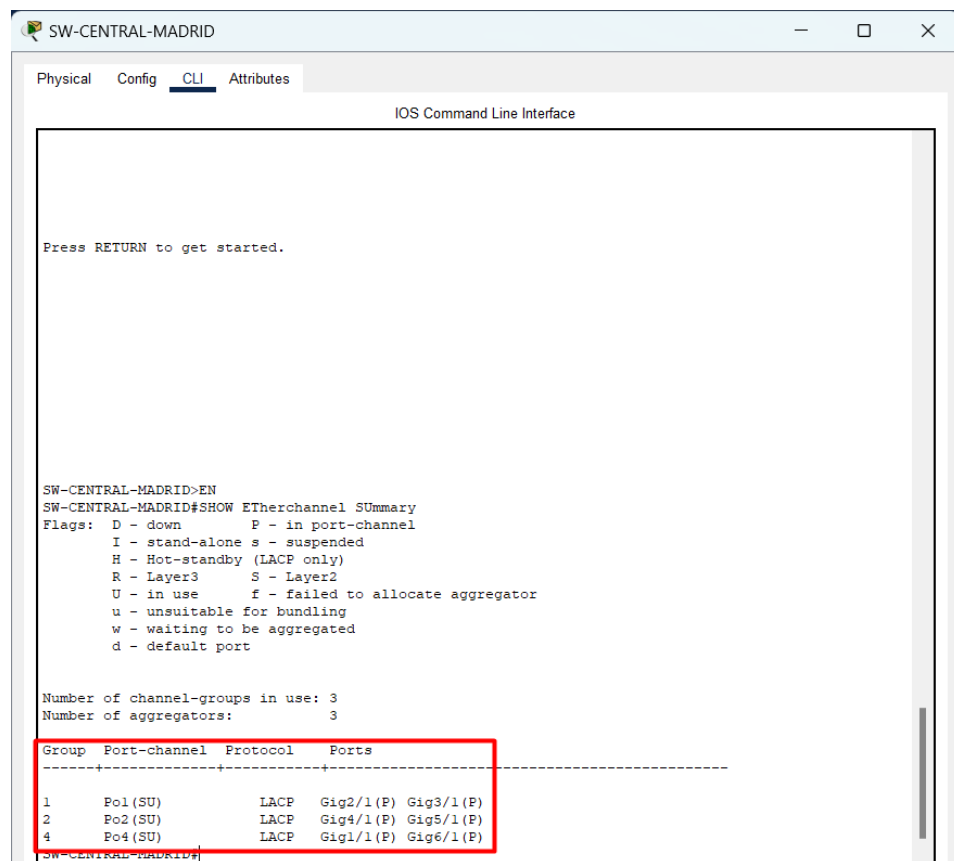
en el otro switch tenemos producción y diseño



\_\_\_\_\_

SW-CENTRAL-MADRID

y para ver el/los canal que hemos creado utilizamos el comando **Show etherchannel Summary**



```
SW-CENTRAL-MADRID>EN
SW-CENTRAL-MADRID#SHOW ETHERchannel Summary
Flags: D - down          P - in port-channel
       I - stand-alone  S - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 3
Number of aggregators:          3

Group  Port-channel  Protocol    Ports
-----
1      Po1 (SU)         LACP       Gig2/1 (P) Gig3/1 (P)
2      Po2 (SU)         LACP       Gig4/1 (P) Gig5/1 (P)
4      Po4 (SU)         LACP       Gig1/1 (P) Gig6/1 (P)
```

\_\_\_\_\_



para saber el **ancho de banda** que tenemos por ejemplo en una conexión como por ejemplo en el gig2/1 que es el grupo 1 y tenemos 1000 Mb/s es decir 1Gbps.





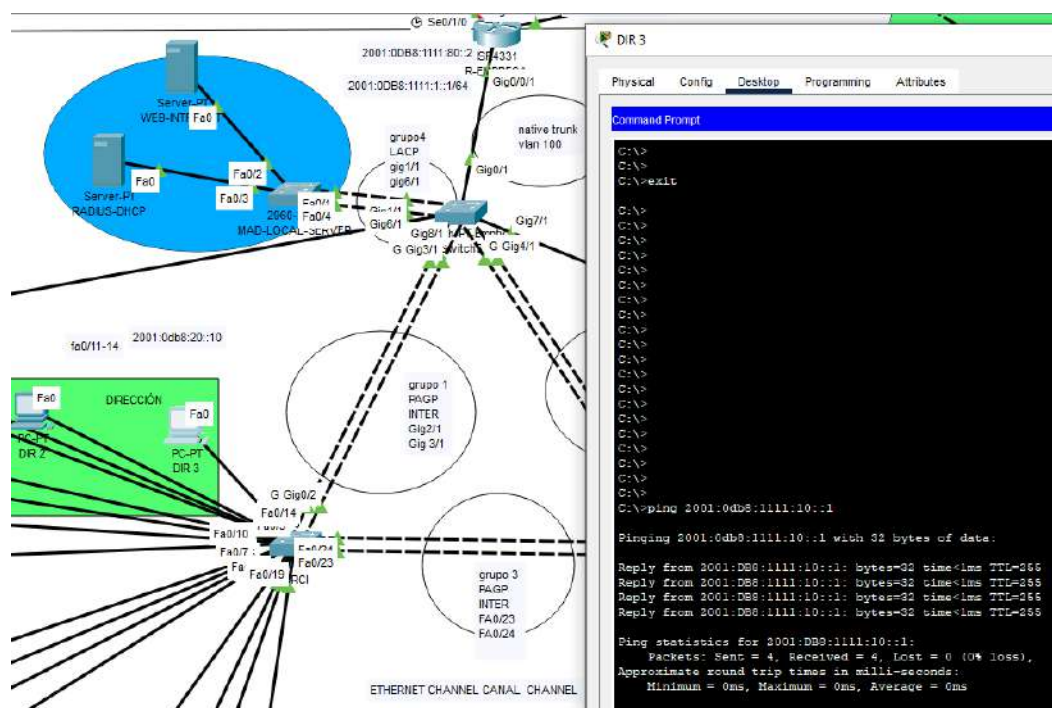
ahora si vemos el canal lógico 1 con las interfaces gig2/1 y gig3/1 tendremos **2Gbps**

```

Switch5
Switch#show interface 1
^
% Invalid input detected at '^' marker.

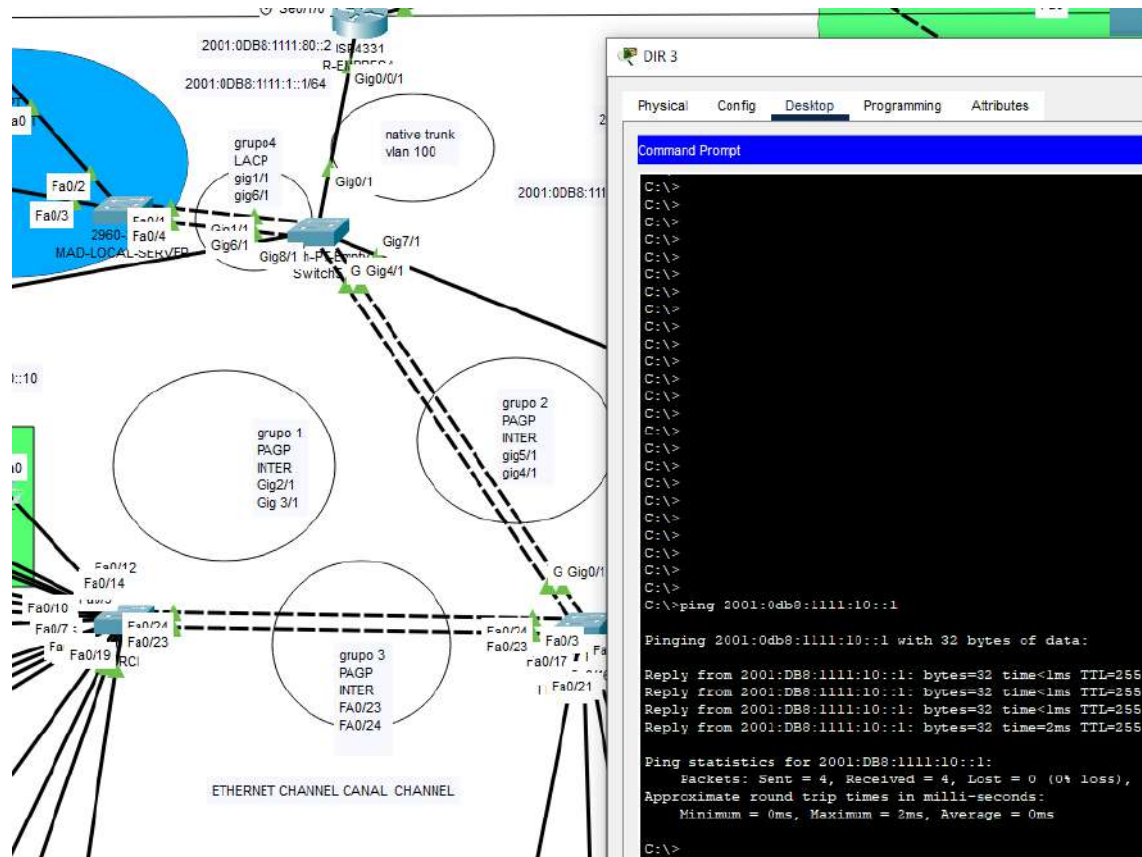
Switch#show interface port-channel 1
Port-channel1 is up, line protocol is up (connected)
Hardware is EtherChannel, address is 0040.0b96.7ac5 (bia 0040.0b96.7ac5)
MTU 1500 bytes, BW 2000000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Half-duplex, 2000Mb/s
  
```

Ahora vamos a ver la redundancia que tenemos con este protocolo para verlo hacemos un ping desde el pc de dirección al router por ejemplo. Vemos que tenemos ping al router.





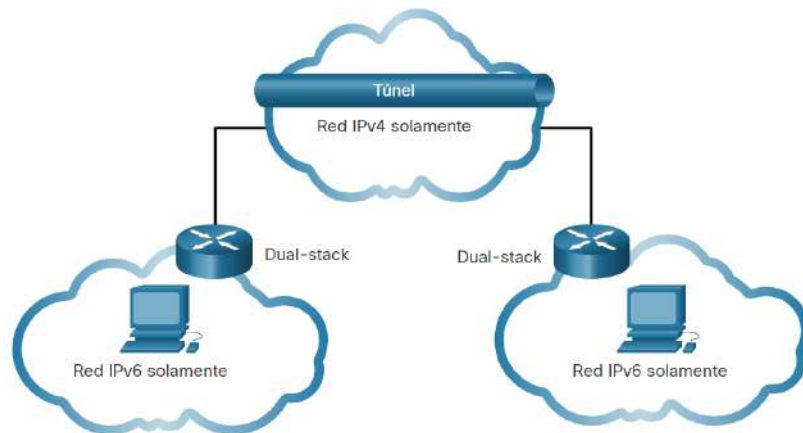
Ahora vamos a quitar los cables que tenemos del grupo 1 con esto tenemos que esperar y comprobamos que hacemos ping al router. Y tenemos.



Con la implementación de Ethernet Channel, se puede observar que, incluso si no hay una conexión directa al switch principal, los paquetes de datos aún pueden llegar al router. Esto se debe a los enlaces troncales configurados entre los demás switches, lo que proporciona una redundancia en caso de fallos en la red.

Esta redundancia en los enlaces troncales brinda una mayor confiabilidad a la infraestructura de red. Si un enlace troncal se desconecta o presenta problemas, los paquetes de datos pueden encontrar rutas alternativas a través de otros enlaces troncales, asegurando la continuidad de la comunicación.

### 4.2.7. Configuración Tunnelización



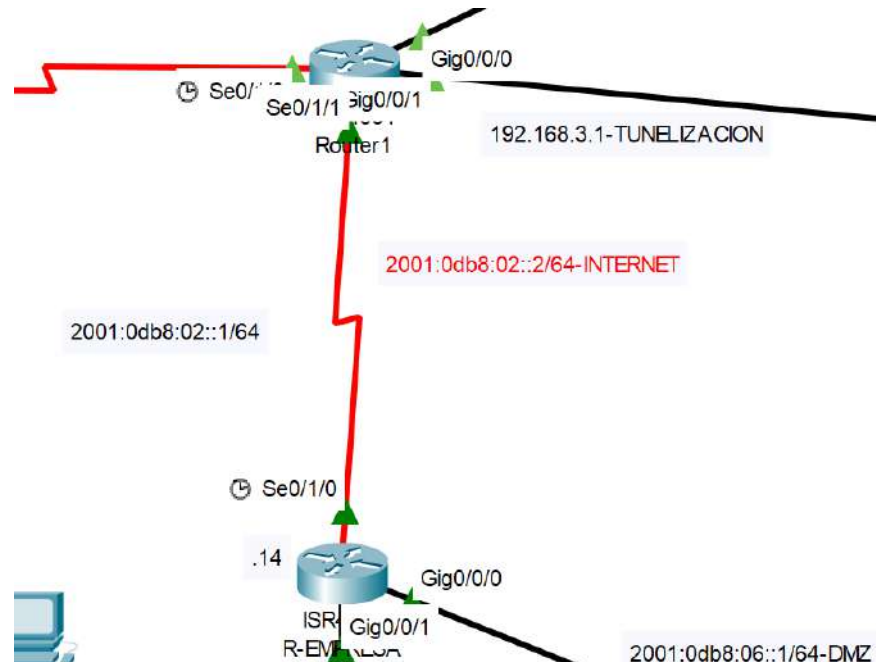
Se ha utilizado Ipv4 para la conexión entre las dos sedes pero en cambio la tunelización es en IPv6 y las sedes también usan ipv6 en cada vlan de cada departamento

#### Router-Madrid

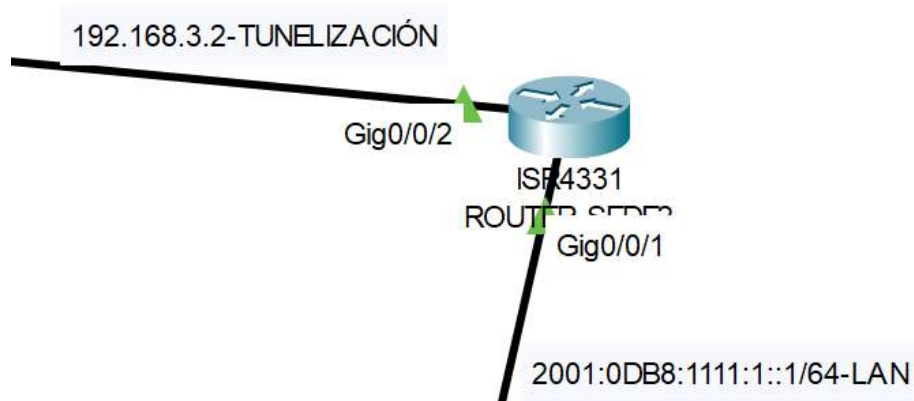
Device Name: R-EMPRESA					
Device Model: ISR4331					
Hostname: Router					
Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet0/0/0	Up	--	<not set>	2001:DB8:6::1/64	0009.7C1A.CB01
GigabitEthernet0/0/1	Up	--	<not set>	2001:DB8:1111:1::1/64	0009.7C1A.CB02
GigabitEthernet0/0/1.10	Up	--	<not set>	2001:DB8:1111:10::1/64	0009.7C1A.CB02
GigabitEthernet0/0/1.20	Up	--	<not set>	2001:DB8:1111:20::1/64	0009.7C1A.CB02
GigabitEthernet0/0/1.30	Up	--	<not set>	2001:DB8:1111:30::1/64	0009.7C1A.CB02
GigabitEthernet0/0/1.40	Up	--	<not set>	2001:DB8:1111:40::1/64	0009.7C1A.CB02
GigabitEthernet0/0/1.50	Up	--	<not set>	2001:DB8:1111:50::1/64	0009.7C1A.CB02
GigabitEthernet0/0/1.60	Up	--	<not set>	2001:DB8:1111:60::1/64	0009.7C1A.CB02
GigabitEthernet0/0/1.90	Up	--	<not set>	2001:DB8:1111:90::1/64	0009.7C1A.CB02
GigabitEthernet0/0/1.110	Up	--	<not set>	2001:DB8:1111:110::1/64	0009.7C1A.CB02
GigabitEthernet0/0/1.120	Up	--	<not set>	2001:DB8:1111:120::1/64	0009.7C1A.CB02
GigabitEthernet0/0/2	Up	--	192.168.3.1/24	<not set>	0009.7C1A.CB03
Serial0/1/0	Up	--	<not set>	2001:DB8:2::2/64	<not set>
Serial0/1/1	Down	--	<not set>	<not set>	<not set>
Tunnel0	Up	--	<not set>	3000::1/112	00D0.97D6.AB38
Vlan1	Down	1	<not set>	<not set>	00D0.BAB3.54AB

Physical Location: Intercity > MADRID > Corporate Office > Main Wiring Closet > Rack > R-EMPRESA

A continuación, debemos configurar los routers de las sedes que deseamos interconectar y asignarles direcciones IPv4 en sus respectivas interfaces. Para simplificar, hemos seleccionado la dirección IPv4 192.168.3.0 para esta prueba de conexión. Y la tunelización hemos usado la dirección 3000::1/112

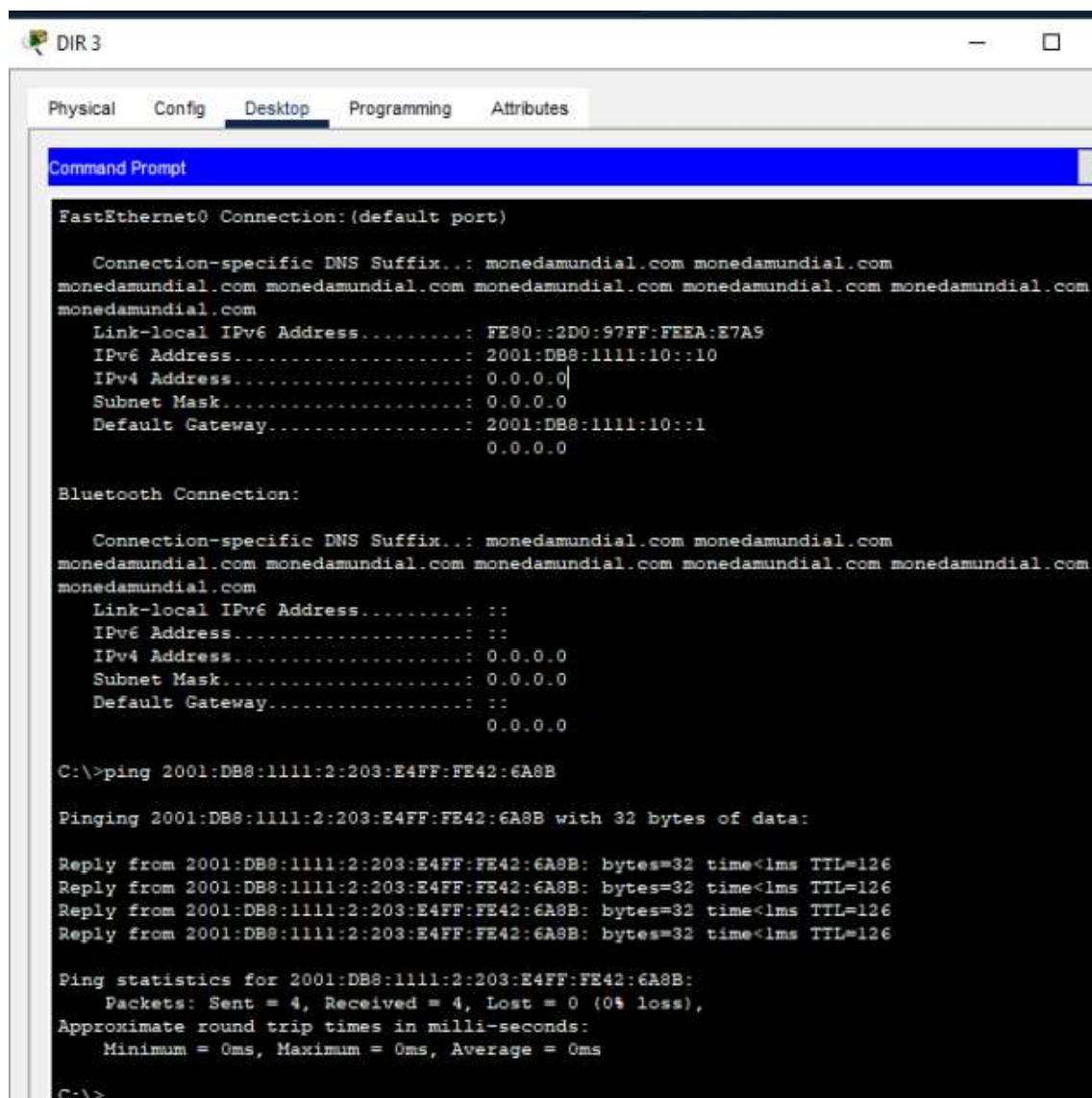


En nuestro escenario, hemos seleccionado la interfaz gig0/0/1 del router Router1 como punto de configuración para establecer la tunelización. Le hemos asignado la dirección IPv4 192.168.3.1 con una máscara de subred 255.255.255.0. Esta configuración permitirá establecer la comunicación a través del túnel IPv6 sobre IPv4.



Una vez que hemos realizado la configuración mencionada anteriormente, es necesario establecer un túnel en la interfaz gig0/0/2 para permitir una comunicación sin problemas con la sede 1 a través de IPv6. Del mismo modo, se debe realizar una configuración similar en la sede 1. Una vez completada la configuración del túnel, procederemos a comprobar la conectividad utilizando el protocolo ICMP entre los equipos de cada sede.

Desde el equipo de la sede 1 en el departamento de dirección con ipv6 tiene ip 2001:0db8:1111:10::10 y accede a la dirección 2001:0db8:1111:100::10 y con lo que incluimos el tracert para ver por donde pasa y ver qué dirección se encapsula y obtenemos la ipv6 que hemos asignado 3000::/112.



```
DIR 3
Physical Config Desktop Programming Attributes
Command Prompt

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...: monedamundial.com monedamundial.com
monedamundial.com monedamundial.com monedamundial.com monedamundial.com
monedamundial.com
Link-local IPv6 Address.....: FE80::2D0:97FF:FEA:E7A9
IPv6 Address.....: 2001:DB8:1111:10::10
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 2001:DB8:1111:10::1
0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix...: monedamundial.com monedamundial.com
monedamundial.com monedamundial.com monedamundial.com monedamundial.com
monedamundial.com
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
0.0.0.0

C:\>ping 2001:DB8:1111:2:203:E4FF:FE42:6A8B

Pinging 2001:DB8:1111:2:203:E4FF:FE42:6A8B with 32 bytes of data:

Reply from 2001:DB8:1111:2:203:E4FF:FE42:6A8B: bytes=32 time<1ms TTL=126
Reply from 2001:DB8:1111:2:203:E4FF:FE42:6A8B: bytes=32 time<1ms TTL=126
Reply from 2001:DB8:1111:2:203:E4FF:FE42:6A8B: bytes=32 time<1ms TTL=126
Reply from 2001:DB8:1111:2:203:E4FF:FE42:6A8B: bytes=32 time<1ms TTL=126

Ping statistics for 2001:DB8:1111:2:203:E4FF:FE42:6A8B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

```

C:\>tracert 2001:DB8:1111:100::10

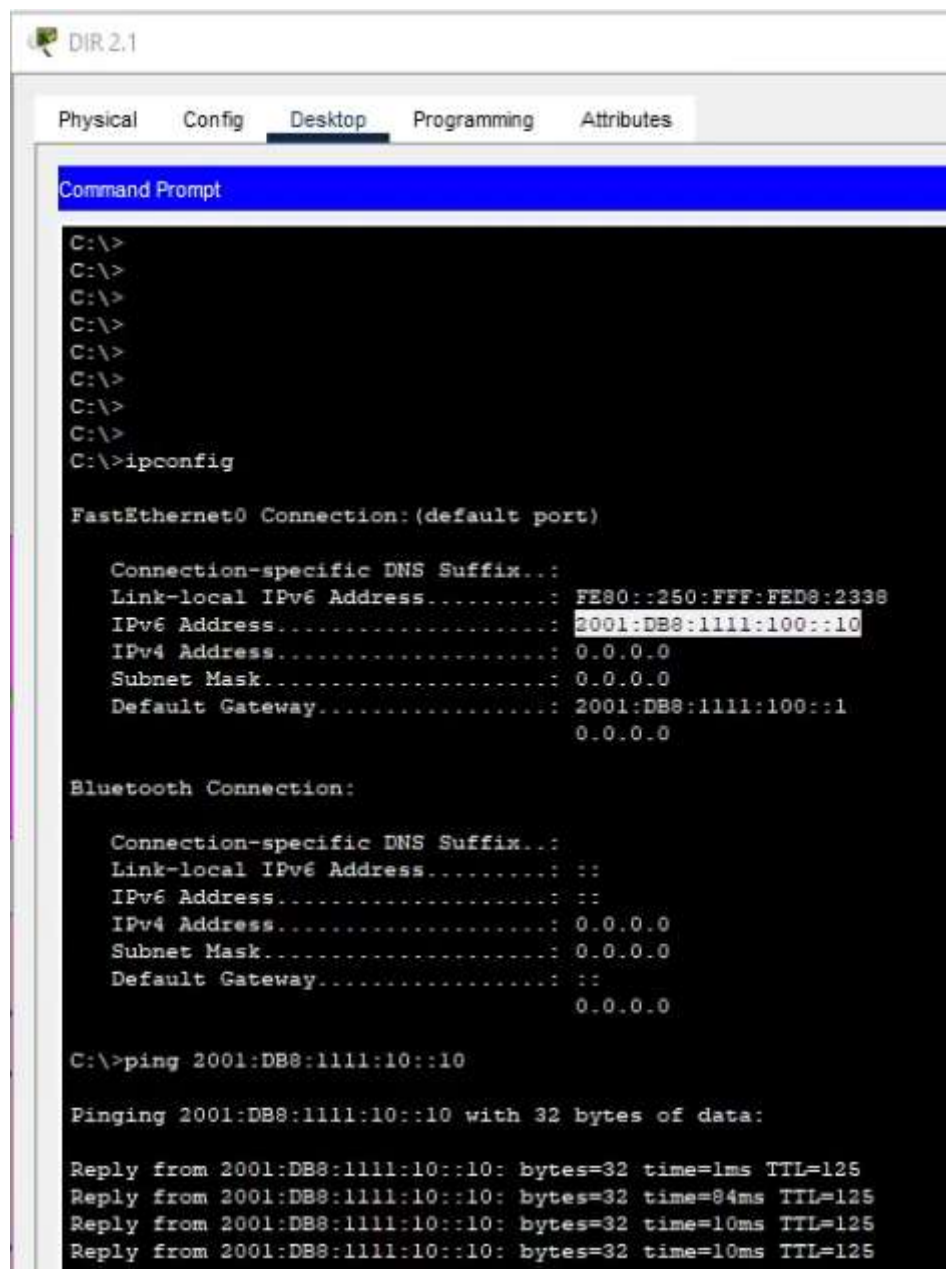
Tracing route to 2001:DB8:1111:100::10 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    2001:DB8:1111:10::1
  2  1 ms    0 ms    1 ms    2001:DB8:2::1
  3  1 ms    35 ms   1 ms    3000::2
  4  10 ms   10 ms   0 ms    2001:DB8:1111:100::10

Trace complete.

```

## Equipo de sede 2



```

DIR 2.1
Physical Config Desktop Programming Attributes

Command Prompt

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::250:FFF:FED8:2338
    IPv6 Address . . . . .: 2001:DB8:1111:100::10
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: 2001:DB8:1111:100::1
                               0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                               0.0.0.0

C:\>ping 2001:DB8:1111:100::10

Pinging 2001:DB8:1111:100::10 with 32 bytes of data:

Reply from 2001:DB8:1111:100::10: bytes=32 time=1ms TTL=125
Reply from 2001:DB8:1111:100::10: bytes=32 time=84ms TTL=125
Reply from 2001:DB8:1111:100::10: bytes=32 time=10ms TTL=125
Reply from 2001:DB8:1111:100::10: bytes=32 time=10ms TTL=125

```

```

C:\>tracert 2001:DB8:1111:10::10

Tracing route to 2001:DB8:1111:10::10 over a maximum of 30 hops:

  1  0 ms      0 ms      0 ms      2001:DB8:1111:100::1
  2  0 ms      61 ms     1 ms      3000::1
  3  0 ms      0 ms      0 ms      2001:DB8:2::2
  4  1 ms      1 ms      0 ms      2001:DB8:1111:10::10

Trace complete.

```

#### 4.2.8. Configuración VPN

Se ha utilizado el protocolo Ipsec para configurar una vpn de tipo acceso remoto para los empleados que teletrabajan, solo tendrán acceso a los servidores correspondientes a su departamento.

Se ha realizado una configuración para demostrar una conexión remota utilizando el protocolo IPSec en un entorno con direccionamiento IPv4. Debido a las limitaciones del simulador Packet Tracer, se han agregado direcciones IPv4 en las interfaces, además de direcciones IPv6. El cliente remoto cuenta con una dirección IPv4 e IPv6 asignada, siendo la dirección IPv4 utilizada para acceder al servidor de la empresa. Para lograrlo, se han llevado a cabo las siguientes acciones:

- Asignación de direcciones IPv4 e IPv6 en las interfaces.
- Configuración del modelo de autenticación AAA y creación de usuarios y contraseñas.

```

!
aaa new-model
!
aaa authentication login UserVPN_SERVIDORES local
!
!
aaa authorization network GroupVPN_SERVIDORES local
!

```

- Define el nombre de usuario y la contraseña para el usuario VPN:

```

!
username luis secret 5 $1$mERr$Hz.95IyOHimhrSwO9HzIo/
!
!

```



- Establecimiento de políticas de encriptación y criptomas para definir los parámetros de seguridad.

ISAKMP Phase 1 Policy Parameters

Parameters		R1	R3
Key Distribution Method	Manual or ISAKMP	ISAKMP	ISAKMP
Encryption Algorithm	DES, 3DES, or AES	AES 256	AES 256
Hash Algorithm	MD5 or SHA-1	SHA-1	SHA-1
Authentication Method	Pre-shared keys or RSA	pre-share	pre-share
Key Exchange	DH Group 1, 2, or 5	DH 5	DH 5
IKE SA Lifetime	86400 seconds or less	86400	86400
ISAKMP Key		vpnpa55	vpnpa55

```
!
crypto isakmp policy 100
  encr aes 256
  hash md5
  authentication pre-share
  group 5
  lifetime 3600
!
```

- Configura el grupo de configuración del cliente ISAKMP:

```
!
crypto isakmp client configuration group GroupVPN_SERVIDORES
  key madridservers
  pool MY-VLAN90
!
```

- Configuración de transformaciones criptográficas para proteger los datos.

IPsec Phase 2 Policy Parameters

Parameters	R1	R3
Transform Set Name	VPN-SET	VPN-SET
ESP Transform Encryption	esp-aes	esp-aes
ESP Transform Authentication	esp-sha-hmac	esp-sha-hmac
Peer IP Address	10.2.2.2	10.1.1.2
Traffic to be Encrypted	access-list 110 (source 192.168.1.0 dest 192.168.3.0)	access-list 110 (source 192.168.3.0 dest 192.168.1.0)
Crypto Map Name	VPN-MAP	VPN-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

```
!
crypto ipsec transform-set SetVPN esp-aes 256 esp-md5-hmac
!
```

- Configura el mapa dinámico de IPsec:

```
!
crypto dynamic-map DynamicVPN 100
  set transform-set SetVPN
!
```

- Configura el mapa estático de IPsec:

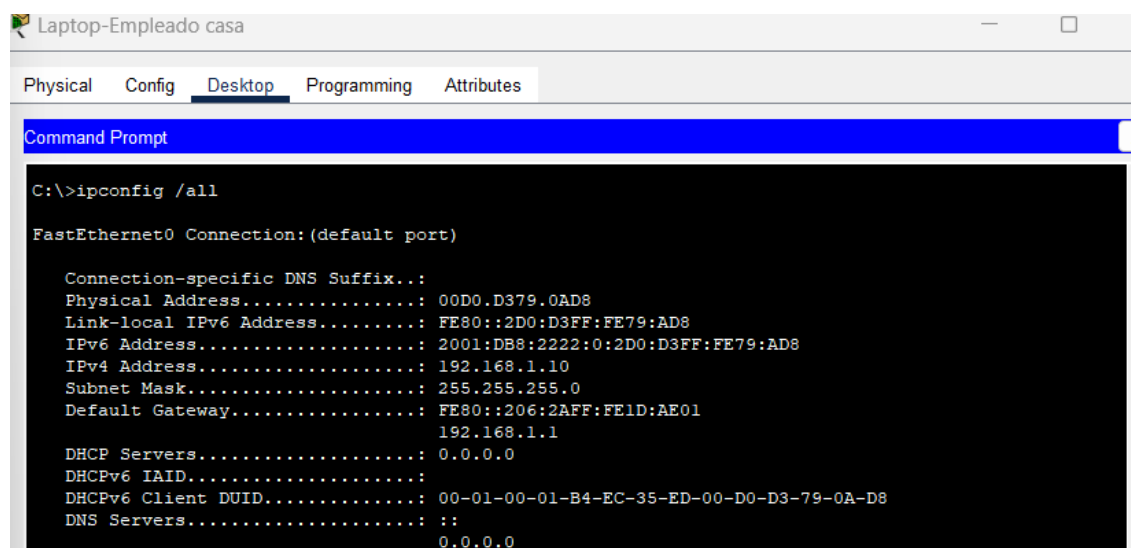
```
!
crypto map StaticMap client authentication list UserVPN_SERVIDORES
crypto map StaticMap isakmp authorization list GroupVPN_SERVIDORES
crypto map StaticMap client configuration address respond
crypto map StaticMap 20 ipsec-isakmp dynamic DynamicVPN
!
```

- Aplicación de la protección IPsec en las interfaces del router mediante mapas criptográficos.

```
Enter configuration commands, one per line. End with CNTRL/Z.
Router(config)#interface s0/1/0
Router(config-if)#crypto map StaticMap
*Jan  3 07:16:26.785: %CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
Router(config-if)#exit
Router(config)#
```

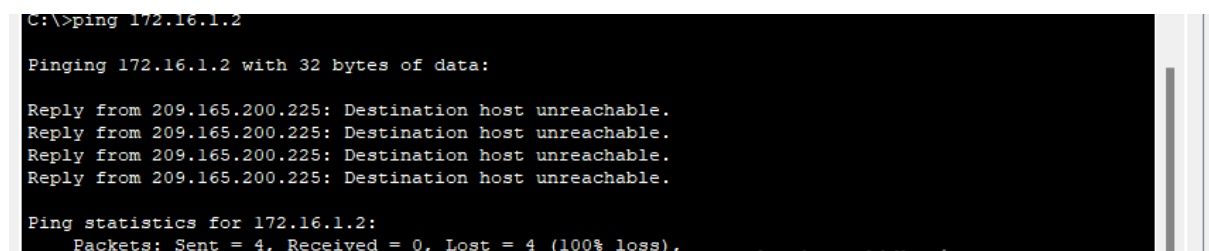
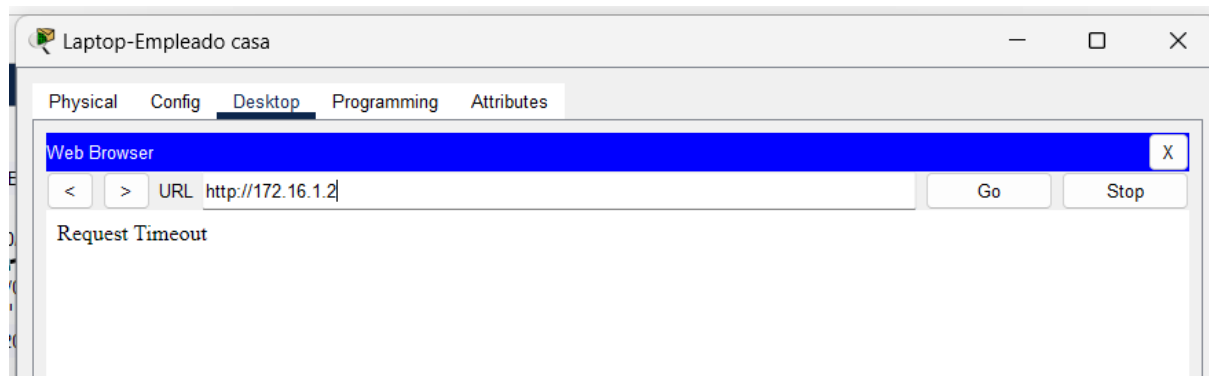
Es importante tener en cuenta que esta configuración se adaptó a las limitaciones del simulador y que la implementación real puede requerir ajustes adicionales.

## antes de conexion remota



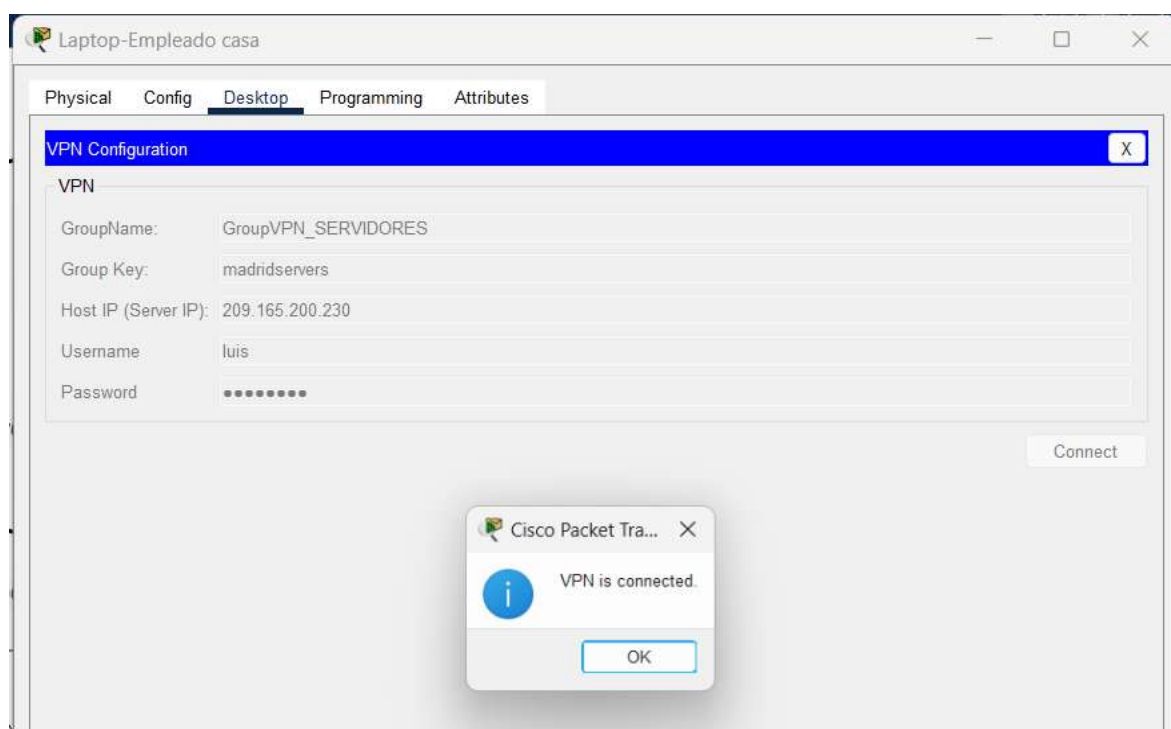


este usuario No puede acceder a ningun servidor ya que no se encuentra dentro de la red de la empresa



## Prueba Conexión Remota

Cuando se establece una conexión remota a través de VPN, al cliente se le asigna una dirección de las reservadas para dichas conexiones. El objetivo principal es permitir al cliente acceder únicamente a la subred de la red de servidores, con el propósito de obtener acceso a los datos y archivos necesarios durante la conexión.



```
Laptop-Empleado casa
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ipconfig /all

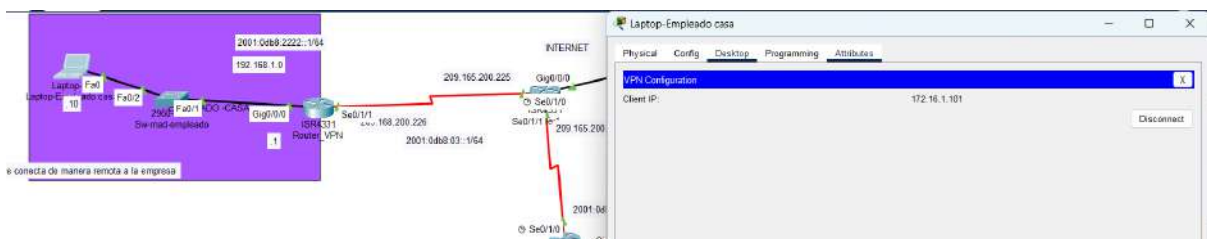
FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address...: 00D0.D379.0AD8
Link-local IPv6 Address...: FE80::2D0:D3FF:FE79:AD8
IPv6 Address...: 2001:DB8:2222:0:2D0:D3FF:FE79:AD8
IPv4 Address...: 192.168.1.10
Subnet Mask...: 255.255.255.0
Default Gateway...: FE80::206:2AFF:FE1D:AE01
192.168.1.1
DHCP Servers...: 0.0.0.0
DHCPv6 IAID...:
DHCPv6 Client DUID...: 00-01-00-01-B4-EC-35-ED-00-D0-D3-79-0A-D8
DNS Servers...:
0.0.0.0

Bluetooth Connection:

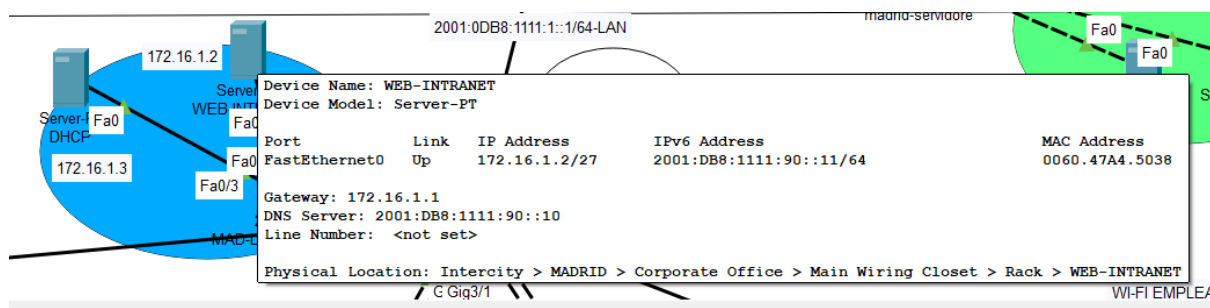
Connection-specific DNS Suffix...:
Physical Address...: 0010.1181.60A4
Link-local IPv6 Address...: ::
IPv6 Address...: ::
IPv4 Address...: 0.0.0.0
Subnet Mask...: 0.0.0.0
Default Gateway...: ::
0.0.0.0
DHCP Servers...: 0.0.0.0
DHCPv6 IAID...:
DHCPv6 Client DUID...: 00-01-00-01-B4-EC-35-ED-00-D0-D3-79-0A-D8
DNS Servers...:
0.0.0.0

Tunnel Interface IP Address.....: 172.16.1.101
```



Ahora sí podrá tener conexión con los servidores.





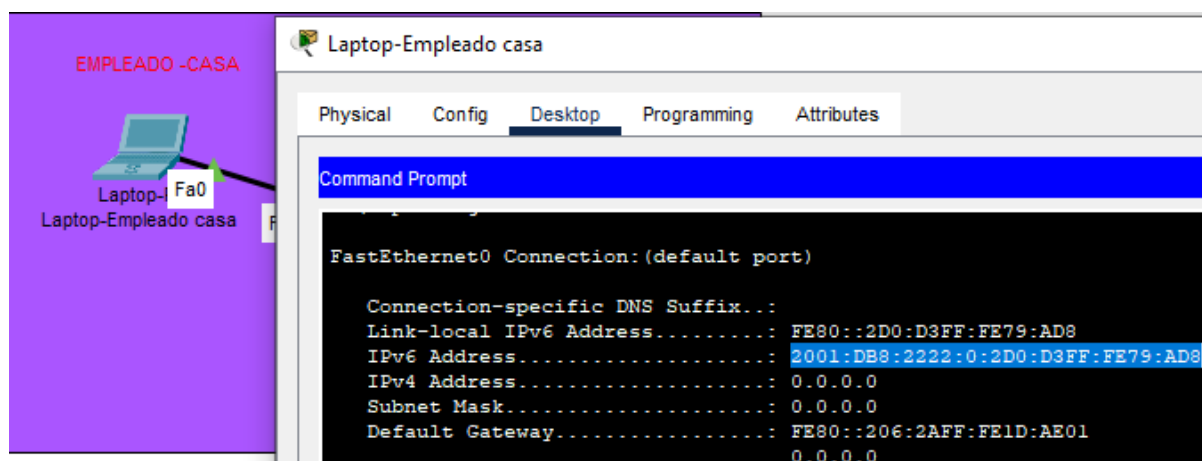
#### 4.2.9. Listas de control de acceso (ACL)

Para gestionar la seguridad de la red de la empresa, se configurarán varias listas de control de acceso que permitirán establecer políticas adecuadas. Se realizará una segmentación de zonas dentro de la red para garantizar una protección óptima.

Las medidas de seguridad consideradas incluyen:

- ❖ Limitar el acceso a personal no autorizado proveniente de direcciones públicas no reconocidas por el servidor. Esto significa que cualquier tráfico no solicitado previamente por un equipo de nuestra LAN será descartado.

Por ejemplo ya que tenemos implementado un empleado que está en su domicilio no tendría acceso con una dirección ipv6 **2001:DB8:2222:0:2D0:D3FF:FE79:AD8**



Con ACL para controlar esta petición el usuario no podrá establecer una conexión con el router e inclusive algún equipo de la red.

```
ipv6 access-list icmp-tcp-a-lan
permit tcp any 2001:DB8:6::/64 eq www
permit icmp any 2001:DB8:6::/64
permit ipv6 2001:DB8:1111:100::/64 2001:DB8:1111:10::/64
deny icmp any any echo-request
deny tcp any 2001:DB8:1111:90::/64 eq www
permit ipv6 any any
permit ipv6 host 2001:DB8:1111:100::10 host 2001:DB8:1111:10::10
```

**"permit tcp any 2001:DB8:6::/64 eq www"**: Se permite el tráfico TCP hacia el puerto 80 (HTTP) exclusivamente desde la red con dirección IPv6 2001:DB8:6::/64, permitiendo el acceso a servicios web desde esta red específica.

**"permit icmp any 2001:DB8:6::/64"**: Se permite el tráfico ICMP (ping) únicamente desde la red con dirección IPv6 2001:DB8:6::/64, lo cual posibilita responder a solicitudes de ping provenientes de esta red en particular.

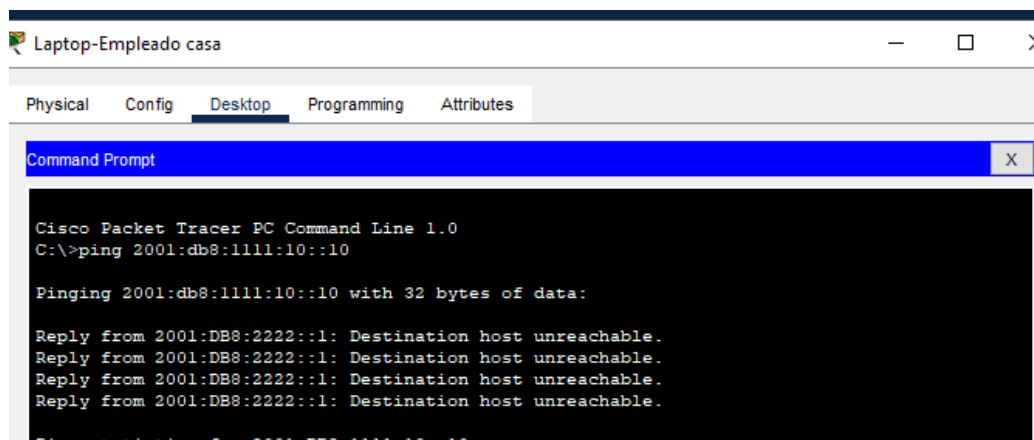
**"permit ipv6 2001:DB8:1111:100::/64 2001:DB8:1111:10::/64"**: Esta regla permite el tráfico IPv6 desde la subred 2001:DB8:1111:100::/64 hacia la subred 2001:DB8:1111:10::/64. Permite la comunicación entre estas dos subredes específicas.

**"deny icmp any any echo-request"**: Se deniegan las solicitudes de ping (ICMP echo-request) desde cualquier origen hacia cualquier destino en la red, evitando así el acceso no autorizado mediante esta forma de comunicación.

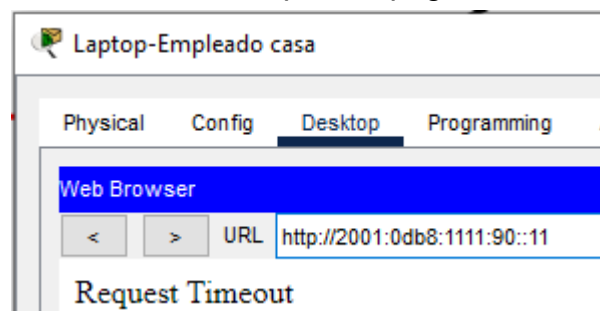
**"deny tcp any 2001:DB8:1111:90::/64 eq www"**: Se deniega el tráfico TCP hacia el puerto 80 (HTTP) desde cualquier origen en la red con dirección IPv6 2001:DB8:1111:90::/64, lo cual bloquea el acceso no autorizado al servidor web desde esta red específica.

**"permit ipv6 any any"**: Se permite cualquier otro tipo de tráfico IPv6 desde cualquier origen hacia cualquier destino en la red, asegurando que el tráfico no especificado previamente sea permitido.

bien entonces si hacemos conexión con un equipo de nuestro departamento que es dirección con dirección ipv6 2001:0db8:1111:10::10



ahora con la conexión del servidor web para la página web



ahora el equipo del empleado tendrá que acceder a la página de la corporación



y por último a la página web que sería como una conexión de google



- ❖ La zona de desmilitarización contendrá los servidores que podrán ser accedidos desde el exterior, es decir, desde cualquier conexión proveniente de Internet. Entre estos servidores se encuentran el servidor de la página web y el servidor de nombres de dominio. Sin embargo, cualquier intento de tráfico hacia la red LAN será bloqueado, excepto las conexiones establecidas con el servidor que permitirán su correcto funcionamiento y accesibilidad.

```
ipv6 access-list dmz
deny icmp 2001:DB8:6::/64 any echo-request
deny tcp any 2001:DB8:1111:90::/64 eq www
permit ipv6 any any
```

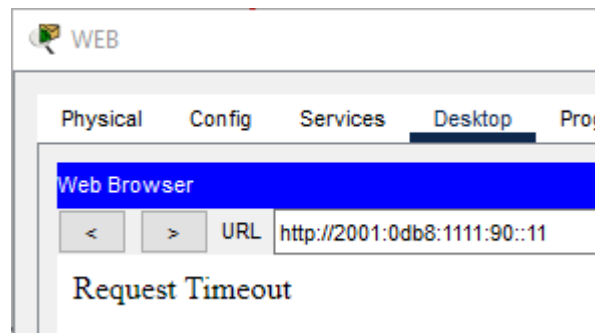
**"deny icmp 2001:DB8:6::/64 any echo-request":** Esta regla deniega el tráfico ICMP de tipo echo-request (ping) desde la subred 2001:DB8:6::/64 hacia cualquier destino. En otras palabras, bloquea los intentos de hacer ping desde la DMZ hacia cualquier otro host o red.

**"deny tcp any 2001:DB8:1111:90::/64 eq www":** Esta regla deniega el tráfico TCP desde cualquier origen hacia la subred 2001:DB8:1111:90::/64 en el puerto 80 (www). Específicamente, bloquea el acceso a servicios web (como una página web) alojados en esa subred dentro de la DMZ.

**"permit ipv6 any any":** Esta regla permite cualquier tráfico IPv6 desde cualquier origen hacia cualquier destino dentro de la DMZ. Permite la comunicación IPv6 entre cualquier origen y cualquier destino en la DMZ.



ahora en nuestro caso si de la dmz accede a nuestra página web (intranet) no tendría acceso



- ❖ Todos los departamentos de la red LAN tendrán conectividad entre sí y podrán acceder a los servidores locales de manera segura. Los servidores locales solo podrán ser accedidos por usuarios autorizados que estén conectados a la red local y cuenten con la correspondiente autorización.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	DIREC 1	RRHH 3	ICM...		0.000	N	0	(edit)	
	Successful	RRHH 3	CONT 1	ICM...		0.000	N	1	(edit)	
	Successful	CONT 1	INF 3	ICM...		0.000	N	2	(edit)	
	Successful	INF1	DISEÑ 4	ICM...		0.000	N	3	(edit)	

### 4.3. Implementación de diseño de red

En la segunda fase de nuestro proyecto, nos enfocamos en la implementación del diseño de la red. En esta etapa, nos gustaría compartir información sobre las características de los dispositivos que hemos seleccionado para garantizar un funcionamiento óptimo en un entorno real.

Hemos realizado una cuidadosa evaluación de los dispositivos de red disponibles en el mercado y hemos seleccionado aquellos que mejor se adaptan a nuestras necesidades y requisitos específicos. A continuación, destacaremos las características clave de estos dispositivos y cómo contribuyen a la eficiencia y seguridad de nuestra red.



### 4.3.1. Dispositivos Físicos

#### - Repartidores de planta Switch

En primer lugar, hemos optado por utilizar switches de alta gama que ofrecen una amplia capacidad de conmutación y múltiples puertos para satisfacer las demandas de nuestra red empresarial. Estos switches cuentan con características avanzadas de gestión, como VLANs, enlaces troncales y QoS (Calidad de Servicio), que nos permiten segmentar la red, mejorar el rendimiento y garantizar la priorización del tráfico crítico.

#### **Cisco Catalyst 2960X**



Los switches **Cisco Catalyst 2960X** son una elección óptima para establecer la redundancia en la zona DMZ debido a las siguientes características y ventajas clave:

- **Confiabilidad y rendimiento:** Los switches Catalyst 2960X ofrecen una alta confiabilidad y rendimiento, lo que garantiza una conectividad estable y eficiente para los servidores ubicados en la zona DMZ.
- **Capacidad de apilamiento:** Estos switches admiten el apilamiento físico y lógico, lo que permite crear una única unidad lógica compuesta por varios switches. Esto proporciona una mayor capacidad de administración y simplifica la configuración y supervisión de los switches redundantes.
- **Soporte de VLANs:** Los Catalyst 2960X ofrecen soporte para el etiquetado de VLANs (Virtual LANs), lo que permite la segmentación y el aislamiento de tráfico en la red. Esta característica es fundamental para mantener la seguridad y el control de acceso en la zona DMZ.
- **Protocolo de agregación de enlaces:** Estos switches admiten el protocolo de agregación de enlaces EtherChannel, que permite combinar varios

enlaces físicos en un solo enlace lógico de mayor capacidad. Esto proporciona redundancia y mayor ancho de banda para la zona DMZ.


- **Características de seguridad avanzadas:** Los switches Catalyst 2960X cuentan con una amplia gama de características de seguridad, como listas de control de acceso (ACLs), autenticación de puertos y prevención de ataques de denegación de servicio (DoS). Estas características ayudan a proteger la zona DMZ contra posibles amenazas y ataques externos.
- **Protocolos de redundancia:** Para garantizar la alta disponibilidad en la zona DMZ, los switches Catalyst 2960X admiten protocolos de redundancia como Spanning Tree Protocol (STP) y Rapid Spanning Tree Protocol (RSTP). Estos protocolos permiten la detección y el bloqueo de bucles en la red, evitando interrupciones y asegurando una conmutación rápida en caso de fallas.
- **Router**

En cuanto a los routers, hemos elegido modelos robustos que proporcionan capacidades de enrutamiento avanzadas y seguridad de nivel empresarial. Estos routers admiten protocolos de enrutamiento dinámico, como OSPF o **EIGRP**, lo que nos permite una mayor flexibilidad y escalabilidad en la gestión de la red. Además, incorporan características de seguridad, como **VPN** (Red Privada Virtual) y firewalls, para proteger nuestros datos y mantener la integridad de la red.

### **ROUTER Cisco 4451-X**



El router Cisco 4451-X ha sido seleccionado para nuestra implementación de red debido a sus características destacadas. Este modelo ofrece un throughput de hasta 2 Gbps, múltiples interfaces RJ-45 y compatibilidad con el protocolo **EIGRP**. Estas características son ideales para redes que necesitan manejar un alto tráfico y conectarse a proveedores de servicios de Internet.



Además, el router Cisco 4451-X cuenta con funciones de seguridad avanzadas, como la configuración de conexiones seguras mediante **IPsec** para establecer una **VPN** y proteger la información transmitida. También ofrece inspección de paquetes y prevención de intrusiones, lo que garantiza una mayor seguridad en la red.

Otra ventaja del router Cisco 4451-X es su capacidad para configurar un **etherchannel**, que permite combinar múltiples enlaces de alta velocidad para aumentar el ancho de banda y brindar redundancia en la red. Entre sus demás características tenemos:

## **Seguridad**

- Firewall integrado con inspección de paquetes y prevención de intrusiones (IPS)
- VPN IPsec de alto rendimiento
- Control de acceso basado en políticas (PACL, VACL, etc.)
- Listas de control de acceso (ACL)

## **Conectividad WAN**

- Soporte para múltiples opciones de conectividad WAN, incluyendo T1/E1, xDSL, Ethernet, etc.
- Opción de conectividad 4G LTE Advanced Pro con soporte para múltiples operadores

## **Administración y servicios**

- Interfaz de línea de comandos (CLI)
- Interfaz gráfica de usuario (GUI)
- Protocolo de administración SNMP (Simple Network Management Protocol)
- Protocolo de administración SSH (Secure Shell)
- Protocolo de administración HTTPS (HTTP Secure)
- Protocolo de administración SYSLOG

## **Alimentación**

- Opción de fuente de alimentación AC o DC

## - Puntos de acceso

Para asegurar la conectividad inalámbrica, hemos seleccionado puntos de acceso Wi-Fi de alta calidad. Estos puntos de acceso son compatibles con los últimos estándares de Wi-Fi, ofrecen una amplia cobertura y son capaces de manejar un alto volumen de usuarios simultáneos. Además, implementamos medidas de seguridad, como autenticación de usuarios y encriptación de datos, para proteger nuestra red inalámbrica de accesos no autorizados.

### **Cisco CBW150AX (CBW150AX-E-EU)**



Entre la ficha técnica que se recoge desde su página oficial en referencia a sistema y seguridad tenemos:

#### **Sistema**

- 1 GB de DRAM, 256 MB de memoria flash
- Procesador de cuatro núcleos de 1 GHz

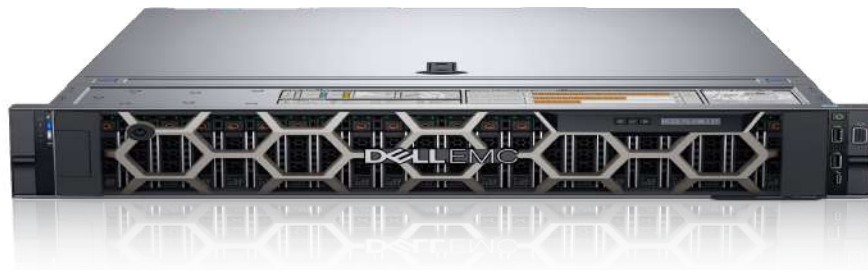
#### **Autenticación y Seguridad**

- Acceso protegido WiFi: WPA2 y WPA3, incluida la autenticación WPA2-Enterprise.
- 802.1X, autenticación RADIUS, autorización y contabilidad (AAA).
- Segmentación vía VLANs (hasta 16).
- 802.11r y 802.11i
- La red de invitados también puede autenticarse con una cuenta de inicio de sesión social (Google y Facebook)

Es una buena opción ya que ofrece conectividad de alta velocidad, cobertura mejorada, seguridad avanzada, facilidad de gestión y compatibilidad con soluciones existentes. Estas características lo convierten en una opción sólida para mejorar y optimizar tu red.

- **Servidor Web Y Correo**

### **El Dell PowerEdge R740**



Es un servidor de alto rendimiento y densidad optimizado para cargas de trabajo empresariales. Algunas de sus características más importantes incluyen:

- **Procesadores:** admite hasta dos procesadores escalables Intel Xeon de segunda generación, con un máximo de 28 núcleos por procesador.
- **Memoria:** admite hasta 24 módulos de memoria DDR4 de 2666 MT/s, con un máximo de 3 TB de memoria.
- **Almacenamiento:** admite hasta 16 unidades de disco duro o de estado sólido (SSD) de 2,5" o 8 unidades de disco duro o SSD de 3,5". También es compatible con configuraciones de almacenamiento con unidades NVMe PCIe.
- **Conectividad:** cuenta con una variedad de opciones de conectividad, incluyendo 4 puertos de red de 1 GbE y 2 o 4 puertos de red de 10GbE. También puede ser configurado con adaptadores InfiniBand de alta velocidad.
- **Gestión y seguridad:** incluye herramientas de gestión de sistemas como Dell EMC OpenManage Enterprise y Integrated Dell Remote Access Controller (iDRAC) con Lifecycle Controller. También cuenta con características de seguridad como un chip TPM (Trusted Platform Module) y la posibilidad de configurar módulos de seguridad físicos.

En cuanto al valor del equipo, el precio del Dell PowerEdge R740 varía dependiendo de la configuración, pero suele oscilar entre los 3,000 y 5,000 euros aproximadamente. En resumen, el Dell PowerEdge R740 es una excelente opción para ser utilizado como servidor Web y DNS en este proyecto, debido a su alto rendimiento, capacidad de procesamiento y facilidad de gestión. Sin embargo, su capacidad para manejar grandes cargas de trabajo y su fiabilidad justifican su costo.

- **Servidor DHCP,DNS y VPN**

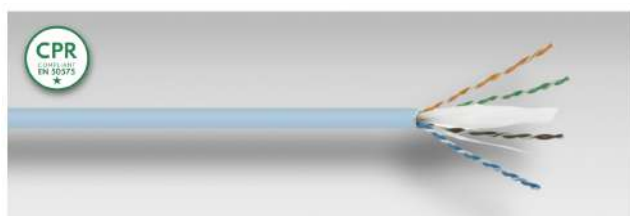


El Dell PowerEdge R940 es un servidor de alta gama que cuenta con características destacadas, como:

- Procesadores escalables Intel Xeon de 2ª generación, que permiten un alto rendimiento y una capacidad de procesamiento excepcional.
- Hasta 6TB de memoria RAM DDR4, lo que permite una gestión eficiente y rápida de grandes cantidades de datos.
- Capacidad de almacenamiento de hasta 24 unidades de disco duro de 2,5" o 12 unidades de disco duro de 3,5", lo que ofrece una gran flexibilidad y escalabilidad para el almacenamiento de datos.
- Funcionalidad de redundancia de alimentación y refrigeración, que garantiza una alta disponibilidad y fiabilidad.
- Capacidad de virtualización mejorada, lo que permite una gestión más eficiente de los recursos y un ahorro de costes significativo.

Este servidor ofrece rendimiento, escalabilidad, confiabilidad, facilidad de gestión y un sólido soporte técnico. Estas características lo convierten en una opción adecuada para implementar servicios de **DHCP, DNS y VPN** en tu red, brindando un funcionamiento eficiente y confiable de estos servicios críticos.

- **Cable CAT6A**



El cable CAT6 no solo proporciona una interferencia mucho menor o Near-End Crosstalk (NEXT), sino que también mejora la diafonía remota (ELFEXT), pérdida de retorno (RL) y pérdida de inserción (IL). El resultado es un menor ruido del sistema, menos errores y mayores velocidades de transmisión de datos.

El sistema de cableado estructurado UTP Cat6A permite montar una infraestructura de telecomunicaciones genérica dentro de un edificio, creando una red de área local (LAN). La categoría 6A se describe dentro de los estándares TIA e ISO EN para clase Ea y categoría 6A, y permite trabajar a velocidades de hasta 10Gbps dentro de un entorno Ethernet.

- **Patch pannel:**



Los Patch Panel permiten hacer cambios de forma rápida y sencilla conectando y desconectando los cables de parcheo. Esta manipulación de los cables se hará habitualmente en la parte frontal, mientras que la parte de atrás del panel tendrá los cables más permanentes y que van directamente a los equipos centrales (Switches, Routers, concentradores.).

- **Centralización de conexiones:** El patch panel actúa como un concentrador pasivo de conexiones de red. Permite la conexión de cables de red, tanto de cobre como de fibra óptica, en un solo lugar, lo que facilita el acceso y la gestión de las conexiones.
- **Flexibilidad:** El patch panel brinda flexibilidad al permitir el traslado, la adición o el cambio de la infraestructura de cableado de manera sencilla. Esto es especialmente útil en entornos donde se requiere una reconfiguración frecuente de la red.
- **Organización y etiquetado:** El patch panel generalmente cuenta con una disposición ordenada de puertos numerados o etiquetados, lo que facilita la identificación y el seguimiento de las conexiones. Esto contribuye a una administración eficiente del cableado y a la solución de problemas.

## Kit Puesto Trabajo Eléctrico 4 Schukos/ 2 RJ45 Blanco y



10 Kits caja CS Standard de 3 módulos con 2 schukos blancos, 2 schukos rojos y una placa de datos para dos conectores de cat.6 UTP

**Medidas:** 115 (alto) x 186 (largo) x 63 (ancho) mm

Normativa: UNE 20451:1997 - CE - IK07

Instalación: Superficie

Material: Policarbonato libre de halógenos

**Módulos** de seis RJ45 Cat6. color blanco. material del Panel: ABS

Base: componentes electrónicos

Tamaño: 86x86mm

### - RACK





El armario o Rack será donde se encuentren todos los repartidores y elementos de conexionado de cada planta.

Los Rack tienen unos espacios donde se ubican los equipos, a cada espacio se le denomina U. El tamaño de 1U es igual a 44,45mm. Se deben considerar la profundidad y la altura necesarias para los equipos que se van a montar. La profundidad del bastidor debe ser suficiente para que los equipos puedan montarse sin que sobresalgan, y se recomienda un mínimo de 80 centímetros para los equipos más grandes, como los servidores.

En cuanto a la altura, se encontró el número de equipos que se quieren instalar, pero se recomienda una altura de 42U o 47U para racks grandes.

Además, es importante tener en cuenta que se debe contar con espacio adicional en el rack para la gestión de cables y la ventilación de los equipos, lo que también influirá en la elección de las dimensiones adecuadas del rack.

- **SAI**  
**APC SMT1500C**



Es un dispositivo importante en una red de computadoras, ya que proporciona energía de respaldo en caso de una interrupción del suministro eléctrico.

## - Firewall



Las características y beneficios de los firewalls de la serie ASA 5500-X de Cisco son los siguientes:

- Protección robusta contra amenazas de múltiples capas.
- Combina el firewall con estado más implementado de la industria con servicios de seguridad de red de próxima generación.
- Proporciona visibilidad integral y control granular.
- Ofrece seguridad web potente tanto en las instalaciones como en la nube.
- Cuenta con un sistema de prevención de intrusiones (IPS) líder en la industria para protección contra amenazas conocidas.
- Brinda una protección completa contra amenazas y malware avanzado.
- Es el firewall ASA más instalado del mundo y cuenta con acceso remoto altamente seguro a través de Cisco AnyConnect.

## - ORDENADORES



El HP EliteBook 830 G5 es un portátil de alta calidad que puede ser adecuado para un proyecto de redes. Sus características principales incluyen una pantalla táctil de 13,3 pulgadas, un procesador Intel Core i5-8350U, 16 GB de RAM, almacenamiento SSD de 256 GB y opciones de conectividad versátiles. Viene con Windows 10

preinstalado y cuenta con puertos USB-A, USB-C y HDMI. También incluye una webcam, micrófono y altavoces integrados. En términos de precio, se encuentra en el rango de 290 a 380 euros por ordenador si es reacondicionado. En resumen, el HP EliteBook 830 G5 ofrece rendimiento, portabilidad y capacidad de red, siendo una opción a considerar para el proyecto de 40 ordenadores dentro del rango de precio mencionado. Se ofrece garantía de 2 años y 30 días de devolución en Back Market.

#### - IMPRESORAS



#### **HP Color LaserJet Pro M479FDW**

Resolución máxima: 600x600DPI

Conexión: wifi

Tipo de impresión: laser

Consumo: 550W

Tipo de impresora: multifunción

### **4.3.2. Virtualización de Servidores**

La consolidación de servidores Linux o Windows mediante el uso de tecnologías de virtualización ofrece numerosos beneficios para nuestro proyecto. A continuación, se detallan algunas ventajas destacadas de esta tecnología:

- **Reducción del número de servidores físicos:** Al consolidar servidores en entornos virtuales, podemos reducir la cantidad de hardware necesario. Esto se traduce en una disminución directa de los costos de mantenimiento de hardware.
- **Aprovechamiento eficiente del espacio de almacenamiento:** Implementar una estrategia de consolidación de servidores nos permite maximizar la utilización del espacio disponible de almacenamiento. Esto nos brinda la posibilidad de optimizar el uso de recursos y obtener un mayor rendimiento en términos de almacenamiento.

- **Aislamiento de aplicaciones:** Al asignar cada aplicación a su propio "servidor virtual", evitamos que una aplicación pueda afectar a otras durante mejoras o cambios. Esto proporciona un entorno más seguro y confiable para la implementación de actualizaciones y modificaciones.
- **Implementación ágil y escalable:** Podemos desarrollar normas de construcción de servidores virtuales que sean fácilmente replicables, lo que acelera la implementación y configuración de nuevos servidores. Esto nos brinda flexibilidad y agilidad para adaptarnos a las necesidades cambiantes de nuestra infraestructura.
- **Soporte para múltiples sistemas operativos:** La virtualización nos permite ejecutar diferentes tecnologías de sistemas operativos en una misma plataforma de hardware. Esto significa que podemos utilizar sistemas operativos como Windows Server, Linux y otros, según nuestras necesidades y requisitos específicos.

A continuación, se presenta una variedad de software de virtualización disponibles en el mercado, como se muestra en la siguiente imagen:

Nombre	Fabricante	HOST CPU	GUEST CPU	Host OS(s)	Guest (OS)	Tipo Licencia
<b>Hyper-V</b>	Microsoft	X64 + hardware-assisted virtualization (Intel VT or AMD-VT)	X64, x86	Windows 2008/Hyper-V, Windows Hyper-V Server	Drivers <u>soportados</u> para Windows 2000, Windows 2003, Windows 2008, Windows XP, Windows Vista, etc. Linux (SUSE10, <u>etc</u> )	Propietaria (Sin cargo con Windows Server 2008)
<b>Oracle VM</b>	Oracle Corp.	Intel x86, x86-64, Intel VT-x	Intel x86, x86-64, Intel VT-x	Sistema Operativo propio	Microsoft Windows, Oracle Enterprise, Linux, Red Hat Enterprise Linux	Libre
<b>Sun xVM VirtualBox</b>	Sun Microsystems	X86-64, SPARC	X86, (x86-64 only on <u>VirtualBox 2</u> with hardware virtualization)	Windows, Linux, Mac OS X (Intel), Solaris, <u>eComStation</u>	Dos, Windows, Linux, OS/2, <u>FreeBSD</u> , Solaris	Libre para uso personal y educación y evaluación
<b>VMWare ESXi</b>	VMWare	X86, x86-64	X86, x86-64	Sistema Operativo Propio	Windows, Linux, Netware, Solaris, FreeBSD	Propietaria
<b>VMWare Server</b>	VMWare	X86, x86-64	X86, x86-64	Windows, Linux	DOS, Windows, Linux, FreeBSD, Netware, Solaris, Virtual appliances	Propietaria
<b>Xen</b>	Citrix <u>Systems</u>	X86, AMD64	Mismo que el Host	<u>NetBSD</u> , Linux, Solaris	FreeBSD, <u>NetBSD</u> , Linux, Solaris, Windows XP & 2003	GPL

Hemos seleccionado **VMware** como nuestro hipervisor de elección debido a su amplia adopción, funcionalidad avanzada, soporte confiable, integración con nuestro entorno existente y capacidad de escalabilidad. Estamos convencidos de que esta elección nos permitirá lograr nuestros objetivos de virtualización de manera efectiva y eficiente en nuestro proyecto.

#### 4.3.2.1. Preparación del entorno y Creación de las máquinas virtuales

- Tener los dos servidores físicos adecuadamente configurados y conectados en la red.
- Instalar y configurar VMware vSphere ESXi en ambos servidores. Este es el hipervisor de VMware que permite la virtualización y administración de las máquinas virtuales.
- Utilizando VMware vSphere Client o VMware vCenter Server, crea las máquinas virtuales correspondientes a los servidores que deseas virtualizar (base de datos, DHCP, DNS, web y correo).
- Asignaremos la cantidad adecuada de recursos (CPU, memoria RAM, almacenamiento) a cada máquina virtual según sus requerimientos.

#### 4.3.2.2. Configuración de recursos para máquinas virtuales:

##### Servidor DNS:

- **Procesador:** Se recomienda asignar al menos 2 núcleos de procesador.
- **Memoria RAM:** Asigna al menos 2 GB de RAM.
- **Espacio de almacenamiento:** Selecciona una capacidad de almacenamiento suficiente para el sistema operativo y los archivos de configuración del servidor DNS. Un mínimo de 20 GB es recomendado.

##### Servidor DHCP:

- **Procesador:** Asigna al menos 2 núcleos de procesador.
- **Memoria RAM:** Asigna al menos 2 GB de RAM.
- **Espacio de almacenamiento:** Al igual que en el servidor DNS, reserva al menos 20 GB de espacio de almacenamiento para el sistema operativo y los archivos de configuración del servidor DHCP.

##### Servidor web:

- **Procesador:** Recomienda asignar al menos 4 núcleos de procesador para manejar las solicitudes web de manera eficiente.
- **Memoria RAM:** Asigna al menos 4 GB de RAM para el servidor web y los servicios asociados.
- **Espacio de almacenamiento:** Dependiendo del tamaño y la cantidad de sitios web que planeas alojar, reserva una capacidad de almacenamiento adecuada. Considera al menos 50 GB para el sistema operativo y los archivos del servidor web.

##### Servidor de correo:

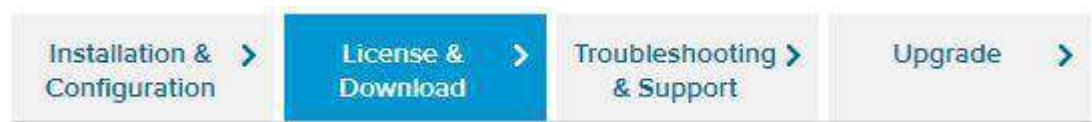
- **Procesador:** Asigna al menos 4 núcleos de procesador para manejar el procesamiento de correos electrónicos y tareas relacionadas.
- **Memoria RAM:** Asigna al menos 4 GB de RAM para garantizar un rendimiento óptimo del servidor de correo.
- **Espacio de almacenamiento:** Considera una capacidad de almacenamiento adecuada para alojar los buzones de correo de los usuarios y los archivos adjuntos. Dependiendo del tamaño y las necesidades de tu empresa, asigna al menos 100 GB de espacio de almacenamiento.

#### 4.3.2.3. Instalación de hipervisor en servidor

##### Instalación VMWare ESXi

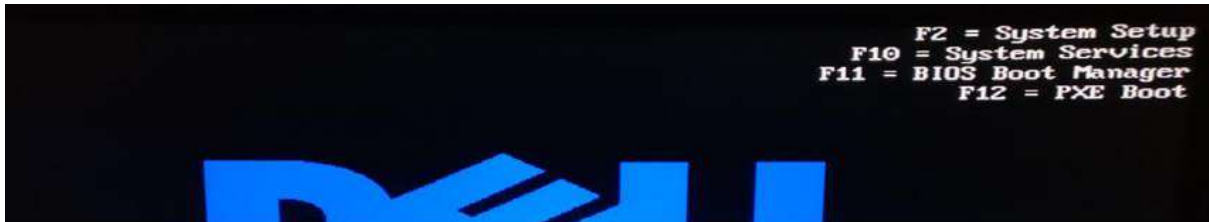


Se instalará vmware sobre el servidor, posteriormente vía web accederemos a nuestro hypervisor para configurar máquinas virtuales un elemento necesario para poder gestionar dentro de un mismo servidor físico diferentes máquinas a nivel virtual. Cabe decir, que VMware vSphere ESXi es de pago, descargamos directamente desde la página de [VMware](https://www.vmware.com). Simplemente, creamos una cuenta para poder acceder al apartado de descargas (License & Download):

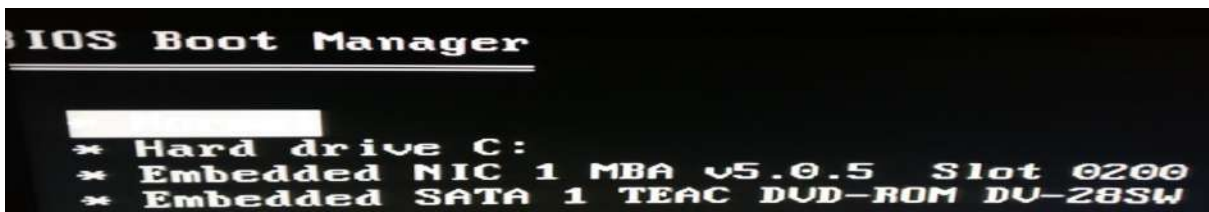


Posteriormente seleccionamos la versión de todas las disponibles y pinchamos en el botón "Manually Download". Empezará la descarga automáticamente. Una vez descargada la ISO, la grabamos en un Dvd o USB como imagen para poder usarla de arranque con el servidor, en nuestro caso usaremos un servidor DELL, Nada más encender el servidor tendréis que introducir el Dvd/USB en el lector e

inmediatamente activar la opción para arrancar desde vuestro lector. En mi caso, me aparece la opción arriba a la izquierda pulsando F11 justo al arranque:



es posible que en ciertos casos debéis entrar incluso en la BIOS (F2 – System Setup) para ajustar el arranque, Una vez pulsado F11 y después de cargar varios elementos, veremos el menú de boot con las diferentes opciones para arrancar

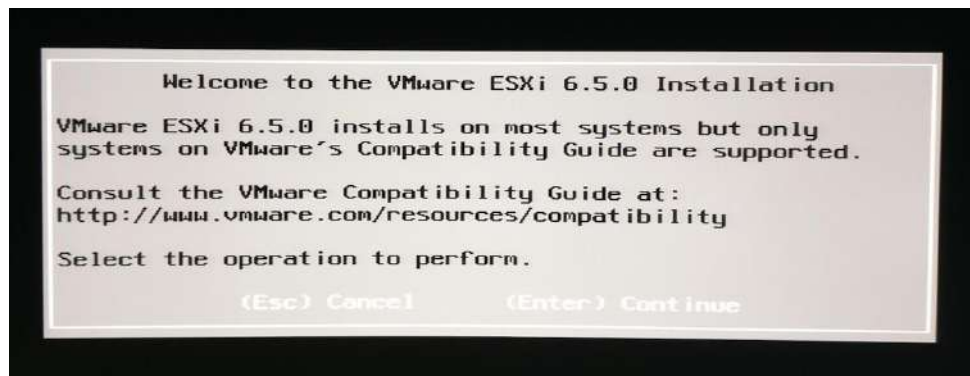


Una vez seleccionado el arranque , veremos la siguiente pantalla, en la cual seleccionaremos la primera opción para empezar a instalar el ESXi

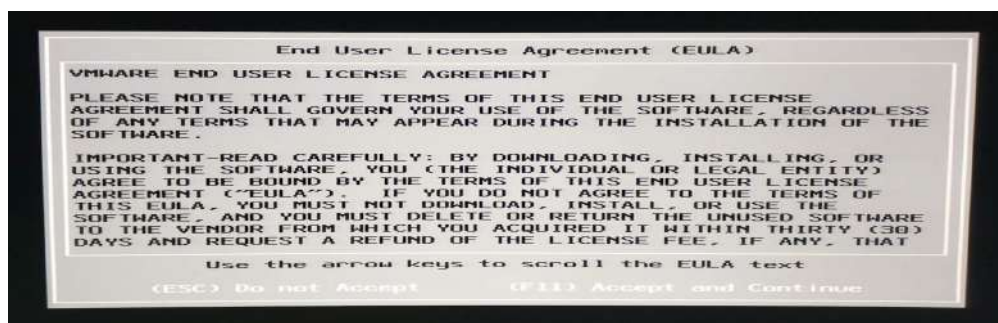


Veremos cómo empieza la carga de ficheros hasta que comience propiamente la instalación. Una vez terminada dicha carga, nos darán la bienvenida donde tecleamos "Enter" para continuar.

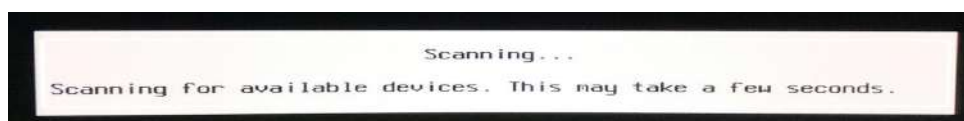




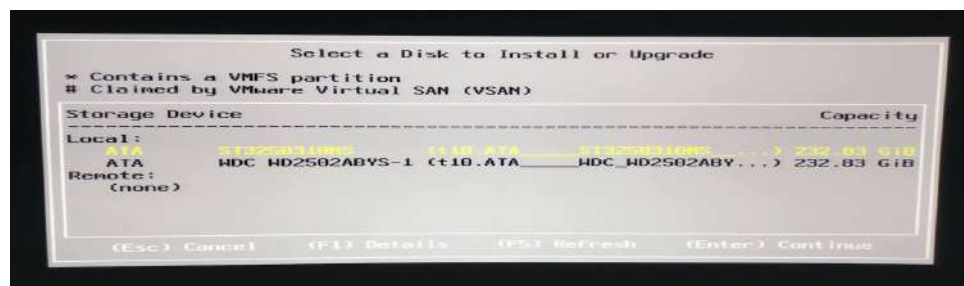
aceptaremos los términos de contrato mediante la tecla "F11"



realizará un escaneo de los medios donde instalar ESXi:



escogeré el primer recurso disponible para instalar ESXi. El espacio que sobre de este primero lo usaré para máquinas virtuales y el segundo disco lo usaré entero para almacenaje:

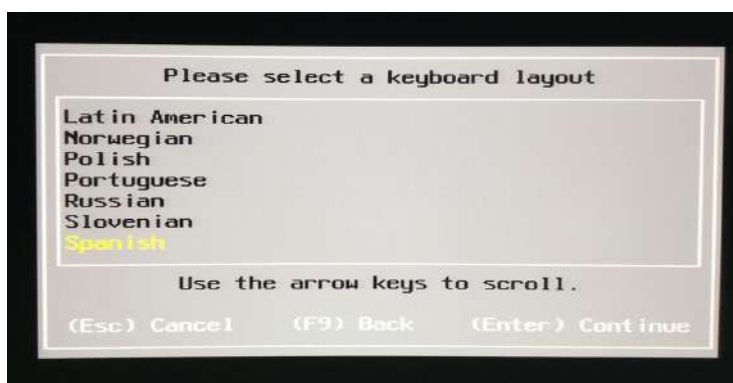


Aceptamos que se van a destruir/sobrescribir todos los datos contenidos en el disco duro donde colocaremos ESXi (presionamos "enter"):

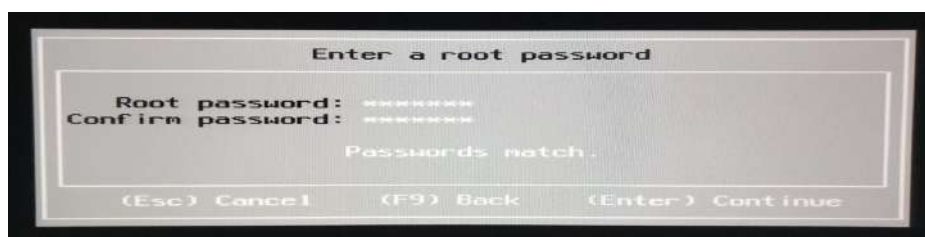




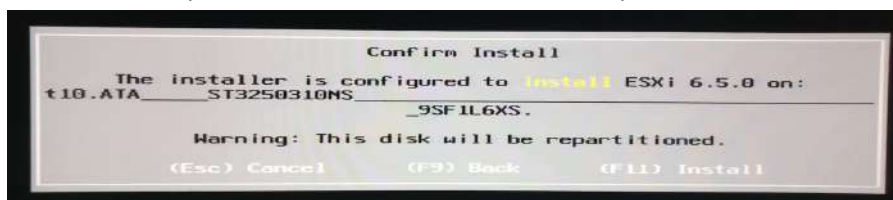
Confirmación de sobreescritura de disco duro de destino, Seleccionamos el idioma del teclado a usar:



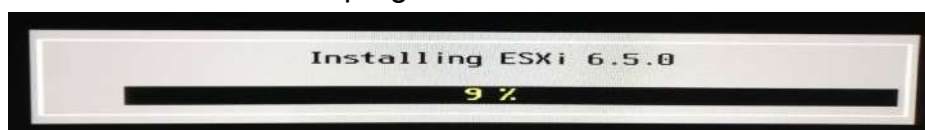
Y escogemos un password para el usuario “root” de nuestro ESXi, importante que lo guardéis bien:



Confirmamos la instalación (Presionamos “F11” de teclado):



Y a continuación veremos la barra de progreso:



Una vez acabada la instalación veremos el siguiente mensaje mediante el cual nos pide que retiremos el DVD/USB desde donde hemos instalado ESXi y reiniciemos el Servidor:

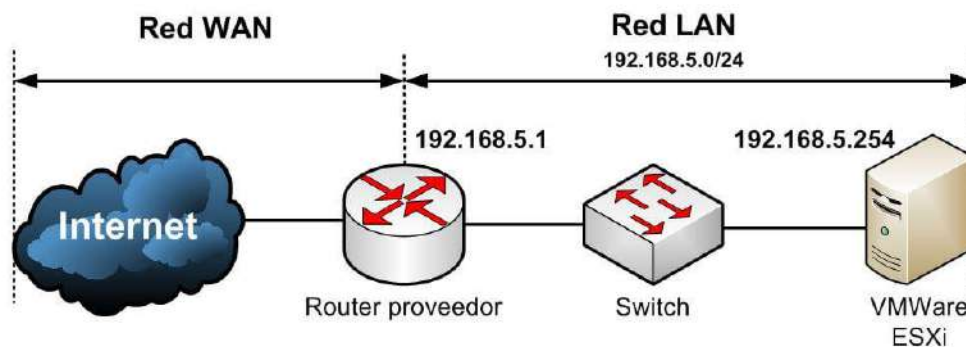


Una vez reiniciado, nuestro servidor acabará de realizar alguna que otra carga de archivos hasta ver la siguiente pantalla de inicio:



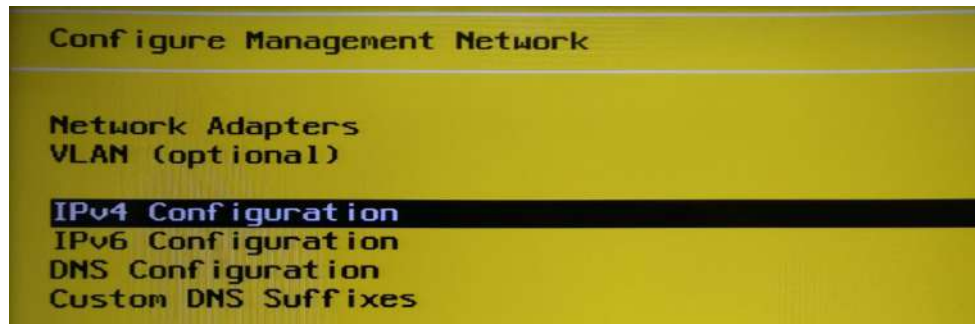
## Pantalla de inicio de VMWare después de la instalación

Pues bien, ya tenemos nuestro hypervisor instalado. Ahora, necesitamos configurarlo correctamente para integrarlo en nuestra red y poder empezar a configurar máquinas virtuales. Lo primero que deberíamos hacer es ponerle una IP del rango de nuestra red LAN donde irá conectado. Para que os hagáis una idea y poder ilustrar un poco este post, os muestro el escenario que tengo físicamente montado,

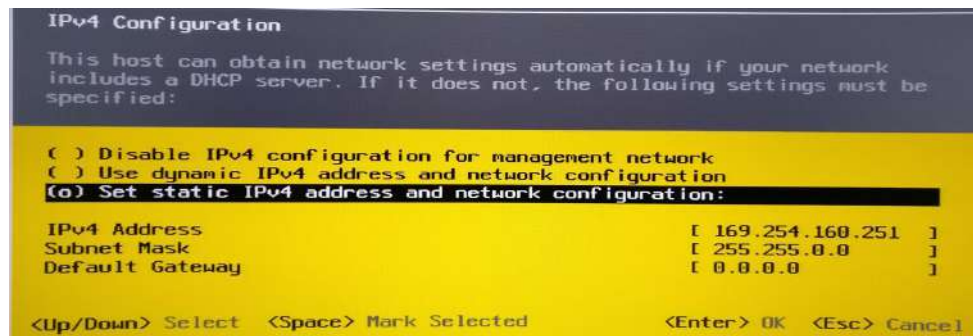


tecleamos “F2” para entrar en el apartado “Customized System/view logs”. Antes de poder entrar en el cuadro de configuración propiamente, debemos entrar el password de root que habíamos configurado durante la instalación y presionar “enter”. A continuación nos dirigimos a la opción “Configure Management Network” y presionamos “enter”.

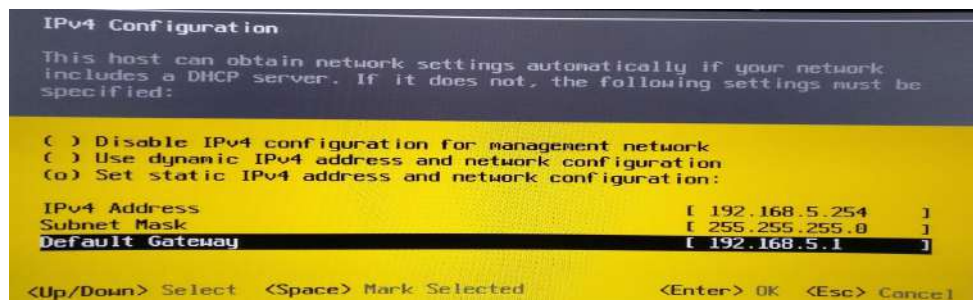




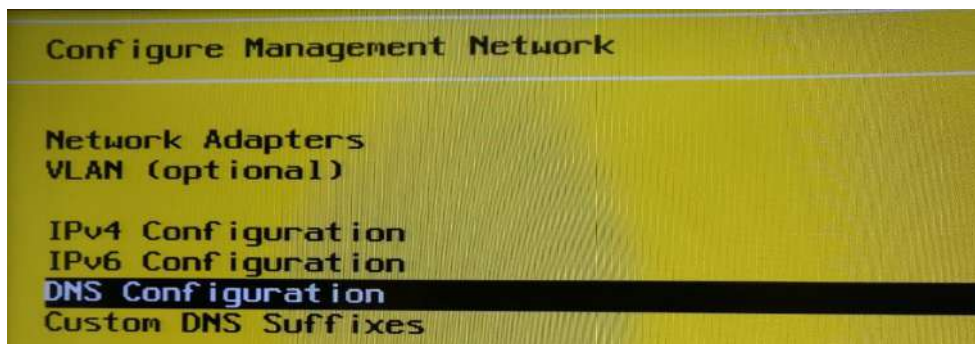
### Selección para configuración IPv6 VMWare



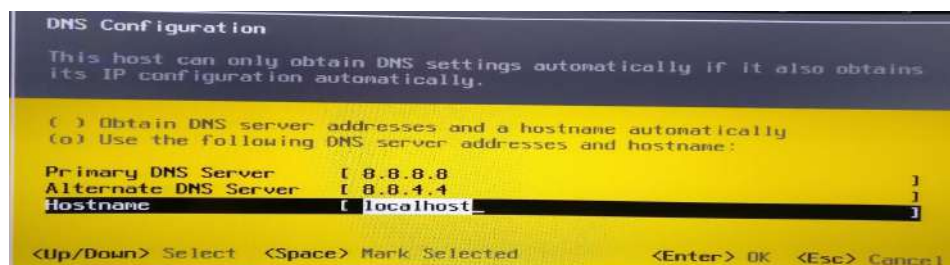
### Selección para IP estática en VMWare



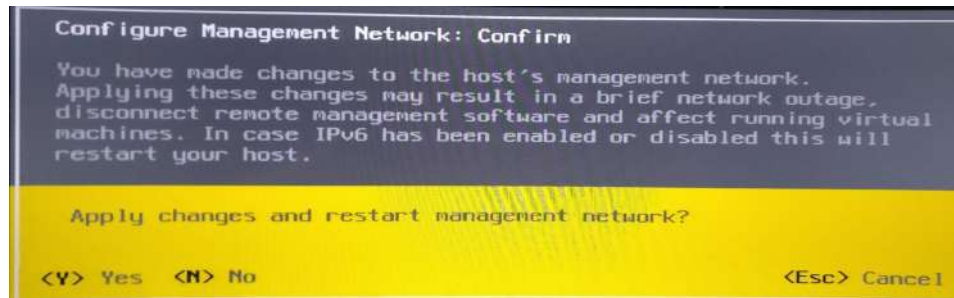
### Introducción IP máscara gateway VMWare



### Selección para DNS estático en VMWare



## Introducción DNS primario y secundario VMWare



## Confirmación aplicación cambios de red

```
C:\WINDOWS\system32>ping 192.168.5.254 -t

Haciendo ping a 192.168.5.254 con 32 bytes de datos:
Respuesta desde 192.168.5.254: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.5.254: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.5.254: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.5.254: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.5.254: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.5.254:
    Paquetes: enviados = 5, recibidos = 5, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Comprobación alcance de máquina VMWare desde PC, ahora nos quedaría acceder a nuestro hypervisor ESXi a través de cualquier PC conectado a la misma red. Para ello, abrimos un navegador con la IP, Veremos la siguiente pantalla:

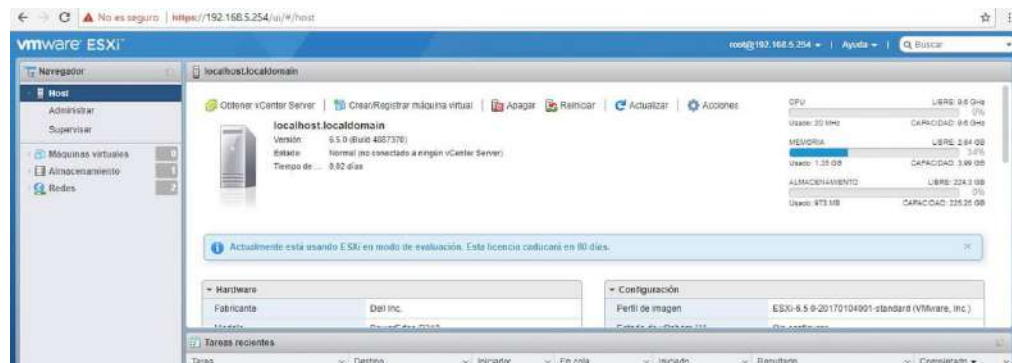




#### 4.3.2.4. Creación de máquinas virtuales

Se crearán las máquinas virtuales y luego se instalará el software correspondiente. Para crear una máquina virtual desde el vmware se deben seguir los siguientes pasos:

- Para ello, abrimos un navegador con la IP del servidor y nos autenticamos mediante usuario y contraseña entramos a la consola de configuración de las máquinas virtuales:



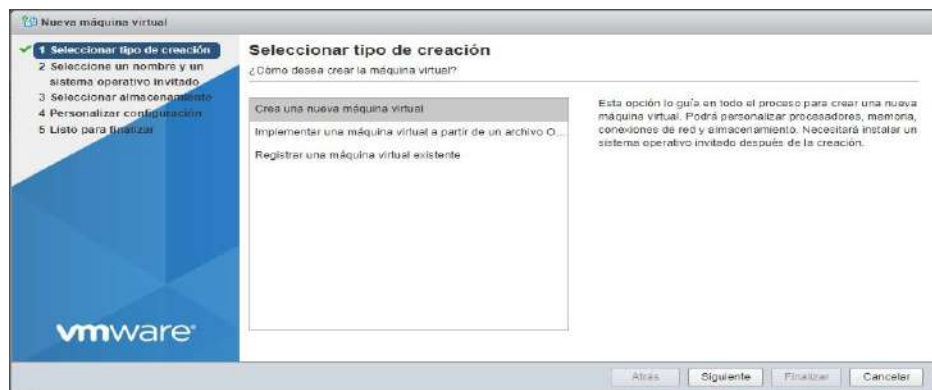
- Panel control web VMWare. Para ello nos dirigimos al menú derecho “máquinas virtuales”:



- Menú máquinas virtuales VMWare, A continuación vamos a la opción “Crear/regarstrar máquina virtual”:

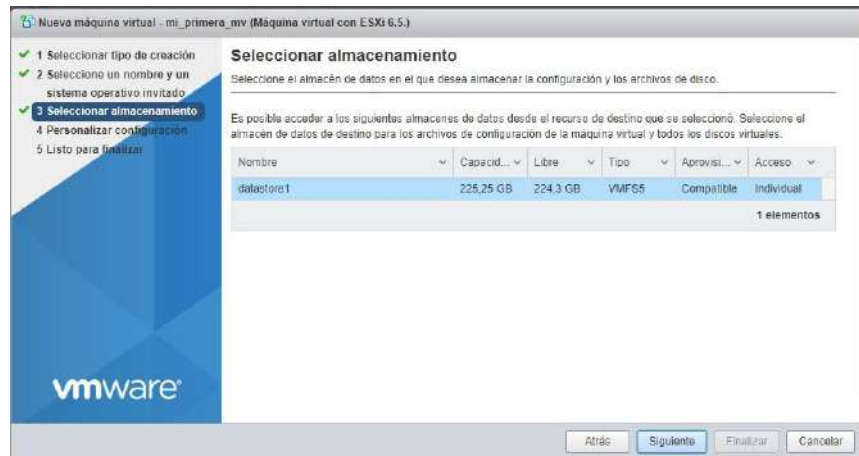


- Como vamos a crear una nueva máquina virtual a partir de una ISO previamente descargada seleccionaremos la opción “Crear una nueva máquina virtual”:



- Seleccionamos el nombre, la compatibilidad, el tipo de sistema operativo y la versión del sistema operativo:

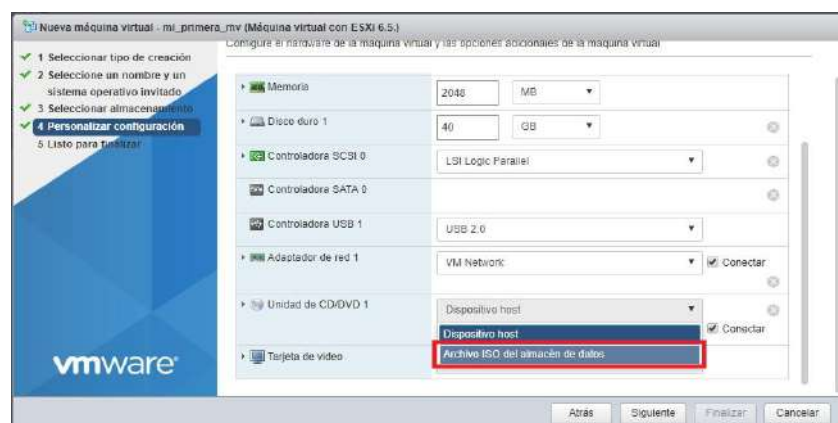




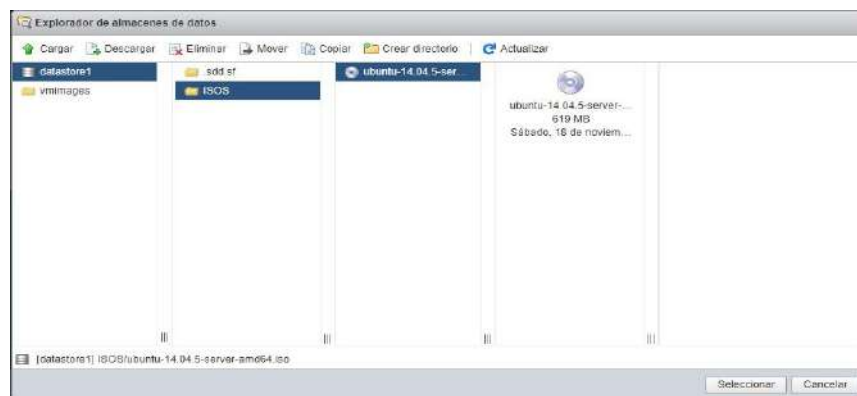
- Seleccionamos a continuación la cantidad de memoria, procesador, disco duro etc. que usaremos para nuestra máquina virtual:



- Selección personalizada de configuración VMWare



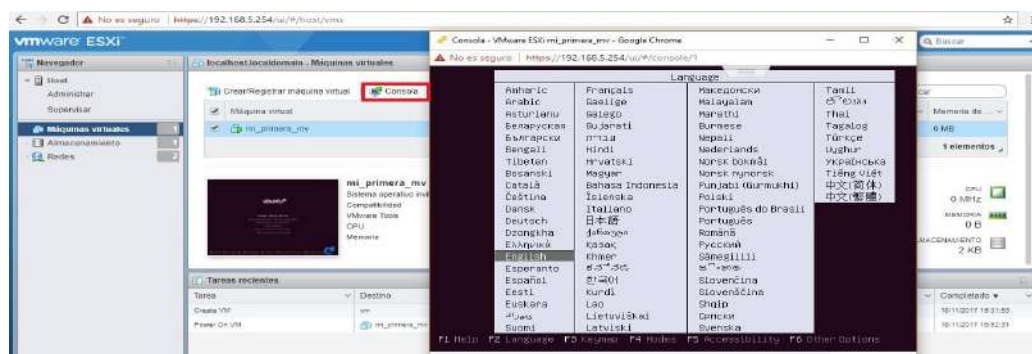
- Archivo ISO del almacén de datos VMWare



- Selección de ISO en almacén de datos VMWare



- Resumen de opciones en máquina virtual VMWare





Una vez que se ha creado la máquina virtual con las características necesarias, se procede a instalar el Sistema operativo

#### 4.3.2.5. Virtualización servidor web y correo :

Se configura en una máquina virtual con un sistema operativo ubuntu, una vez creada con vmware la máquina virtual en el servidor.

##### Máquina virtual para el servidor web:

Configuraremos una máquina virtual en linux que ejecute el servidor web en Apache para alojar el sitio web de la empresa.

- **Amplia adopción y popularidad:** Apache es uno de los servidores web más utilizados y populares en el mundo. Es de código abierto y cuenta con una amplia comunidad de usuarios y desarrolladores que ofrecen soporte y contribuyen a su desarrollo continuo. Esta amplia adopción asegura que puedas encontrar una gran cantidad de recursos y documentación en línea para ayudarte en la configuración y administración de Apache.
- **Estabilidad y rendimiento:** Apache es conocido por su estabilidad y rendimiento. Ha sido utilizado en entornos empresariales durante muchos años y se ha demostrado su capacidad para manejar un alto volumen de solicitudes de manera eficiente. Apache también tiene un bajo consumo de recursos, lo que es importante para asegurar un rendimiento óptimo de tu sitio web.
- **Flexibilidad y personalización:** Apache ofrece una gran flexibilidad y opciones de personalización. Puedes configurar el servidor web para adaptarse a las necesidades específicas de la web empresarial. Apache soporta diversos módulos y extensiones que permiten agregar funcionalidades adicionales, como el soporte de diferentes lenguajes de programación, compresión de datos, autenticación y cifrado SSL/TLS.
- **Compatibilidad con sistemas operativos:** Apache es compatible con una amplia gama de sistemas operativos, incluyendo Windows, Linux, macOS y otros. Esto te brinda la flexibilidad para ejecutar tu máquina virtual con Apache en el sistema operativo que mejor se adapte a tus necesidades y preferencias.
- **Seguridad:** Apache cuenta con una sólida reputación en términos de seguridad. La comunidad de desarrollo de Apache mantiene actualizaciones regulares y parches de seguridad para abordar las vulnerabilidades conocidas. Además, puedes configurar reglas de seguridad y protección específicas en el servidor web para mitigar posibles ataques y asegurar la integridad de tu sitio web y los datos de tus usuarios.
- **Soporte para estándares web:** Apache cumple con los estándares web y los protocolos más comunes, como HTTP, HTTPS, SSL/TLS, IPv6 y otros. Esto

asegura que tu sitio web sea compatible con diversos navegadores web y pueda proporcionar una experiencia óptima a tus usuarios.

### **Máquina virtual para el servidor de correo:**

Configurar una máquina virtual en windows que ejecute el servidor de correo electrónico para manejar los correos electrónicos de la empresa. Microsoft Exchange Server es una solución de servidor de correo electrónico ampliamente utilizada en entornos empresariales.

- **Integración con entornos de Microsoft:** Microsoft Exchange Server se integra de manera nativa con otros productos y servicios de Microsoft, como Active Directory. Esto facilita la gestión de usuarios, grupos y permisos de correo electrónico, así como la sincronización de la información del directorio y la autenticación centralizada.
- **Características completas de correo electrónico:** Microsoft Exchange Server ofrece una amplia gama de características para la administración y entrega de correos electrónicos. Podemos configurar buzones de correo para los usuarios, administrar listas de distribución, establecer políticas de retención y archivado de correos electrónicos, configurar reglas de flujo de correo y aplicar medidas de seguridad como cifrado y autenticación.
- **Colaboración y productividad:** Exchange Server proporciona características de colaboración y productividad adicionales, como la posibilidad de compartir calendarios, contactos y tareas. Los usuarios pueden programar reuniones, invitar a otros a eventos y administrar sus horarios de manera eficiente dentro de la organización.
- **Administración centralizada:** Exchange Server ofrece herramientas de administración centralizada, como el "Centro de administración de Exchange", que permite configurar y administrar el servidor de correo electrónico de manera intuitiva y eficiente. Puedes realizar tareas como la creación de buzones de correo, la configuración de políticas de retención, el seguimiento del rendimiento del servidor y la solución de problemas.
- **Alta disponibilidad y escalabilidad:** Exchange Server proporciona opciones para implementar una arquitectura de alta disponibilidad, lo que significa que puedes asegurar que el servicio de correo electrónico esté disponible de manera continua incluso en caso de fallas. También es escalable, lo que te permite agregar más capacidad a medida que tu empresa crece y aumenta la carga de correo electrónico.

- **Seguridad y cumplimiento normativo:** Exchange Server cuenta con medidas de seguridad integradas, como filtrado de correo no deseado, antivirus y antimalware. También cumple con estándares de cumplimiento normativo, como el cumplimiento de la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) y la Ley de Protección de Datos (GDPR).

#### 4.3.2.6. Virtualización servidor DHCP, DNS, VPN

##### Máquina virtual para el servidor DHCP:

Esta máquina virtual que ejecutaremos como servidor DHCP es un Windows 10, será utilizado para asignar direcciones IP automáticamente a los dispositivos de la red. A Través de Windows Server que es un sistema operativo de servidor desarrollado por Microsoft que incluye una funcionalidad de servidor DHCP integrada.

- **Integración con el entorno de Windows:** Si ya estamos utilizando otros productos y servicios de Microsoft en la infraestructura, Windows Server puede integrarse fácilmente con ellos. Esto simplifica la administración y el control centralizado de la red.
- **Amplia compatibilidad:** Windows Server admite una amplia variedad de sistemas operativos de clientes, incluidos Windows, macOS, Linux y otros dispositivos de red. Podemos configurar el servidor DHCP para asignar direcciones IP y otros parámetros de configuración a diferentes tipos de dispositivos en tu red.
- **Interfaz gráfica intuitiva:** Windows Server ofrece una interfaz gráfica de usuario (GUI) fácil de usar para configurar y administrar el servidor DHCP. Podemos utilizar la herramienta "Administrador del servidor" para habilitar el rol de servidor DHCP, configurar los ámbitos (rangos de direcciones IP) y establecer las opciones de configuración.
- **Funcionalidades avanzadas:** Además de asignar direcciones IP automáticamente, Windows Server también proporciona características avanzadas de DHCP. Podemos configurar opciones adicionales, como la asignación de direcciones IP estáticas basadas en direcciones MAC, opciones de configuración personalizadas y administración de reenviadores DHCP para redes múltiples.

**La configuración básica** de Windows Server como servidor DHCP implica los siguientes pasos:

- Instala el rol de servidor DHCP en Windows Server desde la herramienta "Administrador del servidor".
- Configura los ámbitos, que son los rangos de direcciones IP disponibles para asignar a los clientes.
- Establece las opciones de configuración DHCP, como la puerta de enlace predeterminada, los servidores DNS y otros parámetros específicos de la red.
- Habilita y configura la concesión de direcciones IP estáticas para dispositivos específicos (esto es opcional).
- Realiza pruebas para asegurarte de que el servidor DHCP esté asignando correctamente las direcciones IP a los dispositivos de la red.

### **Máquina virtual para el servidor DNS:**

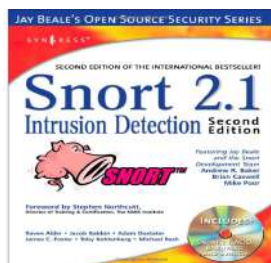
Configuraremos una máquina virtual en entorno windows que ejecute el servidor DNS en windows server para resolver nombres de dominio dentro de la red corporativa. Es una buena elección por las siguientes razones:

- **Integración nativa:** Windows Server incluye el servicio de DNS de Microsoft, lo que significa que no necesitarás instalar software adicional. El servicio de DNS se integra de forma nativa con otros componentes de Windows Server, como Active Directory, lo que facilita la administración centralizada de los registros DNS en tu red corporativa.
- **Amplia compatibilidad:** Windows Server es ampliamente utilizado en entornos corporativos y es compatible con una variedad de sistemas operativos cliente. Esto asegura que los dispositivos en tu red, ya sean Windows, macOS o Linux, puedan resolver los nombres de dominio correctamente utilizando el servidor DNS de Windows Server.
- **Gestión centralizada:** Windows Server ofrece herramientas de administración centralizadas, como el "Administrador del servidor", que facilitan la configuración y la administración del servidor DNS. Puedes configurar zonas DNS, registros de recursos, políticas de resolución y otras opciones a través de una interfaz gráfica de usuario intuitiva.
- **Seguridad y estabilidad:** Microsoft realiza actualizaciones periódicas y brinda soporte para Windows Server, lo que garantiza un alto nivel de seguridad y estabilidad para tu servidor DNS. Además, Windows Server cuenta con características de seguridad adicionales, como la integración con Active Directory para autenticación y control de acceso.
- **Integración con Active Directory:** utilizando Active Directory en la infraestructura de red, configurar el servidor DNS de Windows Server permite una integración estrecha con Active Directory. Esto facilita la resolución de

nombres de dominio de los controladores de dominio y otros servicios asociados a Active Directory.

- **Escalabilidad y rendimiento:** Windows Server puede escalar para manejar redes corporativas de cualquier tamaño. Puedes agregar servidores DNS adicionales en tu infraestructura para distribuir la carga y garantizar un rendimiento óptimo de resolución de nombres de dominio.

### 4.3.3. Software de seguridad



Para proteger la red corporativa contra amenazas externas, se recomienda implementar firewalls de red y sistemas de detección y prevención de intrusiones (IDS/IPS). Establecer políticas de seguridad, como contraseñas sólidas, actualizaciones de software y políticas de acceso, también es fundamental para proteger los activos y datos de la empresa.

Además, se puede introducir un servidor proxy en la red corporativa para gestionar y controlar el tráfico de Internet de los usuarios. El servidor proxy actuará como intermediario y mejorará la seguridad y el rendimiento de la red. Se pueden configurar reglas y políticas en el servidor proxy para controlar el acceso a los sitios web, autenticar a los usuarios y aplicar filtros de contenido.

Para la implementación de estos servicios de seguridad, los softwares Squid y Snort pueden ser utilizados. Squid actúa como servidor proxy y caché web, mientras que Snort es un sistema de detección de intrusos. Squid se instala en un servidor dedicado o en una máquina virtual, y se configura para filtrar y controlar el tráfico web. Por otro lado, Snort se instala en sensores estratégicamente ubicados dentro de la red, y se encarga de monitorear y detectar posibles intrusiones.

#### 4.3.4. FortiClient VPN



En este punto, se propone la implementación de una solución de acceso remoto VPN, utilizando FortiClient VPN en el enrutador para asegurar la conectividad segura y confiable de usuarios remotos con acceso a la red local, esta es una solución líder en el mercado, con el objetivo de proporcionar una conectividad segura y proteger la integridad de los datos en la red. Se tomarán en cuenta las listas de control de acceso (ACL) para permitir el acceso de la VPN a la red local

Para este proyecto FortiClient VPN es una solución de software basada en cliente que proporciona una serie de funciones de seguridad para ordenadores de sobremesa y portátiles. Cuando se utiliza junto con FortiGate, FortiClient proporciona cifrado IPsec y SSL, optimización de WAN, conformidad de terminales y autenticación de dos factores, a continuación destacamos sus principales características:

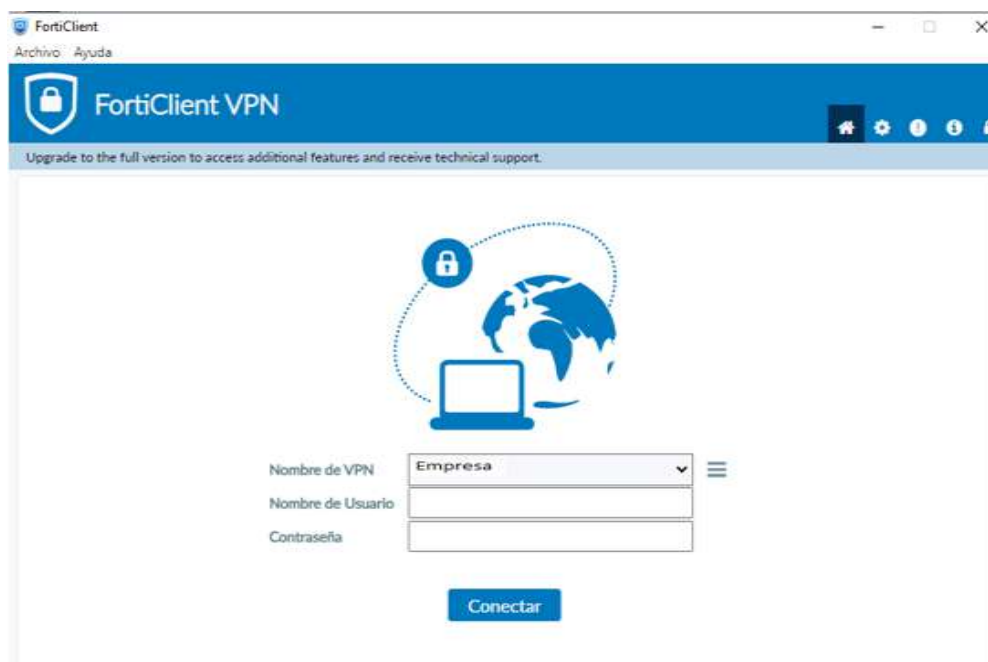
- **Seguridad robusta:** FortiClient VPN ofrece una seguridad sólida con protocolos de cifrado fuertes y opciones de autenticación avanzadas. La prioridad en la seguridad de Fortinet y su enfoque en la protección de la red hacen de FortiClient VPN una elección confiable para asegurar las comunicaciones en un entorno empresarial.
- **Gestión centralizada:** La capacidad de administrar y configurar FortiClient VPN de manera centralizada a través de la consola de administración de Fortinet simplifica la gestión de las conexiones VPN. Esto permite una implementación más eficiente, monitoreo en tiempo real y actualizaciones de configuraciones a través de la red, lo que ahorra tiempo y recursos.
- **Amplia compatibilidad:** FortiClient VPN es compatible con múltiples plataformas, incluyendo Windows, macOS, Linux, iOS y Android. Esto

garantiza que los usuarios puedan acceder a la red empresarial desde una variedad de dispositivos, proporcionando flexibilidad y conveniencia.

- **Integración con soluciones Fortinet:** FortiClient VPN se integra perfectamente con otros productos de seguridad de Fortinet, como firewalls y sistemas de prevención de intrusiones (IPS). Esta integración facilita la implementación y el monitoreo conjunto de múltiples capas de seguridad, creando un entorno de red más resistente y confiable.
- **Resultados esperados:**  
Conexiones remotas seguras y confiables a la red local a través de la VPN implementada en el router.

Cumplimiento de los requisitos de seguridad establecidos para el acceso remoto.  
Garantía de la integridad y confidencialidad de los datos transmitidos a través de la VPN. Correcta configuración de la VPN y las políticas de seguridad implementadas en la red.

Como cualquier solución, FortiClient VPN también tiene algunas desventajas a considerar, como el costo y la curva de aprendizaje para familiarizarse con la configuración y administración de la solución. Sin embargo, en general, considero que FortiClient VPN es una elección sólida debido a su enfoque en la seguridad, la gestión centralizada y la compatibilidad multiplataforma para nuestra Red.





#### 4.3.5. Presupuesto

Material	Precio unidad (€) por	Cantidad	Total (€)
Ordenadores	280-380	40	13.000
Switches	500	5	2.500
Routers	1400	1	1.400
Firewall	500	1	500
Puntos de acceso	157	2	314
Servidores	2000/11000/500	3	13.500
Cables	40(50m)	15	600
Racks	600/300	2	900
Sai	680	1	680
Software	500(Media)	8	4.000
Rosetas,Patch panel,etc.	70(Media)	20	1.400
<b>TOTAL PRESUPUESTO</b>			<b>38.794</b>



## 4.4. Limitaciones

Durante la implementación de IPv6 en Cisco Packet Tracer, nos dimos cuenta de que la plataforma no cuenta con las características necesarias para satisfacer nuestras necesidades específicas. Esto se debe a que la versión actual no incluye las funcionalidades requeridas para el uso completo de IPv6.

A medida que avanzamos paso a paso en la configuración del proyecto, nos dimos cuenta de que se nos estaba agotando el tiempo de entrega. Encontramos varios desafíos que afectaron nuestra implementación de IPv6. Por ejemplo, en el protocolo DHCP, no contamos con la opción de desactivar la autoconfiguración de SLAAC (Stateless Address Autoconfiguration), lo cual era necesario para nuestra configuración.

Por último, nos enfrentamos a un problema con la tunelización, ya que descubrimos que la funcionalidad de RIP (Routing Information Protocol) no funcionaba correctamente en nuestro escenario. Esto afectó la capacidad de establecer una comunicación eficiente entre diferentes redes IPv6 a través de túneles.

Debido a estas limitaciones y desafíos encontrados en Cisco Packet Tracer, hemos tenido que adaptar nuestra implementación y buscar alternativas para abordar estos problemas.

## 4.5. Conclusiones

Tras el diseño de esta red y considerando nuestros objetivos iniciales del proyecto de establecer una red segura y eficiente que satisfaga las necesidades de comunicación de los diferentes departamentos, así como implementar políticas y procedimientos de seguridad, incluyendo la gestión de contraseñas, y configurar una conexión VPN para el acceso remoto seguro a los recursos internos, hemos llegado a las siguientes conclusiones.

1. Se ha logrado una exitosa segmentación de la red por departamentos, lo cual ha permitido mantener un mayor control y seguridad en el acceso a los recursos. Cada departamento cuenta con su propia subred y se han establecido medidas de seguridad para restringir el acceso no autorizado entre ellos.
2. Gracias al uso del protocolo LACP (Link Aggregation Control Protocol) en la configuración de los enlaces de Ethernet, se ha logrado establecer conexiones rápidas y eficientes entre los diferentes dispositivos de red. Esto ha contribuido a una mayor velocidad de transferencia de datos y una mejor experiencia de comunicación en la red.
3. Se ha realizado la configuración de la red Wi-Fi para proporcionar conectividad inalámbrica a los dispositivos de la empresa. Se han implementado medidas de seguridad, como la encriptación y la autenticación, para proteger la red inalámbrica contra accesos no autorizados.
4. Se ha implementado un túnel IPv6 a través de una red IPv4 para permitir la transmisión de tráfico IPv6 a través de una infraestructura que solo admite IPv4.
5. Se han configurado las listas de control de acceso necesarias según los requerimientos solicitados para mejorar la seguridad de la red y los empleados.

## 5. Anexo

Configuración de todos los equipos con show running-config

### Router-empresa

```
!  
version 15.4  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname Router  
!  
no ip cef  
ipv6 unicast-routing  
!  
no ipv6 cef  
!  
ipv6 dhcp pool VLAN10  
address prefix 2001:0db8:1111:10::/64 lifetime 172800 86400  
dns-server 2001:DB8:1111:90::10  
domain-name monedamundial.com  
!  
ipv6 dhcp pool VLAN20  
address prefix 2001:0db8:1111:20::/64 lifetime 172800 86400  
dns-server 2001:DB8:1111:90::10  
domain-name monedamundial.com  
!  
ipv6 dhcp pool VLAN30  
address prefix 2001:0db8:1111:30::/64 lifetime 172800 86400  
dns-server 2001:DB8:1111:90::10  
domain-name monedamundial.com  
!  
ipv6 dhcp pool VLAN40  
address prefix 2001:0db8:1111:40::/64 lifetime 172800 86400  
dns-server 2001:DB8:1111:90::10  
domain-name monedamundial.com  
!  
ipv6 dhcp pool VLAN50  
address prefix 2001:0db8:1111:50::/64 lifetime 172800 86400  
dns-server 2001:DB8:1111:90::10  
domain-name monedamundial.com  
!
```

```

ipv6 dhcp pool VLAN60
address prefix 2001:0db8:1111:60::/64 lifetime 172800 86400
dns-server 2001:DB8:1111:90::10
domain-name monedamundial.com
!
ipv6 dhcp pool VLAN110
address prefix 2001:0db8:1111:110::/64 lifetime 172800 86400
dns-server 2001:DB8:1111:90::10
domain-name monedamundial.com
!
ipv6 dhcp pool VLAN120
address prefix 2001:0db8:1111:120::/64 lifetime 172800 86400
dns-server 2001:DB8:1111:90::10
domain-name monedamundial.com
!
!
spanning-tree mode pvst

!
interface GigabitEthernet0/0/0
no ip address
ipv6 traffic-filter dmz in
duplex auto
speed auto
ipv6 address 2001:DB8:6::1/64
ipv6 rip 9 enable
ipv6 enable
!
interface GigabitEthernet0/0/1
no ip address
duplex auto
speed auto
ipv6 address 2001:DB8:1111:1::1/64
ipv6 rip 9 enable
ipv6 enable
!
interface GigabitEthernet0/0/1.10
description vlan direccion
encapsulation dot1Q 10
no ip address
ipv6 address 2001:DB8:1111:10::1/64
ipv6 rip 9 enable
ipv6 enable

```

```
ipv6 dhcp server VLAN10
!
interface GigabitEthernet0/0/1.20
description vlan RRHH
encapsulation dot1Q 20
no ip address
ipv6 address 2001:DB8:1111:20::1/64
ipv6 rip 9 enable
ipv6 enable
ipv6 dhcp server VLAN20
!
interface GigabitEthernet0/0/1.30
description vlan contabilidad
encapsulation dot1Q 30
no ip address
ipv6 address 2001:DB8:1111:30::1/64
ipv6 rip 9 enable
ipv6 enable
ipv6 dhcp server VLAN30
!
interface GigabitEthernet0/0/1.40
description vlan informatica
encapsulation dot1Q 40
no ip address
ipv6 address 2001:DB8:1111:40::1/64
ipv6 rip 9 enable
ipv6 enable
ipv6 dhcp server VLAN40
!
interface GigabitEthernet0/0/1.50
description vlan disenio
encapsulation dot1Q 50
no ip address
ipv6 address 2001:DB8:1111:50::1/64
ipv6 rip 9 enable
ipv6 enable
ipv6 dhcp server VLAN50
!
interface GigabitEthernet0/0/1.60
description vlan produccion
encapsulation dot1Q 60
no ip address
ipv6 address 2001:DB8:1111:60::1/64
```

```
ipv6 rip 9 enable
ipv6 enable
ipv6 dhcp server VLAN60
!
interface GigabitEthernet0/0/1.90
encapsulation dot1Q 90
no ip address
ipv6 address 2001:DB8:1111:90::1/64
ipv6 rip 9 enable
ipv6 enable
!
interface GigabitEthernet0/0/1.110
description vlan-wifi-empleados
encapsulation dot1Q 110
no ip address
ipv6 address 2001:DB8:1111:110::1/64
ipv6 rip 9 enable
ipv6 enable
ipv6 dhcp server VLAN110
!
interface GigabitEthernet0/0/1.120
description vlan-wifi-empleados
encapsulation dot1Q 120
no ip address
ipv6 address 2001:DB8:1111:120::1/64
ipv6 rip 9 enable
ipv6 enable
ipv6 dhcp server VLAN120
!
interface GigabitEthernet0/0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/1/0
description internet
no ip address
ipv6 traffic-filter icmp-tcp-a-lan in
ipv6 address 2001:DB8:2::2/64
ipv6 rip 9 enable
ipv6 enable
clock rate 2000000
```

```

!
interface Serial0/1/1
  no ip address
  clock rate 2000000
  shutdown
!
interface Vlan1
  no ip address
  shutdown
!
ipv6 router rip 9
!
ip classless
!
ip flow-export version 9
!
ipv6 route ::/0 Serial0/1/0
!
ipv6 access-list lan
  deny ipv6 any any
  permit icmp 2001:DB8:1111:2::/64 any
ipv6 access-list icmp-tcp-a-lan
  permit tcp any 2001:DB8:6::/64 eq www
  permit icmp any 2001:DB8:6::/64
  permit ipv6 2001:DB8:1111:100::/64 2001:DB8:1111:10::/64
  deny icmp any any echo-request
  deny tcp any 2001:DB8:1111:90::/64 eq www
  permit ipv6 any any
  permit ipv6 host 2001:DB8:1111:100::10 host 2001:DB8:1111:10::10
ipv6 access-list dmz
  deny icmp 2001:DB8:6::/64 any echo-request
  deny tcp any 2001:DB8:1111:90::/64 eq www
  permit ipv6 any any

!
line con 0
!
line aux 0
!
line vty 0 4
  login
!
!

```



```
!  
end
```

### Switch central

```
!  
version 12.1  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname Switch  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
interface Port-channel1  
  switchport trunk native vlan 100  
  switchport trunk allowed vlan 10,20,30,40,50,60,90,100  
  switchport mode trunk  
!  
interface Port-channel2  
  switchport trunk native vlan 100  
  switchport trunk allowed vlan 10,20,30,40,50,60,90,100  
  switchport mode trunk  
!  
interface Port-channel4  
  switchport trunk native vlan 100  
  switchport trunk allowed vlan 10,20,30,40,50,60,90,100  
  switchport mode trunk  
!  
interface GigabitEthernet0/1  
  switchport trunk native vlan 100  
  switchport trunk allowed vlan 10,20,30,40,50,60,90,100,110,120  
  switchport mode trunk  
!  
interface GigabitEthernet1/1  
  switchport trunk native vlan 100  
  switchport trunk allowed vlan 10,20,30,40,50,60,90,100  
  switchport mode trunk  
  channel-group 4 mode active
```



```
!  
interface GigabitEthernet2/1  
  switchport trunk native vlan 100  
  switchport trunk allowed vlan 10,20,30,40,50,60,90,100  
  switchport mode trunk  
  channel-group 1 mode active  
!  
interface GigabitEthernet3/1  
  switchport trunk native vlan 100  
  switchport trunk allowed vlan 10,20,30,40,50,60,90,100  
  switchport mode trunk  
  channel-group 1 mode active  
!  
interface GigabitEthernet4/1  
  switchport trunk native vlan 100  
  switchport trunk allowed vlan 10,20,30,40,50,60,90,100  
  switchport mode trunk  
  channel-group 2 mode active  
!  
interface GigabitEthernet5/1  
  switchport trunk native vlan 100  
  switchport trunk allowed vlan 10,20,30,40,50,60,90,100  
  switchport mode trunk  
  channel-group 2 mode active  
!  
interface GigabitEthernet6/1  
  switchport trunk native vlan 100  
  switchport trunk allowed vlan 10,20,30,40,50,60,90,100  
  switchport mode trunk  
  channel-group 4 mode active  
!  
interface GigabitEthernet7/1  
  switchport access vlan 110  
  switchport mode access  
!  
interface GigabitEthernet8/1  
  switchport access vlan 120  
  switchport mode access  
!  
interface GigabitEthernet9/1  
!  
interface Vlan1  
  no ip address
```

```
shutdown
!  
line con 0
!  
line vty 0 4
login
line vty 5 15
login  
  
end
```

### **Switch lateral izquierdo (DRCI)**

```
!  
version 15.0  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname Switch  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
interface Port-channel1  
switchport trunk native vlan 100  
switchport trunk allowed vlan 10,20,30,40,100  
switchport mode trunk  
!  
interface Port-channel3  
switchport trunk native vlan 100  
switchport trunk allowed vlan 10,20,30,40,50,60,90,100  
switchport mode trunk  
!  
interface Port-channel4  
switchport trunk native vlan 100  
switchport trunk allowed vlan 10,20,30,40,50,60,100  
switchport mode trunk  
!  
interface FastEthernet0/1  
switchport trunk native vlan 100  
switchport trunk allowed vlan 10,20,30,40,50,60,100  
switchport mode trunk
```

```
channel-group 4 mode active
!
interface FastEthernet0/2
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 30
switchport trunk native vlan 100
switchport trunk allowed vlan 10,20,30,40,50,60,100
switchport mode access
channel-group 4 mode active
!
interface FastEthernet0/5
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/8
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/11
switchport access vlan 10
```

```
switchport mode access
!
interface FastEthernet0/12
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/13
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/14
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/15
switchport access vlan 40
switchport mode access
!
interface FastEthernet0/16
switchport access vlan 40
switchport mode access
!
interface FastEthernet0/17
switchport access vlan 40
switchport mode access
!
interface FastEthernet0/18
switchport access vlan 40
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 40
switchport mode access
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
switchport trunk native vlan 100
switchport trunk allowed vlan 10,20,30,40,50,60,90,100
```

```
switchport mode trunk
channel-group 3 mode active
!
interface FastEthernet0/24
switchport trunk native vlan 100
switchport trunk allowed vlan 10,20,30,40,50,60,90,100
switchport mode trunk
channel-group 3 mode active
!
interface GigabitEthernet0/1
switchport trunk native vlan 100
switchport trunk allowed vlan 10,20,30,40,100
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet0/2
switchport trunk native vlan 100
switchport trunk allowed vlan 10,20,30,40,100
switchport mode trunk
channel-group 1 mode active
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
no ip address
!
interface Vlan20
no ip address
!
interface Vlan30
no ip address
!
interface Vlan40
no ip address
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
```



```
!  
end
```

### Switch derecho DIS\_PD

```
!  
version 15.0  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname Switch  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
interface Port-channel2  
  switchport trunk native vlan 100  
  switchport trunk allowed vlan 10,20,30,40,50,60,90,100  
  switchport mode trunk  
!  
interface Port-channel3  
  switchport trunk native vlan 100  
  switchport trunk allowed vlan 10,20,30,40,50,60,90,100  
  switchport mode trunk  
!  
interface FastEthernet0/1  
  switchport access vlan 60  
  switchport mode access  
!  
interface FastEthernet0/2  
  switchport access vlan 60  
  switchport mode access  
!  
interface FastEthernet0/3  
  switchport access vlan 60  
  switchport mode access  
!  
interface FastEthernet0/4  
  switchport access vlan 60  
  switchport mode access  
!  
interface FastEthernet0/5
```

```
switchport access vlan 60
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 60
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 60
switchport mode access
!
interface FastEthernet0/8
switchport access vlan 60
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 60
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 60
switchport mode access
!
interface FastEthernet0/11
switchport access vlan 60
switchport mode access
!
interface FastEthernet0/12
switchport access vlan 60
switchport mode access
!
interface FastEthernet0/13
switchport access vlan 60
switchport mode access
!
interface FastEthernet0/14
switchport access vlan 60
switchport mode access
!
interface FastEthernet0/15
switchport access vlan 60
switchport mode access
!
```

```
interface FastEthernet0/16
  switchport access vlan 60
  switchport mode access
!
interface FastEthernet0/17
  switchport access vlan 50
  switchport mode access
!
interface FastEthernet0/18
  switchport access vlan 50
  switchport mode access
!
interface FastEthernet0/19
  switchport access vlan 50
  switchport mode access
!
interface FastEthernet0/20
  switchport access vlan 50
  switchport mode access
!
interface FastEthernet0/21
  switchport access vlan 50
  switchport mode access
!
interface FastEthernet0/22
  switchport access vlan 50
  switchport mode access
!
interface FastEthernet0/23
  switchport trunk native vlan 100
  switchport trunk allowed vlan 10,20,30,40,50,60,90,100
  switchport mode trunk
  channel-group 3 mode active
!
interface FastEthernet0/24
  switchport trunk native vlan 100
  switchport trunk allowed vlan 10,20,30,40,50,60,90,100
  switchport mode trunk
  channel-group 3 mode active
!
interface GigabitEthernet0/1
  switchport trunk native vlan 100
  switchport trunk allowed vlan 10,20,30,40,50,60,90,100
```



```
switchport mode trunk
channel-group 2 mode active
!
interface GigabitEthernet0/2
switchport trunk native vlan 100
switchport trunk allowed vlan 10,20,30,40,50,60,90,100
switchport mode trunk
channel-group 2 mode active
!
interface Vlan1
no ip address
shutdown
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
end
```

### Switch MAD-LOCAL-SERVER


```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel4
switchport trunk native vlan 100
switchport trunk allowed vlan 10,20,30,40,50,60,90,100
switchport mode trunk
```

```
!  
interface FastEthernet0/1  
  switchport trunk native vlan 100  
  switchport trunk allowed vlan 10,20,30,40,50,60,90,100  
  switchport mode trunk  
  channel-group 4 mode active  
!  
interface FastEthernet0/2  
  switchport access vlan 90  
  switchport mode access  
!  
interface FastEthernet0/3  
  switchport access vlan 90  
  switchport mode access  
!  
interface FastEthernet0/4  
  switchport trunk native vlan 100  
  switchport trunk allowed vlan 10,20,30,40,50,60,90,100  
  switchport mode trunk  
  channel-group 4 mode active  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!
```

```
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
  shutdown
!
!
!
!
line con 0
!
line vty 0 4
  login
line vty 5 15
  login
!
!
end
```

### **SWITCH MADRID\_SERVIDORES**

```
!
version 15.0
no service timestamps log datetime msec
```



```
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
```

```
!
spanning-tree mode pvst
spanning-tree extend system-id
!
```

```
interface FastEthernet0/1
```

```
!
interface FastEthernet0/2
```

```
!
interface FastEthernet0/3
```

```
!
interface FastEthernet0/4
```

```
!
interface FastEthernet0/5
```

```
!
interface FastEthernet0/6
```

```
!
interface FastEthernet0/7
```

```
!
interface FastEthernet0/8
```

```
!
interface FastEthernet0/9
```

```
!
interface FastEthernet0/10
```

```
!
interface FastEthernet0/11
```

```
!
interface FastEthernet0/12
```

```
!
interface FastEthernet0/13
```

```
!
interface FastEthernet0/14
```

```
!
interface FastEthernet0/15
```

```
!
interface FastEthernet0/16
```

```
!
interface FastEthernet0/17
```

```
!
```

```
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
  shutdown
!
line con 0
!
line vty 0 4
  login
line vty 5 15
  login

!
!
end
```

## **ROUTER 1**

```
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
```

```
!
no ip cef
ipv6 unicast-routing
!
no ipv6 cef

!
!
spanning-tree mode pvst
!
!
interface Tunnel0
no ip address
mtu 1476
ipv6 address 3000::1/112
ipv6 rip 9 enable
tunnel source GigabitEthernet0/0/1
tunnel destination 192.168.3.2
tunnel mode ipv6ip
!
!
interface GigabitEthernet0/0/0
no ip address
duplex auto
speed auto
ipv6 address 2001:DB8:8::1/64
ipv6 rip 9 enable
ipv6 enable
!
interface GigabitEthernet0/0/1
ip address 192.168.3.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/1/0
no ip address
ipv6 address 2001:DB8:3::2/64
```

```
ipv6 rip 9 enable
ipv6 enable
clock rate 2000000
!
interface Serial0/1/1
no ip address
ipv6 address 2001:DB8:2::1/64
ipv6 rip 9 enable
ipv6 enable
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
router-id 1.1.1.1
log-adjacency-changes
network 192.168.3.0 0.0.0.255 area 0
!
ipv6 router rip 9
!
ip classless
!
ip flow-export version 9
!
ipv6 route ::/0 3000::

!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```

**ROUTER-VPN**

!

```
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!

!
!
no ip cef
ipv6 unicast-routing
!
no ipv6 cef
!

!
spanning-tree mode pvst
!
interface GigabitEthernet0/0/0
no ip address
duplex auto
speed auto
ipv6 address 2001:DB8:2222::1/64
ipv6 rip 9 enable
!
interface GigabitEthernet0/0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/1/0
no ip address
ipv6 rip 9 enable
ipv6 enable
clock rate 2000000
```




```
shutdown
!
interface Serial0/1/1
no ip address
ipv6 address 2001:DB8:3::1/64
ipv6 rip 9 enable
ipv6 enable
!
interface Vlan1
no ip address
shutdown
!
ipv6 router rip 9
!
ip classless
!
ip flow-export version 9
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```


## **ROUTER-SEDE-2**

```
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router

!
!
```



```
no ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0/0
no ip address
duplex auto
speed auto
ipv6 address 2001:DB8:2222::1/64
ipv6 rip 9 enable
!
interface GigabitEthernet0/0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/1/0
no ip address
ipv6 rip 9 enable
ipv6 enable
clock rate 2000000
shutdown
!
interface Serial0/1/1
no ip address
ipv6 address 2001:DB8:3::1/64
ipv6 rip 9 enable
ipv6 enable
!
interface Vlan1
no ip address
```



```
shutdown
!  
ipv6 router rip 9  
!  
ip classless  
!  
ip flow-export version 9  
!  
line con 0  
!  
line aux 0  
!  
line vty 0 4  
  login  
!  
!  
!  
end
```

## 6. Bibliografía

### Tecnologías

<https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene>

[https://www.cisco.com/c/es\\_mx/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html](https://www.cisco.com/c/es_mx/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html)

<https://www.netacad.com/es/courses/packet-tracer>

<https://ccnadesdecero.es/funcionamiento-etherchannel>.

### Protocolos

[https://edea.juntadeandalucia.es/protocolo\\_de\\_transferencia\\_de\\_hipertexto\\_http](https://edea.juntadeandalucia.es/protocolo_de_transferencia_de_hipertexto_http)

<https://massive.io/es/transferencia-de-archivos/que-es-el-protocolo-de-transferencia-de-archivos/>

<https://www.ionos.es/digitalguide/servidores/know-how/udp-user-datagram-protocol/>

<https://es.khanacademy.org/transmission-control-protocol--tcp>

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_rip/configuration/xr-3s/asr-1000/ip6-rip-xr.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_rip/configuration/xr-3s/asr-1000/ip6-rip-xr.html)

<https://www.raulprietofernandez.net/blog/packet-tracer/enrutamiento-dinamico-ospf-con-packet-tracer>

<http://cdrbenitest.blogspot.com/2016/02/protocolo-8021q.html>

<https://nordvpn.com/es/blog/protocolo-ipsec/>

<https://riunet.upv.es/bitstream/handle/10251/16310/Art%C3%ADculo%20docente%20configuraci%C3%B3n%20b%C3%A1sica%20VLANs.pdf>

[https://www.cisco.com/c/es\\_mx/support/docs/lan-switching/vtp/10558-21.html](https://www.cisco.com/c/es_mx/support/docs/lan-switching/vtp/10558-21.html)

<https://todopacketracer.wordpress.com/2017/09/07/ethernet-channel-y-port-channel/>

#### - Servidores:

[https://www.dell.com/en-us/shop/servers-storage-and-networking/poweredge-r740-rack-server/spd/poweredge-r740/pe\\_r740\\_tm\\_vi\\_vp\\_sb](https://www.dell.com/en-us/shop/servers-storage-and-networking/poweredge-r740-rack-server/spd/poweredge-r740/pe_r740_tm_vi_vp_sb)

[https://www.dell.com/en-us/shop/cty/pdp/spd/poweredge-r940/pe\\_r940\\_12229\\_vi\\_vp](https://www.dell.com/en-us/shop/cty/pdp/spd/poweredge-r940/pe_r940_12229_vi_vp)

#### - Patch pannel :

<https://www.pccomponentes.com/equip-769224-patch-panel-24-puertos-cat-6-1u-19?campaigntype=eshopping&campaignchannel=shopping>

[https://www.cablepelado.es/kit-puesto-trabajo-electrico-4-schukos-y-2-rj45-blanco?product\\_id=3421&gad=1](https://www.cablepelado.es/kit-puesto-trabajo-electrico-4-schukos-y-2-rj45-blanco?product_id=3421&gad=1)

#### - Switch:

<https://it-planet.com/es/p/cisco-ws-c2960x-24ts-l-13178.html?number=2847986001.1>

- **Router:**

<https://it-planet.com/es/p/cisco-isr4451-x-k9-9615.html?number=3122642000.1>

- **Punto de acceso**

<https://www.amazon.es/Cisco-Business-protecci%C3%B3n-Hardware-CBW150AX/dp/B0B7KHJZ4Y>

- **Firewall**

<https://it-planet.com/es/p/cisco-asa5506-k9-7763.html?number=3650298000>

- **Cableado**

<https://www.cervi.es/ES/3-productos/36--sistemas-de-cableado-y-racks/270-sistema-de-cableado-utp-cat6a.html>.

- **Rack**

<https://cablematic.com/es/productos/armario-rack-19>

- **Ordenador**

<https://www.backmarket.es/es-es/p/hp-elitebook-830-g5-13-core-i5-17-ghz-ssd-256-gb-16gb-teclado-suec>

- **acl-DMZ**

<https://www.youtube.com/watch?v=nuzTbu13AtM&t=1s>

- **Virtualización:**

- vmware**

<https://kb.vmware.com/s/ar>

<https://www.dell.com/support/manuals/es-es/vmware-esxi-6.7>

- dhcp**

<https://learn.microsoft.com/es-es/troubleshoot/windows-server/networking/install-configure-dhcp-server-workgroup>

- dns**

<https://docs.vmware.com/es/VMware-NSX-Data-Center-for-vSphere/6.4/com.vmware.nsx.admin.doc/GUID-29B09FBD-31ED-4022-99B6-DCBF1A4B6AC6.html>

- apache**

<https://httpd.apache.org/>

<https://docs.vmware.com/es/VMware-vRealize-Automation-SaltStack-Config/SaaS/using-and-managing-saltstack-config-guide>

- server web**



<https://www.ionos.es/digitalguide/correo-electronico/cuestiones-tecnicas/microsoft-exchange-software-profesional-para/>

**software**

<https://www.snort.org/>

<https://www.fortinet.com/lat/support/product-downloads#vpn>