UNIVERSIDAD DE GRANADA

REDES DE ACCESO Y CORPORATIVAS

INGENIERÍA DE TECNOLOGÍAS DE TELECOMUNICACIÓN

Diseño de una red corporativa

Diseño en Packet Tracer

Autores
Pedro Gabriel Fernández Cañete
Enrique Gómez Pacheco
Francisco Castarnado Ruiz

Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación

—

Granada, enero de 2026

Índice general

Índice de figuras

Índice de tablas

Acrónimos

VLAN Virtual LAN

WLAN Wireless LAN

WLC Wireless LAN Controller

LAP Light Access Point

CPD Centro de Procesamiento de Datos

DMZ Demilitarized Zone

IDS Intrusion Detection System

Capítulo 1

Introducción

1.1. Resumen ejecutivo

El presente documento detalla la propuesta técnica para el diseño e implementación integral de una nueva red corporativa que interconecte la Sede Principal (Campus) y las sedes remotas (B1 y B2). El objetivo principal es dotar a la organización de una infraestructura de comunicaciones robusta, segura y preparada para el futuro, capaz de soportar las operaciones críticas de sus 260 empleados y colaboradores externos.

Nuestra solución plantea una arquitectura de red jerárquica y redundante que garantiza la continuidad del negocio. El diseño integra servicios de alta disponibilidad en el Campus, conectividad segura mediante túneles VPN para las sedes remotas y un entorno de teletrabajo flexible. Además, se ha priorizado la seguridad mediante una estrategia de defensa en profundidad, incluyendo el despliegue de Firewalls, sistemas IDS/IPS y una zona desmilitarizada (DMZ) para aislar los servicios públicos.

La implementación de este proyecto aportará los siguientes beneficios estratégicos:

- **Productividad y Rendimiento:** Se asegura un ancho de banda de 1 Mbps por usuario y acceso ininterrumpido a los recursos corporativos gracias a la redundancia de enlaces y servidores.
- **Seguridad:** Protección de los datos y sistemas mediante segmentación de red, cifrado de comunicaciones y control de acceso estricto tanto para usuarios internos como invitados.

- **Escalabilidad:** Una infraestructura modular, incorporando soporte nativo para IPv6 y capacidad para futuras expansiones de plantilla o nuevas sedes.
- **Gestión Eficiente:** Centralización de la administración de la red, lo que permite reducir los costes operativos y agilizar la resolución de incidencias técnicas.

1.2. Objetivo/s

El objetivo principal de este proyecto es diseñar e implementar una infraestructura de red corporativa integral que, más allá de satisfacer los requerimientos técnicos de conectividad segura entre la sede central y las sucursales remotas, actúe como un catalizador para el negocio. Se busca maximizar la productividad operativa mediante la provisión de servicios de alta disponibilidad y acceso remoto eficiente, optimizar los costes operativos a través de una gestión centralizada y asegurar la continuidad del negocio frente a amenazas, entregando una plataforma escalable que soporte el crecimiento sostenible de la organización.

1.3. Alcance

El alcance del proyecto abarca el diseño e implementación completa de la infraestructura de red para la totalidad de la organización, cubriendo tanto la red de área local (LAN) de cada sede como la red de área amplia (WAN) que las interconecta.

La estructura organizativa y dimensional que soportará la red es la siguiente:

- **Sede Principal (Campus):** Constituye el núcleo de la red. Albergará los 5 departamentos operativos de la empresa (Investigación, Comercial, Ventas, Cursos y Soporte Técnico). Dará servicio a 200 puestos de trabajo fijos y alojará el Centro de Procesamiento de Datos (CPD) principal.
- **Sede Remota B1:** Sucursal de tamaño medio que replica la estructura departamental del Campus (los 5 departamentos), contando con 50 puestos de trabajo fijos.

- **Sede Remota B2:** Sucursal satélite con requisitos específicos, limitándose a los departamentos de Investigación y Cursos, con un total de 10 puestos fijos.
- **Servicios Públicos y DMZ:** Implementación de una zona desmilitarizada para exponer servicios públicos, específicamente el servidor web corporativo, garantizando su acceso seguro desde Internet.

1.4. Estado de la red y Caracterización

La arquitectura propuesta parte de un diseño "Greenfield"(desde cero), sin deudas técnicas heredadas. Las características técnicas principales que definirán el estado final de la red son:

- **Segmentación y VLANs:** Se implementará una política de segmentación estricta mediante VLANs separadas para cada uno de los 5 departamentos. Para facilitar la gestión, se mantendrá un esquema de identificación de VLANs consistente entre la Sede Central y la Sede B1.
- **Adopción de IPv6 en Sede B2:** La sede B2 operará como un entorno nativo IPv6 ('IPv6-only'). Para garantizar la interoperabilidad con el resto de la red corporativa (que opera en IPv4/Dual Stack), se desplegarán mecanismos de transición NAT64/DNS64.
- **Arquitectura Jerárquica en Campus:** La red de la sede principal seguirá el modelo de diseño jerárquico de Cisco, implementando:
  - **Capa de Acceso:** Conectividad para usuarios finales.
  - **Capa de Distribución/Core:** Agregación de tráfico y enrutamiento de alta velocidad.
  - **Bloque de Servicios (CPD):** Alojamiento de servidores críticos (FTP para almacenamiento y DHCP para direccionamiento dinámico) en un entorno de alta disponibilidad.
  - **Bloque de Internet/DMZ:** Zona perimetral segura que aloja los servicios públicos y filtra el tráfico de entrada/salida.
- **Conectividad WAN y VPN:** La interconexión entre sedes se realizará mediante túneles VPN Site-to-Site (IPsec) sobre infraestructura pública de Internet, garantizando la confidencialidad de los datos en tránsito. Adicionalmente, se habilitarán servicios VPN de acceso remoto para teletrabajadores.

1.5. Organización del documento

La presente memoria técnica se estructura en cinco capítulos que detallan el ciclo de vida del proyecto:

- **Capítulo 1: Introducción.** (El presente capítulo). Establece el contexto, la motivación, los objetivos estratégicos y el alcance del diseño de red.
- **Capítulo 2: Planificación.** Detalla los requisitos formales, la definición de tareas, la estimación de recursos humanos y técnicos necesarios, el cronograma de ejecución y el presupuesto estimado.
- **Capítulo 3: Diseño Lógico.** Profundiza en la arquitectura lógica de la red: topologías, planes de direccionamiento IP (IPv4 e IPv6), diseño de VLANs, protocolos de enrutamiento y políticas de seguridad y gestión.
- **Capítulo 4: Diseño Físico.** Describe la selección de dispositivos hardware (routers, switches, firewalls) y medios de transmisión necesarios para materializar el diseño lógico propuesto.
- **Capítulo 5: Conclusiones.** Presenta las conclusiones finales del proyecto, destacando las contribuciones realizadas y planteando posibles líneas de mejora futura.

Capítulo 2

Planificación

2.1. Requisitos

Este apartado detalla los pilares sobre los cuales se ha construido la arquitectura de red, alineando las necesidades operativas de la empresa con las soluciones tecnológicas implementadas. Vamos a ver varios de los requisitos fundamentales de varios ámbitos que nos han llevado a tomar nuestras decisiones:

- De negocio
  - Continuidad y Productividad: Garantizar la interconexión constante entre la Sede Principal y las sedes remotas (B1 y B2), además de la conexión de todas ellas a Internet, para asegurar que los procesos de los 5 departamentos no se detengan.
  - Habilitación del Teletrabajo: Permitir que los empleados accedan a los recursos internos desde cualquier lugar, manteniendo el ritmo de trabajo sin necesidad de presencia física.
  - Presencia Digital: Exposición pública de la página web corporativa para captación de clientes y visibilidad de mercado.
  - Eficiencia de Costes: Uso de tecnologías VPN sobre internet público en lugar de costosas líneas dedicadas para la interconexión de sedes.
- Técnicos
  - Seguridad: necesidad de que toda la red sea un entorno seguro, tanto las zonas internas de las sedes, como la interconexión de las

mismas o la conexión remota de los teletrabajadores. Este requisito es imprescindible para el correcto funcionamiento diario de la empresa y evitar que agentes maliciosos puedan entorpecerlo.

- Escalabilidad: Diseño preparado para el crecimiento modular de usuarios en cualquiera de las sedes y la adición de nuevos departamentos mediante puertos SFP de fibra.
- Disponibilidad: Minimizar puntos únicos de fallo mediante redundancia de dispositivos y uso de protocolos como HSRP.Además, asegurar un ancho de banda de al menos 1 Mbps por usuario en picos de tráfico.
- Gestionabilidad: Centralización de la red inalámbrica mediante un Wireless LAN Controller (WLC), disposición de una VLAN de gestión para facilitar la configuración de todos los equipos, y monitorización de eventos de seguridad.
- Interoperabilidad IPv4/IPv6: Debido a la necesidad de interconectar las sedes Central y B1, que disponen de un direccionamiento IPv4, con la Sede B2, que opera exclusivamente bajo el protocolo IPv6.

- Comunidades de usuarios y CPD/almacenes de datos.
  - Segmentación por Departamentos: Definición de 5 grupos de usuarios (Investigación, Comercial, Ventas, Cursos y Soporte Técnico) con políticas de acceso diferenciadas.
  - Acceso de Terceros: Creación de una red de Invitados aislada de la red corporativa pero con acceso a Internet. En este caso se trata de una red WI-FI.
  - Centro de Procesamiento de Datos (CPD): Ubicación centralizada de servidores de almacenamiento y cómputo y servidores DHCP en la Sede Principal, con acceso desde todas las sedes pero restringido por jerarquía departamental.
- Aplicaciones.
  - Servicios Web: Alojamiento de la página web corporativa en una zona desmilitarizada (DMZ) para acceso público seguro.
  - Servicios de Red Core: Implementación de DHCP para asignación dinámica de IPs, DNS para resolución de nombres y protocolos de enrutamiento dinámico como OSPF.
  - Gestión de Datos: Servidores de almacenamiento corporativo accesibles mediante el túnel VPN para teletrabajadores y empleados de todas las sedes.

2.2. Tareas

Para garantizar el éxito del despliegue de la red corporativa, hemos desglosado el proyecto en una serie de paquetes de trabajo técnicos y de gestión. Esta estructura permite un seguimiento preciso del avance y facilita la asignación de recursos. Las tareas principales se detallan a continuación:

- **Diseño de Arquitectura de Red:** Definición exhaustiva de las topologías lógicas y físicas para el Campus y las sedes remotas (B1 y B2), asegurando la coherencia estructural.
- **Planificación de Direccionamiento y VLANs:** Elaboración del esquema de direccionamiento IP (IPv4 e IPv6) y segmentación de la red mediante VLANs por departamento, optimizando el tráfico de broadcast y la seguridad.
- **Implementación de Servicios y Protocolos:** Configuración de protocolos de enrutamiento (OSPF, BGP), servicios de infraestructura (DHCP, DNS) y mecanismos de alta disponibilidad en el bloque de servidores.
- **Estrategia de Seguridad y Monitorización:** Despliegue de políticas de firewall, configuración de túneles VPN Site-to-Site y acceso remoto, así como la implementación de sistemas IDS/IPS para la detección de intrusiones.
- **Pruebas de Integración y Conectividad:** Ejecución de baterías de pruebas (ping, traceroute, análisis de tráfico) para validar la conectividad extremo a extremo y la resiliencia de la red ante fallos.

2.3. Recursos humanos y técnicos

La viabilidad del proyecto se sustenta en la adecuada asignación de recursos materiales y humanos. A continuación, se detallan los activos necesarios para la fase de diseño y simulación.

Recursos Hardware y Software

- **Infraestructura Hardware:** Se simulará el entorno de producción mediante el montaje de un **laboratorio de pruebas físic, utilizando equipos de red reales (routers, switches y servidores) para validar

fielmente la configuración y el comportamiento de la red antes del despliegue final.

- **Entorno Software:** Herramientas de gestión y configuración de dispositivos (terminales seriales, SSH), analizadores de tráfico (Wireshark) y sistemas operativos para los hosts de prueba (Windows 11 y Linux).
- **Simulación:** Cisco Packet Tracer como herramienta principal para el diseño lógico, físico y la validación funcional de la configuración de dispositivos.

Recursos humanos

El equipo de proyecto está compuesto por el desarrollador principal y un supervisor técnico. La carga de trabajo estimada para completar el ciclo de vida del proyecto se desglosa en la Tabla 2.1. Se ha puesto especial énfasis en las fases de implementación y diseño físico, dada su criticidad.

Paquete de Trabajo / Tarea	**Desarrollador (h)**	**Supervisor (h)**
Análisis de requisitos y alcance	10	5
Diseño de topología física y selección de hardware	30	20
Caracterización lógica de la red	30	15
Implementación de protocolos y servicios	60	25
Test, validación y control de calidad	10	2
Resolución de incidencias y ajustes	30	10
Documentación técnica y memoria	10	5
Total Esfuerzo Estimado	**180**	**82**

Tabla 2.1: Desglose de horas por rol y tarea.

2.4. Temporización

La ejecución del proyecto se ha planificado en un horizonte temporal estimado de 12 semanas, considerando una dedicación a tiempo parcial. La siguiente tabla sustituye al diagrama de Gantt visual, detallando la distribución temporal de las tareas y su secuenciación lógica.

Se han establecido reuniones de seguimiento quincenales con el tutor para revisar los hitos marcados en el cronograma (Tabla 2.2) y mitigar posibles desviaciones.

Semana	Fase Principal	Estado	Hitos Clave
1-2	Análisis y Requisitos	Completado	Definición de alcance y tecnologías
3-4	Diseño Físico y Lógico	Completado	Topología y selección de hardware
5-6	Caracterización de Red	Completado	Plan IP, VLANs y Diseño IPv6 (B2)
7-9	Implementación	Completado	Configuración de Routers, Switches y Svcs.
10	Seguridad y VPN	Completado	Configuración FW y Túneles IPsec
11	Test y Validación	En proceso	Pruebas en laboratorio físico
12	Documentación y Cierre	Pendiente	Entrega de memoria y presentación

Tabla 2.2: Cronograma de ejecución del proyecto (Temporización).

2.5. Presupuesto y Viabilidad Económica

El siguiente presupuesto detalla la inversión necesaria para la actualización tecnológica de la infraestructura de red. Los costes presentados son estimaciones de mercado (PVP recomendado) para equipos de gama Enterprise, excluyendo impuestos (IVA).

2.5.1. Adquisición de Hardware (Equipos de Red y Servidores)

Para los servidores, se ha optado por una estrategia de virtualización. En lugar de adquirir un servidor físico para cada servicio ligero (NTP, Syslog, DNS), se presupuestan 3 servidores físicos de alto rendimiento (2 para el CPD y 1 para la DMZ) sobre los cuales se ejecutarán las máquinas virtuales correspondientes a los servicios lógicos diseñados (DHCP, DNS, Web, etc.).

Dispositivo	**Modelo Propuesto (Real)**	**Cant.**	**P. Unitario**	**P. Total**
Router de Borde	Cisco Catalyst 8300 Edge	4	3.500 €	14.000 €
Firewall Perimetral	Cisco Firepower 1100 Series	1	1.800 €	1.800 €
Switch Distribución (L3)	Cisco Catalyst 9300 (24p)	6	3.200 €	19.200 €
Switch Acceso (L2 PoE+)	Cisco Catalyst 9200L (48p)	21	1.900 €	39.900 €
Controladora Wi-Fi	Cisco Catalyst 9800-L	1	4.500 €	4.500 €
Puntos de Acceso	Cisco Catalyst 9120 (Wi-Fi 6)	6	650 €	3.900 €
Servidores Físicos	Cisco UCS C220 M6	3	4.200 €	12.600 €
			TOTAL HARDWARE	**95.900 €**

Tabla 2.3: Presupuesto de Hardware

Nota: Los 3 servidores físicos soportan las instancias virtuales de: DHCP, DNS Interno, Syslog, NTP, DNS Público y Servidor Web.

2.5.2. Cableado y Transceptores

Se incluyen los cables de parcheo (latiguillos) y los módulos transceptores (SFP) necesarios para interconectar los equipos de fibra óptica.

Concepto	**Especificación**	**Cant.**	**P. Unit.**	**P. Total**
Cableado Acceso	Latiguillo UTP Cat 6A (1-3m)	300	8 €	2.400 €
Cableado Uplinks	Latiguillo UTP Cat 6A Cruzado	30	10 €	300 €
Cableado Core	Latiguillo UTP Cat 6A (Dist-Router)	6	10 €	60 €
Fibra Óptica	Latiguillo Fibra Monomodo OS2 (LC-LC)	4	25 €	100 €
Módulos SFP+	Cisco 10GBASE-LR SFP Module	4	800 €	3.200 €
			TOTAL CABLEADO	**6.060 €**

Tabla 2.4: Presupuesto de Cableado

2.5.3. Licencias y Software

El hardware moderno de Cisco requiere suscripciones de software (DNA) para habilitar funcionalidades avanzadas y gestión centralizada, así como licencias de virtualización para los servidores.

- **Licencias Cisco DNA Essentials (3 años):** Para 27 switches y 4 routers.
  Estimado: 12.500 €.
- **Licencia de Virtualización (VMware vSphere Standard):** Para 3 procesadores físicos.
  Estimado: 3.000 €.
- **Licencias S.O. Servidores (Windows Server / RHEL):**
  Estimado: 2.500 €.
- **Subtotal Licencias: 18.000 €.**

2.5.4. Soporte y Mantenimiento

Se contrata el servicio de soporte extendido del fabricante para garantizar el reemplazo de hardware ante fallos y acceso a actualizaciones de seguridad.

- **Cisco Smart Net Total Care (8x5xNBD):** Servicio de sustitución de hardware al siguiente día laborable (Next Business Day). Calculado como el 15 % del valor del hardware anual.
- **Coste Anual: 14.385 €.**

2.5.5. Cursos de Formación

Para garantizar que el equipo IT de la empresa pueda operar la nueva infraestructura eficientemente.

- **Curso Cisco ENCOR (CCNP Enterprise Core):** Para 2 administradores de red.
  Precio: 2.500 € x 2 = 5.000 €.

- **Curso de Seguridad (Firepower/ASA):** Para 1 administrador de seguridad.
  Precio: 2.000 €.
- **Subtotal Formación: 7.000 €.**

2.5.6. Honorarios Profesionales (Implementación)

Costes asociados a la mano de obra para la configuración, instalación física (racking) y puesta en marcha.

- **Ingeniero de Red Senior (Diseño y Configuración lógica):** 80 horas a 60 €/h = 4.800 €.
- **Técnico de Campo (Instalación física y cableado):** 120 horas a 30 €/h = 3.600 €.
- **Gestión del Proyecto (Project Manager):** 40 horas a 70 €/h = 2.800 €.
- **Subtotal Honorarios: 11.200 €.**

2.5.7. Resumen Total del Presupuesto

Capítulo	**Importe**
1. Hardware de Red y Servidores	95.900 €
2. Cableado y Conectividad	6.060 €
3. Licencias y Software	18.000 €
4. Soporte y Mantenimiento (Año 1)	14.385 €
5. Formación	7.000 €
6. Honorarios Profesionales	11.200 €
TOTAL GENERAL (Sin IVA)	**152.545 €**

Tabla 2.5: Resumen General de Costes

Capítulo 3

Diseño lógico

En este capítulo vamos a explicar las consideraciones que hemos tenido en cuenta y vamos a justificar porque hemos diseñado nuestra red con la estructura, tecnologías y protocolos elegidos. Esto se corresponde al diseño lógico de nuestra red, sin tener en cuenta características físicas de los dispositivos elegidos, lo cual veremos en el siguiente capítulo.

3.1. Topología Lógica y Modelo Jerárquico

El diseño lógico de la red corporativa que hemos diseñado se basa en el Modelo Jerárquico de Cisco, estructurado en las capas de Núcleo (Core), Distribución y Acceso. Esta arquitectura garantiza que se cumplan los requisitos no funcionales de escalabilidad, disponibilidad y gestionabilidad exigidos por el proyecto.

Además, la topología se ha diseñado de forma que se adecue a la estructura física de la empresa, que cuenta con una sede principal con un solo edificio y dos sedes remotas. Se ha tenido en cuenta el volumen de trabajadores de dichos edificios y todos los requisitos técnicos anteriormente mencionados.

Esta topología la podemos ver en la Figura A.1

3.1.1. Arquitectura de las Sedes (Campus, B1 y B2)

Para dar respuesta a la demanda de usuarios de todas las sedes, incluyendo empleados e invitados, organizados en los distintos departamentos, y a todos los requisitos técnicos exigidos, se ha propuesto la siguiente estructura lógica de los distintos edificios, disponible en la Figura A.2:

- Capa de Acceso: En esta capa hemos utilizado switches de Capa 2 para la conexión directa de los puestos fijos de los distintos departamentos, los puntos de acceso inalámbricos (LAPs) y los servidores ubicados en el CPD de la sede principal con la capa de distribución. Se han definido VLANs independientes para cada uno de los 5 departamentos (Investigación, Comercial, Ventas, Cursos y Soporte Técnico) en el Campus y la Sede B1, mientras que en la Sede B2 se han limitado lógicamente a Investigación y Cursos según el requerimiento de tamaño. Además, se han definido otras VLANs para el CPD, los invitados conectados a la WLAN, y la gestión de los dispositivos.
- Capa de Distribución: Compuesta por switches multicapa que actúan como el gateway de cada subred (vlan). Aquí se gestiona el enrutamiento Inter-VLAN para permitir conexiones entre los distintos usuarios del edificio y se aplican las políticas de seguridad iniciales para restringir el acceso a ciertas zonas para usuarios no autorizados.
- Capa de Núcleo y Borde: Empleamos routers que gestionan la salida de tráfico del interior de las sedes hacia la red WAN (Internet). Necesitamos equipos de nivel 3 de altas prestaciones en esta capa, que solo se encarguen de reenviar el tráfico recibido a la mayor velocidad posible.

3.1.2. Interconexión y Conectividad WAN

La interconexión de las 3 sedes se realiza a través de una red pública proporcionada por un ISP. Sin embargo, hemos securizado la comunicación mediante túneles privados que aislan nuestros datos de dicha red:

- Redundancia y Alta Disponibilidad: Se ha implementado agregación de enlaces (LAG) en las conexiones críticas entre los routers de borde de las sedes para evitar puntos únicos de fallo y asegurar el ancho de banda solicitado de 1 Mbps por usuario.

- Segmentación WAN Segura: La comunicación entre sedes se realiza mediante túneles VPN IPsec, garantizando que nuestras comunicaciones entre sedes sean seguras, ya que estas se envían por una red pública.

3.1.3. Seguridad Perimetral y DMZ

Para cumplir con la exposición pública de la página web corporativa y el acceso de teletrabajadores, se ha integrado un cortafuegos en el diseño lógico de nuestra red. De esta forma evitamos accesos externos no autorizados:

- Zona Desmilitarizada (DMZ): Se ha creado un segmento de red aislado para los servidores Web y DNS, permitiendo el acceso desde Internet sin comprometer la seguridad de la red interna. Esta zona es la observada en la Figura A.6
- Terminación de VPN para Teletrabajo: Hemos incluido un router concentrador de VPN para los usuarios remotos antes del cortafuegos, permitiendo que el personal externo acceda de forma cifrada a la Sede Principal sin comprometer la seguridad de la empresa. Esta parte de la topología la encontramos en la Figura A.7

3.2. Planificación VLANs

La implementación de redes locales virtuales (VLANs) es fundamental para gestionar el tráfico de los departamentos de forma independiente, reducir los dominios de difusión y aplicar políticas de seguridad.

3.2.1. Justificación de la segmentación

Para realizar la segmentación de nuestra red en las distintas VLANs que mencionaremos a continuación, hemos seguido el siguiente planteamiento de acuerdo a satisfacer los requisitos técnicos especificados:

- Seguridad Departamental: hemos creado una VLAN para cada departamento de la empresa, para proporcionar una mayor seguridad y orden en el transporte de los datos de las mismas.
- Gestión de Invitados: Se ha creado una red específica para invitados, con el fin de evitar posibles accesos de estos usuarios a nuestra red

interna. Mediante el uso de ACLs, a esta red se le permitirá el acceso a Internet, pero tendrá prohibida la entrada a la red corporativa.

- Aislamiento del CPD: Se han creado dos VLANs exclusivas para los equipos alojados en el Centro de Procesamiento de Datos, así mantenemos la mayor seguridad posible y evitamos accesos no autorizados a estos dispositivos. Una de estas dos subredes tendrá acceso restringido para ciertos departamentos, ya que esta alojará los servidores más sensibles de la empresa. La otra tendrá un acceso más libre y alojará servidores que toda la red necesita consultar, como los servidores DHCP.
- Optimización del Tráfico y gestionabilidad: Se ha creado una VLAN exclusiva para la gestión de nuestra red, para facilitar la configuración o solución de fallos de nuestros equipos.

3.2.2. Tabla de Definición de VLANs

Tabla 3.1: Definición de VLANs

Identificador	**Descripción**	**Sedes alojadas**
VLAN50	Configuración SLAAC	Sede B2
VLAN100	Departamento Investigación	Sede Central, B1 y B2
VLAN200	Departamento Comercial	Sede Central y B1
VLAN300	Departamento Ventas	Sede Central y B1
VLAN400	Departamento Cursos	Sede Central, B1 y B2
VLAN500	Departamento Soporte Técnico	Sede Central y B1
VLAN600	Red de Invitados	Sede Central, B1 y B2
VLAN900	Red CPD para servidores de cómputo	Sede Central
VLAN950	Red CPD para servidores de infraestructura	Sede Central
VLAN999	Red de gestión	Sede Central, B1 y B2

3.2.3. Enrutamiento inter-VLAN

Para garantizar la comunicación fluida entre los distintos departamentos y segmentos de nuestra red, se ha implementado un esquema de enrutamiento inter-VLAN basado en Switches Multicapa y enlaces "trunk". Este diseño permite que cada VLAN disponga de una interfaz virtual (SVI) que actúa como puerta de enlace (Gateway) predeterminada para los usuarios. Es mediante estas interfaces que los switches multicapa realizan el correcto enrutamiento.

Sin embargo, como existen segmentos de nuestra red con acceso restringido, es también en estas interfaces donde se han aplicado las políticas de control de acceso (ACL) para segmentar el tráfico de forma efectiva.

Además, sobre este enrutamiento hemos configurado y aplicado el protocolo HSRP, que consigue proporcionarnos una gran disponibilidad, ya que alterna la puerta de enlace de los dispositivos de las distintas redes a las interfaces virtuales de los switches multicapa redundantes.

3.3. Direccionamiento IP

3.3.1. IPv6 SLAAC

Es fundamental establecer un mecanismo eficiente y escalable para la asignación de direcciones lógicas en la capa de red. Para ello, hemos optado por el despliegue del protocolo de autoconfiguración libre de estado (SLAAC) para la gestión de direccionamiento IPv6 en los equipos finales de la sede.

Si bien la reducida dimensión de esta delegación (compuesta por aproximadamente 10 dispositivos) podría sugerir la viabilidad de realizar una configuración manual estática en cada terminal, se ha decidido desestimar este enfoque en favor de la automatización. Por la dimensión de la red también se descartó el uso de un DHCP debido al requeremiento de un servidor para la configuración de este.

Esta decisión de diseño se fundamenta en los siguientes objetivos:

- Mitigación de Errores Humanos: A diferencia de IPv4, las direcciones IPv6 poseen una longitud de 128 bits en notación hexadecimal, lo que incrementa exponencialmente la probabilidad de errores tipográficos durante una configuración manual. SLAAC elimina este riesgo permitiendo que los dispositivos generen su propia dirección de interfaz a partir de los mensajes de anuncio del router (RA).
- Eficiencia Administrativa y Escalabilidad: Aunque el parque actual de dispositivos es limitado, el uso de SLAAC suprime la necesidad de llevar un registro manual de direcciones asignadas o de reconfigurar equipos ante cambios en el prefijo de red. Esto garantiza que, ante una eventual expansión de la sede o la conexión de dispositivos móviles temporales, la red mantenga su operatividad sin requerir intervención técnica directa.

3.3.2. Direccionamiento IPv4 y Asignación Dinámica (DHCP)

Para la red corporativa interna (Intranet), se ha seleccionado un esquema de direccionamiento privado basado en el estándar RFC 1918, utilizando el bloque de Clase B **172.16.0.0/16**. Esta elección proporciona un espacio de direcciones contiguo y escalable, permitiendo la creación de más de 65.000 direcciones host, lo cual supera holgadamente los requisitos actuales y futuros de la organización.

Para optimizar el uso de este espacio, se ha aplicado la técnica VLSM (*Variable Length Subnet Masking*), adaptando el tamaño de las subredes a la densidad de usuarios de cada sede y departamento:

- **Sede Central:** Se han asignado máscaras /26 (64 hosts) para departamentos estándar y /25 (128 hosts) para la red de invitados, dado el mayor volumen de tráfico.
- **Sede B1:** Se han asignado máscaras /27 (32 hosts) ajustándose al menor número de puestos de trabajo.
- **Infraestructura (CPD/Gestión):** Se utilizan máscaras ajustadas /27 o /28 para servidores y gestión.

A. Arquitectura DHCP Centralizada y DHCP Relay

En lugar de distribuir múltiples servidores DHCP por cada sede o subred, hemos optado por una arquitectura centralizada para facilitar la gestión y el mantenimiento.

- **Servidor Único:** Se ha desplegado un único servidor DHCP ubicado en el CPD de la Sede Central (VLAN 950) con la dirección IP estática **172.16.2.70**. Este servidor gestiona todos los ámbitos (*scopes*) de la Sede Central y la Sede B1.
- **Agente de Retransmisión (DHCP Relay):** Dado que las solicitudes DHCP (Broadcast) no atraviesan los routers por defecto, hemos configurado el comando `ip helper-address 172.16.2.70` en las Interfaces Virtuales (SVI) de los switches multicapa de distribución. Esto permite encapsular las peticiones de los clientes y enviarlas como Unicast directamente al servidor del CPD, independientemente de la VLAN o sede física donde se encuentre el usuario.

B. Sincronización con Alta Disponibilidad (HSRP)

Un punto crítico del diseño ha sido la coherencia entre el servicio DHCP y el protocolo de redundancia HSRP. En la configuración de los "Pools"del servidor, la dirección de *Default Gateway* entregada a los clientes corresponde a la IP Virtual (VIP) del grupo HSRP de su VLAN, y no a la dirección física del switch. Esto garantiza que, si el router activo falla y el pasivo toma el control, los clientes mantienen su conectividad sin necesidad de renovar su dirección IP.

C. Planificación de Rangos (Estático vs Dinámico)

Se ha definido una política mixta de asignación:

- **Direccionamiento Estático:** Reservado para dispositivos de infraestructura crítica para garantizar su localización y accesibilidad constante.
  - *Servidores CPD:* DHCP (.70), Gestión (.75), DNS Interno (.80).
  - *Electrónica de Red:* Las interfaces de gestión y SVIs de switches y routers.
  - *DMZ:* Los servidores expuestos a internet (Web y DNS Externo) poseen direccionamiento estático privado en el rango **192.168.100.0/24** y son traducidos a IPs públicas fijas (NAT Estático) en el rango **200.1.1.0/29** para su acceso desde el exterior.
- **Direccionamiento Dinámico:** Para usuarios finales (PCs, portátiles, móviles). En cada *Pool* DHCP se han excluido las primeras 10 direcciones (ej. .1 a .10) para uso de gestión y gateways, comenzando la asignación dinámica a partir de la dirección .10 o superior.

La siguiente tabla muestra el resumen de los ámbitos configurados en el servidor:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
CENTRAL_SOPORTE	172.16.1.1	172.16.2.80	172.16.1.10	255.255.255.192	50	0.0.0.0	172.16.200.10
CENTRAL_CURSOS	172.16.0.193	172.16.2.80	172.16.0.202	255.255.255.192	50	0.0.0.0	172.16.200.10
CENTRAL_VENTAS	172.16.0.129	172.16.2.80	172.16.0.138	255.255.255.192	50	0.0.0.0	172.16.200.10
CENTRAL_COMERCIAL	172.16.0.65	172.16.2.80	172.16.0.74	255.255.255.192	50	0.0.0.0	172.16.200.10
CENTRAL_INVESTIGACION	172.16.0.1	172.16.2.80	172.16.0.10	255.255.255.192	50	0.0.0.0	172.16.200.10
CENTRAL_INVITADOS	172.16.1.129	172.16.2.80	172.16.1.140	255.255.255.128	110	0.0.0.0	172.16.200.10
B1_INVESTIGACION	172.16.64.1	172.16.2.80	172.16.64.10	255.255.255.224	20	0.0.0.0	172.16.100.10
B1_SOPORTE	172.16.64.129	172.16.2.80	172.16.64.138	255.255.255.224	20	0.0.0.0	172.16.100.10
B1_COMERCIAL	172.16.64.33	172.16.2.80	172.16.64.42	255.255.255.224	20	0.0.0.0	172.16.100.10
B1_CURSOS	172.16.64.97	172.16.2.80	172.16.64.106	255.255.255.224	20	0.0.0.0	172.16.100.10
B1_VENTAS	172.16.64.65	172.16.2.80	172.16.64.74	255.255.255.224	20	0.0.0.0	172.16.100.10
B1_INVITADOS	172.16.64.193	172.16.2.80	172.16.64.202	255.255.255.192	50	0.0.0.0	172.16.100.10
serverPool	0.0.0.0	0.0.0.0	172.16.2.64	255.255.255.224	26	0.0.0.0	0.0.0.0

Figura 3.1: Asignación de direcciones DHCP

[1]

3.4. Enrutamiento Dinámico (OSPF)

Para la gestión de la tabla de enrutamiento interna de la red corporativa, se ha descartado el uso de enrutamiento estático debido a su falta de escalabilidad y tolerancia a fallos. En su lugar, se ha implementado el protocolo **OSPFv2 (Open Shortest Path First)**, un protocolo de estado de enlace (*Link-State*) estándar abierto.

La elección de OSPF frente a otros protocolos como RIP o EIGRP se justifica por su rápida convergencia ante la caída de enlaces y su capacidad para calcular las rutas más eficientes basándose en el ancho de banda (coste) de los enlaces, algo vital dada la heterogeneidad de nuestras conexiones (Fibra vs Cobre).

3.4.1. Arquitectura de Área Única (Backbone)

Dada la topología actual de la empresa, se ha diseñado una estructura OSPF de **Área Única** (*Single Area*). Todos los dispositivos participantes (Routers de Borde y Switches de Distribución) se han configurado dentro del **Área 0 (Backbone)**. Esta decisión simplifica la administración y evita la complejidad de los LSA de resumen, manteniendo una visión completa de la topología en todos los nodos.

Los equipos que forman parte de este dominio de enrutamiento son:

- **Sede Central:** Router Central y Switches de Distribución (Dist1 y

Dist2).

- **Sede B1:** Router B1 y Switches de Distribución.
- **Sede B2:** Router B2 (únicamente para la conectividad del túnel IPv4).

3.4.2. Optimización y Seguridad del Protocolo

Para asegurar un funcionamiento eficiente y seguro del protocolo, se han aplicado las siguientes configuraciones avanzadas extraídas de los equipos:

A. Interfaces Pasivas (Passive Interfaces)

En los switches de capa de distribución, se ha configurado el comando `passive-interface` para todas las VLANs de usuarios (Vlan100 a Vlan950).

- **Justificación:** Esto permite anunciar las redes de las subredes a los demás routers, pero suprime el envío de mensajes "Hello"de OSPF hacia los puertos de los usuarios finales. Esto mejora la seguridad (evita que un usuario malicioso conecte un router pirata y altere las rutas) y reduce el tráfico de broadcast innecesario en la LAN.

B. Propagación de Ruta por Defecto

El Router Central actúa como la puerta de enlace predeterminada hacia el exterior para toda la organización. Para propagar esta capacidad, se ha configurado el comando `default-information originate`.

- **Efecto:** El Router Central inyecta dinámicamente una ruta por defecto (`0.0.0.0/0`) en el proceso OSPF. De esta forma, el Router B1, el Router B2 y todos los switches de distribución aprenden automáticamente que, para llegar a cualquier red desconocida (Internet), deben enviar el tráfico hacia el Router Central.

C. Identificadores de Router (Router-ID)

Para garantizar la estabilidad de la topología y facilitar la monitorización, se ha asignado manualmente un **Router-ID** único a cada dispositivo

con formato de dirección loopback (ej. `4.4.4.4` para el Central, `5.5.5.5` para Dist1, etc.), evitando que el ID cambie si una interfaz física fluctúa.

D. Enrutamiento sobre VPN

Es importante destacar que la red `10.10.10.0/30`, correspondiente a los túneles GRE que conectan las sedes a través de Internet, también se ha incluido en el proceso OSPF. Esto permite que las sedes remotas intercambien rutas privadas y mantengan la conectividad interna de forma transparente, utilizando la infraestructura pública de manera segura.

[2]

3.5. Red WLAN

Para dar servicio de conectividad a Internet a los trabajadores de la empresa y a su vez a los distintos usuarios que se encuentren en alguna de nuestras sedes, hemos optado por desplegar una red inalámbrica. De esta forma permitimos la movilidad de los usuarios por las distintas sedes sin necesidad de estar físicamente conectados, pero sin sacrificar la seguridad de la red corporativa.

Esta red está totalmente aislada del resto de la red interna, y solo proporcionará a los usuarios conectividad a Internet. Podemos ver cómo la hemos configurado en el apéndice encontrado en la Subsección A.2.2

3.5.1. Arquitectura de Gestión Centralizada

Para esta red se ha seguido una arquitectura de gestión centralizada, basada en Wireless LAN Controllers (WLC) y puntos de acceso ligeros (Lightweight APs - LAPs), cuya función es:

- Control y Provisión: El WLC ubicado en la Sede Principal actúa como el cerebro del sistema, gestionando las políticas de seguridad, la potencia de las antenas y los canales de radiofrecuencia de forma automática.
- Túneles CAPWAP: Los puntos de acceso de todas las sedes establecen túneles lógicos con el controlador central, permitiendo que el tráfico

inalámbrico sea supervisado y segmentado antes de entrar en la red cableada.

3.5.2. Definición de SSIDs y Segmentación Lógica

Para cumplir con el requisito de acceso diferenciado, y que el tráfico de trabajadores e invitados no sean tratados por igual, se han configurado dos identificadores de red (SSID) principales:

- SSID "trabajadores": Destinado a los trabajadores de todos los departamentos. Para la seguridad se ha implementado WPA2 basado en PSK, asegurando que solo dispositivos autorizados accedan a la red interna.
- SSID "invitados": Destinado a los usuarios invitados de cualquiera de las sedes. Para la seguridad también se ha implementado WPA2 basado en PSK, para proteger y dar mayor confianza a los usuarios que transitan las oficinas, evitando que usuarios maliciosos o externos a las sedes puedan conectarse.

3.6. Encaminamiento Inter-Sede y Conectividad WAN

La interconexión de las sedes se ha diseñado para ofrecer una comunicación transparente, dinámica y altamente segura, utilizando Internet como medio de transporte pero protegiendo el tráfico corporativo mediante tecnologías de cifrado avanzadas. Además, la conexión entre sedes se realiza mediante cables de fibra óptica, para que las comunicaciones entre los núcleos de nuestras sedes sean lo más rápidas posibles.

Para garantizar la privacidad de los datos entre el Campus y las sedes remotas, se ha implementado una arquitectura de VPN Site-to-Site basada en el estándar IPsec:

- Cifrado y Autenticación: Se han configurado protocolos de fase 1 (ISAKMP) y fase 2 (IPsec) para establecer un acuerdo de seguridad que cifra todo el tráfico mediante algoritmos robustos (como AES).
- Túneles GRE sobre IPsec: Con el fin de permitir el paso de tráfico de multidifusión y protocolos de enrutamiento dinámico, se han encapsulado los paquetes en túneles GRE. Esto permite que las sedes se

vean lógicamente como si estuvieran conectadas por un cable directo, a pesar de estar separadas por la red del ISP.

Se ha elegido esta opción porque el coste del despliegue de una red privada sería demasiado elevado para nuestro presupuesto, pero una red pública está expuesta a demasiados ataques, lo cual pondría en riesgo la integridad de la empresa. Es por ello que implementamos el túnel VPN sobre una red pública, para abaratar costes y seguir manteniendo una alta seguridad. La configuración del túnel VPN la encontramos en el apéndice disponible en la Subsección A.2.3

3.7. Conectividad a Internet y Traducción de Direcciones (NAT)

El diseño de la salida a Internet es un punto crítico de la infraestructura, ya que debe garantizar tanto el acceso de los empleados a recursos externos como la disponibilidad de nuestros servicios públicos (Web y DNS) para clientes en Internet. Para simular este entorno de forma realista, se ha configurado un escenario con un Proveedor de Servicios de Internet (ISP) y una estrategia de traducción de direcciones (NAT) dividida en dos niveles.

3.7.1. Simulación del ISP (Internet Service Provider)

Para representar la "nube"de Internet, se ha desplegado un router denominado **Router_ISP**. Este dispositivo actúa como el nexo de unión entre nuestra red corporativa y el resto del mundo.

Su configuración cumple tres funciones vitales:

- **Gateway de Último Recurso:** Es el siguiente salto (*Next Hop*) de nuestro Router de Borde para todo el tráfico saliente (`0.0.0.0/0`).
- **Simulación de Internet:** Conecta a otros routers (simulando usuarios domésticos u otras empresas) en las redes `80.0.0.0` y `10.0.0.0`, permitiendo realizar pruebas de conectividad desde redes externas hacia nuestra web corporativa.
- **Enrutamiento de Retorno:** Dado que nuestra empresa posee un bloque de direcciones públicas (`200.1.1.0/29`) asignado a la zona del Firewall/DMZ, el Router ISP dispone de una ruta estática que dirige el

tráfico destinado a nuestros servidores públicos de vuelta hacia nuestra interfaz WAN:

```
ip route 200.1.1.0 255.255.255.248 200.1.10.2
```

3.7.2. Estrategia de NAT/PAT

Debido a la escasez de direcciones IPv4 públicas y por motivos de seguridad (ocultación de la topología interna), se ha implementado un esquema de traducción de direcciones diferenciado según el tipo de tráfico:

A. Navegación de Usuarios (NAT Overload / PAT)

Para el tráfico generado por los empleados desde la red interna (`172.16.0.0/16`) hacia Internet, la traducción se realiza en el Router de Borde (*Edge Router*).

- **Técnica:** Se utiliza PAT (*Port Address Translation*), configurado mediante el comando:

  ```
  ip nat inside source list 160 interface GigabitEthernet0/0
  overload
  ```

- **Funcionamiento:** Todos los paquetes de los cientos de usuarios internos se traducen a una única dirección IP pública, la de la interfaz WAN del router (`200.1.10.2`), utilizando distintos puertos de origen efímeros para diferenciar las sesiones. Esto maximiza el aprovechamiento de direcciones IP.

B. Publicación de Servicios DMZ (Static NAT)

Para los servidores alojados en la Zona Desmilitarizada (DMZ) que deben ser accesibles desde el exterior, la traducción se realiza en el Firewall ASA.

- **Técnica:** Se utiliza NAT Estático (*Object NAT*).
- **Funcionamiento:** Se ha establecido una relación üno a uno.[en]tre las direcciones privadas de los servidores y las direcciones públicas reservadas, permitiendo conexiones entrantes:

- **Servidor Web:** La IP privada `192.168.100.10` se traduce estáticamente a la pública `200.1.1.3`.
- **Servidor DNS Externo:** La IP privada `192.168.100.11` se traduce estáticamente a la pública `200.1.1.4`.

Esta separación de funciones descarga al Firewall del procesamiento masivo de conexiones de navegación de los empleados (que gestiona el Router) y centraliza el control de seguridad de los servidores públicos en el ASA.

3.8. Servicios de Red

Para garantizar la operatividad de la infraestructura y la presencia digital de la organización, se han desplegado servicios de resolución de nombres y alojamiento web. La arquitectura elegida prioriza la seguridad y la eficiencia del tráfico mediante la segregación de vistas (*Split-DNS*) y el endurecimiento de protocolos web.

3.8.1. Sistema de Nombres de Dominio (DNS) Dividido

Se ha implementado una arquitectura de "*Split-Horizon DNS*"(DNS con horizonte dividido). Esta técnica consiste en mantener dos zonas DNS distintas para el mismo dominio (`empresarac.com`), dependiendo del origen de la consulta:

A. DNS Externo (Zona Pública)

Ubicado en la DMZ (Servidor con IP Privada `192.168.100.11` y traducción estática a `200.1.1.4`).

- **Función:** Resuelve las peticiones provenientes de Internet.
- **Resolución:** Asocia el nombre `www.empresarac.com` a la dirección IP Pública del servidor web (`200.1.1.3`), tal y como se observa en la Figura **??**. Esto permite que clientes externos accedan a través del Firewall.

Figura 3.2: Registro A en el Servidor DNS Externo apuntando a la IP Pública.

B. DNS Interno (Zona Privada)

Ubicado en el CPD de la Sede Central (Servidor `172.16.2.80`).

- **Función:** Resuelve las peticiones de los empleados de las sedes Central, B1 y B2.
- **Resolución:** Asocia el nombre `www.empresarac.com` directamente a la dirección IP Privada del servidor web en la DMZ (`192.168.100.10`), visible en la Figura **??**.
- **Ventaja:** Evita el "*hair-pinning*" (que el tráfico interno tenga que salir hasta la interfaz pública del firewall y volver a entrar), reduciendo la latencia y la carga de procesamiento NAT en el dispositivo de seguridad.

Figura 3.3: Registro A en el Servidor DNS Interno apuntando a la IP Privada de la DMZ.

3.8.2. Servidor Web Corporativo

El servicio de alojamiento web se encuentra centralizado en un servidor dedicado dentro de la Zona Desmilitarizada (DMZ), aislado tanto de la red interna como de Internet mediante políticas estrictas de firewall.

- **Seguridad en Capa de Aplicación:** Se ha deshabilitado el puerto 80 (HTTP) y se ha forzado el uso exclusivo del puerto 443 (HTTPS), garantizando que toda la comunicación entre los clientes y el portal corporativo viaje cifrada, protegiendo la integridad y confidencialidad de los datos.
- **Contenido:** Se ha personalizado la página de inicio (`index.html`) para reflejar la identidad corporativa y la autoría del proyecto.

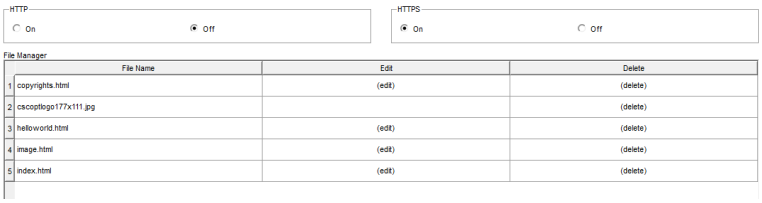


Figura 3.4: Configuración de seguridad del servicio Web forzando HTTPS.

3.9. Gestión y Monitorización

Para mantener el control operativo sobre una infraestructura distribuida y heterogénea, es fundamental implementar sistemas centralizados de gestión. Hemos desplegado los protocolos NTP y Syslog para garantizar la trazabilidad y la coherencia de los eventos de red.

3.9.1. Sincronización de Tiempo (NTP)

La correlación de eventos entre dispositivos dispersos geográficamente es imposible si los relojes internos no están sincronizados. Un desfase de pocos segundos puede impedir el análisis forense de un ataque que atraviesa múltiples routers. Para solucionar esto, se ha configurado el protocolo NTP (*Network Time Protocol*) en arquitectura cliente-servidor:

- **Maestro de Tiempo:** El servidor de Gestión ubicado en el CPD (`172.16.2.75`) actúa como la fuente de tiempo autoritativa para toda la organización.
- **Clientes:** Todos los Routers (Borde, VPN, Sedes B1/B2) y Switches de la red sincronizan sus relojes periódicamente contra este servidor a través de la red interna y los túneles VPN. Esto garantiza que los registros de logs (*timestamps*) sean coherentes y precisos en toda la topología.

3.9.2. Registro de Eventos (Syslog)

Dado que el almacenamiento local de logs en routers y switches es volátil y limitado, se ha implementado un sistema de Syslog centralizado.

- **Servidor de Destino:** El mismo servidor de gestión (`172.16.2.75`) recibe los mensajes de estado.
- **Nivel de Severidad:** Se ha configurado el nivel `debugging` (nivel 7) y `informational` en los dispositivos críticos. Esto asegura que no solo se registren los fallos graves (como la caída de una interfaz), sino también eventos de seguridad como intentos de conexión fallidos o cambios de configuración.
- **Visibilidad:** Esta centralización permite al administrador de red monitorizar el estado de salud de las tres sedes desde un único panel de control ("Dashboard") en la sede central, facilitando la detección proactiva de incidencias antes de que afecten a los usuarios.

3.10. Mecanismos de seguridad

Además de configurar medidas y protocolos de seguridad para evitar que usuarios maliciosos puedan acceder a nuestra red desde el exterior, como pueden ser el tunel VPN entre sedes o el firewall, también es necesario proteger las comunicaciones internas de nuestras sedes. Para ello hemos implementado políticas de control de acceso (ACL) en los switches multicapa ubicados en la capa de distribución de nuestras sedes.

Estas listas de control de acceso se han realizado con el objetivo de:

- Aislamiento de la Red de Invitados: No permitir a los usuarios pertenecientes a la red de invitados acceder a cualquier punto de la red corporativa. A estos usuarios solo se les permite acceder a Internet, para no poner en riesgo la seguridad interna de nuestras sedes.
- Acceso restringido al CPD: Algunos servidores ubicados en el CPD son de acceso restringido según los requisitos indicados por el cliente, siendo estos los servidores de almacenamiento y cómputo, que solo deben ser accesibles por los departamentos de investigación y soporte técnico.

Cada uno de estos objetivos da lugar a una lista de control de accesos. La lista correspondiente al acceso del CPD solo está implementada en la Sede Central, ya que es donde se encuentra dicho Centro de Procesamiento. La lista de los invitados se encuentra implementada en todas las sedes. Encontramos la creación y aplicación de estas listas en el apéndice de la Subsección A.2.4

3.10.1. Cortafuegos Perimetral y Gestión de Zonas (Firewall ASA)

Como elemento central de la estrategia de ciberseguridad, se ha desplegado un dispositivo Cisco ASA (*Adaptive Security Appliance*). Este equipo no solo realiza la traducción de direcciones para los servidores (como se detalló en el apartado 3.10), sino que su función principal es la inspección de estados (*Stateful Inspection*) y la segmentación de la red en zonas de confianza.

Estrategia de Zonas y Niveles de Seguridad

El diseño del cortafuegos se basa en el concepto de "Niveles de Seguridad"(*Security Levels*), definiendo tres interfaces físicas con roles diferenciados:

- **INSIDE (Nivel 100 - Gig1/3):** Conectada al Router Central (`192.168.254.2`). Es la zona de máxima confianza. Por defecto, el tráfico originado aquí puede salir hacia cualquier otra zona (DMZ o Internet) sin restricciones explícitas, y el firewall guarda el estado de la conexión para permitir el retorno del tráfico.
- **OUTSIDE (Nivel 0 - Gig1/1):** Conectada al Router VPN y hacia Internet. Es la zona de nula confianza. Todo tráfico originado aquí que intente entrar a nuestra red es bloqueado por defecto, salvo que exista una lista de control de acceso (ACL) que lo permita explícitamente.
- **DMZ (Nivel 50 - Gig1/2):** Zona Desmilitarizada. Posee un nivel de seguridad intermedio.
  - **Protege a la red interna:** Si un servidor web en la DMZ es comprometido, el atacante no puede saltar a la red Inside porque el nivel 50 es menor que el 100.
  - **Es accesible desde fuera:** Al tener mayor nivel que Outside (0), se pueden publicar servicios controlados.

Políticas de Filtrado (ACLs)

Se han implementado Listas de Control de Acceso extendidas para regular el tráfico entrante y saliente, aplicando el principio de "mínimo privilegio":

1. Política de Entrada desde Internet (PERMITIR_INTERNET)
Aplicada en la interfaz *outside*, filtra el tráfico proveniente de la red pública. Solo se permiten tres tipos de flujos:

- **Servicios Públicos:** Se permite el tráfico web seguro (HTTPS/443) hacia el servidor Web y consultas de nombres (UDP/53) hacia el servidor DNS externo.
- **Gestión y Monitorización:** Se han creado excepciones específicas para que el Router VPN (`200.1.1.1`) pueda enviar alertas de Syslog (UDP 514) y sincronización de tiempo NTP (UDP 123) al servidor de gestión interno, garantizando que incluso el equipo de borde esté monitorizado.
- **Diagnóstico:** Se permite tráfico ICMP para pruebas de conectividad (Ping), controlado mediante inspección de paquetes (`inspect icmp`).

2. Política de Aislamiento de la DMZ (DMZ)
Aplicada en la interfaz *dmz*, regula lo que los servidores públicos pueden hacer. Esta es la política más crítica para la seguridad interna:

- **Bloqueo a la Red Interna:** La regla `deny ip 192.168.100.0 ... 172.16.0.0` prohíbe explícitamente cualquier intento de conexión desde la DMZ hacia la Intranet corporativa. Esto asegura que un compromiso en el servidor web no se propague a los ordenadores de los empleados.
- **Excepciones de Gestión:** Únicamente se permite el paso de logs (Syslog) y tráfico NTP hacia el servidor de gestión específico (`172.16.2.75`), necesario para la auditoría de los servidores.
- **Salida a Internet:** Se permite (`permit ip ... any`) que los servidores de la DMZ inicien conexiones hacia Internet (por ejemplo, para descargar actualizaciones del sistema operativo).

Enrutamiento e Inspección

Para garantizar la conectividad entre las zonas, se han configurado rutas estáticas en el ASA:

- Una ruta por defecto hacia el Router VPN (`200.1.1.1`) para la salida a Internet.

- Rutas hacia las redes internas (`172.16.0.0/16`) a través del Router Central, asegurando que el firewall sepa devolver el tráfico a las sedes correspondientes.

Adicionalmente, se ha activado una política de inspección global (`service-policy global_policy`) que analiza protocolos complejos como DNS, FTP y TFTP, asegurando que las conexiones cumplan con los estándares de la RFC y previniendo ataques de túneles o desbordamientos de búfer en estos servicios. [3]

3.11. Acceso Remoto y Movilidad Segura

Para dar respuesta a la necesidad de movilidad y continuidad del negocio, uno de los requisitos que se nos exigía, se ha implementado una solución de acceso remoto que permite a los empleados trabajar desde sus hogares con el mismo nivel de seguridad que si estuvieran en las oficinas físicas.

Para ello hemos configurado un concentrador VPN en la Sede Central, antes del firewall, para tener controladas todas las conexiones que se realicen por medio de dicho concentrador. De esta forma, los teletrabajadores podrán acceder a los recursos de la Sede Central de la empresa mediante una conexión VPN client-to-site. La configuración del concentrador se puede ver en el apéndice ubicado en la Subsección A.2.5

Para realizar dicha conexión, los clientes deberán introducir unas credenciales y la dirección IP del concentrador. Una vez conectados, el concentrador les asignará una IP correspondiente a un rango reservado para los teletrabajadores, y ya dichos usuarios podrán navegar libremente por la red corporativa.

De esta forma conseguimos que nuestros trabajadores no necesiten estar fisicamente en alguna de las sedes para poder realizar su trabajo, sin comprometer la seguridad de nuestros trabajadores y datos de la empresa. Esto es porque la comunicación desde el hogar del teletrabajador hasta el concentrador VPN está cifrada gracias al túnel creado, además de que se necesita autenticación para acceder a dicho túnel.

3.12. Protocolos para alta disponibilidad

Uno de los requisitos más importantes de nuestra red corporativa es que debe tener una alta disponibilidad, pues necesitamos ofrecer nuestros servicios de forma ininterrumpida, tanto a nuestros trabajadores como a nuestros clientes. Para ello, además de disponer de redundancia de casi todos nuestros equipos de red, hemos aplicado protocolos que nos ayudan a aumentar esta disponibilidad. En la capa de distribución hemos implementado HSRP en los switch multicapa, mientras que en la capa de "core" hemos realizado agregación de enlaces mediante el protocolo LACP.

3.12.1. HSRP

Hemos implementado HSRP (Hot Standby Router Protocol) en la capa de distribución de todas las sedes. El uso de este protocolo evita que el fallo de un único dispositivo interrumpa la salida a Internet o la comunicación entre departamentos, ya que trata de disponer de varios gateways para los dispositivos e ir cambiandolos según estén disponibles. También aprovechamos el uso de este protocolo para realizar compartición de carga, para evitar la saturación de la red.

El funcionamiento consiste en asignar a los equipos una IP virtual de gateway, y es a esta IP virtual a la que le asignamos una IP y MAC física según el switch multicapa que queramos que se encargue del enrutamiento de ese tráfico. Estos serán los equipos "Active" y los demás estarán en "Standby".

Para realizar la compartición de carga, asignamos un equipo como "Active" para que se encargue el enrutamiento del tráfico de algunas VLANs, y así otros equipos para que enrute otros tipos de tráfico.

Para que este protocolo funcione correctamente junto a otros mecanismos de nuestra red, como pueden ser las ACL, HSRP se ha configurado directamente sobre las Interfaces Virtuales de Switch (SVI) de los switches multicapa.

Toda esta configuración se encuentra disponible en el apéndice correspondiente a la Subsección A.2.1 [4]

3.12.2. LACP

Para la interconexión entre la Sede Central y las Sedes B1 y B2, se ha diseñado una agregación de enlaces bajo el estándar IEEE 802.3ad (LACP). El objetivo principal es triplicar el ancho de banda disponible (utilizando tres interfaces GigabitEthernet) y garantizar la alta disponibilidad de la red. De esta form optimizamos el rendimiento para cumplir con el requisito de 1 Mbps por usuario.

Consideramos de gran importancia el uso de este protocolo, ya que la disponibilidad y una alta velocidad de transporte del tráfico resulta vital en la capa troncal, que es la parte más crítica de la red. Además, este protocolo nos ofrece también la posibilidad de realizar balanceo de cara y disponer de una mayor tolerancia a fallos.

Sin embargo, Packet Tracer, el simulador de red que hemos utilizado, no dispone de modelos de routers que satisfagan todos los requisitos para realizar las configuraciones anteriormente mencionadas y que además soporten el protocolo LACP. Es por ello que no hemos podido implementarlo en el simulador, y tendría que probarse en un entorno real con otros routers. No obstante, dejamos una documentación sobre la configuración de este protocolo en otros modelos CISCO en el apéndice de la Subsección A.2.6.

3.12.3. Prevención de Bucles y Protocolo STP

Dado que nuestra capa de distribución cuenta con enlaces redundantes (físicos) para garantizar la disponibilidad, es imperativo el uso del protocolo STP (*Spanning Tree Protocol*) para evitar la formación de bucles de capa 2 (tormentas de *broadcast*) que podrían colapsar la red.

Para nuestra implementación, hemos seleccionado la variante **PVST+ (Per-VLAN Spanning Tree Plus)**. A diferencia del estándar clásico (CST) que crea un único árbol para toda la red, PVST+ crea una instancia de árbol de expansión separada para cada VLAN. Esto nos permite realizar un balanceo de carga de capa 2: mientras unas VLANs utilizan el enlace de la izquierda como camino principal, otras utilizan el de la derecha, optimizando el ancho de banda de los enlaces troncales (*Uplinks*).

Alineación de Topologías (STP + HSRP)

El aspecto más crítico de este diseño ha sido la sincronización entre la topología de STP y el protocolo de redundancia de gateway HSRP detallado

en el apartado anterior.

El objetivo es garantizar que el switch que actúa como **Gateway Activo (HSRP)** para una VLAN específica sea, al mismo tiempo, el **Puente Raíz (Root Bridge)** de dicha VLAN. Si no se alinean ambos protocolos, el tráfico seguiría rutas subóptimas, atravesando enlaces innecesarios entre switches de distribución antes de salir de la red.

Para lograr esto, hemos manipulado determinísticamente las prioridades del puente (*bridge priority*), reduciéndolas respecto al valor por defecto (32768) para forzar la elección del Root Bridge:

- **Prioridad 24.576 (Root Primario):** Se asigna al switch que debe ser el "Jefe"de esa VLAN. Este valor asegura que ganará la elección frente a cualquier otro switch con prioridad por defecto.

  Ejemplo: Si el Switch Dist-1 es el HSRP Activo para la VLAN 400, se le configura:
  `spanning-tree vlan 400 priority 24576`

- **Prioridad 28.672 (Root Secundario/Backup):** Se asigna al switch redundante. Si el primario cae, este switch tiene la siguiente prioridad más baja, asumiendo el rol de Root Bridge inmediatamente.

  Ejemplo: El Switch Dist-2, que es HSRP Standby para la VLAN 400, se configura con:
  `spanning-tree vlan 400 priority 28672`

De esta forma, hemos configurado los switches de distribución de manera cruzada para repartir la carga de procesamiento de forma eficiente.

Capítulo 4

Diseño físico y evaluación

4.1. Diseño físico

Para la materialización del diseño lógico, se ha desarrollado una infraestructura física distribuida en tres sedes geográficas: Sede Central, Sede B1 y Sede B2. El diseño se ha modelado utilizando Cisco Packet Tracer, adaptando los recursos disponibles en el software a los requisitos de tráfico calculados y proponiendo una solución de mercado equivalente para el despliegue real.

4.1.1. Medios de Transmisión y Cableado

Se ha establecido un esquema de cableado que diferencia la simulación realizada de la propuesta de compra real, especificando las categorías necesarias para soportar las velocidades de Gigabit y 10-Gigabit Ethernet.

Tipo de Conexión	**Simulación**	**Propuesta Real de Compra**	**Velocidad**
Acceso (PC/AP - Switch)	Cobre UTP (Straight)	Cable UTP Cat 6A	1 / 10 Gbps
Backbone (Acceso - Dist.)	Cobre UTP (Cross-over)	Fibra Óptica Multimodo OM4 (LC-LC)	10 / 40 Gbps
Backbone (Dist. - Router)	Cobre UTP (Straight)	Cable UTP Cat 6A	1 / 10 Gbps
WAN (Inter-sedes)	Fibra Monomodo	Fibra Óptica Monomodo OS2	1 - 100 Gbps

Tabla 4.1: Comparativa de Conexiones

Nota sobre la conexión al ISP: Aunque en la simulación se ha utilizado cobre en el último tramo por limitación de puertos de fibra, en la implementación real se recomienda una acometida de fibra óptica directa al equipo del proveedor.

4.1.2. Selección de Dispositivos de Red

Para garantizar la homogeneidad y facilitar el mantenimiento, se ha unificado la elección de modelos para todas las sedes, variando únicamente los módulos de expansión según la necesidad de puertos.

El dimensionamiento del hardware se ha realizado considerando un perfil de tráfico de 1 Mbps por usuario. Esto implica soportar una carga mínima de 200 Mbps en la Sede Central, 50 Mbps en B1 y 10 Mbps en B2, sumado al tráfico de gestión y la red de invitados Wi-Fi.

A continuación, se detalla el equipamiento utilizado en la maqueta (Packet Tracer) y la propuesta de equipos actuales de mercado para cumplir con la escalabilidad y los requisitos técnicos:

A. Routers de Borde y Servicios (Sedes Central, B1 y B2)

- **Simulación:** Cisco 2911 (Central/B1) y ISR 4331 (B2).
- **Propuesta Real:** Cisco Catalyst 8300 Series Edge Platforms (Modelo C8300-1N1S-4T2X).
- **Características Técnicas:**
  - **Throughput:** Hasta 5 Gbps (IPSec SD-WAN), superando holgadamente los 200 Mbps requeridos en la sede central.
  - **Puertos Integrados:** 4 puertos Gigabit Ethernet (Cobre) y 2 puertos SFP+ (10G Fibra).
  - **Modularidad:** Dispone de slots para módulos NIM (Network Interface Modules).
- **Adaptación a la Sede Central:** Dado que el Router Central requiere 5 puertos Gigabit (3 de cobre y 2 de fibra), al modelo base se le añadirá un módulo NIM-ES2-4 (Switch module) o un transceptor SFP adicional para cubrir todas las conexiones sin cuellos de botella.

B. Switches de Distribución (Capa 2/3)

- **Simulación:** Cisco 3560.
- **Propuesta Real:** Cisco Catalyst 9300 Series.
- **Rol:** Switch Multicapa (L2/L3) encargado del enrutamiento inter-VLAN.
- **Rendimiento:** Capacidad de conmutación de hasta 480 Gbps (con StackWise).
- **Uplinks:** Módulos de red con puertos de fibra 10G SFP+ para conectar con los routers y el backbone del edificio a alta velocidad.

C. Switches de Acceso (Capa 2)

- **Simulación:** Cisco 2960.
- **Propuesta Real:** Cisco Catalyst 9200L Series.
- **Rol:** Switch de Capa 2 puro para conectividad de usuarios finales.
- **PoE+:** Capacidad para alimentar teléfonos IP y APs (hasta 740W).
- **Escalabilidad (Stacking):** En la Sede Central, para cubrir zonas con alta densidad (50 usuarios por zona), se utilizará la tecnología Cisco StackWise-80, permitiendo apilar 2 unidades de 48 puertos y gestionarlas como un único dispositivo lógico, simplificando la administración y proporcionando redundancia.

D. Seguridad Perimetral

- **Simulación:** Cisco ASA 5506-X.
- **Propuesta Real:** Cisco Firepower 1100 Series.
- **Throughput:** 1.2 Gbps (Firewall + AVC + IPS), garantizando que la seguridad no sea un cuello de botella para el tráfico de todos los usuarios.
- **Puertos:** 8 x 1 GE (Cobre) y 4 x 1 GE (SFP), permitiendo las conexiones físicas requeridas hacia el Router Central, Router de Borde y Switch DMZ.

E. Infraestructura Inalámbrica: Controlador (WLC)

- **Simulación:** Cisco 3504 Wireless Controller.
- **Propuesta Real:** Cisco Catalyst 9800-L Wireless Controller.
- **Justificación:** Aunque el modelo 3504 es funcional, la serie 9800 es el estándar actual basado en IOS-XE.
- **Capacidad:** Soporta hasta 250 Puntos de Acceso y 5000 clientes concurrentes, cubriendo sobradamente los requisitos de invitados de nuestras tres sedes.
- **Seguridad:** Soporte nativo para WPA3 y segmentación de tráfico de invitados.

F. Infraestructura Inalámbrica: Puntos de Acceso (AP)

- **Simulación:** Cisco AP-PT (Genérico) / LAP-PT.
- **Propuesta Real:** Cisco Catalyst 9120 Series (Wi-Fi 6).
- **Tecnología:** Wi-Fi 6 (802.11ax). Esto es crítico para el requisito de 50 invitados por AP, ya que tecnologías como OFDMA y MU-MIMO permiten gestionar múltiples conexiones simultáneas sin degradar el servicio, algo que los APs antiguos no gestionaban eficientemente.
- **Conexión:** Puerto Gigabit Ethernet PoE+, recibiendo datos y electricidad directamente del switch de acceso.

G. Servidores (CPD y DMZ)

- **Simulación:** Server-PT (Genérico).
- **Propuesta Real:** Cisco UCS C-Series Rack Servers (Modelo C220 M6).
- **Justificación:** Servidores de rack de 1 unidad (1RU) de alto rendimiento.
- **Configuración:** Equipados con doble fuente de alimentación (redundancia), almacenamiento en RAID para protección de datos y múltiples interfaces de red Gigabit/10G.

- **Roles:** Estos servidores físicos tienen capacidad de virtualización para alojar los roles lógicos definidos en el diseño (DHCP, DNS, Syslog, NTP, Web), optimizando el espacio en el rack y el consumo energético.

4.1.3. Organización Física y Salas Técnicas

El diseño físico contempla la centralización de servicios para optimizar el mantenimiento y la seguridad.

Sede Central: Sala MDF (Main Distribution Frame)

En la sede principal hemos diseñado una sala técnica unificada (CPD) que integra los componentes críticos. Este espacio alberga:

- **Rack de Comunicaciones:** Contiene el Router Central, el Firewall, el Router VPN/NAT y la electrónica de red.
- **Rack de Servidores:** Aloja los servidores de Cómputo, DHCP, DNS y Gestión, conectados a switches Gigabit.
- **Rack DMZ:** Segmentado físicamente, contiene los servidores Web y DNS Público.

Sedes Remotas (B1 y B2)

Las sedes B1 y B2 funcionan como delegaciones conectadas por WAN. En estas, se ha dispuesto un armario de comunicaciones (IDF) que contiene el Router (modelo unificado Catalyst 8300/ISR 4331 simulado) y los switches de acceso apilados o individuales según la demanda de la zona.

Topología Geográfica

La interconexión de las tres sedes a través de la infraestructura de la ciudad simulada y su salida hacia la nube de Internet se observa en la Figura ??.

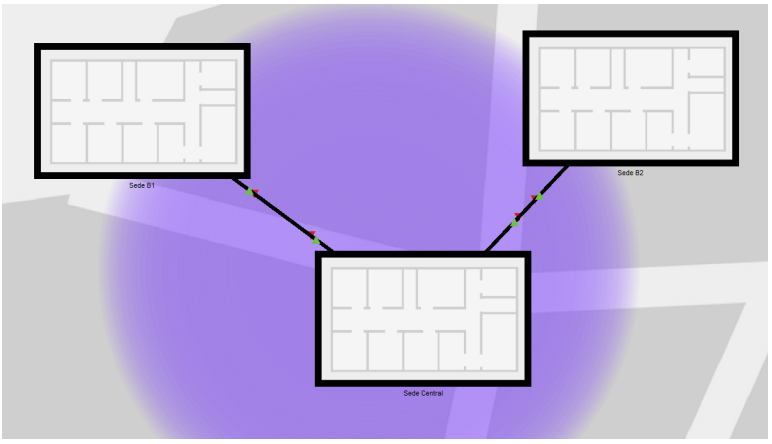


Figura 4.1: Distribución geográfica de las tres sedes y enlaces de fibra

4.2. Evaluación

Test realizados y resultados. Estamos limitados por el simulador/emulador elegido así que la evaluación de que se cumplen los requisitos establecidos estará condicionada a las características que nos proporcione la herramienta elegida de simulación/emulación de redes.

4.2.1. HSRP

Para comprobar que hemos configurado el protocolo HSRP correctamente y que este está ofreciendo las funcionalidades esperadas, introducimos en la interfaz de comandos de los switches multicapa el siguiente comando, que nos indica si el switch está en modo "Active" o "Standby"para cada una de sus interfaces. En este caso las interfaces son SVI, ya que estamos encaminando distintas VLANs:

```
Switch#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl100       100  105 P Active   local           172.16.0.62     172.16.0.1
Vl200       200  105 P Active   local           172.16.0.126    172.16.0.65
Vl300       300  105 P Active   local           172.16.0.190    172.16.0.129
Vl400       400  95  P Standby  172.16.0.254    local           172.16.0.193
Vl500       500  95  P Standby  172.16.1.62     local           172.16.1.1
Vl600       600  105 P Active   local           172.16.1.253    172.16.1.129
Vl900       900  95  P Standby  172.16.2.62     local           172.16.2.1
Vl950       950  95  P Standby  172.16.2.94     local           172.16.2.65
Vl999       999  95  P Standby  172.16.200.30   local           172.16.200.1
Switch#
```

Figura 4.2: Comprobación interfaces HSRP

Además, para terminar de comprobar su funcionamiento, realizamos un ping desde un PC de un departamento a un PC de otro departamento, y en mitad de la conexión desactivamos la interfaz que estaba en modo "Active" para este enrutamiento. El resultado fue el esperado, pues el ping no se cortó y la interfaz encargada de este enrutamiento que estaba en "Standby"pasó a modo "Active".

4.2.2. Red WI-FI

Para comprobar que la red WI-FI está operativa y da conectividad a los usuarios que se quieran conectar, simplemente vamos a la aplicación "PC Wireless"de un PC o Laptop y comprobamos que nos da opción a conectarnos a una red.

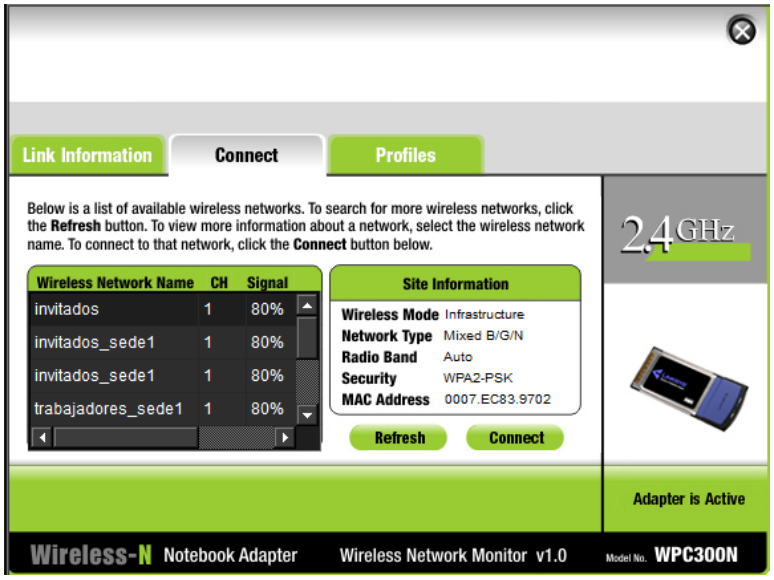


Figura 4.3: Comprobación redes WI-FI

Si seleccionamos la red e introducimos la contraseña ("password"para todas las redes), nos permite conectarnos y vemos la conexión directamente en la topología.

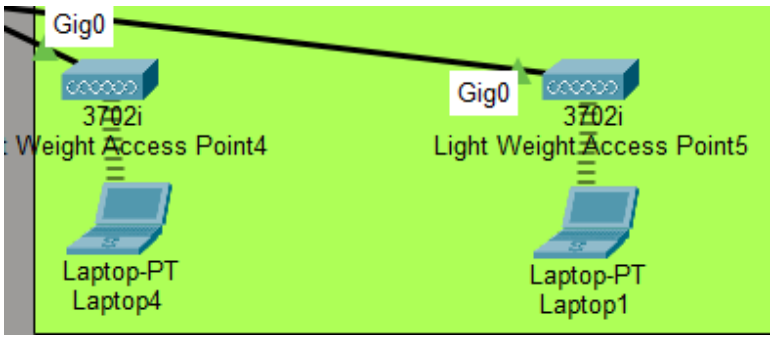


Figura 4.4: Comprobación conexión WI-FI

Una vez conectados, vemos que el servidor DHCP asigna al dispositivo una IP del rango asignado para los invitados y que si hacemos un ping, podemos acceder a Internet pero no a dispositivos internos de las sedes.

4.2.3. Túnel VPN entre sedes

Para comprobar que el túnel VPN entre sedes realmente se ha establecido, introducimos el siguiente comando en los routers de borde de las sedes para, entre otros datos ofrecidos, observar que los paquetes realmente están siendo cifrados y descifrados:

```
Router-Central#show crypto ipsec sa

interface: GigabitEthernet0/3/0
    Crypto map tag: MYMAP, local addr 192.168.200.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.200.1/255.255.255.255/47/0)
   remote  ident (addr/mask/prot/port): (192.168.200.2/255.255.255.255/47/0)
   current_peer 192.168.200.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 615, #pkts encrypt: 615, #pkts digest: 0
   #pkts decaps: 619, #pkts decrypt: 619, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 192.168.200.1, remote crypto endpt.:192.168.200.2
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/3/0
     current outbound spi: 0xA89F71FA(2829021690)

     inbound esp sas:
      spi: 0x6C5B7DC2(1817935298)
--More--
```

Figura 4.5: Comprobación cifrado VPN

4.2.4. ACLs

Ya hemos configurado las listas de acceso disponibles en el anexo, pero para comprobar que estas se están aplicando, además de intentar realizar las conexiones que no hemos permitido, podemos ver cuales son las reglas específicas que están bloqueando o permitiendo el paso de tráfico. Para ello introducimos el siguiente comando en los switches multicapa:

```
Switch#show ip access-lists
Extended IP access list invitados->sedeCentral
    10 permit ip any host 172.16.2.70
    20 permit ip 172.16.1.128 0.0.0.127 172.16.1.128 0.0.0.127
    30 permit ip any host 8.8.8.8
    40 deny ip any 172.16.0.0 0.0.255.255 (4 match(es))
    50 permit ip any any (21 match(es))
Extended IP access list servidoresComputo
    10 permit ip 172.16.0.0 0.0.0.63 172.16.2.0 0.0.0.255
    20 permit ip 172.16.1.0 0.0.0.63 172.16.2.0 0.0.0.255
    30 permit ip 172.16.64.0 0.0.0.31 172.16.2.0 0.0.0.255
    40 permit ip 172.16.64.128 0.0.0.31 172.16.2.0 0.0.0.255

Switch#
```

Figura 4.6: Comprobación aplicación ACLs

Vemos que al lado de las reglas aparece el número de "matches", que corresponde al número de paquetes a los que se le ha aplicado dicha regla.

4.2.5. Conexión VPN de los teletrabajadores

Tras configurar el túnel VPN para la conexión de los teletrabajadores a la Sede Central, podemos comprobar la conexión desde la aplicación "VPN"del ordenador de la casa del teletrabajador. En ella introducimos las credenciales correspondientes a nuestro túnel (la contraseña es "password") y al conectarnos nos da una IP correspondente al pool de direcciones configurado en el concentrador VPN.

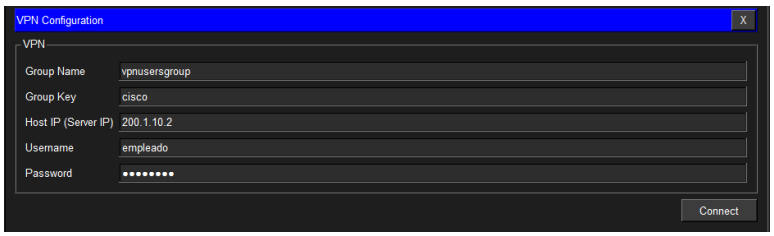


Figura 4.7: Intento conexión VPN

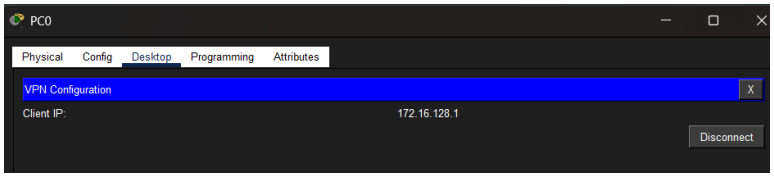


Figura 4.8: Conexión VPN exitosa

Una vez nos hemos conectado y hemos recibido la IP, ya podemos realizar conexiones a los distintos dispositivos de la sede.

4.2.6. Validación de Direccionamiento y Redundancia (DHCP + HSRP)

Se ha verificado que los dispositivos finales obtienen correctamente su configuración de red de forma dinámica y que la puerta de enlace asignada corresponde a la dirección virtual de alta disponibilidad.

Prueba realizada: Ejecución del comando `ipconfig /all` en un PC de la VLAN de Ventas (Sede Central).

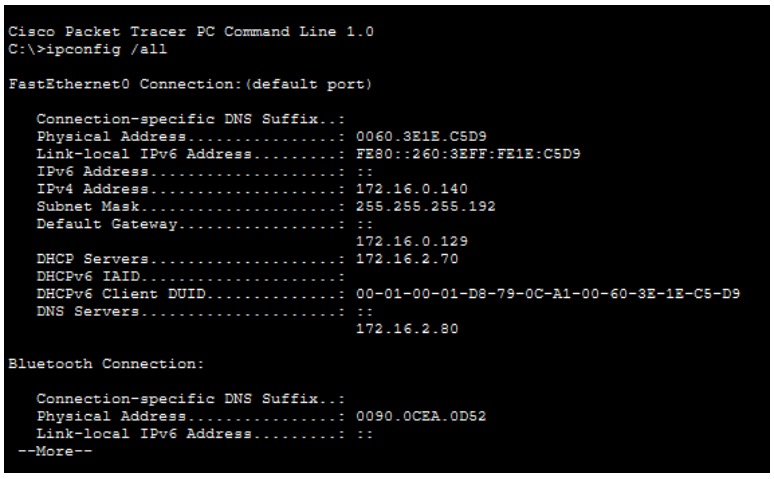


Figura 4.9: Asignación dinámica de direcciones y Gateway virtual HSRP.

Como se aprecia en la Figura 4.9, el equipo ha recibido automáticamente una dirección IP dentro del rango `172.16.0.X`. Asimismo, se confirma que la Puerta de Enlace Predeterminada es la `172.16.0.129`, que corresponde a la IP Virtual (VIP) configurada en el grupo HSRP, y no a la dirección física del switch, validando así la redundancia del primer salto.

4.2.7. Verificación del Enrutamiento Dinámico (OSPF)

Para validar la convergencia de la red y la propagación de rutas entre sedes, se ha inspeccionado la tabla de enrutamiento de los dispositivos de borde.

Prueba realizada: Ejecución del comando `show ip route` en el Router de la Sede B1.

```
Router-B1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.10.10.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.10.10.0/30 is directly connected, Tunnel0
L       10.10.10.2/32 is directly connected, Tunnel0
     172.16.0.0/16 is variably subnetted, 23 subnets, 5 masks
O       172.16.0.0/26 [110/1002] via 10.10.10.1, 00:01:01, Tunnel0
O       172.16.0.64/26 [110/1002] via 10.10.10.1, 00:01:01, Tunnel0
O       172.16.0.128/26 [110/1002] via 10.10.10.1, 00:01:01, Tunnel0
O       172.16.0.192/26 [110/1002] via 10.10.10.1, 00:01:01, Tunnel0
O       172.16.1.0/26 [110/1002] via 10.10.10.1, 00:01:01, Tunnel0
O       172.16.1.128/25 [110/1002] via 10.10.10.1, 00:01:01, Tunnel0
O       172.16.2.0/26 [110/1002] via 10.10.10.1, 00:01:01, Tunnel0
O       172.16.2.64/26 [110/1002] via 10.10.10.1, 00:01:01, Tunnel0
O       172.16.3.0/30 [110/1001] via 10.10.10.1, 00:01:01, Tunnel0
O       172.16.3.4/30 [110/1001] via 10.10.10.1, 00:01:01, Tunnel0
O       172.16.3.8/30 [110/1001] via 10.10.10.1, 00:01:01, Tunnel0
O       172.16.64.0/27 [110/2] via 172.16.65.2, 00:01:01, GigabitEthernet0/0
                       [110/2] via 172.16.65.6, 00:01:01, GigabitEthernet0/1
O       172.16.64.32/27 [110/2] via 172.16.65.2, 00:01:01, GigabitEthernet0/0
                        [110/2] via 172.16.65.6, 00:01:01, GigabitEthernet0/1
O       172.16.64.64/27 [110/2] via 172.16.65.2, 00:01:01, GigabitEthernet0/0
                        [110/2] via 172.16.65.6, 00:01:01, GigabitEthernet0/1
O       172.16.64.96/27 [110/2] via 172.16.65.2, 00:01:01, GigabitEthernet0/0
                        [110/2] via 172.16.65.6, 00:01:01, GigabitEthernet0/1
O       172.16.64.128/27 [110/2] via 172.16.65.2, 00:01:01, GigabitEthernet0/0
                         [110/2] via 172.16.65.6, 00:01:01, GigabitEthernet0/1
O       172.16.64.192/26 [110/2] via 172.16.65.2, 00:01:01, GigabitEthernet0/0
                         [110/2] via 172.16.65.6, 00:01:01, GigabitEthernet0/1
C       172.16.65.0/30 is directly connected, GigabitEthernet0/0
L       172.16.65.1/32 is directly connected, GigabitEthernet0/0
C       172.16.65.4/30 is directly connected, GigabitEthernet0/1
L       172.16.65.5/32 is directly connected, GigabitEthernet0/1
O       172.16.100.0/27 [110/2] via 172.16.65.2, 00:01:01, GigabitEthernet0/0
                        [110/2] via 172.16.65.6, 00:01:01, GigabitEthernet0/1
O       172.16.200.0/27 [110/1002] via 10.10.10.1, 00:01:01, Tunnel0
     192.168.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.200.0/30 is directly connected, GigabitEthernet0/3/0
L       192.168.200.2/32 is directly connected, GigabitEthernet0/3/0
O*E2 0.0.0.0/0 [110/1] via 10.10.10.1, 00:01:36, Tunnel0
```

Figura 4.10: Tabla de enrutamiento en Sede B1 con rutas OSPF.

En la Figura 4.10 se observa cómo el router ha aprendido las rutas de las otras sedes (marcadas con la letra **O**). Destaca especialmente la presencia de la ruta `O*E2 0.0.0.0/0`, lo que indica que el Router Central está propagando correctamente la ruta por defecto hacia Internet a toda la organización.

4.2.8. Conectividad a Internet y NAT (Navegación de Usuarios)

Se ha comprobado la capacidad de los usuarios internos para acceder a recursos externos, verificando simultáneamente el enmascaramiento de IPs privadas (PAT).

Prueba realizada: Prueba de conectividad (Ping) hacia Internet y verificación de la tabla de traducciones NAT.

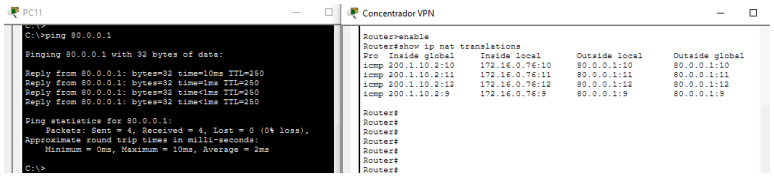


Figura 4.11: Conectividad externa y verificación de NAT Overload (PAT).

Tal y como muestra la Figura 4.11, el ping hacia el servidor externo (80.0.0.1) es exitoso. En la parte derecha de la imagen, la tabla de traducciones del router confirma que la dirección privada de origen ha sido traducida a la dirección pública de la interfaz WAN (`200.1.10.2`) utilizando un puerto efímero, ocultando así la topología interna.

4.2.9. Servicios Públicos y Seguridad Perimetral (DMZ)

Esta prueba valida la correcta configuración del Firewall ASA, las reglas de acceso (ACL) y la publicación de servicios mediante NAT estático.

Prueba realizada: Acceso seguro (HTTPS) al servidor web corporativo desde un equipo externo situado en Internet.

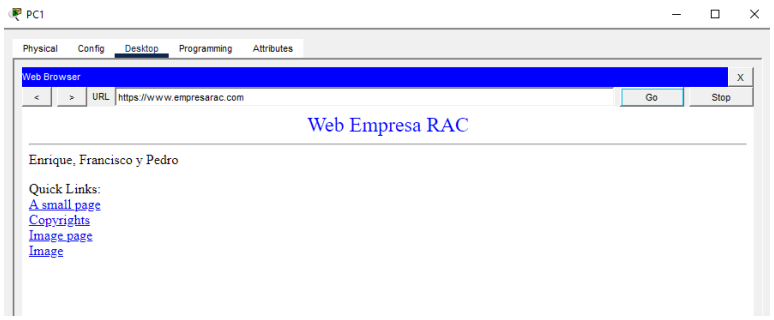


Figura 4.12: Acceso exitoso al servidor Web seguro a través del Firewall.

En la Figura 4.12 se observa cómo el navegador del cliente externo carga correctamente la página corporativa. Esto evidencia que el Firewall ha permitido el tráfico entrante al puerto 443 (HTTPS) y que el NAT Estático ha redirigido correctamente la petición pública (`200.1.1.3`) hacia el servidor interno de la DMZ (`192.168.100.10`).

4.2.10. Resolución de Nombres (Split-DNS)

Se ha validado la arquitectura de DNS de horizonte dividido, comprobando que la resolución de nombres se adapta al origen de la petición para optimizar el tráfico.

Prueba realizada: Ejecución del comando `nslookup www.empresarac.com` desde la red interna y desde Internet.

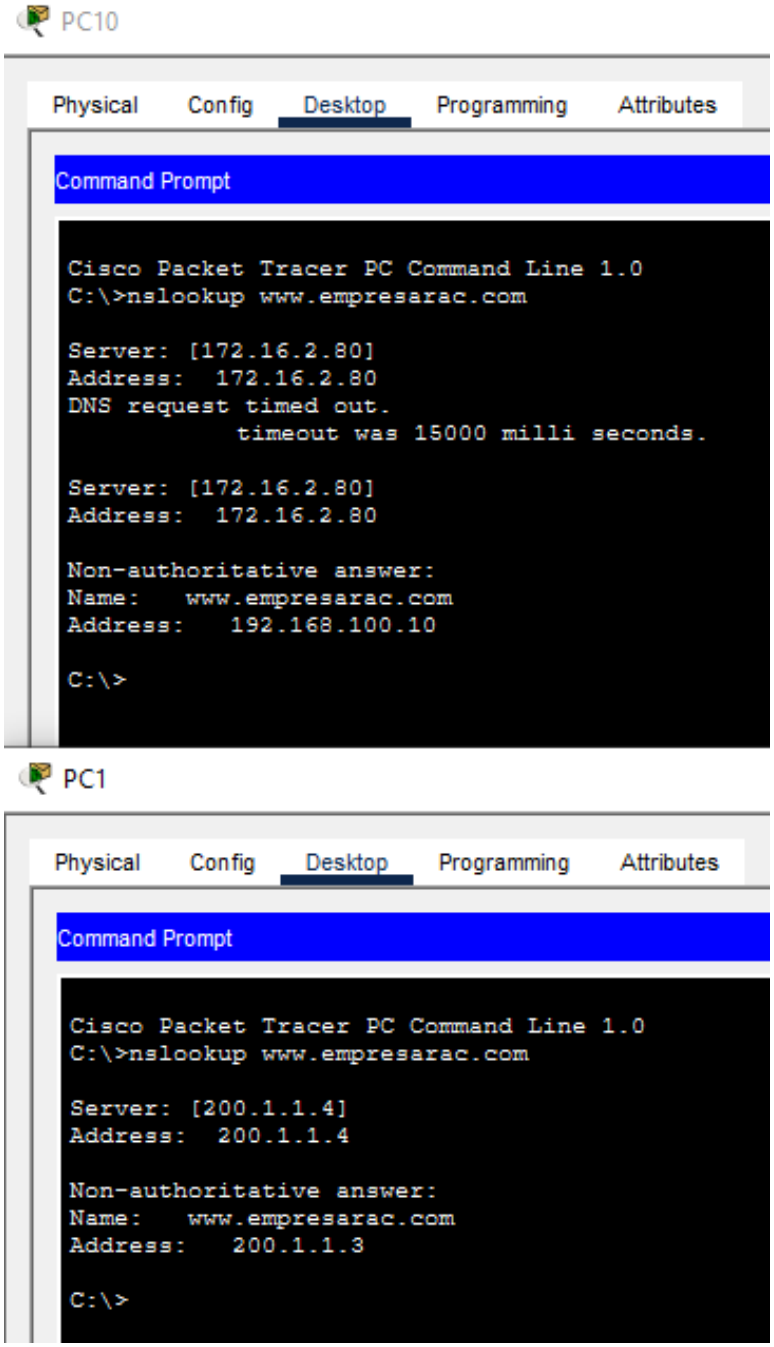


Figura 4.13: Verificación de la arquitectura Split-DNS.

La Figura 4.13 muestra claramente la diferencia en la resolución:

- En la **consola superior (Red Interna)**, el dominio resuelve a la IP

Privada (`192.168.100.10`), permitiendo el acceso directo.

- En la **consola inferior (Internet)**, el mismo dominio resuelve a la IP Pública (`200.1.1.3`), confirmando el correcto funcionamiento de las dos vistas DNS.

[5]

4.2.11. Gestión y Monitorización (Syslog y NTP)

Finalmente, se prueba la capacidad de auditoría y la sincronización temporal de la infraestructura.

Prueba realizada: Generación de eventos de red y revisión del servidor Syslog centralizado.

Syslog

Service — On — Off

	Time	HostName	Message
1	01.07.2026 05:09:53.924 PM	200.1.1.1	%SYS-5-CONFIG_I: Configured from console by console
2	01.07.2026 05:00:49.443 PM	172.16.2.93	%HSRP-6-STATECHANGE: Vlan500 Grp 500 state Speak -> Standby
3	01.07.2026 05:00:50.118 PM	172.16.2.94	%HSRP-6-STATECHANGE: Vlan600 Grp 600 state Speak -> Standby
4	01.07.2026 05:00:50.450 PM	172.16.2.93	%HSRP-6-STATECHANGE: Vlan999 Grp 999 state Speak -> Standby
5	01.07.2026 05:00:50.754 PM	172.16.2.93	%HSRP-6-STATECHANGE: Vlan900 Grp 900 state Speak -> Standby
6	01.07.2026 05:00:50.776 PM	172.16.2.94	%HSRP-6-STATECHANGE: Vlan100 Grp 100 state Speak -> Standby
7	01.07.2026 05:00:50.820 PM	172.16.2.93	%HSRP-6-STATECHANGE: Vlan950 Grp 950 state Speak -> Standby
8	01.07.2026 05:00:51.003 PM	172.16.2.93	17:00:51: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on GigabitEthernet0/1 ...
9	01.07.2026 05:00:51.922 PM	172.16.2.94	%HSRP-6-STATECHANGE: Vlan200 Grp 200 state Speak -> Standby
10	01.07.2026 05:00:52.325 PM	172.16.2.93	%HSRP-6-STATECHANGE: Vlan400 Grp 400 state Speak -> Standby
11	01.07.2026 05:00:53.008 PM	172.16.2.94	%HSRP-6-STATECHANGE: Vlan300 Grp 300 state Speak -> Standby
12	01.07.2026 05:00:56.254 PM	172.16.2.94	17:00:56: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on GigabitEthernet0/1 ...
13	01.07.2026 05:00:56.316 PM	172.16.2.94	17:00:56: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Vlan999 from ...
14	01.07.2026 05:00:56.370 PM	172.16.2.93	17:00:56: %OSPF-5-ADJCHG: Process 1, Nbr 6.6.6.6 on Vlan999 from ...
15	01.07.2026 05:01:22.650 PM	172.16.65.6	%HSRP-6-STATECHANGE: Vlan100 Grp 100 state Speak -> Standby

Figura 4.14: Recepción centralizada de logs con sincronización horaria NTP.

En la Figura 4.14 se visualizan las entradas de registro provenientes de diferentes dispositivos. Se verifica que los mensajes llegan al servidor de gestión atravesando el Firewall y, fundamentalmente, que la marca de tiempo (*Timestamp*) coincide con la hora real del sistema, demostrando la correcta sincronización NTP a través de los túneles VPN.

Capítulo 5

Conclusiones

En este capítulo se presentan las conclusiones obtenidas al llevar a cabo el presente trabajo.

5.1. Problemáticas encontradas y resolución

Exponer aquí las problemáticas encontradas y cómo se han resuelto.

Durante la realización de este proyecto hemos encontrado bastantes problemáticas, pero la mayoría están relacionadas con limitaciones y/o inestabilidades del simulador utilizado, en este caso Packet Tracer.

En esta sección resumiremos varias de las problemáticas encontradas junto a la solución considerada, si se ha encontrado.

5.1.1. WLAN

Durante la configuración de la WLAN de las distintas sedes hemos encontrado ciertos problemas que no nos permitían que los puntos de acceso emitiesen la señal de la red.

La problemática principal era la página de configuración del WLC, que era bastante inestable y no respondía en muchas ocasiones. Sin embargo, tras intentarlo en varias ocasiones conseguimos realizar la configuración correctamente, salvo porque el WLC no reconocía los LAP. Finalmente, observamos que esto se debía a un problema en el direccionamiento IP y pudimos

solucionarlo.

5.1.2. Concentrador VPN

Encontramos otro problema al configurar el concentrador VPN y probar la conexión de los teletrabajadores. El problema consistía en que Packet Tracer no soporta del todo las conexiones VPN client-to-site como tal, y al principio los equipos externos no podían acceder a la red.

Solucionamos este problema creando un pool de direcciones en el propio concentrador para asignárselo a los equipos de los teletrabajadores, y realizando una configuración en el concentrador diferente a la pensada en un primer momento, la cual si soportaba Packet Tracer. Finalmente, de esta forma, los equipos se pueden conectar a la red interna y navegar por ella sin problemas, cifrando correctamente la información que transporta el túnel.

5.1.3. Implementación LACP

Como hemos mencionado en el capítulo de Diseño Lógico, no hemos encontrado modelos de routers en Packet Tracer que soporten LACP y todas las funciones necesarias para el resto de configuraciones que hemos realizado. En este caso no hemos encontrado solución, pero hemos proporcionado la documentación para implementarlo en un entorno real con otros modelos de routers CISCO.

5.1.4. Implementación NAT64

Packet Tracer no soporta este protocolo, pese a ser un estándar en la industria. Por la poca cantidad de dispositivos que se prevee que usen IPv6 de forma nativa se ha decidido usar esta tecnología. Una vez adquiridos los equipos se realizará una fase de experimentación en la que se probará antes de su implementación definita.

5.1.5. Filtrado de tráfico de gestión en el Firewall ASA

Durante la implementación de la monitorización centralizada, nos encontramos con que el servidor Syslog y NTP, ubicado en la red interna, no recibía los registros provenientes del Router de Borde (VPN) ni del Switch de la DMZ. Esto se debía a que, por defecto, el Firewall ASA bloquea todo

el tráfico que intenta pasar de un nivel de seguridad bajo (Outside/DMZ) a uno alto (Inside).

La resolución de este conflicto consistió en la implementación de reglas de acceso (ACLs) granulares. Tuvimos que permitir explícitamente el tráfico UDP en los puertos 514 (Syslog) y 123 (NTP) en las interfaces externas, creando excepciones específicas para los dispositivos de infraestructura sin comprometer la política de seguridad general que bloquea el tráfico de usuarios externos.

5.1.6. Simulación de arquitectura Split-DNS

Uno de los requisitos de diseño era implementar un sistema de nombres que devolviese la IP privada a los empleados y la IP pública a los usuarios externos (Split-Horizon DNS). Sin embargo, el servicio de servidor DNS incluido en Packet Tracer es genérico y no soporta la configuración de "vistas.º zonas diferenciadas según el origen de la petición.

Para resolver esta limitación del simulador y mantener la lógica del diseño, optamos por desplegar dos servidores DNS físicos diferenciados: uno en el CPD (para la red interna) y otro en la DMZ (para las peticiones externas). De esta forma, simulamos fielmente el comportamiento de resolución diferenciada que en un entorno real se podría virtualizar en una única máquina física.

5.1.7. Disponibilidad de interfaces de Fibra Óptica

En el diseño físico de la Sede Central, se planificó el uso de enlaces de fibra óptica para todas las conexiones WAN (hacia sedes remotas y hacia el ISP) para garantizar el ancho de banda y la distancia. No obstante, el modelo de router disponible en el simulador (Cisco 2911) cuenta con una limitación en el número de slots para módulos SFP de fibra.

Para poder cerrar la topología funcional en Packet Tracer, se optó por simular el enlace hacia el ISP utilizando cableado de cobre (Gigabit Ethernet), reservando los puertos de fibra disponibles para la interconexión crítica entre sedes. Esta modificación es exclusiva de la simulación, ya que en el presupuesto y diseño real se han seleccionado equipos (Serie Catalyst 8300) que sí disponen de la densidad de puertos de fibra necesaria.

Apéndice A

Apéndices adicionales

Insertar un Apéndice por cada uno de los apartados siguientes.

- Mapas de topología detallados
- Configuración de dispositivos
- Detalles en el direccionamiento y nombres
- Información de contacto
- Información sobre la compañía que presenta el diseño

A.1. A.1. Mapas de topología detallados

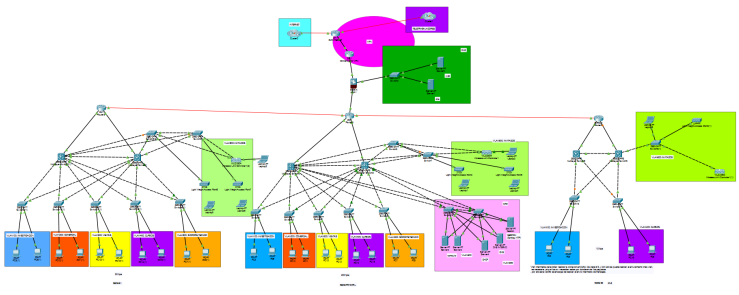


Figura A.1: Mapa de Topología completa

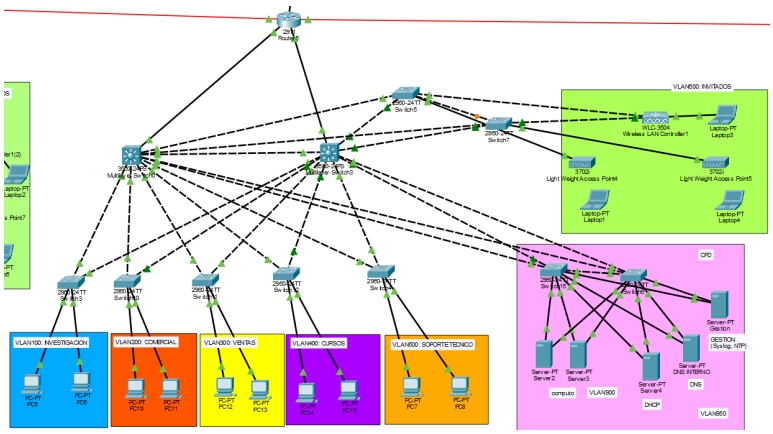


Figura A.2: Mapa de la Sede Central

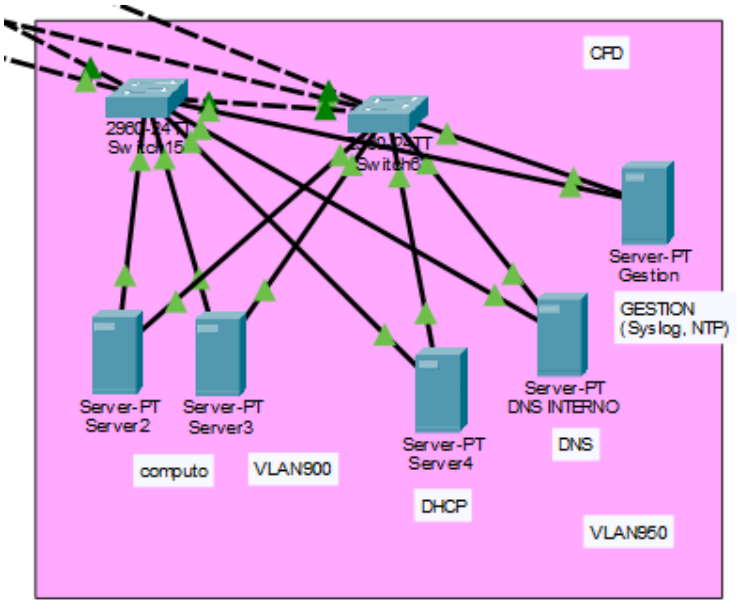


Figura A.3: Mapa del CPD de la Sede Central

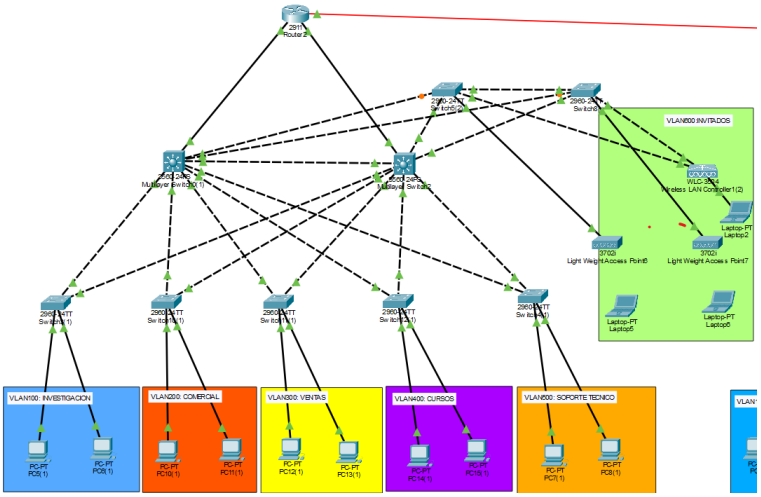


Figura A.4: Mapa de la Sede B1

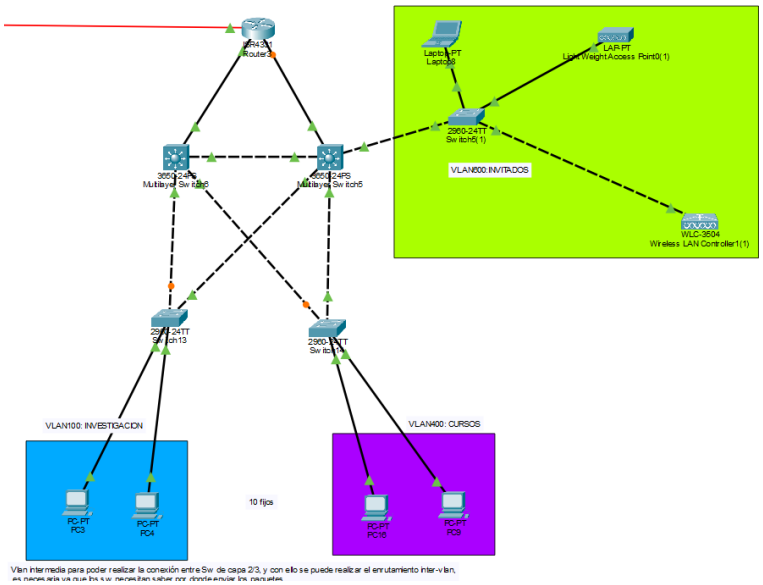


Figura A.5: Mapa de la Sede B2

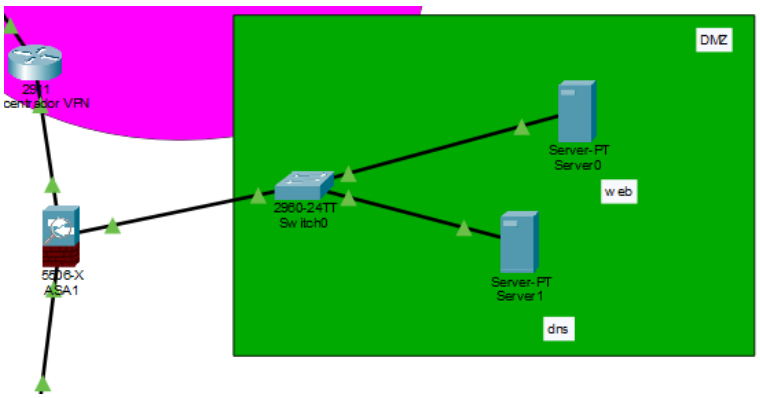
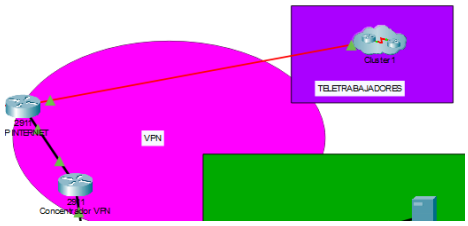
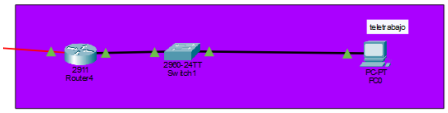


Figura A.6: Mapa DMZ

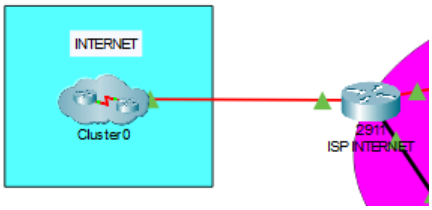


(a) Mapa de Concentrador VPN

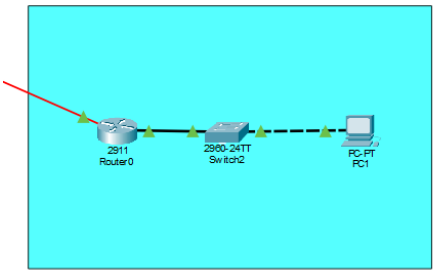


(b) Mapa de oficina de los teletrabajadores

Figura A.7: Mapa de conexión remota



(a) Mapa de ISP



(b) Mapa der simulaciíon de ISP

Figura A.8: Mapa de conexión con ISP

A.2. A.2. Configuración de dispositivos

A.2.1. Configuración de HSRP

Para la configuración de HSRP en nuestros switches multicapa, con objetivo de proporcionar disponibilidad y balanceo de carga, tendremos que crear una SVI para cada VLAN que queremos enrutar, y es esta interfaz la que tenemos que configurar.

Lo único que necesitamos hacer es asignar una HSRP Virtual Interface a cada SVI, y esta IP será el Gateway de los equipos que pertenezcan a esta VLAN. Tras esto, solo debemos asignar una prioridad, para decidir que switch es el activo por defecto. Para realizar el balanceo de carga, asignamos una prioridad mayor para algunas interfaces en un switch y menor para otras.

Proporcionamos un ejemplo de como lo hemos configurado para las interfaces dedicadas a la VLAN100:

```
1 Switch2(config)# interface Vlan100
2 Switch2(config-if)# ip address 172.16.0.61 255.255.255.192
3 Switch2(config-if)# standby 100 ip 172.16.0.1    // HSRP Virtual IP
4 Switch2(config-if)# standby 100 priority 105 // Mayor prioridad (ACTIVE)
5 Switch2(config-if)# standby 100 preempt // Toma rol activo si mayor prioridad
6 Switch2(config-if)# no shutdown
7 Switch2(config-if)# exit
```

En el otro switch simplemente asignamos una SVI y HSRP Virtual IP distintas y una menor prioridad (95).

La configuración en la sede B2 se realizará de forma similar usando en este caso HSRPv2.Esto habrá que indicarlo con el comando *standby version 2*. Posteriormente se sustituyen las ips por las correspondientes IPv6 además de cambiar ip por ipv6.

A.2.2. Configuración de redes WI-FI

Para la configuración de las redes Wi-Fi, asignamos direcciones IP de gestión a los WLC y nos conectamos con un dispositivo a su dirección IP, para realizar la configuración en la interfaz web que nos ofrece CISCO. Explicamos como hemos configurado la red de invitados.

Para la configuración de la WLAN hemos tomado de referencia la fuente [6]

Por un lado creamos la interfaz de red, correspondiente a la VLAN de invitados:

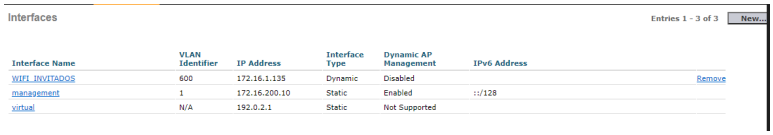


Figura A.9: Interfaces del WLC

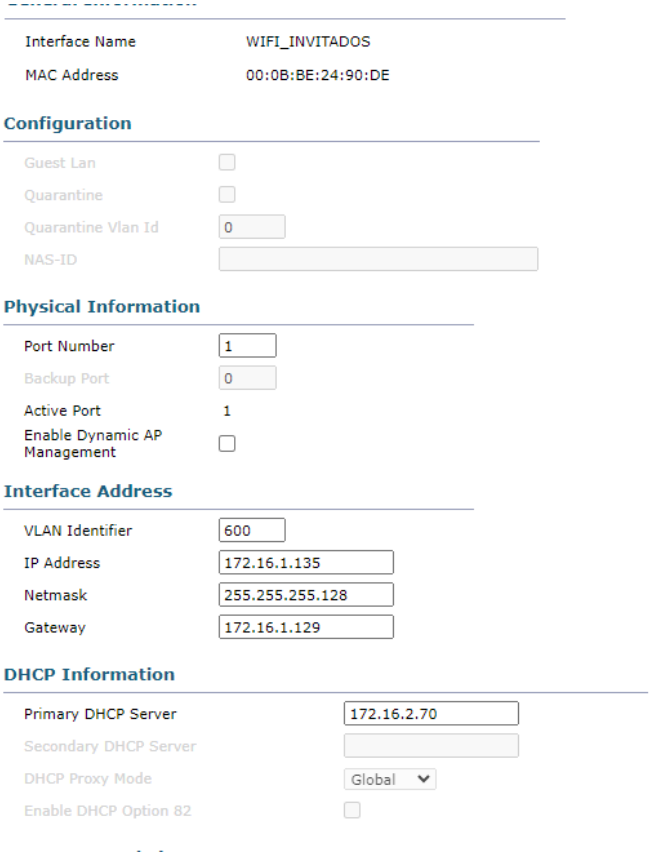
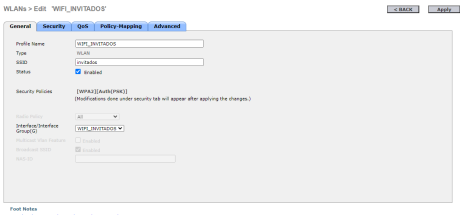
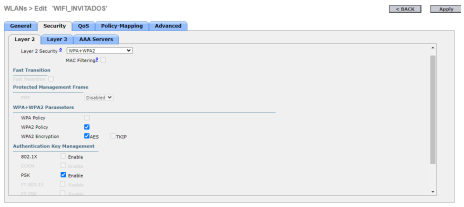


Figura A.10: Configuración de la interfaz Wi-Fi

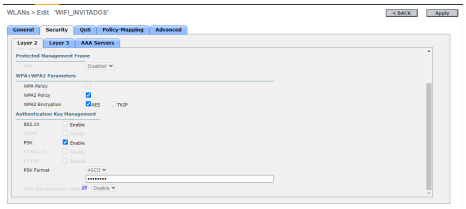
Por otro lado configuramos la WLAN, asignandola a la interfaz que acabamos de crear:



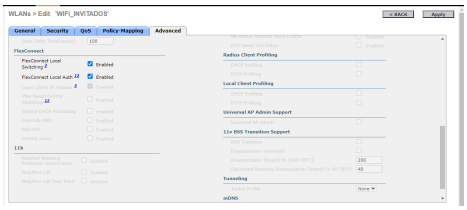
(a) Configuración WLAN I



(b) Configuración WLAN II



(c) Configuración WLAN III



(d) Configuración WLAN IV

Figura A.11: Conjunto de cuatro imágenes en una cuadrícula.

Figura A.12: WLANs activas

Una vez hecha esta configuración, podemos comprobar los puntos de acceso conectados al WLC, que ya son capaces de emitir la señal:

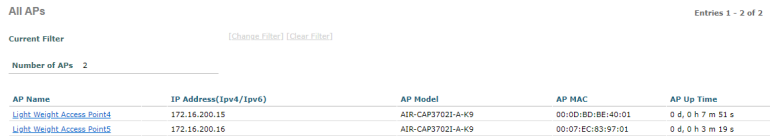


Figura A.13: APs disponibles

A.2.3. Configuración de túnel VPN entre sedes

Para crear el túnel VPN que mantiene nuestros datos protegidos de la red pública sobre la que transitan, hemos seguido 3 pasos, los cuales hay que seguir en los dos routers extremos del túnel:

En primer lugar, definir el acuerdo, es decir, configurar la autenticación de los routers y como se va a establecer el canal:

```
Router-Central(config)#crypto isakmp policy 10
Router-Central(config-isakmp)# encryption aes
Router-Central(config-isakmp)# hash sha
Router-Central(config-isakmp)# authentication pre-share
Router-Central(config-isakmp)# group 2
Router-Central(config-isakmp)# exit
Router-Central(config)#crypto isakmp key cisco123 address 192.168.200.2
```

En segundo lugar, configurar IPSEC para el cifrado y protección de los datos:

```
Router-Central(config)#crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
Router-Central(config)#access-list 110 permit gre host 192.168.200.1
#host 192.168.200.2
Router-Central(config)#crypto map MYMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router-Central(config-crypto-map)#set peer 192.168.200.2
Router-Central(config-crypto-map)#set transform-set MYSET
Router-Central(config-crypto-map)#match address 110
Router-Central(config-crypto-map)#exit
Router-Central(config)#interface GigabitEthernet0/3/0
Router-Central(config-if)#crypto map MYMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Y por último, crear el túnel GRE mediante una interfaz virtual:

```
Router-Central(config)#interface Tunnel0
Router-Central(config-if)# ip address 10.10.10.1 255.255.255.252
Router-Central(config-if)# tunnel source GigabitEthernet0/3/0
Router-Central(config-if)# tunnel destination 192.168.200.2
```

Esta configuración es únicamente la realizada en el router de la sede central para formar el túnel con destino a la sede B1, pero el resto sería equivalente cambiando IPs e interfaces.

A.2.4. Configuración de ACLs

En este apéndice mostramos las listas de acceso configuradas en el router central, tanto para evitar que los invitados puedan acceder a la red interna, como para restringir el acceso a ciertos usuarios de la sede a los servidores de cómputo ubicados en el CPD.

La lista de acceso para que los usuarios de la red de invitados solo puedan acceder a Internet es la siguiente, la cual aplicamos de entrada en la SVI de la VLAN600 (invitados):

```
Extended IP access list invitados->sedeCentral
    permit ip any host 172.16.2.70
    permit ip 172.16.1.128 0.0.0.127 172.16.1.128 0.0.0.127
    permit ip any host 8.8.8.8
    deny ip any 172.16.0.0 0.0.255.255
    permit ip any any

Switch(config)#interface vlan 600
Switch(config-if)#ip access-group invitados->sedeCentral in
```

La lista de acceso para restringir el acceso solo a los departamentos de Investigación y Soporte Técnico a los servidores de cómputo del CPD es la siguiente, la cual aplicamos de salida en la SVI de la VLAN900 (servidores cómputo):

```
Extended IP access list servidoresComputo
    10 permit ip 172.16.0.0 0.0.0.63 172.16.2.0 0.0.0.255
    20 permit ip 172.16.1.0 0.0.0.63 172.16.2.0 0.0.0.255
    30 permit ip 172.16.64.0 0.0.0.31 172.16.2.0 0.0.0.255
    40 permit ip 172.16.64.128 0.0.0.31 172.16.2.0 0.0.0.255

Switch(config)#interface vlan 900
Switch(config-if)#ip access-group servidoresComputo out
```

A.2.5. Configuración de Concentrador VPN

La configuración para el túnel VPN client-to-site se basa en tres pilares fundamentales que garantizan la integridad y confidencialidad de los datos:

Gestión de Identidad (AAA), Asignación Dinámica de Direccionamiento (IP Pool) y Criptografía Dinámica (IPsec Dynamic Maps).

De esta forma garantizamos la seguridad de nuestros empleados y sus datos, asignandole a su vez una dirección IP de la empresa para que puedan trabajar como si estuviesen físicamente en la sede.

La configuración realizada es la siguiente, la cual hemos aprendido de la referencia [7]:

```
Router(config)#ip local pool vpnpool 172.16.128.1 172.16.128.254
Router(config)#aaa new
Router(config)#aaa new-model
Router(config)#aaa authentication login vpnusersgroup local
Router(config)#aaa authorization network vpngroup local
Router(config)#username empleado secret password
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#hash sha
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#exit
Router(config)#crypto isakmp client configuration group vpnusersgroup
Router(config-isakmp-group)#key cisco
Router(config-isakmp-group)#pool vpnpool
Router(config-isakmp-group)#exit
Router(config)#crypto ipsec transform-set vpnset esp-aes  esp-sha-hmac
Router(config)#crypto dynamic-map dynamicmap 10
Router(config-crypto-map)#set transform-set vpnset
Router(config-crypto-map)#reverse-route
Router(config-crypto-map)#exit
Router(config)#crypto map vstatic client configuration address respond
Router(config)#crypto map vstatic client authentication list vpnusersgroup
Router(config)#crypto map vstatic isakmp authorization list vpngroup
Router(config)#crypto map vstatic 30 ipsec-isakmp dynamic dynamicmap
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#crypto map vstatic
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#
```

De los comandos cabe destacar que usamos credenciales para la autenticación y sha para el cifrado, además de hacer un mapeo dinámico de las direcciones IP.

A.2.6. Configuración de LACP

La configuración de LACP es muy sencilla, simplemente habría que agrupar las 3 interfaces físicas en cada uno de los routers bajo el identificador de grupo 1, estableciendo el modo como .ªctive"para que el router inicie o acepte la negociación. Tras esto, solo habría que asignar nuestra IP pública a la nueva interfaz virtual:

```
Router_B1(config)# interface range GigabitEthernet0/1/0,
#GigabitEthernet0/2/0, GigabitEthernet0/3/0
Router_B1(config-if-range)# no ip address
Router_B1(config-if-range)# channel-group 1 mode active
Router_B1(config-if-range)# no shutdown
Router_B1(config-if-range)# exit

Router_B1(config)# interface port-channel 1
Router_B1(config-if)# ip address 192.168.200.2 255.255.255.252
Router_B1(config-if)# no shutdown
```

A.2.7. Configuración NAT64

Para la configuración de NAT64 en nuestro router de borde (o switch multicapa con capacidad de enrutamiento), con el objetivo de permitir la comunicación entre nuestros equipos IPv6 y servidores en Internet que son IPv4, tendremos que definir las interfaces que participan en la traducción y establecer las reglas de mapeo.

Necesitamos habilitar nat64 en las interfaces involucradas (tanto la que mira hacia la red IPv6 como la que mira hacia la red IPv4). Tras esto, solo debemos definir un prefijo de estado (generalmente el estándar `64:ff9b::/96`), crear una lista de acceso para identificar el tráfico IPv6 permitido, y finalmente vincular esa lista con una dirección o pool IPv4 para realizar la sobrecarga (Overload/PAT).

Como ya se ha mencionado anteriormente esta configuración no es posible llevarla a cabo por la incompatibilidad de packet tracer con nat64, por lo que será necesario montar un escenario de pruebas antes de proceder a la implementación real con el fin de evitar fallos.

Proporcionamos un ejemplo de como se debería de configurar la red interna IPv6 con la salida a Internet IPv4:

```
Router(config)# ipv6 unicast-routing
Router(config)# nat64 prefix stateful 64:ff9b::/96
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ipv6 address 2001:db8:acad::1/64
Router(config-if)# nat64 enable
Router(config-if)# exit
Router(config)# interface Serial0/1/0
Router(config-if)# ip address 203.0.113.1 255.255.255.252
Router(config-if)# nat64 enable
Router(config-if)# exit
Router(config)# ipv6 access-list PERMITIDOS_IPV6
Router(config-ipv6-acl)# permit ipv6 2001:db8:acad::/64 any
Router(config-ipv6-acl)# exit
Router(config)# nat64 translation list PERMITIDOS_IPV6 interface Serial0/1/0 overload
```

Bibliografía

[1] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear, "Address Allocation for Private Internets," Febrero 1996, [Online; Accedido 08-Enero-2026] Estándar para el direccionamiento IPv4 privado utilizado en la Intranet. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc1918

[2] J. Moy, "OSPF Version 2," Abril 1998, [Online; Accedido 08-Enero-2026] Especificación del protocolo de enrutamiento dinámico de estado de enlace. [Online]. Available: https://www.ietf.org/rfc/rfc2328.txt

[3] Cisco Systems Inc., *Cisco ASA 5500-X Series Firewalls Configuration Guide*, Cisco Systems, 2021, [Online; Accedido 08-Enero-2026] Documentación técnica oficial para la gestión de zonas de seguridad y DMZ. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/security/asa/asa916/configuration/general/asa-916-general-config/intro-fw.html

[4] G. Singh and G. Kaur, "High Availability in Enterprise Networks using HSRP and GLBP," *International Journal of Computer Applications*, vol. 117, no. 18, pp. 15–19, Mayo 2015, análisis sobre la redundancia de gateway en redes de campus.

[5] ITFreeTraining. (2013) Dns split brain. YouTube. Fundamentos para la implementación de resolución de nombres diferenciada interna/externa. [Online]. Available: https://www.youtube.com/watch?v=55YONDU22qc

[6] kyateyatiende. (2025) Configurar WLC en Packet Tracer: wifi profesional con WLC 3504 y AP 3702i con VLANs y AP groups. YouTube. Video tutorial sobre gestión centralizada de redes inalámbricas. [Online]. Available: https://www.youtube.com/watch?v=z3O8Vh0u68A

[7] INNOVATEK. (2021) Como configurar VPN IPsec de acceso remoto en packet tracer. YouTube. Tutorial detallado sobre la implementación de túneles VPN IPsec con autenticación local. [Online]. Available: https://www.youtube.com/watch?v=5FJV2LRrci0