Universitat
de les Illes Balears

TRABAJO DE FIN DE GRADO

# DISEÑO Y SIMULACIÓN DE UNA RED HOSPITALARIA CON GESTIÓN DE DISPOSITIVOS IOMT


**Víctor Canelo Galera**

Grau d'Enginyeria Informàtica

Escola Politècnica Superior



Año académico 2024-25

# DISEÑO Y SIMULACIÓN DE UNA RED HOSPITALARIA CON GESTIÓN DE DISPOSITIVOS IOMT


## Víctor Canelo Galera


### Trabajo de Fin de Grado


### Escola Politècnica Superior

### Universitat de les Illes Balears


**Año académico 2024-25**


Palabras clave del trabajo: Redes, IoMT, Seguridad



*Tutores: Sebastià Galmés, Juan Lladó*


| Autoritz la Universitat a incloure aquest treball en el repositori institucional per consultar-lo en accés obert i difondre'l en línia, amb finalitats exclusivament acadèmiques i d'investigació | Autor/a Sí | Autor/a No | Tutor/a Sí | Tutor/a No |
|---|---|---|---|---|
| | ☑ | ☐ | ☑ | ☐ |

Gracias a todos los que me han ayudado a llegar hasta aquí.

# ÍNDICE GENERAL

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# ACRÓNIMOS

**ACL** Access Control List

**IoMT** Internet of Medical Things

**VLAN** Virtual Local Area Network

**LAN** Local Area Network

**IP** Internet Protocol

**DHCP** Dynamic Host Configuration Protocol

**DNS** Domain Name System

**NAT** Network Address Translation

**HSRP** Hot Standby Router Protocol

**TCP** Transmission Control Protocol

**UDP** User Datagram Protocol

**HTTP** Hypertext Transfer Protocol

**HTTPS** Hypertext Transfer Protocol Secure

**FTP** File Transfer Protocol

**SSH** Secure Shell

**SNMP** Simple Network Management Protocol

**ICMP** Internet Control Message Protocol

**OSI** Open Systems Interconnection

**MAC** Media Access Control

**IEEE** Institute of Electrical and Electronics Engineers

**DoS** Denial of Service

**DDoS** Distributed Denial of Service

**LPWAN** Low Power Wide Area Network

**LOPDGDD** Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales

**RGPD** Reglamento General de Protección de Datos

**VPN** Virtual Private Network

**OSPF** Open Shortest Path First

**UCI** Unidad de Cuidados Intensivos

**IoT** Internet of Things

**DMZ** Demilitarized Zone

**IT** Information Technology

# RESUMEN

En la actualidad, el correcto diseño y la adecuada seguridad de las redes hospitalarias son aspectos críticos para garantizar la continuidad asistencial, la privacidad de los datos clínicos y la disponibilidad de los sistemas médicos. Dado que los hospitales manejan información sensible y dispositivos vitales que requieren una conectividad estable y protegida, resulta imprescindible implementar infraestructuras de red seguras, segmentadas y adaptadas a las particularidades de este entorno. Además, la creciente incorporación de dispositivos médicos (IoMT) aumenta la superficie de exposición y demanda estrategias mas restrictivas para su protección.

En este proyecto se presenta el diseño y simulación de dos redes hospitalarias utilizando Cisco Packet Tracer, una propone una red detallada para el Hospital Son Espases y la otra propone una red de interconexión entre los cuatro hospitales mas grandes de Mallorca (Son Espases, Hospital de Manacor, Hospital Comarcal de Inca y Son Llàtzer), incorporando diversas medidas de seguridad tanto a nivel físico como lógico. La solución propuesta segmenta la red mediante VLANs para aislar los distintos departamentos del hospital y establece políticas de seguridad mediante listas de control de acceso (ACLs), además de incluir redundancia tanto a nivel de hardware como a nivel de enlace y protocolos y servicios de red esenciales como DHCP o NAT. Como elemento diferencial, se ha implementado una subred específica para dispositivos IoMT, configurada con restricciones y medidas de seguridad avanzadas que limitan su interacción con el resto de la infraestructura, minimizando así los riesgos asociados a su conectividad.

CAPÍTULO 1

# INTRODUCCIÓN

## 1.1. Contexto y Motivación

### 1.1.1. Contexto

La digitalización de los servicios sanitarios ha supuesto una transformación profunda en la forma en que los hospitales gestionan su información clínica, administrativa y operativa. Actualmente, la mayoría de los procesos hospitalarios dependen de sistemas informáticos interconectados, que requieren de infraestructuras de red robustas, estables y seguras. Desde el acceso a historiales médicos electrónicos hasta los sistemas de monitorización de pacientes o la gestión de dispositivos médicos, todos estos servicios se apoyan sobre una red de comunicaciones fiable que garantice la disponibilidad continua y la integridad de los datos transmitidos.

En paralelo a este proceso de digitalización, se ha producido un aumento exponencial en la conectividad de dispositivos médicos mediante tecnologías IoT, fenómeno conocido como Internet of Medical Things (IoMT). Este tipo de dispositivos permite monitorizar parámetros clínicos en tiempo real, mejorar la trazabilidad de pacientes y optimizar la gestión hospitalaria, pero también introduce nuevos riesgos de seguridad, debido a su alta exposición en la red y sus limitaciones en materia de protección de datos.

En este contexto, el correcto diseño de una red hospitalaria no solo debe garantizar la conectividad y el buen funcionamiento de los servicios clínicos y administrativos, sino también ofrecer mecanismos de seguridad física y lógica que protejan la infraestructura frente a amenazas externas e internas. La segmentación de red, la creación de VLANs específicas y la protección de subredes destinadas a dispositivos IoMT se han convertido en elementos estratégicos para asegurar la continuidad asistencial y la privacidad de los datos clínicos en entornos hospitalarios modernos.

### 1.1.2. Motivación

La motivación principal para la realización de este proyecto surge de la relevancia crítica que tienen las infraestructuras de red en centros hospitalarios y del interés personal por el diseño de redes seguras en entornos sensibles y de alta disponibilidad. El auge de los dispositivos IoMT, con sus particulares desafíos de seguridad y gestión, supone un área de gran proyección profesional y tecnológica, lo que convierte este proyecto en una oportunidad para profundizar en soluciones actuales de segmentación, control de accesos y políticas de seguridad adaptadas a estas nuevas tecnologías.

Además, el planteamiento del proyecto permite aplicar conocimientos teóricos adquiridos durante el grado en un entorno simulado profesional, utilizando herramientas como Cisco Packet Tracer y gestionando la documentación técnica y las configuraciones de red de forma controlada.

Este proyecto no solo supone un reto técnico, sino también una aportación académica de valor para futuros estudiantes o profesionales interesados en infraestructuras de red hospitalarias, ya que documenta una propuesta de red segmentada, segura y adaptada a las necesidades actuales de conectividad y protección de dispositivos IoMT.

## 1.2. Objetivos del Proyecto

El presente proyecto tiene como finalidad diseñar, implementar y simular una red hospitalaria segura y segmentada mediante la herramienta Cisco Packet Tracer, aplicando buenas prácticas de seguridad a nivel físico y lógico, y adaptándola a las necesidades actuales de conectividad y protección de dispositivos médicos conectados (IoMT). Para ello, se han definido un objetivo general y varios objetivos específicos que guían el desarrollo del trabajo:

### 1.2.1. Objetivo General

Diseñar y simular una infraestructura de red hospitalaria segura y segmentada, implementando medidas de seguridad física y lógica, incluyendo una subred específica para dispositivos Internet of Medical Things (IoMT), utilizando Cisco Packet Tracer como entorno de simulación.
Además de diseñar y simular una infraestructura de red hospitalaria entre cuatro hospitales, centrando el trabajo en la interconexión entre los dispositivos finales de cada hospital y los servidores de otros hospitales, garantizando la seguridad de la información transmitida por los enlaces de interconexión.

### 1.2.2. Objetivos Específicos

- **Analizar los requisitos funcionales y de seguridad** de una red hospitalaria moderna, como la de Son Espases, considerando la incorporación de dispositivos IoMT y las particularidades de entornos asistenciales.

- **Definir una topología de red física y lógica adecuada**, organizando los diferentes departamentos y servicios hospitalarios mediante técnicas de segmentación, como la creación de VLANs y subredes.
- **Diseñar una red de interconexión entre cuatro hospitales**, garantizando la comunicación segura y eficiente entre ellos.
- **Planificar y configurar el direccionamiento IP** de la red hospitalaria, garantizando su correcto funcionamiento y escalabilidad.
- **Implementar medidas de seguridad a nivel lógico**, mediante el uso de ACLs, segmentación de tráfico, configuración de resiliencia contra atques reales (DHCP Spoofing) y asegurar una comunicación interhospitalaria segura.
- **Diseñar e integrar una subred específica para dispositivos IoMT**, aplicando controles de seguridad reforzados y limitando su acceso a los recursos esenciales de la red.
- **Realizar pruebas de conectividad, seguridad y funcionamiento**, validando la correcta comunicación entre los diferentes dispositivos, el cumplimiento de las políticas de seguridad y la eficiencia de la segmentación implementada.
- **Documentar todas las fases del proyecto**, incluyendo análisis de requisitos, diseño de la topología, configuración de dispositivos, resultados de las pruebas y conclusiones finales.

## 1.3. Alcance del Proyecto

El presente proyecto tiene como objetivo el diseño, configuración y simulación de una infraestructura de red hospitalaria segura y segmentada, adaptada a los requisitos actuales de conectividad, segmentación y protección de dispositivos médicos conectados (IoMT). Para ello, se han establecido unos límites funcionales y técnicos claramente definidos que determinan el alcance real de este trabajo.

### 1.3.1. Alcance Funcional

El proyecto contempla:

- **El diseño de dos infraestructuras de red diferenciadas:**
  - Una red de interconexión entre cuatro hospitales (Son Espases, Son Llatzer, Hospital Comarcal d'Inca y Hospital de Manacor).
  - El diseño detallado de la red de un hospital individual (Son Espases).
- **Segmentación de cada hospital en tres subredes independientes:**
  - Red de invitados (192.168.0.0/16).
  - Red de dispositivos IoMT (172.16.0.0/12).
  - Red interna hospitalaria (10.0.0.0/8).

- **División de cada hospital en VLANs por departamentos**, separando administración, servicios quirúrigicos, servicios médicos, servicios centrales, áreas de enfermería y áreas de apoyo.
- **Implementación de políticas de seguridad mediante ACLs**, para:
  - Bloquear el tráfico entre la red de invitados y cualquier otra subred.
  - Restringir la comunicación de dispositivos IoMT exclusivamente a dispositivos del área médica o del departamento de la UCI.
  - Limitar el acceso entre VLANs en función de criterios de seguridad departamentales.
- **Configuración de DMZ específicas para cada subred**, con su propio servidor DHCP. En el caso de la subred IoMT, se añaden dos servidores DHCP, uno principal y otro de respaldo.
- **Implementación de servicios de red:**
  - **DHCP** para la asignación dinámica de direcciones IP a los dispositivos de cada subred.
  - **DNS** para la resolución de nombres de dominio internos.
  - **NAT** para permitir el acceso a Internet desde las subredes internas.
  - **HSRP** para garantizar la alta disponibilidad de los routers principales.
  - **SSH** para la gestión segura de los dispositivos de red.
  - **OSPF** para el enrutamiento dinámico entre las diferentes VLANs y subredes.
  - **EtherChannel** para la agregación de enlaces entre switches, mejorando la capacidad y redundancia de la red.
  - **IPSec** para la interconexión segura entre hospitales, garantizando la privacidad de los datos transmitidos.
- **Pruebas de conectividad, seguridad y tolerancia a fallos**, incluyendo:
  - Verificación de la comunicación entre dispositivos de diferentes VLANs.
  - Validación de las políticas de seguridad implementadas mediante ACLs.
  - Comprobación del funcionamiento de los servicios de red configurados.
  - Pruebas de tolerancia a fallos mediante la simulación de caídas de enlaces y dispositivos.

### 1.3.2. Límites y Exclusiones

Para delimitar correctamente el trabajo realizado, se establecen las siguientes exclusiones y limitaciones:

- No se realiza una simulación de ciberataques avanzados, sino únicamente pruebas básicas de seguridad mediante restricciones de ACLs y control de tráfico.

- El hardware de red empleado en la simulación se limita a los dispositivos disponibles en Cisco Packet Tracer, que pueden no corresponder con equipamiento hospitalario de última generación.

- Se asume disponibilidad presupuestaria ilimitada para la adquisición de hardware y software, priorizando el cumplimiento de los objetivos técnicos y de seguridad sobre las restricciones económicas o logísticas.

Además también existen las limitaciones propias de la herramienta Cisco Packet Tracer, a continuación se muestran las más relevantes:

- Limitaciones de puertos en routers, esto imposibilita que la interconexión entre hospitales tenga enlaces redundantes.

- Limitaciones de puertos en routers, esto imposibilita que se configure HSRP en todos los switches de distribución que conectan con switches de acceso.

## 1.4. Estructura del Documento

El presente proyecto se organiza en varios capítulos que recogen de forma ordenada y estructurada las diferentes fases y contenidos desarrollados durante el proyecto. A continuación, se describe brevemente la estructura del documento:

- **Capítulo 1: Introducción.** Se contextualiza la importancia de las redes hospitalarias, se define el objetivo general y los objetivos específicos del proyecto, se delimitan su alcance y limitaciones y se explica la estructura del documento.

- **Capítulo 2: Marco Teórico.** Se recogen los conceptos fundamentales necesarios para entender el proyecto, incluyendo una descripción de las redes LAN y VLAN, las particularidades de las redes hospitalarias, los requisitos de seguridad específicos en este tipo de entornos y una introducción a la tecnología IoMT.

- **Capítulo 3: Análisis de Requisitos.** Se detallan las necesidades funcionales, de seguridad, de conectividad y de gestión que debe cubrir la red hospitalaria simulada, incluyendo los requisitos particulares para los dispositivos IoMT.

- **Capítulo 4: Metodología de Trabajo.** Se expone el enfoque metodológico adoptado, basado en un desarrollo secuencial por fases siguiendo un modelo en cascada, se describe la planificación del proyecto, las herramientas utilizadas y el cronograma de trabajo.

- **Capítulo 5: Diseño de la Red.** Se presenta la topología física y lógica de la red hospitalaria, el direccionamiento IP, la segmentación mediante VLANs, las políticas de seguridad y la estructura de la subred específica para IoMT.

- **Capítulo 6: Implementación.** Se detalla la configuración de los dispositivos de red en Cisco Packet Tracer, la creación de VLANs, la aplicación de ACLs, la configuración de servicios de red y la integración de los dispositivos IoMT.

- **Capítulo 7: Pruebas y Validación.** Se describen las pruebas de conectividad, seguridad y funcionamiento realizadas sobre la red simulada, se presentan los resultados obtenidos y se analizan las incidencias detectadas y las soluciones aplicadas.
- **Capítulo 8: Conclusión.** Se resumen los logros alcanzados, las dificultades encontradas y se proponen posibles mejoras y ampliaciones del proyecto para su aplicación en un entorno real.
- **Anexos.** Se incluyen las configuraciones completas de los dispositivos de red, diagramas adicionales y documentación complementaria.
- **Bibliografía.** Se recogen todas las fuentes de información utilizadas para la realización del proyecto, siguiendo el formato de citación IEEE.

CAPÍTULO 2

# MARCO TEÓRICO

Para comprender en profundidad el desarrollo de este proyecto y justificar las decisiones adoptadas durante su diseño e implementación, resulta imprescindible establecer una base teórica que aborde los conceptos y tecnologías implicadas. Este marco teórico tiene como finalidad proporcionar una visión general sobre las infraestructuras de red en entornos hospitalarios, protocolos de comunicación, seguridad y tecnologías específicas para entornos sanitarios.

Este capítulo establece las bases conceptuales necesarias para comprender el diseño e implementación de una infraestructura de red hospitalaria que garantice conectividad , redundancia y seguridad.

## 2.1. Arquitectura de Redes Hospitalarias

### 2.1.1. Modelo Jerárquico de Red

Las redes hospitalarias adoptan un modelo jerárquico de tres capas que optimiza el rendimiento, escalabilidad y mantenimiento. Esta arquitectura se compone de:

- **Capa de Núcleo (Core):** Proporciona conectividad de alta velocidad entre diferentes áreas internas del hospital y acceso a servicios externos. Se encarga de interconectar los switches de distribución con los routers principales y gestionar el tráfico entre las distintas subredes.

- **Capa de Distribución:** Actúa como intermediaria entre la capa de acceso y la capa de núcleo, gestionando el tráfico local y balanceando la carga entre los distintos switches core. También implementa políticas de seguridad, segmentación de tráfico y control de acceso, permitiendo la comunicación entre las distintas VLANs y subredes del hospital.

- **Capa de Acceso:** Conecta los dispositivos finales, como estaciones de trabajo, impresoras y dispositivos médicos. Esta capa se encarga de proporcionar conectividad a los usuarios y dispositivos, permitiendo el acceso a los recursos de red y servicios compartidos.

### 2.1.2. Segmentación de la Red

La segmentación mediante VLANs (Virtual Local Area Networks) es fundamental en entornos hospitalarios para separar diferentes tipos de tráfico y mejorar la seguridad. Una VLAN permite agrupar lógicamente dispositivos dentro de una misma red física, segmentando el tráfico de datos aunque se encuentren conectados al mismo switch o infraestructura física. Los beneficios principales incluyen:

- **Aislamiento de tráfico:** Cada VLAN mantiene su propio dominio de broadcast, reduciendo la propagación de tráfico innecesario.
- **Seguridad:** Permite aplicar políticas de seguridad específicas a cada VLAN, restringiendo el acceso a recursos críticos y protegiendo datos sensibles.
- **Optimización del rendimiento:** Minimiza los cuellos de botella y mejora la eficiencia de la comunicación.

## 2.2. Protocolos de Enrutamiento Dinámico

### 2.2.1. OSPF (Open Shortest Path First)

OSPF es un protocolo de enrutamiento de estado de enlace (link-state) que utiliza el algoritmo de Dijkstra para calcular las rutas más cortas. Sus características principales son:

**Funcionamiento Básico:**

- Cada router mantiene una Base de Datos de Estado de Enlace (LSDB) con información topológica completa de la red.
- Utiliza LSAs (Link State Advertisements) para intercambiar información entre routers.
- Calcula rutas óptimas mediante el algoritmo SPF (Shortest Path First) de Dijkstra.

**Ventajas en Entornos Hospitalarios:**

- Convergencia rápida ante cambios en la topología de la red, lo que es crítico en entornos donde la disponibilidad es esencial.
- Soporta redes de gran tamaño y complejidad, permitiendo una escalabilidad adecuada para hospitales con múltiples departamentos y servicios.
- Uso eficiente del ancho de banda al enviar actualizaciones solo cuando hay cambios en la red, reduciendo el tráfico innecesario.

### 2.2.2. Algoritmo de Dijkstra

El algoritmo de Dijkstra es fundamental para el funcionamiento de OSPF, ya que permite calcular la ruta más corta entre nodos en una red. Su funcionamiento se basa en:

1. **Descubrimiento de topología local:** Cada router identifica sus enlaces directos y sus costos asociados.
2. **Inundación con LSAs:** Los routers envían información sobre sus enlaces a todos los demás routers de la red, actualizando la LSDB.
3. **Construcción del grafo:** A partir de la LSDB, cada router construye un grafo que representa la topología de la red.
4. **Cálculo de rutas:** Utilizando el algoritmo de Dijkstra, cada router determina la ruta más corta a cada destino basado en los costos de los enlaces.

## 2.3. Protocolos de Redundancia y Alta Disponibilidad

### 2.3.1. HSRP (Hot Standby Router Protocol)

HSRP es un protocolo propietario de Cisco que proporciona redundancia a nivel de gateway mediante la creación de un router virtual que actúa como puerta de enlace predeterminada para los dispositivos conectados directamente. Sus características principales son:

**Arquitectura HSRP:**

- **Router Activo:** Un router se designa como activo y gestiona el tráfico hacia el gateway virtual.
- **Router Pasivo (Standby):** Otro router se configura como pasivo, listo para asumir el rol de activo en caso de fallo del router activo.
- **Router Pasivo (Listen):** El tercer router se configura como pasivo en modo listen, listo para asumir el rol de router pasivo en modo Standby en caso de fallo del router activo.
- **Gateway Virtual:** Se asigna una dirección IP virtual que actúa como puerta de enlace para los dispositivos de la red.

**Mecanismos de Detección de Fallos:**

- Paquetes Hello enviados cada 10 segundos a la dirección multicast 224.0.0.2 para detectar la disponibilidad del router activo.
- Dead interval para detectar routers no funcionales, que se establece en 30 segundos.
- Configuración de prioridades para determinar el router activo, donde el router con mayor prioridad se convierte en activo.

### 2.3.2. EtherChannel y Agregación de Enlaces

EtherChannel es una tecnología que permite agregar múltiples enlaces físicos para actuar como un único enlace lógico. Los beneficios incluyen:

- **Mayor ancho de banda:** Combina el ancho de banda de varios enlaces físicos, mejorando la capacidad de la red.
- **Redundancia:** Si un enlace falla, el tráfico se redistribuye automáticamente entre los enlaces restantes, garantizando la continuidad del servicio.
- **Balanceo de carga:** Distribuye el tráfico entre los enlaces agregados, optimizando el uso de recursos y evitando cuellos de botella.

## 2.4. Servicios de Red Fundamentales

### 2.4.1. DHCP (Dynamic Host Configuration Protocol)

DHCP es un protocolo de red que permite la asignación dinámica de direcciones IP a dispositivos conectados a la red. Sus características principales son:

**Funcionamiento:**

1. **Descubrimiento:** El cliente envía un mensaje DHCP Discover para localizar servidores DHCP disponibles.
2. **Oferta:** Los servidores DHCP responden con un mensaje DHCP Offer que incluye una dirección IP y otros parámetros de configuración.
3. **Solicitud:** El cliente selecciona una oferta y envía un mensaje DHCP Request al servidor elegido.
4. **Confirmación:** El servidor responde con un mensaje DHCP Acknowledgment, confirmando la asignación de la dirección IP.
5. **Renovación:** Antes de que expire el tiempo de concesión, el cliente solicita una renovación de la dirección IP para continuar utilizándola.
6. **Liberación:** Cuando el cliente ya no necesita la dirección IP, envía un mensaje DHCP Release al servidor para liberar la dirección.

**Beneficios en Entornos Hospitalarios:**

- **Facilidad de gestión:** Permite la asignación automática de direcciones IP, simplificando la administración de dispositivos conectados.
- **Reducción de errores:** Minimiza la posibilidad de conflictos de direcciones IP al asignar dinámicamente direcciones únicas a cada dispositivo.
- **Flexibilidad:** Facilita la incorporación de nuevos dispositivos a la red sin necesidad de configuraciones manuales, lo que es esencial en entornos hospitalarios con alta rotación de equipos.

### 2.4.2. NAT (Network Address Translation)

NAT permite que múltiples dispositivos compartan una única dirección IP pública, siendo esencial para la conectividad a Internet en redes hospitalarias. Los tipos principales son:

- **NAT Estático:** Asocia una dirección IP privada a una dirección IP pública específica, permitiendo el acceso externo a un dispositivo concreto.
- **NAT Dinámico:** Asigna direcciones IP públicas de un grupo a dispositivos privados según sea necesario, optimizando el uso de direcciones IP.
- **PAT (Port Address Translation):** Permite que múltiples dispositivos compartan una única dirección IP pública utilizando diferentes números de puerto para distinguir las conexiones.

**Ventajas de NAT en Entornos Hospitalarios:**

- **Conservación de direcciones IP:** Permite que múltiples dispositivos utilicen una única dirección IP pública, lo que es crucial en entornos con recursos limitados.
- **Seguridad:** Oculta las direcciones IP internas de la red, dificultando el acceso no autorizado desde el exterior.
- **Flexibilidad:** Facilita la conexión a Internet de dispositivos que no requieren acceso directo desde el exterior, como impresoras o dispositivos IoMT.

## 2.5. Seguridad de Red y Control de Acceso

La seguridad en redes hospitalarias se ha convertido en un aspecto esencial dentro de la gestión tecnológica sanitaria, dado que en estos entornos no solo se maneja información crítica de carácter personal y médico, sino que además se conectan dispositivos clínicos cuyo correcto funcionamiento puede incidir directamente en la seguridad y salud de los pacientes. La evolución hacia infraestructuras digitales más complejas y la incorporación masiva de dispositivos médicos conectados (IoMT) ha incrementado notablemente la superficie de exposición a posibles ciberataques, lo que obliga a diseñar políticas de seguridad específicas, adaptadas a las necesidades de este tipo de entornos.

Para garantizar la seguridad de la infraestructura de red hospitalaria, se pueden usar mecanismos de control de tráfico como las Listas de Control de Acceso (ACLs) o las zonas demitilarizadas.

### 2.5.1. Listas de Control de Acceso (ACLs)

Las ACLs permiten filtrar el tráfico de red según criterios específicos, como direcciones IP, protocolos o puertos. Las ACLs se configuran en los dispositivos de red (switches y routers). Estas se clasifican en dos tipos principales:

- **ACLs estándar:** Filtran el tráfico únicamente por dirección IP de origen, permitiendo o denegando el acceso a toda la red o a subredes específicas.

- **ACLs extendidas:** Permiten un filtrado más granular, considerando tanto la dirección IP de origen como la de destino, protocolos y puertos específicos.

Los componenetes de una ACL incluyen:

- **Sujeto:** Entidad que solicita acceso a un recurso, como un usuario o dispositivo.

- **Acción:** Permite o deniega el acceso al recurso solicitado.

- **Objeto:** Recurso al que se solicita acceso, como un servidor, base de datos o dispositivo de red.

- **Condición:** Criterios que determinan si se permite o deniega el acceso, como direcciones IP, protocolos o puertos.

### 2.5.2. SSH (Secure Shell)

SSH es un protocolo de red que permite la administración segura de dispositivos a través de una conexión cifrada. Sus características principales son:

- **Cifrado de datos:** Protege la confidencialidad e integridad de la información transmitida, evitando que sea interceptada por terceros.

- **Autenticación segura:** Utiliza claves públicas y privadas para autenticar a los usuarios, garantizando que solo personal autorizado pueda acceder a los dispositivos.

- **Túneles seguros:** Permite crear túneles cifrados para transmitir datos sensibles, como credenciales o información médica, entre dispositivos.

**Beneficios de SSH en Entornos Hospitalarios:**

- **Seguridad en la administración remota:** Facilita la gestión de dispositivos de red sin comprometer la seguridad de la información.

- **Protección contra ataques:** Reduce el riesgo de ataques de intermediarios (MITM) y suplantación de identidad, asegurando que las comunicaciones sean auténticas.

- **Auditoría y seguimiento:** Permite registrar las actividades realizadas durante las sesiones SSH, facilitando la auditoría y el seguimiento de acciones administrativas.

### 2.5.3. Zonas Desmilitarizadas (DMZ)

Las zonas desmilitarizadas (DMZ) son una técnica de seguridad que permite aislar servicios accesibles desde Internet de la red interna del hospital, proporcionando una capa adicional de protección. En entornos hospitalarios, las DMZ se utilizan para alojar servicios como servidores web, servidores de correo electrónico o aplicaciones accesibles desde el exterior.

**Beneficios de las DMZ en Entornos Hospitalarios:**

- **Aislamiento de servicios:** Permite que los servicios accesibles desde Internet estén separados de la red interna, reduciendo el riesgo de comprometer sistemas críticos.
- **Control de acceso:** Facilita la implementación de políticas de seguridad más estrictas para los servicios expuestos, limitando el acceso a recursos internos.
- **Monitoreo y detección de intrusiones:** Las DMZ permiten una mejor supervisión del tráfico entrante y saliente, facilitando la detección de actividades sospechosas.

### 2.5.4. DHCP Snooping

DHCP Snooping es una característica de seguridad que protege la red contra ataques de suplantación de servidor DHCP (DHCP Spoofing). Funciona filtrando las solicitudes DHCP y permitiendo solo aquellas provenientes de servidores DHCP autorizados. Sus características principales son:

- **Filtrado de mensajes DHCP:** Permite que solo los mensajes DHCP provenientes de servidores autorizados sean aceptados, bloqueando solicitudes maliciosas.
- **Prevención de ataques:** Protege contra ataques de suplantación de servidor DHCP, donde un atacante intenta responder a solicitudes DHCP con información falsa.
- **Registro de asignaciones:** Mantiene un registro de las asignaciones de direcciones IP realizadas por los servidores DHCP autorizados, facilitando la auditoría y el seguimiento.

### 2.5.5. IPSec (Internet Protocol Security)

IPsec es un conjunto de protocolos que proporciona seguridad a nivel de red mediante la autenticación y cifrado de paquetes IP. Sus características principales son:

- **Autenticación de origen:** Verifica la identidad del remitente de los paquetes IP, asegurando que provienen de una fuente confiable.
- **Cifrado de datos:** Protege la confidencialidad de los datos transmitidos mediante el cifrado de los paquetes IP, evitando que sean interceptados por terceros.
- **Integridad de datos:** Garantiza que los datos no han sido alterados durante la transmisión, utilizando funciones hash para verificar la integridad.

**Beneficios de IPsec en Entornos Hospitalarios:**

- **Protección de datos sensibles:** Asegura que la información médica y personal transmitida a través de la red esté protegida contra accesos no autorizados.
- **Seguridad en comunicaciones remotas:** Facilita la creación de túneles seguros para la comunicación entre dispositivos médicos y sistemas de otros hospitales.

## 2.6. Introducción a IoMT (Internet of Medical Things)

Internet of Medical Things (IoMT) es una evolución natural de Internet of Things (IoT) aplicada al ámbito sanitario, que permite la interconexión de dispositivos médicos, sensores y sistemas de información clínica a través de redes seguras. Esta tecnología posibilita la monitorización remota de pacientes, el control en tiempo real de parámetros fisiológicos y la gestión eficiente de recursos hospitalarios, contribuyendo a mejorar la calidad asistencial y la toma de decisiones clínicas basadas en datos fiables y actualizados.

En la práctica hospitalaria, el IoMT se ha consolidado como una herramienta fundamental para optimizar los procesos sanitarios, incrementando la capacidad de respuesta ante situaciones críticas y reduciendo la carga de trabajo del personal clínico. Gracias a la integración de sensores biomédicos, dispsoitivos portátiles y plataformas de gestión de datos, los profesionales sanitarios pueden disponer de información vital en tiempo real, lo que favorece diagnósticos más precisos y tratamientos personalizados.

Además, el IoMT desempeña un papel esencial en la mejora de la eficiencia operativa hospitalaria. Como se recoge en la literatura, su implementación permite localizar y gestionar equipamiento médico, optimizar la trazabilidad de pacientes y activos, y mejorar la monitorización de entornos hospitalarios críticos, como quirófanos y unidades de cuidados intensivos. Este ecosistema conectado se apoya en tecnologías de comunicación de baja potencia y largo alcance (LPWAN) como Sigfox, LoRa y NB-IoT, que proporcionan conectividad eficiente para dispositivos médicos que requieren bajo consumo energético y cobertura extendida dentro y fuera de los centros sanitarios.

Desde el punto de vista arquitectónico, las soluciones IoMT han evolucionado hacia modelos distribuidos basados en edge/fog computing, donde los datos se procesan parcialemnte en pasarelas inteligentes cercanas a los dispositivos, antes de enviarse a plataformas en la nube para su almacenamiento y análisis avanzado. Este enfoque permite reducir la latencia, mejorar la seguridad de los datos sensibles y aliviar la carga de tráfico hacia los servidores centrales, favoreciendo la continuidad asistencial en entornos hospitalarios con elevada demanda de recursos.

El auge del IoMT también plantea desafíos en materia de seguridad, privacidad e interoperabilidad, dado que la cantidad de información médica gestionada por estos sistemas es altamente sensible y está sujeta a estrictos marcos normativos.

En definitiva, la implantación del IoMT en entronos hospitalrios representa una oportunidad estratégica para transformar la asistencia sanitaria, dotándola de mayor flexibilidad, capacidad predictiva y resiliencia frente a sistuaciones de crisis como la vivida durante la pandemia de COVID-19, donde estas tecnologías demostraron su potencial para mejorar la monitorización, la toma de decisiones y la gestión de recursos clínicos en tiempo real.

CAPÍTULO 3

# ANÁLISIS

## 3.1. Interesados

Los interesados son aquellas personas o entidades que tienen un interés en el proyecto y pueden influir en su desarrollo o verse afectadas por él. En este caso, los interesados son los siguientes:

- **Personal médico y sanitario:** Son los usuarios principales de los sistemas clínicos conectados a la red. Utilizan aplicaciones para la gestión de historiales médicos, diagnósticos, prescripciones y monitorización en tiempo real de los pacientes. Para este colectivo, la red debe garantizar alta disponibilidad, bajo retardo y confidencialidad de los datos clínicos, ya que cualquier interrupción puede afectar directamente a la atención sanitaria.

- **Personal administrativo:** Encargados de la gestión de citas, facturación, expedientes, inventario y coordinación interna del hospital. Aunque sus tareas no están directamente relacionadas con la atención clínica, requieren acceso constante a sistemas de información conectados a la red. Su trabajo depende de la fiabilidad de los servicios internos como bases de datos y aplicaciones de gestión.

- **Departamento de IT:** Responsables del mantenimiento, configuración y supervisión de la infraestructura de red. Este grupo necesita una red segura, escalable y fácilmente monitorizable, así como herramientas para la detección de fallos, gestión de dispositivos IoMT y control de accesos.

- **Dirección del hospital:** Interesada en que la red contribuya a mejorar la eficiencia operativa del centro, optimice los recursos y garantice el cumplimiento de la legislación vigente, especialmente en lo relativo a la protección de datos (LOPDGDD y RGPD). También se preocupan por el coste y la sostenibilidad del sistema a largo plazo.

- **Pacientes:** Interesados en que la red de invitados funcione correctamente y no tenga fallos de seguridad. Su experiencia asistencial mejora cuando los procesos internos son ágiles, seguros y eficientes. La red hospitalaria debe garantizar que su información médica esté protegida, que los dispositivos de monitorización funcionen en tiempo real y que la atención sea fluida y sin errores derivados de caídas de red.

## 3.2. Requisitos del Sistema

Para garantizar el correcto diseño, funcionamiento y seguridad de la infraestructura de red hospitalaria simulada en este proyecto, se han definido una serie de requisitos que determinan las condiciones que debe cumplir el sistema. Estos requisitos se clasifican en funcionales, no funcionales, de conectividad y de seguridad, abarcando tanto los aspectos técnicos como los operativos de la red.

### 3.2.1. Requisitos Funcionales

Son aquellos requisitos que definen las funciones y servicios que debe ofrecer la infraestructura de red para satisfacer las necesidades del entorno hospitalario y los dispositivos conectados.

- El sistema debe permitir la interconexión entre los cuatro hospitales.
- Cada hospital debe disponer de tres subredes diferenciadas: una para invitados, una para dispositivos IoMT y otra para la red interna hospitalaria.
- Cada hospital debe estar dividido en VLANs por departamentos, asegurando la separación lógica de las áreas clínicas, administrativas, de investigación y de servicios generales.
- La red debe permitir la asignación dinámica de direcciones IP mediante servidores DHCP en cada subred.
- Debe garantizar la resolución de nombres internos mediante DNS.
- Los dispositivos autorizados deben poder acceder a servidores de datos y dispositivos médicos críticos entre hospitales.
- Los dispositivos médicos IoMT deben disponer de una subred propia con dos servidores DHCP, uno de ellos de respaldo.
- Deben implementarse servicios de NAT para acceso a Internet desde las subredes autorizadas.
- Se debe permitir gestión remota segura de los dispositivos de red mediante SSH.
- La red debe contar con redundancia de enlaces y gateways mediante EtherChannel y HSRP.
- Tanto la red intrahospitalaria como la interhospitalaria debe estar configurada de tal forma que haya configuraciones dinámicas de enrutamiento utilizando OSPF.

### 3.2.2. Requisitos No Funcionales

Son aquellos que definen condiciones de calidad, operativas o de gestión que debe cumplir el sistema, sin especificar funciones concretas.

- La infraestructura debe garantizar una alta disponibilidad, con redundancia en enlaces y puntos críticos.
- La red debe estar diseñada de forma modular y escalable, permitiendo incorporar nuevos departamentos o dispositivos sin afectar al rendimiento.

### 3.2.3. Requisitos de Disponibilidad y Redundancia

Establecen las condiciones que debe cumplir la red para garantizar su funcionamiento continuo y la disponibilidad de los servicios críticos. En términos generales se establecen los siguientes requisitos:

- Los enlaces entre switches L2 y L3 deben contar con redundancia física para evitar puntos únicos de fallo.
- Los routers principales deben estar configurados en alta disponibilidad para tolerar fallos de hardware o enlaces.
- Los servidores DHCP deben contar con un servidor de respaldo para garantizar la asignación continua de direcciones IP, únicamente para los dispositivos IoMT.
- La infraestructura debe permitir la monitorización continua del estado de los dispositivos y enlaces para detectar fallos proactivamente.

### 3.2.4. Requisitos de Seguridad

Establecen las condiciones que debe cumplir la red para proteger su infraestructura, los datos transmitidos y los servicios prestados. En términos generales se establecen los siguientes requisitos:

- Se debe implementar una segmentación lógica mediante VLANs para aislar departamentos, subredes y servicios críticos.
- Deben configurarse listas de control de acceso (ACLs) para:
    - Bloquear el tráfico desde la red de invitados hacia la red interna y la red de dispositivos IoMT.
    - Restringir el acceso a la base de datos de cada hospital, permitiendo únicamente a los dispositivos autorizados de cada hospital acceder a ella.
    - Restringir el acceso a los dispositivos IoMT según su clasificación y función, limitando la conectividad entre ellos.
    - Permitir el acceso a los dispositivos de la red interna únicamente a los dispositivos autorizados de las áreas de servicios quirúrgicos, médicos, centrales y UCI.

- La gestión de dispositivos de red debe realizarse mediante conexiones seguras (SSH).
- Todos los dispositivos de red deben contar con una configuración de autenticación, con contraseñas seguras, para evitar accesos no autorizados.
- La interconexión entre hospitales debe realizarse a través de enlaces seguros, utilizando VPNs o túneles cifrados para proteger la información transmitida.

Para establecer los requisitos de seguridad específicos para los dispositivos IoMT, se deben considerar las sigueintes clasificaciones de dispositivos:

- **Dispositivos IoMT Comunes (Tipo 1):** Son aquellos dispositivos comunes para la atención médica que pueden ser utilizados por el personal médico. Estos dispositivos pueden incluir sistemas de monitoreo remoto de pacientes, sensores de localización, dispositivos implantables, etc.
- **Dispositivos IoMT Importantes UCI (Tipo 2):** Son aquellos dispositivos que no son críticos dentro de la UCI, es decir, que su función princiapl no es vital de forma inmediata. Estos dispositivos inluyen bobmas de vacío para heridas, lámparas de fototerapia, dispositivos de rehabilitación, etc [1].
- **Dispositivos IoMT Críticos UCI (Tipo 3):** Son aquellos dispositivos que son críticos dentro de la UCI, es decir, son aquellos que permiten el monitoreo y soporte vital de pacietnes en estado grave, donde la vigilancia constante y la intervención inmediata pueden marcar la diferencia entre la vida y la muerte, y que por tanto necesitan medidas de seguridad extras. Estos dispositivos incluyen monitores cardíacos y de signos vitales, ventiladores mecánicos, bombas de infusión, sistemas de hemodiálisis, etc[1].

A continuación se detallan los requisitos de seguridad específicos para los dispositivos IoMT:

- Los dispositivos IoMT deben estar aislados en una subred propia para evitar interferencias con la red interna y de invitados.
- Los dispositivos IoMT deben contar con un servidor propio de DHCP para asignación de direcciones IP, con un servidor de respaldo para garantizar la continuidad del servicio.
- Los dispositivos IoMT Tipo 1 solo deben tener conectividad con los dispositivos de las areas médicas de servicios quirúrgicos, médicos y centrales, además de por los dispositivos del departamento de la UCI.
- Los dispositivos IoMT Tipo 2 deben tener conectividad únicamente con los dispositivos del departamento de la UCI.
- Los dispositivos IoMT Tipo 3 solo pueden tener conectividad con un único dispositivo autorizado del departamento de la UCI.

### 3.2.5. Requisitos de Conectividad

Definen las condiciones relacionadas con la transmisión de datos y la comunicación entre dispositivos y servicios dentro de la red, en términos generales.

- Solo los dispositivos autorizados de cada hospital pueden acceder a la base de datos de otros hospitales.
- Cualquier dispositivo de la red de invitados no puede tener conectividad con la red interna o con la red de dispositivos IoMT.
- Dentro de la red interna, los dispositivos del area de administración, de enfermeria (exceptuando la UCI) y de apoyo, no pueden tener conectividad con las areas de servicios quirúrgicos, médicos, centrales y UCI.
- Cualquier dispositivo de las areas de servicios quirúrgicos, médicos, centrales y UCI puede tener conectividad con cualquier otro dispositivo de la red interna.

CAPÍTULO 4

# METODOLOGÍA DE TRABAJO

## 4.1. Enfoque y Planificación del Proyecto

Para garantizar el correcto desarrollo de este proyecto de diseño y simulación de una red hospitalaria, se optó por un enfoque metodológico secuencial y estructurado, basado en el modelo tradicional de desarrollo en cascada. Este modelo resulta especialmente adecuado para proyectos de carácter técnico y con una secuencia de tareas bien definida, como es el caso de la implementación de una infraestructura de red simulada, donde cada fase depende del correcto desarrollo de la anterior.

La metodología se articuló en torno a fases independientes y consecutivas, en las que se desarrollaron de forma separada y ordenada las distintas partes del proyecto: desde el análisis inicial de requisitos hasta las pruebas finales de validación, pasando por el diseño, la implementación y la configuración de los dispositivos y servicios de red.

### 4.1.1. Enfoque de Trabajo Adoptado

El trabajo se ha estructurado en cinco fases principales, organizadas secuencialmente:

1. **Análisis de Requisitos:** recopilación y análisis de las necesidades funcionales, de conectividad y de seguridad que debía cubrir la red hospitalaria, incluyendo las particularidades de la subred IoMT.

2. **Diseño de la red:** elaboración de los diagramas de topología física y lógica, planificación del direccionamiento IP, definición de VLANs, políticas de seguridad y segmentación.

3. **Implementación de la infraestructura en Cisco Packet Tracer:** configuración de routers, switches, creación de VLANs, definición de ACLs y puesta en funcionamiento de los servicios de red.

4. **Pruebas y validación:** realización de pruebas de conectividad, comprobación de los servicios implementados y verificación de las políticas de seguridad aplicadas.

5. **Documentación y cierre del proyecto:** redacción de las configuraciones, resultados de pruebas, y elaboración de la memoria técnica y académica del proyecto.

Cada fase se abordó de forma secuencial, de modo que no se iniciaba una nueva hasta haber completado, revisado y validado la anterior, siguiendo así la filosofía del modelo en cascada.

### 4.1.2. Planificación y Seguimiento

Para asegurar el cumplimiento de la planificación establecida y el correcto desarrollo del proyecto, se realizaron reuniones de seguimiento quincenales con los tutores académicos. Estos encuentros resultaron clave para revisar los avances, corregir posibles errores detectados y planificar conjuntamente los siguientes pasos. Gracias a estas sesiones periódicas, se pudo ajustar la planificación en función de los resultados obtenidos en cada fase, resolviendo incidencias y mejorando progresivamente el diseño y configuración de la red.

A continuación se presenta una tabla con el cronograma del proyecto, que detalla las tareas realizadas y su duración estimada:
(tabla con cronograma del proyecto)

## 4.2. Herramientas y Tecnologías Utilizadas

Para el desarrollo y correcta gestión de este proyecto, se han empleado diversas herramientas tecnológicas que han permitido organizar las tareas, llevar a cabo las simulaciones de red y mantener un control estructurado sobre los cambios realizados en la configuración y documentación del proyecto. A continuación, se describen las herramientas utilizadas y su papel dentro del proyecto:

### 4.2.1. Cisco Packet Tracer

Para el diseño, simulación e implementación virtual de la red hospitalaria propuesta, se ha utilizado Cisco Packet Tracer, una herramienta de simulación de redes desarrollada por Cisco Systems que permite emular el comportamiento de dispositivos de red reales en entornos controlados.
Esta aplicación ha facilitado la creación de topologías de red personalizadas, la configuración de routers y switches, la asignación de direccionamientos IP, la implementación de VLANs y ACLs, así como la realización de pruebas de conectividad y seguridad. Además, Packet Tracer ha permitido visualizar de forma gráfica y detallada el tráfico de datos entre dispositivos, lo que ha sido fundamental para comprobar el correcto funcionamiento de la infraestructura antes de una hipotética implementación real.

### 4.2.2. Git y GitHub

Para llevar un control exhaustivo de las versiones de los archivos de configuración, documentación y esquemas de red, se ha empleado GitHub como sistema de control de versiones basado en la herramienta Git. El uso de GitHub ha permitido mantener un histórico de los cambios realizados en el proyecto, facilitando así la recuperación de versiones anteriores en caso de necesidad y garantizando la trazabilidad de las modificaciones. Además, se ha utilizado como repositorio privado para almacenar las configuraciones de dispositivos, los diagramas de topología y los documentos de planificación, centralizando toda la información en un entorno accesible y seguro.

### 4.2.3. Google Calendar

Con el objetivo de organizar de forma eficiente el cronograma de trabajo, se ha empleado Google Calendar como herramienta de planificación y gestión temporal. Esta aplicación ha permitido establecer fechas límite, programar reuniones de seguimiento y distribuir las tareas en función de la carga de trabajo semanal. La posibilidad de añadir recordatorios y notificaciones ha resultado de gran utilidad para garantizar el cumplimiento de los hitos establecidos en el proyecto, manteniendo una correcta planificación y coordinación de las diferentes fases de desarrollo.

### 4.2.4. SketchUp

Para la elaboración del diagrama de topología física de la red hospitalaria, se ha empleado SketchUp, una herramienta de modelado en 3D que permite crear representaciones visuales detalladas de espacios y distribuciones físicas. Gracias a esta aplicación, ha sido posible diseñar de forma visual la disposición de los distintos departamentos del hospital, algunos dispositivos de red, salas de servidores y otros elementos relevantes, facilitando así la comprensión del diseño físico de la infraestructura. Este diagrama ha sido fundamental para complementar la documentación técnica y proporcionar una visión clara de la disposición de los equipos y la segmentación de la red en el entorno hospitalario.

CAPÍTULO 5

# DISEÑO

El correcto diseño de una infraestructura de red es un factor determinante para garantizar la eficiencia, la seguridad y la disponibilidad de los servicios en cualquier entorno, y resulta especialmente crítico en instalaciones hospitalarias, donde el funcionamiento continuo de los sistemas de información y de los dispositivos médicos conectados puede tener un impacto directo en la seguridad y atención de los pacientes. Por ello, el diseño debe contemplar no solo la organización topológica de los dispositivos y enlaces, sino también la segmentación lógica, las políticas de seguridad y la planificación de los servicios de red necesarios.

En este capítulo se presenta el diseño detallado de la infraestructura de red hospitalaria propuesta, partiendo de los requisitos funcionales, de seguridad y de conectividad definidos previamente. El diseño abarca dos niveles: por un lado, la red de interconexión entre los cuatro hospitales simulados, y por otro, el diseño específico y detallado de la red de uno de los hospitales, empleando técnicas de segmentación mediante VLANs y subredes diferenciadas para invitados, dispositivos IoMT y servicios internos.

Asimismo, se describen las decisiones adoptadas respecto a la topología física y lógica, la planificación del direccionamiento IP, la definición de las VLANs, la organización de los servicios de red, las políticas de seguridad implementadas y la configuración de mecanismos de redundancia y tolerancia a fallos. Todos estos elementos se han planificado en base a los criterios de diseño establecidos en capítulos anteriores y conforme a las buenas prácticas recomendadas para entornos sanitarios.

Este capítulo servirá como base para la posterior implementación y simulación de la red en Cisco Packet Tracer, así como para la ejecución de pruebas de conectividad y seguridad orientadas a validar su funcionamiento.

## 5.1. Criterios de Diseño

Antes de definir la infraestructura de red, se realizó un análisis de los requisitos funcionales, de seguridad y de conectividad propios de un entorno hospitalario. Este análisis, junto con las buenas prácticas en entornos sanitarios, permitió establecer una serie de criterios de diseño, como la segmentación mediante VLANs, el aislamiento de subredes críticas como IoMT, la redundancia de enlaces y gateways, y la centralización de servicios en DMZ.

El diseño se divide en dos niveles: una red de interconexión entre cuatro hospitales y un diseño interno detallado de un hospital, dividido en subredes y VLANs según áreas funcionales.

Para la red de interconexión entre hospitales, se optó por simplificar la topología de tal forma que el diseño se enfoque simplemente en la conectividad entre los hospitales, es decir, se omiten las configuraciones de redundancia (HSRP y EtherChannel) y se simplifica la cantidad de VLANs y subredes, manteniendo la funcionalidad básica de comunicación entre ellos. Esta decisión se tomó para no duplicar el esfuerzo de configuración y para centrarse en mejorar las configuraciones de seguridad y conectividad entre los hospitales.

## 5.2. Topología de Red Propuesta

En esta sección se presentan las topologías de red propuestas tanto para el Hospital Universitario Son Espases como para la red de interconexión de los cuatro hospitales, que incluye tanto la topología física como la lógica, detallando en cada caso las decisiones adoptadas y los dispositivos seleccionados para cumplir con los requisitos de conectividad, seguridad y rendimiento.

### 5.2.1. Topología Física Son Espases

La topología física representa la disposición y conexión física de routers, switches, servidores, dispositivos IoMT y departamentos.

#### Routers

En este diseño, como se muestra en la Figura 5.1, se han implementado tres routers principales, los cuales están configurados para proporcionar redundancia y tolerancia a fallos mediante HSRP (Hot Standby Router Protocol). Estos routers se conectan con:

- Red de Invitados.
- DMZ Invitados.
- DMZ IoMT.
- DMZ Interno.
- Dos Switches Core.

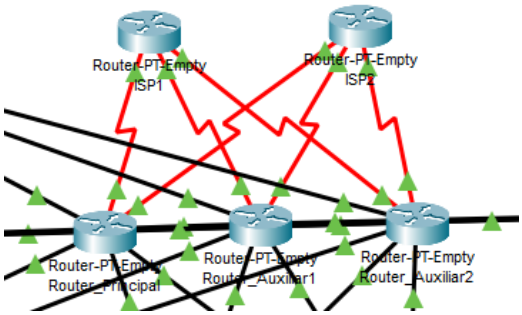



Figura 5.1: Redundancia en Routers

Además, estos routers están conectados a dos routers más, que simularían la conexión a Internet (ISP1 y ISP2).

### Red de Invitados

La red de invitados está diseñada para proporcionar acceso a Internet a los dispositivos de invitados, garantizando que no interfieran con la red interna del hospital. Esta red cuenta con dos switches L2 que conectan con dos puntos de acceso inalámbrico (APs) que proporcionan conectividad a los dispositivos móviles de los invitados. La interconexión entre el router y la red de invitados se realiza a través de un switch L3, que permite la segmentación y el control del tráfico de red. La Figura 5.2 muestra la topología física de la red de invitados.

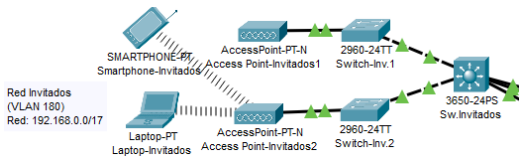



Figura 5.2: Topología Física de la Red de Invitados

Esta red está muy simplificada, ya que no se han implementado configuraciones de redundancia ni de seguridad avanzadas, centrándose únicamente en la conectividad básica entre los dispositivos invitados y el acceso a Internet. Por supuesto, esta red es completamente escalable y se puede ampliar con los dispositivos necesarios para cumplir con futuros requisitos del sistema.

### DMZ Invitados

La DMZ de invitados está diseñada para dar acceso a Internet a los dispositivos invitados, permitiendo que estos dispositivos tengan una dirección IP única dentro de la red, sin interferir con la red interna del hospital. Esta DMZ está conectada a un switch L2 que conecta con los routers, permitiendo la segmentación del tráfico y el control de acceso a los recursos internos. La Figura 5.3 muestra la topología física de la DMZ de invitados.

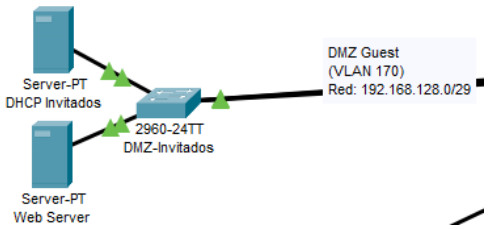



Figura 5.3: Topología Física de la DMZ de Invitados

Como se ha podido ver en la Figura 5.3, también se encuentra en esta DMZ el servidor web del hospital, de esta forma los dispsoitivos de Internet que quieuran acceder a la web del hospital lo harán a través de esta DMZ evitando así que puedan conocer o acceder a la DMZ interna, añadiendo de esta forma una capa extra de seguridad.

**DMZ IoMT**

La DMZ IoMt tiene como finalidad dar direcciones IP dinámicas a los dispositivos IoMT de la red, permitiendo que estos dispositivos puedan tener conectividad con otros dispsoitivos de la red, sin que estos servidores DHCP puedan ser detectados o acceddidos por dispositivos externos. Esta DMZ está conectada a un switch L2 que conecta con los routers, permitiendo la segmentación del tráfico y el control de acceso a los recursos internos. La Figura 5.4 muestra la topología física de la DMZ IoMT.

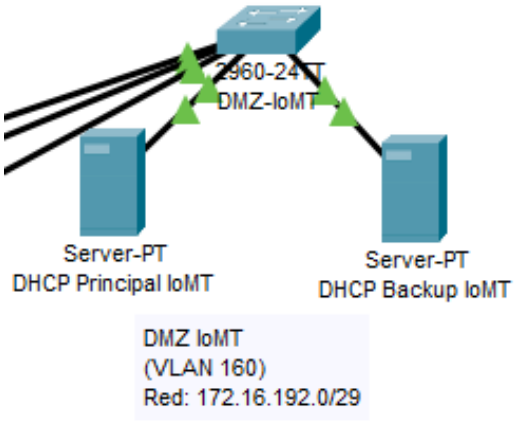



Figura 5.4: Topología Física de la DMZ IoMT

Como se puede apreciar en la Figura 5.4, esta DMZ está formada por dos servidores DHCP, uno que está activo y otro en modo reposo, de esta forma se garantiza que si uno de los servidores falla, el otro pueda tomar el control y seguir proporcionando direcciones IP a los dispositivos IoMT.

**DMZ Interna**

La DMZ Interna está diseñada para albergar los servidores internos del hospital, como el servidor de correo electrónico, el servidor DNS, el servidor DHCP y el servidor

de archivos. Esta DMZ está conectada a un switch L2 que conecta con los routers, permitiendo la segmentación del tráfico y el control de acceso a los recursos internos. La Figura 5.5 muestra la topología física de la DMZ interna.

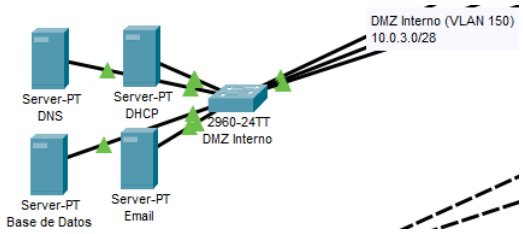



Figura 5.5: Topología Física de la DMZ Interna

Este servidor de archivos es el encargado de almacenar todos los archivos relevantes que pueden ser compartidos con otros hospitales.

### Red Interna

La red interna del hospital está diseñada para albergar todos los dispositivos de red y finales del hospital, incluyendo los switches core, los de distribución, los de acceso y los dispositivos finales de cada departamento. Dentro de la red interna, primero nos encontramos con los switches core, que conectan con los routers y por tanto dan acceso a Internet y a las DMZ a todos los dispositivos de la red Interna. Estos switches core están conectados en forma de malla, permitiendo la redundancia y la tolerancia a fallos. La Figura 5.6 muestra la topología física de la interconexión de los switches core.

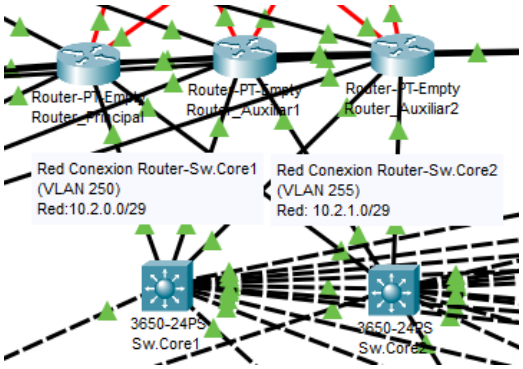



Figura 5.6: Interconexión de Switches Core

Estos switches core están conectados en forma de malla a seis switches de distribución, uno por cada área del hospital (Administración, Servicios Quirúrgicos, Servicios Médicos, Servicios Centrales, Enfermería y Apoyo), permitiendo la segmentación del tráfico y el control de acceso a los recursos internos. Además, cada switch de distribución esta conectado a otro dos switches de distribución, lo que permite implementar redundancia y tolerancia a fallos. La Figura 5.7 muestra la topología física de la interconexión de los switches de distribución.

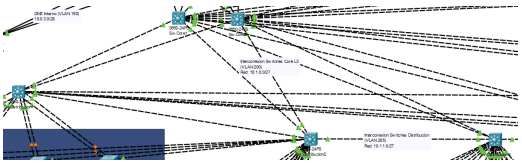


Figura 5.7: Interconexión de Switches de Distribución

Estos switches de distribución están conectados a los switches de acceso, que son los encargados de conectar los dispositivos finales de cada departamento. Cada switch de acceso está conectado a dos switches de distribución, permitiendo la redundancia y tolerancia a fallos, además, también tiene un doble enlace con uno de los switches de distribución, lo que permite que si uno de los enlaces falla, el otro enlace pueda seguir proporcionando conectividad a los dispositivos finales. La Figura 5.8 muestra la topología física de la interconexión de los switches de acceso.

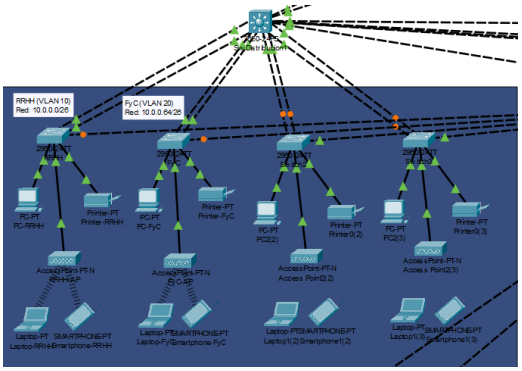



Figura 5.8: Interconexión de Switches de Acceso

Como se puede ver en la Figura 5.8, cada departamento esta formado por un PC de escritorio, una impresora y un punto de acceso que da conectividad inalámbrica a un portátil y un smartphone. Esto es así a modo de ejemplo, para que se vea que es posible conectar varios dispositivos diferentes y con diferentes conexiones, por supuesto cada departamento es completamente escalable ya que se pueden añadir tantos dispositivos como se necesiten, teneiendo en cuenta que el límite de direcciones IP asignables son 56.

**Red IoMT**

La red IoMT esta conectada directamente a los switches core, de esta forma se consigue que no saturen a los routers con su constante tráfico. En la Figura 5.9 se muestra la topología física de la red IoMT. Se puede apreciar claramente que esta dividida en cuatro capas, una por cada planta del hospital, de esta forma podemos distinguir los tipos de dispositivos IoMT según la planta en la que se encuentren. Cada capa está formada por un switch L3 que conecta con tres puntos de acceso, lo que permite que haya cobertura inalámbrica a lo largo de cada planta, y además permite que si los dispositivos IoMT se desplazan, puedan coenctarse a otro punto de acceso bajo el mismo SSID.

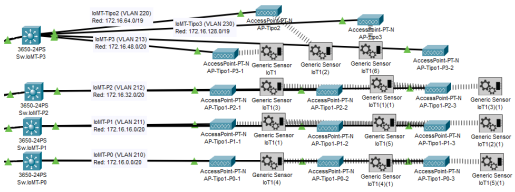


Figura 5.9: Topología Física de la Red de Dispositivos IoMT

**Disposición Física**

La Figura 5.10 muestra una imagen en tres dimensiones de la disposición de los dispositivos de red y diferentes departamentos del hospital, de esta forma se puede apreciar de forma mas clara la disposición física de los diferentes elementos de la red. La ubicación de algunos departamentos se ha extraído de un vídeo de Youtube publicado por el Govern de les Illes Balears [2].

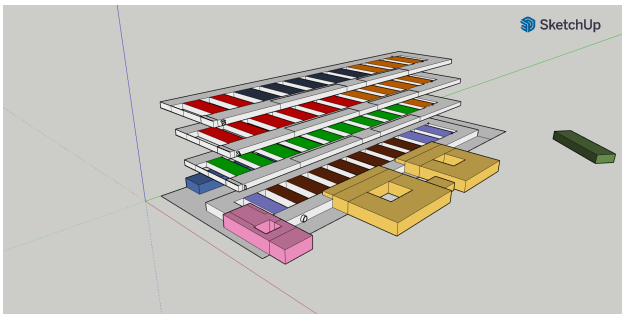



Figura 5.10: Disposición Física Elementos de Red del Hospital Son Espases

Además, las grandes áreas y departamentos del Hospital de Son Espases se han extraído de sitios web oficiales del Govern de les Illes Balears, como el portal de Gerencia del Hospital Universitario de Son Espases [3] o el documento oficial de la plantilla del Hospital Universitario de Son Espases [4].

### 5.2.2. Topología Lógica Son Espases

La topología lógica define la organización del tráfico y las relaciones entre las distintas VLANs, subredes y servicios.

En este diseño, se ha definido una VLAN por cada departamento del hospital, así como VLANs específicas para servicios críticos como IoMT, red de invitados e interconexiones entre dispositivos de red. También se han definido tres grandes subredes:

- **Subred Interna:** Esta subred alberga las VLANs de los departamentos y servicios internos del hospital, garantizando la comunicación entre ellos y el acceso a los recursos compartidos.
- **Subred IoMT:** Esta subred está dedicada a los dispositivos IoMT, garantizando su aislamiento y seguridad, así como la monitorización de su tráfico.

- **Subred de Invitados:** Esta subred permite el acceso a Internet y a servicios básicos para los dispositivos de invitados, garantizando que no interfieran con la red interna del hospital.

Además de esas subredes, también se han definido algunas VLANs específicas para la interconexión entre dispositivos de red, como los routers y switches core, así como para la DMZ interna y la DMZ IoMT.

La subred IoMT esta formada por una VLAN por cada planta, exceptuando la última planta, en la que hay tres VLANs distintas, esto es debido a que en esa planta es donde se encuentra la UCI, y por tanto los dispositivos IoMT de tipo 2 y 3. Por ese motivo, hay una VLAN para cada tipo de dispositivo IoMT en la planta 3, con esto se consigue una segmentación de red robusta y además se mejora la seguridad ya que se pueden implementar medidas de control de tráfico para filtrar según el tipo de dispositivo IoMT al que estén accediendo.

**Nota:** *Para recordar los tipos de dispositivos IoMT que hay, ver la sección 3.2.4*

### 5.2.3. Topología Física de la Red de Interconexión entre Hospitales

Este diseño es el mismo para los cuatro hospitales, permitiendo así que todos dispongan de los mismos recursos, aunque individualmente cada uno tenga sus propios departamentos. En este diseño, el núcleo de la red es la interconexión de los cuatro hospitales, esta se lleva a cabo mediante enlaces directos entre cada router de cada hospital, en la Figura 5.11 se muestra la topología física de los routers de interconexión entre hospitales.

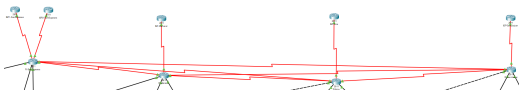


Figura 5.11: Topología Física de la Interconexión entre Hospitales

Como se puede apreciar en la Figura 5.11, cada hospital tiene un único router conectado a otro router, simulando así la conexión a Internet, excepto en el caso del Hospital de Son Espases, que tiene dos ISPs distintos, ya que al ser el hospital principal, se ha decidido que tenga dos conexiones a Internet para garantizar la redundancia y la tolerancia a fallos.

Además, cada router de cada hospital está conectado a dos switches core (L3), que son los que dan conectividad con el router a todos los dispositivos de la red interna, en la Figura 5.12 se muestra la topología física de la interconexión entre el router y los switches core.

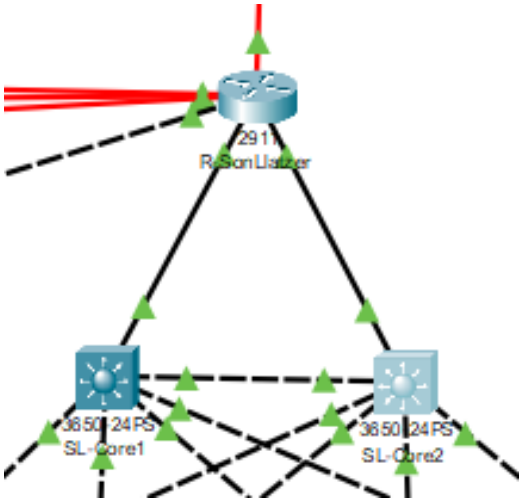



Figura 5.12: Topología Física de la Interconexión entre el Router y los Switches Core en Hospitales

Los dos switches core también estan conectados en forma de malla con 4 switches de distribución, uno por cada area del hospital (Administración, Áreas Médicas, Enfermeria, Área de Apoyo). Con el fin de conseguir redundancia y tolerancia a fallos, estos switches de distribución se interconectan entre ellos dos a dos. En la Figura 5.13 se muestra la topología de interconexión entre los switches core y los switches de distribución.

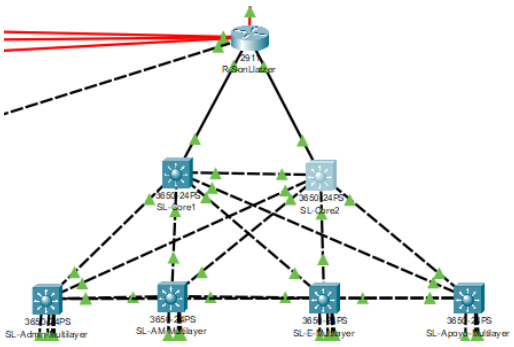


Figura 5.13: Topología Física de la Interconexión entre los Switches L3 en Hospitales

A su vez, los switches de distribución conectan con los switches de acceso, los cuales dan conectividad a los dispositivos finales. En la Figura 5.14 se aprecia como, con fines de ahorrar espacio y tener la red mas ordenada, los switches de distribución se conectan con un cluster, el cual contiene los switches de acceso y por tanto las VLANs de cada departamento, separadas según las principales áreas del hospital.

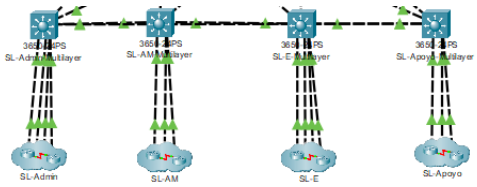



Figura 5.14: Topología Física de la Interconexión con Clusters en Hospitales

En la Figura 5.15 se aprecian las subredes que hay dentro de los clusters, en este caso es la subred del area de adminsitración, la cual se compone por el departamento de Recursos Humanos, Finnazas y Contabilidad, Tecnologías de la Información y Servicios Generales.

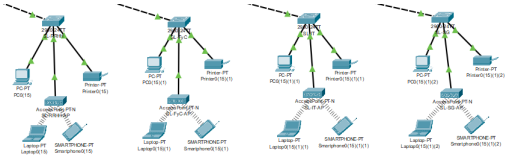


Figura 5.15: Topología Física de la Interconexión con Clusters en Hospitales

### 5.2.4. Topología Lógica de la Red de Interconexión entre Hospitales

En este diseño, se ha definido una VLAN por cada departamento del hospital, además de las VLANs de interconexión entre switches y routers. Además, se han definido cuatro grandes subredes:

- **Subred Son Espases:** Esta subred alberga las VLANs de los departamentos y servicios internos del Hospital Son Espases, garantizando la comunicación entre ellos y el acceso a los recursos compartidos.

- **Subred Manacor:** Esta subred alberga las VLANs de los departamentos y servicios internos del Hospital de Manacor, garantizando la comunicación entre ellos y el acceso a los recursos compartidos.

- **Subred Inca:** vEsta subred alberga las VLANs de los departamentos y servicios internos del Hospital Comarcal de Inca, garantizando la comunicación entre ellos y el acceso a los recursos compartidos.

- **Subred Son Llàtzer:** Esta subred alberga las VLANs de los departamentos y servicios internos del Hospital Son Llàtzer, garantizando la comunicación entre ellos y el acceso a los recursos compartidos.

Cada hospital tiene su propia DMZ, donde alberga los servidores necesarios para dar los servicios al hospital y además cuenta con un servidor de archivos, que almacena información relevante del hospital, con el fin de que sea accesible por dispositivos autorizados de otros hospitales.

### 5.2.5. Descripción de Dispositivos Utilizados

En ambos diseños se han utilizado los siguientes dispositivos:

- **Routers:** Se ha utilizado el modelo *Router-PT-Empty*, ya que permite añadir la cantidad de interfaces tanto GigabitEthernet como Serial necesarias para realizar las conexiones.
- **Switches L2:** Se ha utilizado el modelo *2960 IOS15*, ya que es el modelo mas moderno que ofrece la herramienta Cisco Packet Tracer.
- **Switches L3:** Se ha utilizado el modelo *3650-24PS*, ya que es el modelo mas moderno que ofrece la herramienta Cisco Packet Tracer.
- **Puntos de Acceso Inalámbrico:** Se ha utilizado el modelo *AccessPoint-PT-N*, ya que es el modelo mas potente de los ofrecidos por la herramienta Cisco Packet Tracer.
- **Dispositivos Finales:**
  - **Portátiles:** *Laptop-PT*
  - **PCs de Escritorio:** *PC-PT*
  - **Dispositivos Móviles:** *Smartphone-PT*
  - **Impresoras:** *Printer-PT*
  - **Dispositivos IoMT:** *Generic Sensor*
  - **Servidores:** *Server-PT*

El cableado utilizado en toda la red es de tipo *Cobre*, mientras que las conexiones entre los routers y los ISPs se realizan mediante cableado de tipo *Serial*.

## 5.3. VLANs y Segmentación de Red

Uno de los elementos esenciales para garantizar la seguridad, la eficiencia y la organización de una infraestructura de red hospitalaria es la correcta segmentación del tráfico mediante el uso de Virtual LANs (VLANs). En este proyecto se ha diseñado una segmentación lógica basada en la estructura funcional de los hospitales, asignando una VLAN diferente a cada área o departamento, y separando además las subredes críticas como la de invitados y la de dispositivos IoMT.

Este enfoque permite aislar el tráfico de cada grupo de dispositivos, reducir la propagación de posibles ataques, evitar la congestión de tráfico y facilitar la aplicación de políticas de seguridad específicas entre diferentes segmentos de la red.

### 5.3.1. Definición de VLANs por Departamento

Cada hospital se ha organizado internamente mediante VLANs asignadas a los diferentes departamentos y servicios. En el caso de la red de Son Espases, se han definido y configurado las siguientes VLANs:

- **VLAN 10:** RRHH (Recursos Humanos)
- **VLAN 20:** FyC (Finanzas y Contabilidad)
- **VLAN 30:** Oftalmologia
- **VLAN 40:** Urologia
- **VLAN 50:** Cardiologia
- **VLAN 60:** Dermatologia
- **VLAN 70:** Radiologia
- **VLAN 80:** Inmunologia
- **VLAN 90:** Admision
- **VLAN 100:** UCI (Unidad de Cuidados Intensivos)
- **VLAN 110:** Atencion paciente
- **VLAN 120:** Asesoria Jurídica
- **VLAN 150:** DMZ Interno
- **VLAN 160:** DMZ IoMT
- **VLAN 170:** DMZ Invitados
- **VLAN 180:** Red Invitados
- **VLAN 190:** Interconexión Router-Sw.Invitados
- **VLAN 200:** Interconexión Switches Distribución - Switches Core
- **VLAN 205:** Interconexión Switches Distribución
- **VLAN 210:** Red IoMT Tipo 1 Planta 0
- **VLAN 211:** Red IoMT Tipo 1 Planta 1
- **VLAN 212:** Red IoMT Tipo 1 Planta 2
- **VLAN 213:** Red IoMT Tipo 1 Planta 3
- **VLAN 220:** Red IoMT Tipo 2 Planta 3
- **VLAN 230:** Red IoMT Tipo 3 Planta 3
- **VLAN 250:** Interconexión Routers - Switch Core 1
- **VLAN 255:** Interconexión Routers - Switch Core 2

En el caso de la red de interconexión entre hospitales, se han definido las siguientes VLANs para el hospital de Son Espases:

- **VLAN 10:** RRHH (Recursos Humanos)
- **VLAN 20:** FyC (Finanzas y Contabilidad)
- **VLAN 30:** IT (Tecnologías de la Información)
- **VLAN 40:** SG (Servicios Generales)
- **VLAN 50:** SQ (Servicios Quirúrgicos)
- **VLAN 60:** SM (Servicios Médicos)
- **VLAN 70:** SC (Servicios Centrales)
- **VLAN 80:** UA (Unidad de Admisión)
- **VLAN 90:** UCI (Unidad de Cuidados Intensivos)
- **VLAN 100:** SU (Servicio de Urgencias)
- **VLAN 110:** CE (Consultas Externas)
- **VLAN 120:** AP (Atención al Paciente)
- **VLAN 130:** AJ (Asesoria Jurídica)
- **VLAN 140:** DeI (Docencia e Investigación)
- **VLAN 180:** DMZ Son Espases
- **VLAN 200:** Interconexión Switches Distribución - Switches Core

Para la red del Hospital de Manacor, se han definido las siguientes VLANs:

- **VLAN 210:** RRHH (Recursos Humanos)
- **VLAN 220:** FyC (Finanzas y Contabilidad)
- **VLAN 230:** IT (Tecnologías de la Información)
- **VLAN 240:** SG (Servicios Generales)
- **VLAN 250:** SQ (Servicios Quirúrgicos)
- **VLAN 260:** SM (Servicios Médicos)
- **VLAN 270:** SC (Servicios Centrales)
- **VLAN 280:** UA (Unidad de Admisión)
- **VLAN 290:** SU (Servicio de Urgencias)
- **VLAN 300:** CE (Consultas Externas)
- **VLAN 310:** AP (Atención al Paciente)
- **VLAN 320:** AJ (Asesoria Jurídica)

- **VLAN 380:** Interconexión Switches Distribución - Switches Core
- **VLAN 400:** DMZ Manacor

Para la red del Hospital Comarcal de Inca, se han definido las siguientes VLANs:

- **VLAN 410:** RRHH (Recursos Humanos)
- **VLAN 420:** FyC (Finanzas y Contabilidad)
- **VLAN 430:** IT (Tecnologías de la Información)
- **VLAN 440:** SG (Servicios Generales)
- **VLAN 450:** SQ (Servicios Quirúrgicos)
- **VLAN 460:** SM (Servicios Médicos)
- **VLAN 470:** SC (Servicios Centrales)
- **VLAN 480:** UA (Unidad de Admisión)
- **VLAN 490:** SU (Servicio de Urgencias)
- **VLAN 500:** CE (Consultas Externas)
- **VLAN 510:** UCI (Unidad de Cuidados Intensivos)
- **VLAN 520:** AP (Atención al Paciente)
- **VLAN 530:** AJ (Asesoria Jurídica)
- **VLAN 580:** Interconexión Switches Distribución - Switches Core
- **VLAN 600:** DMZ Inca

Para la red del Hospital Son Llàtzer, se han definido las siguientes VLANs:

- **VLAN 610:** RRHH (Recursos Humanos)
- **VLAN 620:** FyC (Finanzas y Contabilidad)
- **VLAN 630:** IT (Tecnologías de la Información)
- **VLAN 640:** SG (Servicios Generales)
- **VLAN 650:** SQ (Servicios Quirúrgicos)
- **VLAN 660:** SM (Servicios Médicos)
- **VLAN 670:** SC (Servicios Centrales)
- **VLAN 680:** UA (Unidad de Admisión)
- **VLAN 690:** SU (Servicio de Urgencias)
- **VLAN 700:** CE (Consultas Externas)

- **VLAN 710:** UCI (Unidad de Cuidados Intensivos)
- **VLAN 720:** AP (Atención al Paciente)
- **VLAN 730:** AJ (Asesoria Jurídica)
- **VLAN 740:** DeI (Docencia e Investigación)
- **VLAN 780:** Interconexión Switches Distribución - Switches Core
- **VLAN 800:** DMZ Son Llàtzer

En el caso de la red de Son Espases, se ha optado por configurar solamente los departamentos mostrados anteriormente, realmente hay muchos mas departamentos [3], pero con el objetivo de no duplicar esfuerzos en la configuración de dispositivos irrelevantes, se ha optado por no configurar el resto de departamentos.

En el caso de la red de interconexión entre hospitales, se ha optado por configurar todos los departamentos de los hospitales, con el fin de probar la conectividad desde cualquier area o departamento de un hospital a cualquier area o departamento de otro hospital.

### 5.3.2. Configuración de Troncales y Acceso a VLANs

Para garantizar el correcto funcionamiento de las VLANs y la segmentación del tráfico, es necesario configurar los puertos de los switches siguiendo el siguiente criterio:

- **Switches de Acceso (L2)**
  - **FastEthernet:** Son los puertos que conectan con los dispositivos finales (PCs, impresoras, servidores, etc.), se configuran en modo acceso, asignándolos a la VLAN correspondiente del departamento o servicio al que pertenecen.
  - **GigabitEthernet:** Son los puertos que conectan con los switches de distribución o routers (en el caso de los switches del DMZ), se configuran en modo troncal, permitiendo el tráfico de la VLAN definida en ese departamento o servicio.
- **Switches de Distribución (L3):** Todos los puertos deben estar configurados en modo troncal, permitiendo el tráfico de todas las VLANs necesarias.
- **Switches Core (L3):** Todos los puertos conectados a los switches de distribución deben estar configurados en modo troncal, permitiendo el tráfico de todas las VLANs necesarias. Los puertos que coenctan con los routers tienen dirección IP estática y por lo tanto no se configura el switchport en modo troncal.

## 5.4. Direccionamiento IP y Subnetting

Un correcto esquema de direccionamiento IP es esencial para garantizar la organización, la escalabilidad y la seguridad de cualquier infraestructura de red. En entornos

hospitalarios, donde coexisten diferentes tipos de dispositivos y servicios con requisitos de conectividad y seguridad distintos, la planificación del direccionamiento cobra especial relevancia.

Para este proyecto se ha diseñado un esquema jerárquico y estructurado, basado en subredes independientes para cada entorno funcional y departamental, facilitando la segmentación del tráfico, la implementación de políticas de seguridad y la gestión de direcciones IP.

### 5.4.1. Criterios de Diseño de Direccionamiento

El esquema de direccionamiento se ha planificado atendiendo a los siguientes criterios:

- Separación de subredes por tipo de servicio: red de invitados, red IoMT y red interna hospitalaria.
- Uso de rangos de direcciones IP privadas (192.168.0.0/16, 172.16.0.0/12 y 10.0.0.0/8), según las recomendaciones de la RFC 1918.
- Evitar solapamientos entre subredes y facilitar su integración en redes hospitalarias de mayor escala.
- Facilitar la implementación de ACLs y políticas de seguridad basadas en rangos de IP.
- Garantizar escalabilidad para añadir nuevos dispositivos, departamentos o servicios en el futuro.

### 5.4.2. Planificación de Subredes

En el diseño de la red del Hospital de Son Espases, se han definido tres grandes subredes principales:

- **Red Invitados:** 192.168.0.0/16
- **Red Interna:** 10.0.0.0/8
- **Red IoMT:** 172.16.0.0/12

Aparte de estas redes también están las subredes de interconexión entre switches y routers. En la tabla 5.1 podemos ver el subnetting completo de la red del Hospital de Son Espases. En la tabla se puede apreciar que hay 5 columnas, a continuación se muestra una breve descripción de cada una:

1. **Departamento:** Es el nombre del área o servicio funcional al que pertenece esa subred o VLAN. Por ejemplo: UCI.
2. **Network Address:** Es la dirección de red que identifica a toda la subred. Es la primera dirección del bloque de direcciones IP asignadas a esa subred y no puede asignarse a ningún dispositivo. Sirve para que los routers y switches reconozcan la red en su tabla de enrutamiento. Por ejemplo: 192.168.0.0.

3. **Máscara de Subred:** Es el valor que determina cuántos bits se utilizan para identificar la parte de red y cuántos para los hosts dentro de esa subred. Se expresa en notación decimal, por ejemplo 255.255.255.0.

4. **Rango de Direcciones Host:** Indica las direcciones IP que se pueden asignar a dispositivos dentro de esa subred. Es el intervalo de direcciones comprendido entre la primera dirección válida y la dirección anterior a la de broadcast. Por ejemplo, 192.168.0.1.

5. **Dirección Broadcast:** Es la última dirección de cada subred. Se utiliza para enviar mensajes simultáneos a todos los dispositivos de esa subred. No se puede asignar a ningún dispositivo. Por ejemplo, 192.168.0.255 para la subred 192.168.0.0/24.

**Nota:** *Las VLANs correspondientes a cada subred están definidas en la sección 5.3.1*

### Subnetting Son Espases

En la Tabla 5.1 se muestra en detalle el subnetting realizado en la red interna del Hospital Son Espases.

| Departamento | Network Address | Máscara de Subred | Direcciones Host | Dirección Broadcast |
|---|---|---|---|---|
| Recursos Humanos | 10.0.0.0 | 255.255.255.192 | 10.0.0.1 - 10.0.0.62 | 10.0.0.63 |
| Contabilidad | 10.0.0.64 | 255.255.255.192 | 10.0.0.65 - 10.0.0.126 | 10.0.0.127 |
| Oftalmología | 10.0.0.128 | 255.255.255.192 | 10.0.0.129 - 10.0.0.190 | 10.0.0.191 |
| Urología | 10.0.0.192 | 255.255.255.192 | 10.0.0.193 - 10.0.0.254 | 10.0.0.255 |
| Cardiología | 10.0.1.0 | 255.255.255.192 | 10.0.1.1 - 10.0.1.62 | 10.0.1.63 |
| Dermatología | 10.0.1.64 | 255.255.255.192 | 10.0.1.65 - 10.0.1.126 | 10.0.1.127 |
| Radiología | 10.0.1.128 | 255.255.255.192 | 10.0.1.129 - 10.0.1.190 | 10.0.1.191 |
| Inmunología | 10.0.1.192 | 255.255.255.192 | 10.0.1.193 - 10.0.1.254 | 10.0.1.255 |
| Unidad Admisión | 10.0.2.0 | 255.255.255.192 | 10.0.2.1 - 10.0.2.62 | 10.0.2.63 |
| UCI | 10.0.2.64 | 255.255.255.192 | 10.0.0.65 - 10.0.2.126 | 10.0.2.127 |
| Atención Paciente | 10.0.2.128 | 255.255.255.192 | 10.0.2.129 - 10.0.2.190 | 10.0.2.191 |
| Asesoría Jurídica | 10.0.2.192 | 255.255.255.192 | 10.0.2.193 - 10.0.2.254 | 10.0.2.255 |
| DMZ | 10.0.3.0 | 255.255.255.240 | 10.0.3.1 - 10.0.3.14 | 10.0.3.15 |

Tabla 5.1: Subnetting Red Interna Son Espases

En las Tablas 5.2, 5.3, 5.4, 5.5 y 5.6, se pueden apreciar el subnetting de las interconexiones anteriormente mencionadas.

| Dispositivos | Dirección IP |
|---|---|
| Switch Distribución 1 (Administración) | 10.1.0.1 |
| Switch Distribución 2 (Serv. Quirúrgicos) | 10.1.0.2 |
| Switch Distribución 3 (Serv. Médicos) | 10.1.0.3 |
| Switch Distribución 4 (Serv. Centrales) | 10.1.0.4 |
| Switch Distribución 5 (Enfermería) | 10.1.0.5 |
| Switch Distribución 6 (Apoyo) | 10.1.0.6 |
| Switch Core 1 | 10.1.0.7 |
| Switch Core 2 | 10.1.0.8 |
| Switch IoMT-P0 | 10.1.0.9 |
| Switch IoMT-P1 | 10.1.0.10 |
| Switch IoMT-P2 | 10.1.0.11 |
| Switch IoMT-P3 | 10.1.0.12 |

Tabla 5.2: Subnetting Red Interconexión Switches Distribución - Switches Core

| Dispositivo | Dirección IP |
|---|---|
| Switch Distribución 1 (Administración) | 10.1.1.1 |
| Switch Distribución 2 (Serv. Quirúrgicos) | 10.1.1.2 |
| Switch Distribución 3 (Serv. Médicos) | 10.1.1.3 |
| Switch Distribución 4 (Serv. Centrales) | 10.1.1.4 |
| Switch Distribución 5 (Enfermería) | 10.1.1.5 |
| Switch Distribución 6 (Apoyo) | 10.1.1.6 |

Tabla 5.3: Subnetting Red Interconexión Switches Distribuidores

| Dispositivo | Dirección IP |
|---|---|
| IP Virtual | 10.2.0.1 |
| Router Principal | 10.2.0.2 |
| Router Auxiliar 1 | 10.2.0.3 |
| Router Auxiliar 2 | 10.2.0.4 |
| Switch Core 1 | 10.2.0.5 |

Tabla 5.4: Subnetting Red Interconexión Switch Core 1 - Routers

| Dispositivo | Dirección IP |
|---|---|
| IP Virtual | 10.2.1.1 |
| Router Principal | 10.2.1.2 |
| Router Auxiliar 1 | 10.2.1.3 |
| Router Auxiliar 2 | 10.2.1.4 |
| Switch Core 1 | 10.2.1.5 |

Tabla 5.5: Subnetting Red Interconexión Switch Core 2 - Routers

| Dispositivo 1 | Dirección IP 1 | Dispositivo 2 | Dirección IP 2 |
|---|---|---|---|
| Router Principal | 195.136.17.2 | ISP 1 | 195.136.17.1 |
| Router Principal | 195.136.17.6 | ISP 2 | 195.136.17.5 |
| Router Auxiliar 1 | 195.136.17.10 | ISP 1 | 195.136.17.9 |
| Router Auxiliar 1 | 195.136.17.14 | ISP 2 | 195.136.17.13 |
| Router Auxiliar 2 | 195.136.17.18 | ISP 1 | 195.136.17.17 |
| Router Auxiliar 2 | 195.136.17.22 | ISP 2 | 195.136.17.21 |

Tabla 5.6: Subnetting Red Interconexión Routers - ISPs

En la Tabla 5.6 se puede apreciar que la red del Hospital Son Espases tiene como direcciones IP hacia Internet las siguientes:

- 195.136.17.1 (ISP 1)
- 195.136.17.9 (ISP 1)
- 195.136.17.17 (ISP 1)
- 195.136.17.5 (ISP 2)
- 195.136.17.13 (ISP 2)
- 195.136.17.21 (ISP 2)

### Subnetting IoMT

En la Tabla 5.7 se muestra en detalle el subnetting realizado en la red IoMT del Hospital Son Espases.

| Dispositivo | Network Address | Máscara de Subred | Direcciones Host | Dirección Broadcast |
|---|---|---|---|---|
| IoMT Tipo 1 Planta 0 | 172.16.0.0 | 255.255.240.0 | 172.16.0.1 - 172.16.15.254 | 172.16.15.255 |
| IoMT Tipo 1 Planta 1 | 172.16.16.0 | 255.255.240.0 | 172.16.16.1 - 10.0.0.126 | 172.16.31.255 |
| IoMT Tipo 1 Planta 2 | 172.16.32.0 | 255.255.240.0 | 172.16.32.1 - 10.0.0.190 | 172.16.47.255 |
| IoMT Tipo 1 Planta 3 | 172.16.48.0 | 255.255.240.0 | 172.16.48.1 - 10.0.0.254 | 172.16.63.255 |
| IoMT Tipo 2 | 172.16.64.0 | 255.255.192.0 | 172.16.64.1 - 172.64.127.254 | 172.16.127.255 |
| IoMT Tipo 3 | 172.16.128.0 | 255.255.192.0 | 172.16.128.1 - 172.128.191.254 | 172.16.191.255 |
| DMZ | 172.16.192.0 | 255.255.240.0 | 172.16.192.1 - 172.16.192.6 | 172.16.192.7 |

Tabla 5.7: Subnetting Red IoMT Son Espases

### Subnetting Invitados

En la Tabla 5.8 se muestra en detalle el subnetting realizado en la red de invitados del Hospital Son Espases.

| Dispositivo | Network Address | Máscara de Subred | Direcciones Host | Dirección Broadcast |
|---|---|---|---|---|
| Invitados | 192.168.0.0 | 255.255.128.0 | 192.168.0.1 - 192.168.127.254 | 192.168.127.255 |
| DMZ | 192.168.128.0 | 255.255.255.248 | 192.168.128.1 - 192.168.128.6 | 192.168.128.7 |

Tabla 5.8: Subnetting Red Invitados Son Espases

En la Tabla 5.9 se muestra el subnetting realizado en la interconexión de los routers con el switch de acceso de la red de invitados.

| Dispositivo | Dirección IP |
|---|---|
| IP Virtual | 192.168.130.1 |
| Router Principal | 192.168.130.2 |
| Router Auxiliar 1 | 192.168.130.3 |
| Router Auxiliar 2 | 192.168.130.4 |
| Switch Invitados | 192.168.130.5 |

Tabla 5.9: Subnetting Red Invitados Son Espases

### 5.4.3. Asignación de Direcciones IP Estáticas

Para el correcto funcionamiento de la red, es necesaria la definición de direcciones IP estáticas como por ejemplo las de las puertas de enlace o la de los servidores que dan servicios esenciales a la red interna, como el servidor DHCP.

#### Puertas de Enlace

En el diseño de la red de Son Espases, cada VLAN, excepto las de interconexión entre switches de distribución y switches core (que no tienen puerta de enlace), tiene su puerta de enlace configurada en los switches de distribución, ya que son los que permiten el enrutamiento. En la Tabla 5.10 se presentan las puertas de enlace de la red del Hospital Son Espases.

| VLAN | Dirección IP |
|---|---|
| 10 | 10.0.0.1 |
| 20 | 10.0.0.65 |
| 30 | 10.0.0.129 |
| 40 | 10.0.0.193 |
| 50 | 10.0.1.1 |
| 60 | 10.0.1.65 |
| 70 | 10.0.1.129 |
| 80 | 10.0.1.193 |
| 90 | 10.0.2.1 |
| 100 | 10.0.2.65 |
| 110 | 10.0.2.129 |
| 120 | 10.0.2.193 |
| 150 | 10.0.3.1 |
| 160 | 172.16.192.1 |
| 170 | 192.168.128.1 |
| 180 | 192.168.0.1 |
| 190 | 192.168.130.1 |
| 210 | 172.16.0.1 |
| 211 | 172.16.16.1 |
| 212 | 172.16.32.1 |
| 213 | 172.16.48.1 |
| 220 | 172.16.64.1 |
| 230 | 172.16.128.1 |
| 250 | 10.2.0.1 |
| 255 | 10.2.1.1 |

Tabla 5.10: Direcciones IP Estáticas de los Servidores de Son Espases

Las VLANs de interconexión 200 y 205 no tienen puertas de enlace, porque son VLANs en el que todos los puertos de los dispositivos implicados están configurados en modo troncal.

### Servidores

Para que los dispositivos tengan una dirección IP de referencia para poder acceder a los servidores, es necesario que esta sea estática, por eso a cada servidor de cada DMZ se le ha asignado una dirección IP estática. La Tabla 5.11 muestra las direcciones IP de todos los servidores de la red del Hospital Son Espases.

| Dispositivo | Dirección IP |
|---|---|
| Servidor DHCP DMZ Interno | 10.0.3.6 |
| Servidor DNS DMZ Interno | 10.0.3.7 |
| Servidor de Correo DMZ Interno | 10.0.3.8 |
| Servidor de Archivos DMZ Interno | 10.0.3.9 |
| Servidor DHCP DMZ Invitados | 192.168.128.5 |
| Servidor Web Invitados | 192.168.128.6 |
| Servidor DHCP DMZ IoMT | 172.16.192.5 |

Tabla 5.11: Direcciones IP Estáticas de los Servidores de Son Espases

**Dispositivos Finales**

Para garantizar las restricciones de acceso necesarias en los accesos a los dispositivos IoMT de tipo 3, se ha definido que un dispositivo del departamento de la UCI tenga una dirección IP estática, en este caso el PC de escritorio es el que tiene la dirección IP estática, que es 10.0.2.70.

Además, normalmente las impresoras también tienen direcciones IPs estáticas, para evitar problemas con el controlador de impresión, por eso en la red del hospital Son Espases, se ha definido que las impresoras tengan la cuarta dirección IP disponible para hosts de cada VLAN, así por ejemplo la impresora de la VLAN 10, tiene asignada la dirección IP 10.0.0.5 [5].

## 5.5. Protocolos y Servicios de Red

Para garantizar el correcto funcionamiento, la conectividad eficiente y la seguridad de la infraestructura hospitalaria diseñada, se han configurado una serie de protocolos de red y servicios esenciales. Estos protocolos permiten automatizar la asignación de direcciones, gestionar la conectividad entre dispositivos y hospitales, proteger las comunicaciones y asegurar la alta disponibilidad en los puntos críticos de la red.

### 5.5.1. DHCP (Dynamic Host Configuration Protocol)

El Dynamic Host Configuration Protocol (DHCP) se ha configurado para realizar la asignación automática de direcciones IP a los dispositivos finales conectados en cada subred y VLAN, según se detalla en la sección 2.4.1.

En el caso de la red del Hospital Son Espases, cuenta con:

- Un servidor DHCP en la DMZ Interna, que se encarga de asignar direcciones IP a cada dispositivo final de las red interna.
- Un servidor DHCP en la DMZ Invitados, que se encarga de asignar direcciones IP a cada dispositivo final de la red de invitados.
- Dos servidores DHCP en la DMZ IoMT, que se encargan de asignar direcciones IP a cada dispositivo IoMT de la red IoMT. En este caso, uno funciona de backup, para en caso de fallada del servidor principal, que los dispositivos IoMT sigan teniendo este servicio.

Mediante el uso de este servicio obtenemos las siguientes ventajas:

- Evitar conflictos de direcciones IP.
- Facilitar la gestión de direcciones en entornos con alta densidad de dispositivos.
- Separar la asignación de IPs entre subredes, manteniendo su aislamiento lógico.

En el caso de la red de interconexión entre hospitales, se cuenta con un servidor DHCP en la DMZ de cada hospital, que se encarga de asignar direcciones IP a cada dispositivo final del hospital.

Cabe recordar que en la herramienta Cisco Packet Tracer no se puede configurar la opción de DHCP failover, por eso el concepto de implementar dos servidores DHCP es teórico y no es demostrable en este proyecto.

### 5.5.2. NAT (Network Address Translation)

Para permitir la salida controlada a Internet desde las subredes autorizadas, se ha implementado Network Address Translation (NAT) en los routers de cada hospital, según se detalla en la sección 2.4.2. En ambos diseños, el NAT está configurado en los routers principales, permitiendo así que los dispositivos internos puedan acceder a Internet utilizando la misma IP pública. El tipo de NAT configurado es el PAT, lo que permite que múltiples dispositivos puedan utilizar la IP pública usando diferentes números de puerto para distinguir las conexiones.

En la red de inetrconexión entre hospitales, la interconexión entre routers se produce utilizando una subred con direcciones IP privadas, es decir, el NAT solo se usa para las peticiones hacia Internet.

### 5.5.3. HSRP (Hot Standby Router Protocol)

Para garantizar la alta disponibilidad en los gateways de las redes internas y evitar puntos únicos de fallo, se ha configurado HSRP, para mas información sobre HSRP ir a la sección 2.3.1. Como se ha comentado en la sección 5.1, la redundancia de routers o switches solo se ha configurado en la red del Hospital Son Espases. Concretamente, se ha configurado en los switches de distribución que conectan con los switches de acceso, como se puede apreciar en la Figura 5.16.

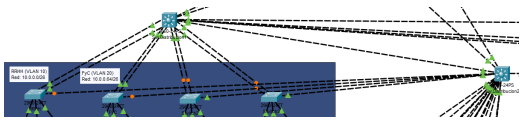


Figura 5.16: HSRP en Switches de Distribución en Hospital Son Espases

También se ha configurado HSRP en los routers principales, permitiendo así que haya dos routers de repuesto por si el router principal falla y deja de dar servicio. En la Figura 5.17 se pueden apreciar los tres routers redundantes.

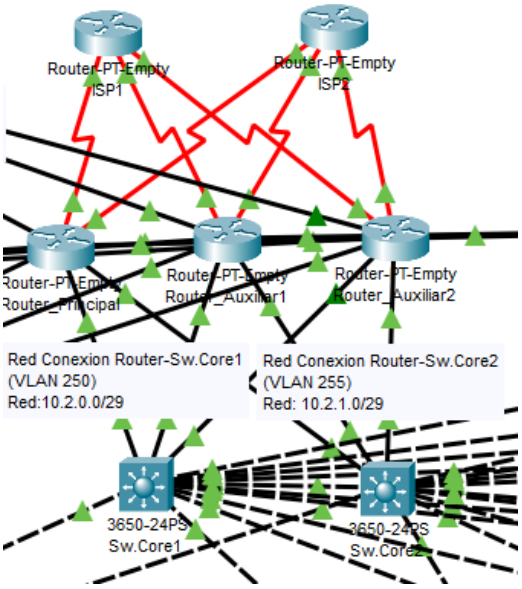



Figura 5.17: HSRP en Routers en Hospital Son Espases

### 5.5.4. OSPF (Open Shortest Path First)

Como protocolo de enrutamiento dinámico se ha implementado OSPF, detallado en la sección 2.2.1, tanto en la red del Hospital Son Espases como en la red de interconexión entre hospitales.

En el caso de la red del Hospital Son Espases, se ha añadido una configuración extra, que permite definir el coste de las rutas OSPF, de esta forma se ha configurado la red de interconexión entre switches de distribución y switches core para que tengan un coste de 10, mientras que la red de interconexión de switches de distribución tengan un coste de 100. De esta forma forzamos a que las comunicaicones se hagan directamente entre los switches de distirbución y los switches core y que las conexiones entre los switches de distribución sean meramente redudnantes y que no congestionen la red innecesariamente.

El protocolo OSPF se ha configurado, en ambos diseños, en cada switch L3 y en los routers, ya que son los dispositivos de red que tienen capacidad de enrutamiento.

### 5.5.5. EtherChannel

Para aumentar el ancho de banda y proporcionar redundancia en los enlaces entre switches de distribución y switches de acceso, se ha configurado EtherChannel, detallado en la sección 2.3.2.

Como se ha comentado en la sección 5.1, la redundancia a nivel de enlaces solo se ha configurado en la red del Hospital de Son Espases. A causa de las limitaciones de la herramienta Cisco Packet Tracer, referenciadas en la sección 1.3.2, solo se ha podido

implementar en algunas conexiones entre switches de acceso y switches de distribución, lo ideal sería implementarlo en tramos de mucho tráfico y en tramos donde hay una conexión entre elementos críticos, como por ejemplo la conexión entre los routers y los switches core.

En la Figura 5.18 se muestra una conexión redundante a nivel de enlace en la red del Hospital Son Espases.

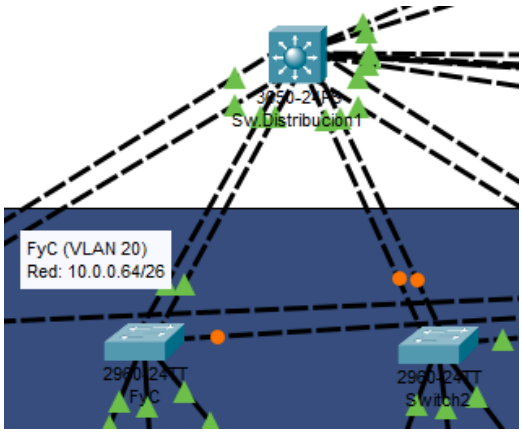



Figura 5.18: EtherChannel entre Switches de Acceso y Distribución en Hospital Son Espases

### 5.5.6. RSTP (Rapid Spanning-Tree Protocol)

## 5.6. Seguridad de la Red

El diseño de la infraestructura de red hospitalaria simulada ha priorizado desde el inicio la seguridad como pilar esencial, dada la sensibilidad de los datos clínicos que se gestionan y la criticidad de los servicios asistenciales que dependen de ella. Además, la incorporación de dispositivos médicos conectados (IoMT) requieren unos controles de tráfico y acceso mas robustos.

En esta sección, se detallan las medidas de seguridad adopatadas en ambos diseños de red.

### 5.6.1. ACLs

Las ACLs permiten tener un control del tráfico que pasa por ciertos tramos, es por eso que, siguiendo con los requisitos establecidos en la sección 3.2.4, se han implementado las siguientes ACLs:

- **En los routers:**
  - Permitir la conexión con Internet a los dispositivos de la red de invitados.
  - Permitir paquetes DHCP y OSPF.

- Denegar cualquier otro tipo de tráfico.

- **Switch IoMT Planta 3:**
  - Permitir la conexión de los dispositivos IoMT de tipo 1 con dispositivos de las áreas de servicios quirúrgicos, médicos y centrales.
  - Permitir la conexión de los dispositivos IoMT de tipo 2 con dispositivos del departamento de la UCI.
  - Permitir la conexión de los dispositivos IoMT de tipo 3 con el dispositivo autorizado de la UCI.
  - Permitir paquetes DHCP y OSPF.
  - Denegar cualquier otro tipo de tráfico.

- **Switch IoMT Planta 0,1 y 2:**
  - Permitir la conexión de los dispositivos IoMT de tipo 1 con dispositivos de las áreas de servicios quirúrgicos, médicos y centrales.
  - Permitir paquetes DHCP y OSPF.
  - Denegar cualquier otro tipo de tráfico.

- **Switches de Distribución:**
  - Denegar la salida de paquetes hacia las áreas de servicios quirúrgicos, médicos y centrales.
  - Permitir cualquier otro tipo de tráfico.

- **Routers de la red de interconexión:**
  - Denegar la conexión entre los dispositivos no autorizados con el servidor de archivos.
  - Denegar la conexión entre los dispositivos de otros hospitales con dispositivos del hospital.
  - Permitir cualquier otro tipo de tráfico.

### 5.6.2. DHCP Snooping

Para evitar ataques de DHCP Spoofing, se ha configurado DHCP Snooping en todos los switches de acceso que no tengan enlaces redundantes (EtherChannel), ya que la herramienta Cisco Packet Tracer no permite configurar DHCP Spoofing en enlaces redundantes. Con la configuración de este mecanismo de seguridad, conseguimos que los dispositivos finales solo acepten las direcciones IP dadas por los servidores DHCP autorizados, ya que el switch de acceso descarta cualquier oferta de dirección IP proveniente de un servidor DHCP no autorizado.

También se ha configurado la opción de limitar la cantidad de paquetes DHCP enviados al servidor DHCP para evitar saturaciones.

Este mecanismo de seguridad solo esta configurado en la red del Hospital de Son Espases.

### 5.6.3. IPSec

Para proprocionar seguridad a las interconexiones entre los routers de cada hospital, se ha configurado una IPsec (Internet Protocol Security), detallado en la sección 2.5.5, en el que se encriptan y autentican todos los paquetes IP que se transmiten a través de esa conexión. De esta forma conseguimos una gran capa de seguridad que nos garantiza la confidencialidad, integridad y autenticidad de los datos que viajan por esa red IP.

Este mecansimo de seguridad solo esta implementado en la red de interconexión entre hospitales, ya que la red del Hospital Son Espases no tiene conexiones entre routers de otros hospitales.

### 5.6.4. SSH

Para la administración remota segura de los dispositivos de red (routers y switches), se ha habilitado SSH como protocolo seguro de gestión, en sustitución de protocolos inseguros como Telnet. Esta configuración se ha implementado en todos los dispositivos de red (switches L2, switches L3 y routers).

### 5.6.5. Configuración DMZ

Para que la DMZ sea una zona segura para los servidores, se han implementado una serie de mecanismos de seguridad:

- **"switchport port-security maximum 1":** Limita el número máximo de direcciones MAC permitidas en el puerto a 1.

- **"switchport port-security mac-address sticky":** Activa el aprendizaje automático de direcciones MAC en modo "sticky", estas direcciones se almacenan en la configuración de ejecución, permitiendo que el puerto solo acepte dispositivos previamente conectados sin necesidad de configurar manualmente cada MAC.

- **"switchport port-security violation shutdown":** Deshabilita el puerto automáticamente cuando se detecta una violación de seguridad (por ejemplo, la conexión de un dispositivo con una MAC diferente a la permitida).

## 5.7. Redes Completas

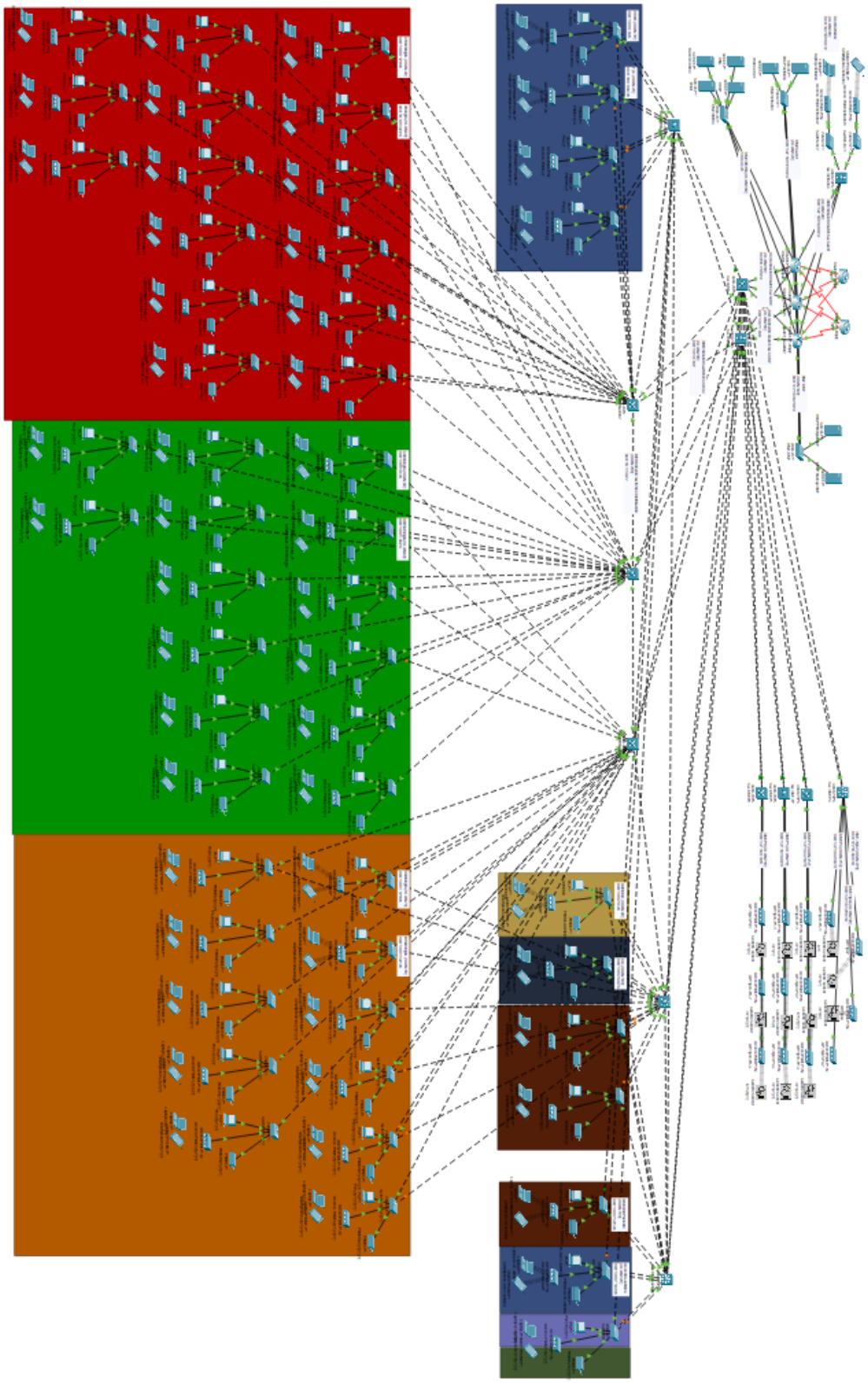


Figura 5.19: Red Completa del Hospital Son Espases

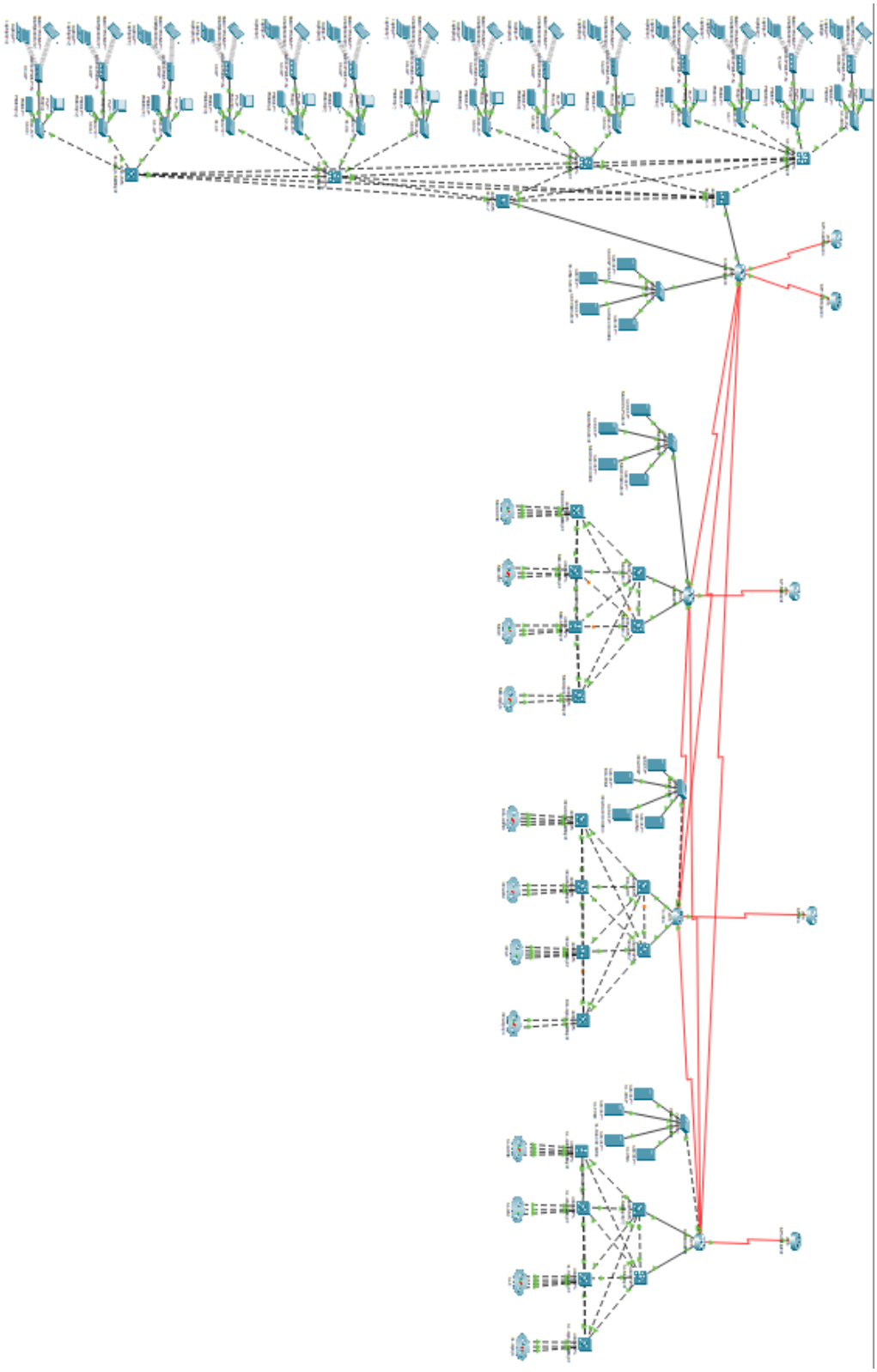


Figura 5.20: Red Completa de Interconexión entre Hospitales

### 5.7.1. Leyenda

Como se puede apreciar en la Figura 5.19, todas las areas estan coloreadas, esto es así para poder ubicarlas físicamente dentro del hospital, teniendo en cuenta lo mencionado en la sección 5.2.1.

- **Rojo:** Área de Servicios Quirúrgicos.
- **Verde:** Área de Servicios Médicos.
- **Naranja:** Área de Servicios Centrales.
- **Azul:** Área de Administración.
- **Azul oscuro:** UCI.
- **Amarillo:** Área de Hospitalización.
- **Verde oscuro:** Área de Investigación.
- **Marrón:** Área de Atención al Paciente.
- **Rosa:** Área de Servidores y Dispositivos de Red.
- **Morado:** Área de Docencia.

CAPÍTULO 6

# IMPLEMENTACIÓN

6.1. Configuración de Dispositivos

6.2. Creación de VLANs y Asignación de Puertos

6.3. Configuración de Direccionamiento IP

6.4. Configuración de Seguridad

6.5. Configuración de la Subred IoMT

CAPÍTULO 7

# PRUEBAS Y VALIDACIÓN

## 7.1. Pruebas de Conectividad

## 7.2. Pruebas de Seguridad

## 7.3. Resultados y Análisis

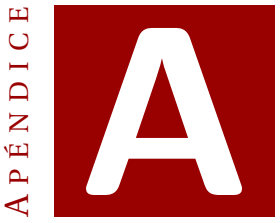
CAPÍTULO 8

# CONCLUSIÓN

## 8.1. Logros Alcanzados

## 8.2. Dificultades Encontradas

## 8.3. Mejoras y Ampliaciones Futuras




# ANEXO

# BIBLIOGRAFÍA


[1] E. HOSPITAL. (2023) ¿qué equipos son esenciales en la unidad de cuidados intensivos de un hospital? Accedido: xxxx-xx-xx. [Online]. Available: https://www.elhospital.com/es/noticias/que-equipos-son-esenciales-en-la-unidad-de-cuidados-intensivos-de-un-hospital 3.2.4

[2] H. U. S. Espases. (2010) Mapa virtual de l'hospital universitari son espases. Accedido: xxxx-xx-xx. [Online]. Available: https://www.youtube.com/watch?v=Q2pxgldGqak 5.2.1

[3] IBSALUT. Hospital universitario son espases - ponent. Accedido: xxxx-xx-xx. [Online]. Available: https://www.ibsalut.es/es/servicio-de-salud/organizacion/gerencias-ibsalut/gerencia-hospital-universitario-son-espases/hospital-universitari-son-espases 5.2.1, 5.3.1

[4] ——. Plantilla: Gerencia del hospital universitario son espases. Accedido: xxxx-xx-xx. [Online]. Available: https://www.ibsalut.es/es/profesionales/recursos-humanos/plantillas/gerencia-del-hospital-universitari-son-espases 5.2.1

[5] XEROX. Asignar o cambiar dirección ip de la impresora (dirección ip estática/fija). Accedido: xxxx-xx-xx. [Online]. Available: https://www.support.xerox.com/es-mx/article/KB0343702 5.4.3