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

IP Internet Protocol

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

NAT Network Address Translation

HSRP Hot Standby Router Protocol

SSH Secure Shell

ICMP Internet Control Message Protocol

MAC Media Access Control

IEEE Institute of Electrical and Electronics Engineers

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

LSDB Link-state Database

LSA Link-state Advertisements

SPF Shortest Path First

PAgP Port Aggregation Protocol

LACP Link Aggregation Control Protocol

PAT Port Address Translation

MITM Man In The Middle

IPSec Internet Protocol Security

LPWAN Low Power Wide Area Network

NB-IoT NarrowBand Internet of Things

LoRa Long Range

PC Personal Computer

RFC Request for Comments

ISP Internet Service Provider

AP Access Point

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 más 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 más 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, así como 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 Internet of Things (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 Virtual Local Area Network (VLAN)s 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 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 Internet Protocol (IP)** de la red hospitalaria, garantizando su correcto funcionamiento y escalabilidad.
- **Implementar medidas de seguridad a nivel lógico**, mediante el uso de Access Control List (ACL)s, segmentación de tráfico, configuración de resiliencia contra ataques 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 Llàtzer, 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 quirúrgicos, 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 Unidad de Cuidados Intensivos (UCI).
  - Limitar el acceso entre VLANs en función de criterios de seguridad departamentales.
- **Configuración de Demilitarized Zone (DMZ) específicas para cada subred**, con su propio servidor Dynamic Host Configuration Protocol (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.
  - **Domain Name System (DNS)** para la resolución de nombres de dominio internos.
  - **Network Address Translation (NAT)** para permitir el acceso a Internet desde las subredes internas.
  - **Hot Standby Router Protocol (HSRP)** para garantizar la alta disponibilidad de los routers principales.
  - **Secure Shell (SSH)** para la gestión segura de los dispositivos de red.
  - **Open Shortest Path First (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.
  - **Internet Protocol Security (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, lo que imposibilita que la interconexión entre hospitales tenga enlaces redundantes.
- Limitaciones de puertos en switches de distribución, lo que imposibilita que se configure HSRP en todos los switches de distribución que conectan con switches de acceso.
- La herramienta no permite la compatibilidad entre EtherChannel y DHCP Snooping, por lo que solo se ha podido implementar en los switches sin enlaces redundantes.

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 los protocolos implementados en el proyecto, una breve introducción a las redes en hospitales y una breve descripción de los dispositivos IoMT.
- **Capítulo 3: Análisis.** Se detallan las necesidades funcionales, de seguridad, de conectividad y de gestión que debe cubrir la red hospitalaria, 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 y las herramientas utilizadas.
- **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, la estructura de la subred específica para IoMT y la descripción de la configuración de los protocolos de red.

- **Capítulo 6: Implementación.** Se detalla la configuración de los dispositivos de red en Cisco Packet Tracer e implementación de los protocolos de red.
- **Capítulo 7: Pruebas y Validación.** Se describen las pruebas de conectividad, seguridad y funcionamiento realizadas sobre la red simulada y se presentan los resultados obtenidos.
- **Capítulo 8: Conclusión.** Se resumen los logros alcanzados 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 figuras complementarias.
- **Bibliografía.** Se recogen todas las fuentes de información utilizadas para la realización del proyecto, siguiendo el formato de citación Institute of Electrical and Electronics Engineers (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.

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 de núcleo. 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.

Esta estructura optimiza el rendimiento, la escalabilidad y la facilidad de mantenimiento, aspectos críticos en entornos hospitalarios donde la disponibilidad y la seguridad son prioritarias.

2.1.2. Segmentación de la Red

La segmentación mediante VLANs permite aislar el tráfico de diferentes áreas o servicios, mejorando la seguridad y el rendimiento. Cada VLAN constituye un dominio de broadcast independiente, permitiendo la aplicación de políticas específicas y reduciendo la propagación de tráfico innecesario.

2.2. Protocolos de Enrutamiento Dinámico

2.2.1. Open Shortest Path First (OSPF)

OSPF es un protocolo de enrutamiento de estado de enlace ampliamente utilizado en redes hospitalarias por su capacidad de rápida convergencia y soporte para redes complejas. Utiliza el algoritmo de Dijkstra para calcular rutas óptimas y mantiene una base de datos topológica completa en cada router, lo que permite una gestión eficiente y escalable del enrutamiento interno [1].

Funcionamiento Básico:

- Cada router mantiene una Link-state Database (LSDB) con información topológica completa de la red.
- Utiliza Link-state Advertisements (LSA)s para intercambiar información entre routers.
- Calcula rutas óptimas mediante el algoritmo Shortest Path First (SPF) de Dijkstra.

Algoritmo de Dijkstra

El algoritmo de Dijkstra, implementado en OSPF, calcula la ruta más corta entre nodos considerando los costos de enlace, lo que resulta esencial para garantizar la disponibilidad y eficiencia en la transmisión de datos críticos en hospitales.

2.3. Protocolos de Redundancia y Alta Disponibilidad

2.3.1. Hot Standby Router Protocol (HSRP)

HSRP es un protocolo propietario de Cisco que proporciona redundancia de gateway mediante la creación de un router virtual. Un router activo gestiona el tráfico, mientras que uno o más routers en standby asumen el control en caso de fallo, asegurando la continuidad del servicio [2].

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 permite agrupar múltiples enlaces físicos en un único enlace lógico, incrementando el ancho de banda, proporcionando redundancia y balanceando la carga de tráfico. Cisco soporta tanto Port Aggregation Protocol (PAgP) como Link Aggregation Control Protocol (LACP) (estándar IEEE) para la negociación de enlaces agregados [3]. Algunos beneficios que ofrece son:

- **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. Dynamic Host Configuration Protocol (DHCP)

DHCP automatiza la asignación de direcciones IP y otros parámetros de red, simplificando la gestión y reduciendo errores de configuración. En entornos hospitalarios, esto facilita la incorporación y administración de numerosos dispositivos médicos y administrativos. Su funcionamiento es el siguiente:

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.

2.4.2. Network Address Translation (NAT)

NAT permite que múltiples dispositivos compartan una única dirección IP pública, siendo esencial para la conectividad a Internet en redes hospitalarias [4]. 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.
- **Port Address Translation (PAT):** 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 desmilitarizadas.

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) [4]. 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 componentes 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. Secure Shell (SSH)

SSH es un protocolo de red que permite la administración segura de dispositivos a través de una conexión cifrada [4]. 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 (Man In The Middle (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 [4].

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 [5]. 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. Virtual Private Network Internet Protocol Security (VPN IPSec)

La Virtual Private Network (VPN) Internet Protocol Security (IPSec) es una tecnología que utiliza el conjunto de protocolos IPSec para crear túneles cifrados seguros a través de redes públicas, como Internet. Su función principal es garantizar la confidencialidad, integridad y autenticidad de los datos transmitidos entre dos puntos, protegiendo la información sensible frente a accesos no autorizados y ataques de intermediarios [6].

IPSec

IPSec es un conjunto de protocolos que proporciona seguridad a nivel de red mediante la autenticación y cifrado de paquetes IP. Esto permite que los datos enviados desde un origen sean cifrados y autenticados para que solo el destinatario legítimo pueda acceder a ellos. IPSec asegura además la integridad de los datos, evitando modificaciones durante la transmisión [6].

Modos de IPSec

IPSec opera principalmente en dos modos:

- **Modo Túnel:** Protege todo el paquete IP original, incluyendo encabezado y carga útil, encapsulándolo dentro de un nuevo paquete con un encabezado IPSec. Este modo es ideal para conexiones a través de redes públicas, ya que oculta la información original y proporciona un túnel seguro entre dos redes o dispositivos. Es el modo utilizado por las VPN IPSec para garantizar la privacidad y seguridad de extremo a extremo [6].

- **Modo Transporte:** Solo cifra la carga útil del paquete IP, dejando el encabezado original sin cifrar para que los enrutadores puedan dirigir el tráfico. Se utiliza en redes confiables o para comunicaciones directas entre dos dispositivos, por ejemplo, en conexiones cliente-servidor dentro de una misma organización [6].

Funcionamiento VPN IPSec

Una VPN IPSec crea un túnel cifrado entre dos puntos finales (por ejemplo, dos routers o un cliente y un servidor), permitiendo que los datos viajen de forma segura a través de redes no confiables [6]. El proceso incluye:

- Negociación de parámetros de seguridad mediante protocolos como ISAKMP/IKE para establecer asociaciones seguras.

- Establecimiento de claves criptográficas para cifrar y descifrar la información.

- Creación del túnel VPN que encapsula y protege el tráfico IP.

- Transmisión segura de datos autenticados y cifrados, con protección contra ataques de repetición y suplantación.

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 [7] [8].

En la práctica hospitalaria, la 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, dispositivos 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 [8].

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 (Low Power Wide Area Network (LPWAN)) como Sigfox, Long Range (LoRa) y NarrowBand Internet of Things (NB-IoT), que proporcionan conectividad eficiente para dispositivos médicos que requieren bajo consumo energético y cobertura extendida dentro y fuera de los centros sanitarios [7].

Desde el punto de vista arquitectónico, las soluciones IoMT han evolucionado hacia modelos distribuidos basados en edge/fog computing, donde los datos se procesan parcialmente 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 [9] [8].

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 [8].

En definitiva, la implantación del IoMT en entornos hospitalarios representa una oportunidad estratégica para transformar la asistencia sanitaria, dotándola de mayor

flexibilidad, capacidad predictiva y resiliencia frente a situaciones 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 [8].

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 (Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) y Reglamento General de Protección de Datos (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.

- 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 médicas, administrativas, de investigación y de enfermería.
- 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 (Personal Computer (PC)s del departamento de IT) 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 del hospital.
- 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.

- Las comunicaciones desde el exterior de la red hacia el interior tienen que pasar por una interfaz diferente de las que van desde el interior hacia el exterior.

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, de la red IoMT, deben contar con un servidor de respaldo para garantizar la asignación continua de direcciones IP.
- La infraestructura debe permitir la monitorización continua del estado de los dispositivos y enlaces para detectar fallos proactivamente.

3.2.4. 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.

- Todos los dispositivos de la red deben tener conectividad con cualquier dispositivo de la red.

3.2.5. 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 un PC autorizado del departamento de IT 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.
    - Solo permitir el tráfico desde Internet hasta el servidor web.

- 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 siguientes 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 monitorización remota 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 principal no es vital de forma inmediata. Estos dispositivos incluyen bombas de vacío para heridas, lámparas de fototerapia, dispositivos de rehabilitación, etc [10].

- **Dispositivos IoMT Críticos UCI (Tipo 3):** Son aquellos dispositivos que son críticos dentro de la UCI, es decir, son aquellos que permiten la monitorización y soporte vital de pacientes 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[10].

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 la asignación de direcciones IP y un servidor de respaldo para garantizar la continuidad del servicio.
- Los dispositivos IoMT Tipo 1 solo deben tener conectividad con los dispositivos de las áreas médicas de servicios quirúrgicos, médicos y centrales, además de 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.

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:

Plan de Acción	**Descripción**	**Fecha Inicio**	**Fecha Fin**
1. Reuniones Iniciales	Contextualización y primeros pasos del proyecto.	03/02/2025	10/02/2025
2. Definición Requisitos	Definir objetivos, alcance, limitaciones y requisitos del sistema.	10/02/2025	21/02/2025
3. Diseño de Red	Definir criterios de diseño, topología física y lógica.	21/02/2025	17/03/2025
4. Implementación	Configuración de las dos redes completadas en la herramienta Cisco Packet Tracer.	17/03/2025	16/05/2025
5. Pruebas	Pruebas de conectividad, seguridad, redundancia y servicios.	16/05/2025	23/05/2025
6. Documentación	Elaboración de la memoria.	23/05/2025	20/06/2025
7. Revisión y Entrega	Revisión de estilos, anexos y citaciones. Entrega del TFG.	20/06/2025	05/07/2025

Tabla 4.1: 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 Hot Standby Router Protocol (HSRP). Estos routers se conectan con:

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

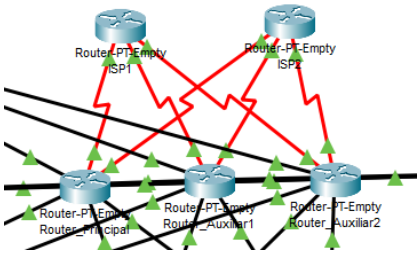


Figura 5.1: Redundancia en Routers

Además, estos routers están conectados a dos routers más, que simularían la conexión a Internet (Internet Service Provider (ISP) 1 y 2).

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 Access Point (AP) 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.

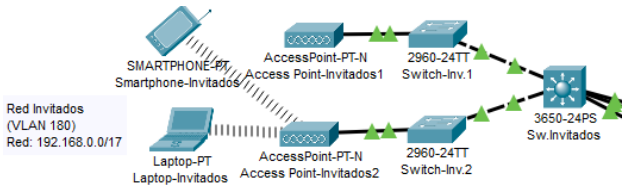


Figura 5.2: Topología Física de la Red de Invitados

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.

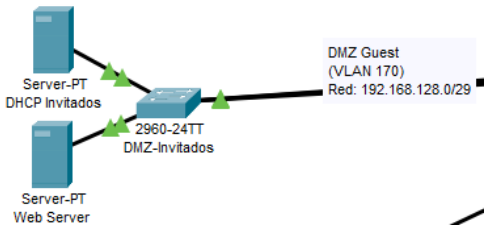


Figura 5.3: Topología Física de la DMZ de Invitados

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 dispositivos de Internet que quieran 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 dispositivos de la red, sin que estos servidores DHCP puedan ser detectados o accedidos 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.

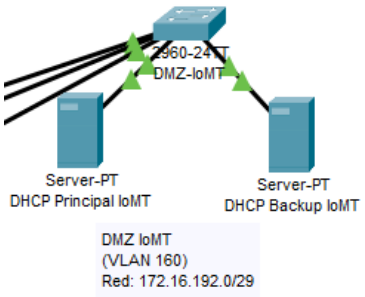


Figura 5.4: Topología Física de la DMZ IoMT

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.

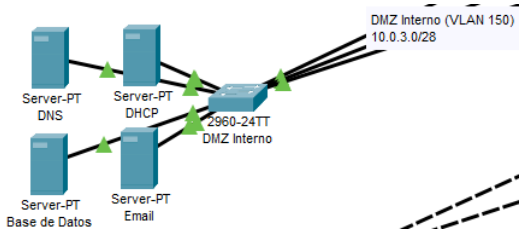


Figura 5.5: Topología Física de la DMZ Interna

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.

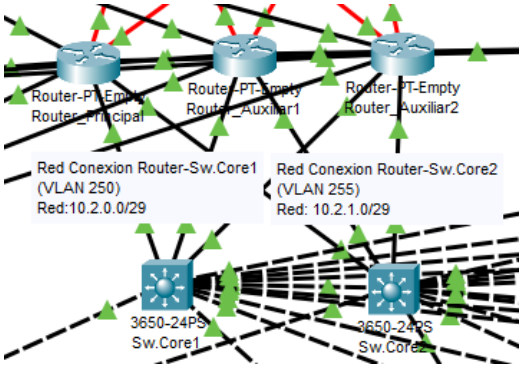


Figura 5.6: Interconexión de Switches Core

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 está conectado a otros 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.

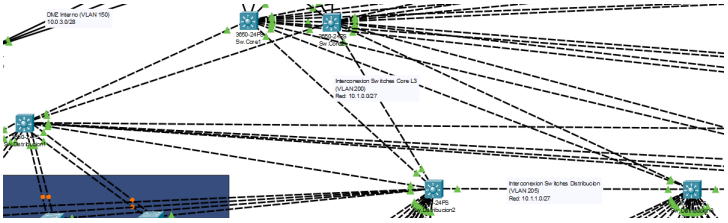


Figura 5.7: Interconexión de Switches de Distribución

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.

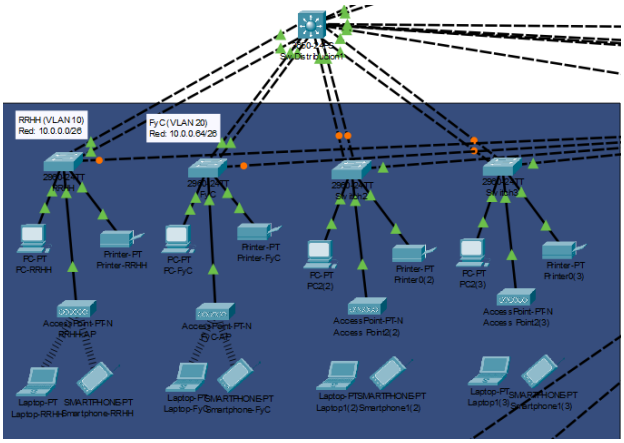


Figura 5.8: Interconexión de Switches de Acceso

Como se puede ver en la Figura 5.8, cada departamento está 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, teniendo en cuenta que el límite de direcciones IP asignables son 56.

Red IoMT

La red IoMT está 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 está 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 conectarse a otro punto de acceso bajo el mismo SSID.

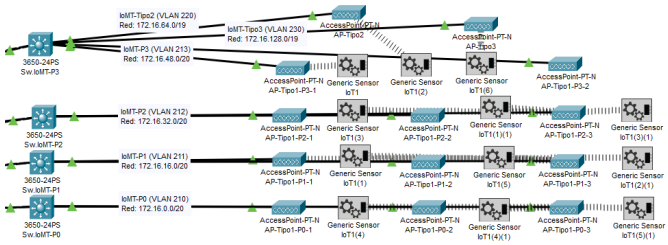


Figura 5.9: Topología Física de la Red de Dispositivos IoMT

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 más 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 [11].

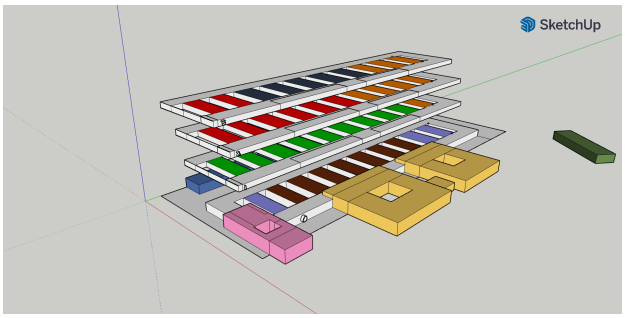


Figura 5.10: Disposición Física Elementos de Red del Hospital Son Espases

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 [12] o el documento oficial de la plantilla del Hospital Universitario de Son Espases [13].

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 3.2.5*

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.

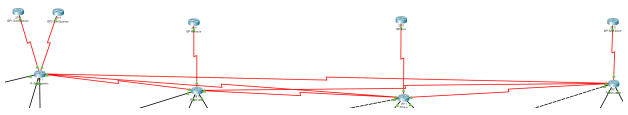


Figura 5.11: Topología Física de la Interconexión entre Hospitales

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 en los requisitos del sistema se definió así (3).

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.

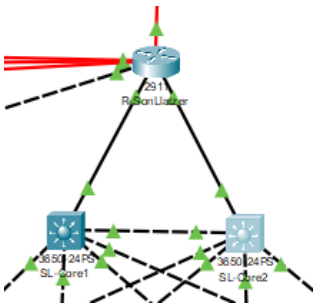


Figura 5.12: Topología Física de la Interconexión entre el Router y los Switches Core en Hospitales

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.

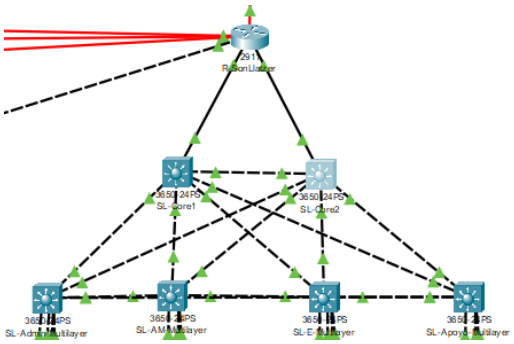


Figura 5.13: Topología Física de la Interconexión entre los Switches L3 en Hospitales

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.

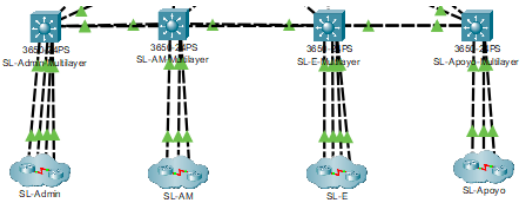


Figura 5.14: Topología Física de la Interconexión con Clusters en Hospitales

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.

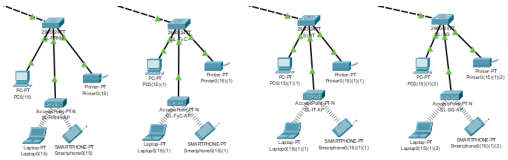


Figura 5.15: Topología Física de la Interconexión con Clusters en Hospitales

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:** Recursos Humanos (RRHH)
- **VLAN 20:** Finanzas y Contabilidad (FyC)
- **VLAN 30:** Oftalmologia
- **VLAN 40:** Urologia
- **VLAN 50:** Cardiologia
- **VLAN 60:** Dermatologia
- **VLAN 70:** Radiologia
- **VLAN 80:** Inmunologia
- **VLAN 90:** Admision
- **VLAN 100:** Unidad de Cuidados Intensivos (UCI)
- **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:** Recursos Humanos (RRHH)
- **VLAN 20:** Finanzas y Contabilidad (FyC)
- **VLAN 30:** Tecnologías de la Información (IT)
- **VLAN 40:** Servicios Generales (SG)
- **VLAN 50:** Servicios Quirúrgicos (SQ)
- **VLAN 60:** Servicios Médicos (SM)
- **VLAN 70:** Servicios Centrales (SC)
- **VLAN 80:** Unidad de Admisión (UA)
- **VLAN 90:** Unidad de Cuidados Intensivos (UCI)
- **VLAN 100:** Servicio de Urgencias (SU)
- **VLAN 110:** Consultas Externas (CE)
- **VLAN 120:** Atención al Paciente (AP)
- **VLAN 130:** Asesoria Jurídica (AJ)
- **VLAN 140:** Docencia e Investigación (DeI)
- **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:** Recursos Humanos (RRHH)
- **VLAN 220:** Finanzas y Contabilidad (FyC)
- **VLAN 230:** Tecnologías de la Información (IT)
- **VLAN 240:** Servicios Generales (SG)
- **VLAN 250:** Servicios Quirúrgicos (SQ)
- **VLAN 260:** Servicios Médicos (SM)
- **VLAN 270:** Servicios Centrales (SC)
- **VLAN 280:** Unidad de Admisión (UA)
- **VLAN 290:** Servicio de Urgencias (SU)
- **VLAN 300:** Consultas Externas (CE)
- **VLAN 310:** Atención al Paciente (AP)
- **VLAN 320:** Asesoria Jurídica (AJ)

- **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:** Recursos Humanos (RRHH)
- **VLAN 420:** Finanzas y Contabilidad (FyC)
- **VLAN 430:** Tecnologías de la Información (IT)
- **VLAN 440:** Servicios Generales (SG)
- **VLAN 450:** Servicios Quirúrgicos (SQ)
- **VLAN 460:** Servicios Médicos (SM)
- **VLAN 470:** Servicios Centrales (SC)
- **VLAN 480:** Unidad de Admisión (UA)
- **VLAN 490:** Servicio de Urgencias (SU)
- **VLAN 500:** Consultas Externas (CE)
- **VLAN 510:** UCI (Unidad de Cuidados Intensivos)
- **VLAN 520:** Atención al Paciente (AP)
- **VLAN 530:** Asesoria Jurídica (AJ)
- **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:** Recursos Humanos (RRHH)
- **VLAN 620:** Finanzas y Contabilidad (FyC)
- **VLAN 630:** Tecnologías de la Información (IT)
- **VLAN 640:** Servicios Generales (SG)
- **VLAN 650:** Servicios Quirúrgicos (SQ)
- **VLAN 660:** Servicios Médicos (SM)
- **VLAN 670:** Servicios Centrales (SC)
- **VLAN 680:** Unidad de Admisión (UA)
- **VLAN 690:** Servicio de Urgencias (SU)
- **VLAN 700:** Consultas Externas (CE)

- **VLAN 710:** UCI (Unidad de Cuidados Intensivos)
- **VLAN 720:** Atención al Paciente (AP)
- **VLAN 730:** Asesoria Jurídica (AJ)
- **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 [12], 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 conectan 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 Request for Comments (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 [14].

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. Dynamic Host Configuration Protocol (DHCP)

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.

Los servidores están configurados con pools de direcciones, de forma que asignan IPs dinámicas a los dispositivos de cada VLAN, siguiendo el subnetting mostrado en la sección 5.1.

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. Network Address Translation (NAT)

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, en el caso de la comunicación desde dentro hacia fuera, es el PAT, lo que permite que múltiples dispositivos puedan utilizar la IP pública usando diferentes números de puerto para distinguir las conexiones. En el caso de las comunicaciones desde Internet hacia dentro (servidor web), se ha configurado un NAT estático, lo que permite que el router traduzca la dirección pública proveniente del ISP y permitir la conexión con el servidor web, que tiene una IP privada.

En este diseño, se ha optado por que las comunicaciones que vyan desde dentro hacia fuera vayan por el ISP 1 y las comunicaciones desde fuera hacia dentro vayan por el ISP 2, de esta forma permitimos que las NATs estén bien configuradas y que no solapen las IPs públicas de las interfaces.

5.5.3. Hot Standby Router Protocol (HSRP)

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.

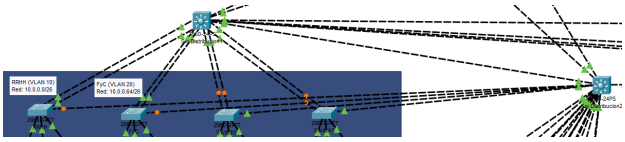


Figura 5.16: HSRP en Switches de Distribución en Hospital Son Espases

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.

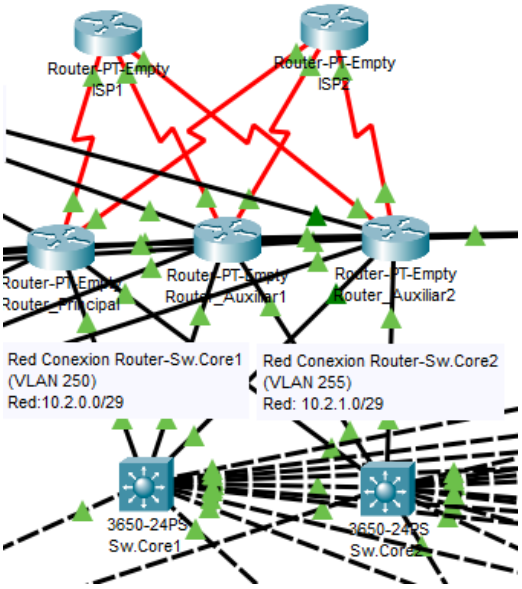


Figura 5.17: HSRP en Routers en Hospital Son Espases

5.5.4. Open Shortest Path First (OSPF)

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.

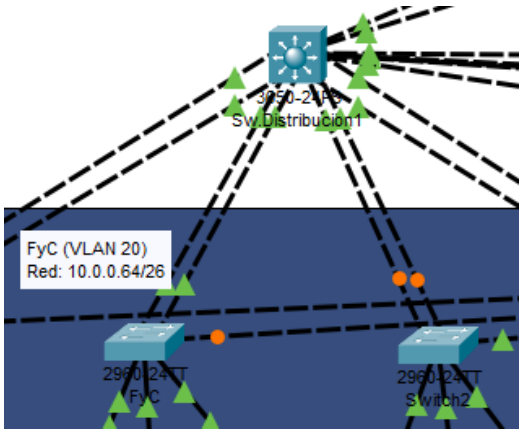


Figura 5.18: EtherChannel entre Switches de Acceso y Distribución en Hospital Son Espases

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 3.2.5, se han implementado las siguientes ACLs:

- **En los routers:**
  - Permitir la conexión con Internet a los dispositivos de la red de invitados.
  - Permitir la conexión desde Internet hasta el servidor web.

- Permitir paquetes DHCP, OSPF y HSRP.
- 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 [5].

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 está configurado en la red del Hospital de Son Espases.

5.6.3. VPN IPSec

Para proprocionar seguridad a las interconexiones entre los routers de cada hospital, se ha configurado una VPN IPsec, detallada en la sección 2.5.5, en la 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. Además cabe recordar que la comunicación entre hospitales solo se puede realizar entre el dispositivo autorizado de un hospital con el servidor de archivos de otro hospital.

5.6.4. Secure Shell (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 Media Access Control (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

Para ver las redes completas de la red del Hospital Son Espases y la red de interconexión entre hospitales, ver el anexo A.36 y A.37, respectivamente.

5.7.1. Leyenda

Como se puede apreciar en la Figura A.37, 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

Una vez definidos los diseños de las infraestructuras de redes hospitalarias, es necesario proceder a su implementación, configurando todos los dispositivos de red, servicios y políticas de seguridad conforme a la planificación establecida. Esta fase es clave para materializar las decisiones de diseño en un entorno funcional y operativo, permitiendo comprobar la viabilidad técnica de la solución propuesta y sentando las bases para su posterior validación.

En este capítulo se describe el proceso de configuración y puesta en funcionamiento de la red simulada en Cisco Packet Tracer, abarcando la configuración básica de los dispositivos de red, la creación de las VLANs, implementación de mecanismos de redundancia, direccionamiento IP, mecanismos de seguridad y servicios esenciales como DHCP o NAT.

Durante la implementación se han seguido los criterios de diseño definidos en capítulos anteriores, adaptando cada configuración a las limitaciones y capacidades del entorno de simulación empleado.

Este capítulo detalla paso a paso el trabajo realizado en la implementación de las redes hospitalarias, siguiendo una estructura ordenada y temporal de las configuraciones realizadas.

6.1. Configuración Básica de Dispositivos

En ambos diseños, cada dispositivo de red cuenta con una configuración básica, que incluye lo siguiente:

- Cambiar el hostname, por el correspondiente a cada dispositivo.

- Configuración de la contraseña genérica çisco"para poder acceder a la configuración de los dispositivos.
- Configuración de la contraseña genérica çisco"para poder acceder a la línea de comandos de los dispositivos.
- Encriptar contraseñas.
- Configuración de SSH para la gestión remota, usando encriptación RSA de 1024 bits.

De esta forma se consigue que cada dispositivo de red cuente con varias capas básicas de seguridad, que evitan el acceso no autorizado a la línea de comandos. Además, se cuenta con un servicio de gestión remota, utilizando un protocolo de red seguro como es SSH.

Para ver los comandos utilizados, ir al anexo A.1.

6.2. Creación de VLANs y Asignación de Puertos

En ambos diseños, las VLANs se han configurado tanto en los switches L2 (Acceso) como en los switches L3 (Distribución y Core). Cada switch cuenta con una configuración diferente, ya que cada uno tiene una función distinta dentro de la red.

6.2.1. VLANs en Switches de Acceso

En los switches de acceso, se ha definido la VLAN correspondiente al departamento o DMZ que da servicio el switch de acceso y seguidamente se han configurado los puertos conectados a los dispositivos en modo access de forma que solo se transmita la VLAN del departamento o DMZ. En el caso de los puertos conectados a los switches de distribución, los puertos se han configurado en modo trunk, de esta forma se pueden transmitir varias VLANs [15].

Ver el anexo A.2, para visualizar una plantilla de los comandos usados en esta configuración.

6.2.2. VLANs en Switches de Distribución

En los switches de distribución, se han definido todas las VLANs de los distintos departamentos de la red, pero dependiendo de sus conexiones directas, los puertos se han configurado de una forma u otra:

- **En conexiones con switches de acceso:** Los puertos se han configurado en modo trunk, transmitiendo únicamente la VLAN del departamento correspondiente.
- **En conexiones con switches de distribución:** Los puertos se han configurado en modo trunk, transmitiendo las VLANs del área del hospital al cual da servicio y la VLAN de interconexión entre switches de distribución (VLAN 205). En el caso de los de la red IoMT, se usa la VLAN de interconexión con los switches core (VLAN 200), ya que estos no tienen red de interconexión entre switches de distribución.

- **En conexiones con switches core:** Los puertos se han configurado en modo trunk, transmitiendo las VLANs del área del hospital al cual da servicio y la VLAN de interconexión entre switches de distribución y switches core (VLAN 200).

Ver el anexo A.3, para visualizar una plantilla de los comandos usados en esta configuración.

6.2.3. VLANs en Switches Core

En los switches core, se han definido todas las VLANs de la red interna y IoMT y seguidamente se han configurado los puertos que conectan con los switches de distribución de forma que solo se transmitan las VLANs que abarca cada switch de distribución. En el caso de la conexión con el otro switch core, se configura el puerto de forma que se transmitan todas las VLANs de la red interna y IoMT.

Ver el anexo A.4, para visualizar una plantilla de los comandos usados en esta configuración.

6.3. Implementación EtherChannel

En la red del Hospital Son Espases se configuró EtherChannel entre los switches de acceso y los de distribución para conseguir redundancia a nivel de enlaces. Para ello, se tuvieron que configurar tanto el switch de acceso como el switch de distribución. La única diferencia entre la configuración entre los switches es que en los switches de distribución hay que hacer el port-channel entre enlaces GigabitEthernet, mientras que en los switches de acceso se hace en enlaces FastEthernet.

Para ver los comandos utilizados para implementar EtherChannel, ver el anexo A.5.

6.4. Seguridad en DMZ

Para garantizar la seguridad en las DMZ, se han implementado algunas configuraciones básicas de seguridad, detalladas en la sección 5.6.5.

Para ver los comandos utilizados para implementar las medidas de seguridad en la DMZ, ver el anexo A.6.

6.5. Implementación de Direccionamiento IP

Para que las redes puedan tener conectividad es necesaria la implementación del direccionamiento IP. En el caso de la red del Hospital Son Espases, se ha implementado HSRP, que permite obtener redundancia a nivel de hardware/dispositivo. Además, también se ha implementado un direccionamiento IP estático en los elementos de la red que necesitasen este recurso. Para más detalles, ver la sección 5.4.

6.5.1. Implementación HSRP

La implementación de HSRP conlleva la asignación de una IP virtual, que será la accedida por los demás dispositivos; a su vez, también hay que asignar una dirección IP a cada dispositivo que tenga configurado HSRP, cada uno con una prioridad diferente.

La configuración de HSRP en routers y en switches L3 difiere un poco, ya que en los routers no se pueden definir VLANs y, por tanto, no se puede transmitir la información de una VLAN en concreto por un enlace. Es por eso que hay que crear una subinterfaz que permita la transmisión de paquetes provenientes de una VLAN.

Para ver los comandos utilizados para configurar HSRP en routers, ver el anexo A.8.

Para ver los comandos utilizados para configurar HSRP en switches L3, ver el anexo A.7.

6.5.2. Direccionamiento Estático

En ambas redes hospitalarias es necesario el direccionamiento IP estático. Para más detalles, ver la sección 5.4.3. Para ver los comandos utilizados para configurar el direccionamiento IP estático, ver el anexo A.9.

6.5.3. DHCP Relay

DHCP Relay es una función que permite que los clientes DHCP en una red o subred reciban direcciones IP y otros parámetros de configuración de un servidor DHCP ubicado en una red diferente [16]. En ambas redes, el servidor DHCP está ubicado en otra VLAN o subred, por lo que, sabiendo la IP estática del servidor DHCP, hay que definirla en las interfaces VLAN de los switches de distribución.

Para ver el comando utilizado para configurar el DHCP Relay, ver el anexo A.10.

6.6. Implementación OSPF

Para la implementación de OSPF en las redes, simplemente hay que definir a qué redes está cada dispositivo conectado. De esta forma, se van comunicando las redes a las que está conectado cada dispositivo de red, permitiendo que otros dispositivos que no están conectados directamente sepan a qué redes están conectados estos. Para más detalles, ver la sección 2.2.1.

Para ver una plantilla de los comandos utilizados para configurar OSPF, ver el anexo A.11.

6.7. Implementación RSTP

Rapid Spanning Tree Protocol (RSTP) está diseñado para proporcionar una convergencia mucho más rápida en redes Ethernet con topologías redundantes [17]. En el caso de la red del Hospital Son Espases, esta configuración es muy útil, ya que mejora

consistentemente la eficiencia y el rendimiento de la red.

Para ver los comandos utilizados para configurar RSTP en los switches L3, ver el anexo A.12.

6.8. Implementación NAT

Para implementar el servicio NAT en los routers de los hospitales, hay que hacer los siguientes pasos:

- Definir como nat outside las interfaces de los routers que dirigen tráfico hacia fuera de la red.
- Definir como nat inside las interfaces de los routers que dirigen tráfico hacia el interior de la red.
- Crear listas de control de acceso que permitan saber qué subredes se van a beneficiar de este servicio.
- Crear las NAT asignándoles las listas de control de acceso a las interfaces pertinentes.

Para ver las NAT configuradas en los routers principales, siguiendo el diseño propuesto en la sección 2.4.2, ver el anexo A.13 para la configuración para el NAT en la interfaz que conecta con el ISP 1 y ver el anexo A.14 para la configuración para el NAT en la interfaz que conecta con el ISP 2.

6.9. Implementación DHCP Snooping

DHCP Snooping es una función de seguridad de Capa 2 en switches que protege la red contra diversos ataques. Ver la sección 2.5.4 para más detalles. Para implementar la configuración de seguridad de DHCP Snooping, hay que seguir los siguientes pasos:

- Activar DHCP snooping en el dispositivo.
- Activar DHCP snooping en la VLAN del departamento del switch de acceso correspondiente.
- Limitar la cantidad de paquetes DHCP en todas las interfaces.
- Asignar la etiqueta trust a las interfaces por las que deberían venir los paquetes DHCP del servidor autorizado.

Para ver una plantilla de los comandos utilizados para configurar DHCP Snooping en los switches de acceso, ver el anexo A.15.

6.10. Implementación ACLs

Teniendo en cuenta las ACLs que se deben implementar, detalladas en la sección 5.6.1, se han implementado de la siguiente forma en los dispositivos de red correspondientes.

- **En los routers:** Ver anexo A.18.
- **Switch IoMT Planta 3:** Ver anexo A.16.
- **Switch IoMT Planta 0, 1 y 2:** Ver anexo A.17.
- **Switches de Distribución:** Ver anexo A.19.
- **Routers de la red de interconexión:** Ver anexo A.20.

6.11. Implementación VPN

Para la implementación de la VPN, hay que seguir los siguientes pasos:

- Cargar un módulo de lanzamiento en los routers, que posibilita la configuración de las VPN.
- Configurar las claves de autenticación.
- Configurar el túnel IPSec.
- Configurar el mapa de la VPN.
- Asignar el mapa de la VPN a la interfaz que conecta con los demás routers.
- Crear ACLs que permitan el tráfico entre los dispositivos autorizados para la comunicación.

Para ver el ejemplo de los comandos utilizados para implementar la VPN entre los hospitales de Son Espases y de Manacor, ver el anexo A.21.

6.12. Configuraciones Completas

Para ver las configuraciones específicas de cada dispositivo de red, ir al anexo A.22.

CAPÍTULO 7

PRUEBAS Y VALIDACIÓN

Una vez completada la implementación de la infraestructura de red hospitalaria simulada, resulta imprescindible realizar un proceso de pruebas y validación que permita verificar que la red funciona correctamente, cumple con los requisitos establecidos y garantiza los niveles de seguridad, segmentación y disponibilidad previstos en el diseño.

El propósito de este capítulo es detallar el conjunto de pruebas funcionales, de conectividad, de seguridad y de tolerancia a fallos realizadas sobre la red implementada en Cisco Packet Tracer. Estas pruebas permiten detectar posibles errores de configuración, comprobar la eficacia de las políticas de acceso y confirmar la correcta comunicación entre los diferentes dispositivos, subredes y hospitales.

Las pruebas se han clasificado según su naturaleza:

- Pruebas de Conectividad.
- Pruebas de Seguridad.
- Pruebas de Disponibilidad.
- Pruebas de Protocolos de red.

Este capítulo documenta los resultados obtenidos en cada prueba, analizando su comportamiento frente a los objetivos planteados y proponiendo, en su caso, mejoras o ajustes sobre la configuración para optimizar la fiabilidad y seguridad de la red hospitalaria diseñada.

7.1. Pruebas de Conectividad

A continuación se muestran las pruebas de conectividad realizadas:

- Conectividad entre dispositivos de la red interna con Internet.

- Conectividad entre dispositivos de la red de invitados con Internet.
- Conectividad entre Internet y el servidor web del hospital.

7.1.1. Conectividad de Dispositivos Internos con Internet

Para comprobar que hay conectividad entre los dispositivos de la red interna con Internet, hay que hacer un ping desde un dispositivo conectado a la red interna hasta la puerta de enlace del ISP 1, que es el que da acceso a Internet.

Para ver la salida por consola del ping realizado en el PC conectado a la red interna, ver el anexo A.30.1.

7.1.2. Conectividad de Dispositivos Invitados con Internet

Para comprobar que hay conectividad entre los dispositivos de la red de invitados con Internet, hay que hacer un ping desde un dispositivo conectado a la red de invitados hasta la puerta de enlace del ISP 1, que es el que da acceso a Internet.

Para ver la salida por consola del ping realizado en el portátil conectado a la red de invitados, ver el anexo A.30.2.

7.1.3. Conectividad de Internet con Servidor Web

Para comprobar que hay conectividad entre Internet y el servidor web, hay que hacer un ping desde el ISP 2 hasta la puerta de enlace con el router del hospital, ya que el NAT estático configurado es el que se encarga de redirigir el tráfico hasta el servidor web del hospital.

Para ver la salida por consola del ping realizado desde Internet hasta el servidor web del hospital, ver el anexo A.30.3.

7.2. Pruebas de Seguridad

A continuación se muestran las pruebas de seguridad realizadas:

- Encriptación del tráfico entre hospitales (VPN IPSec).
- Correcto funcionamiento de DHCP Snooping.
- Correcto funcionamiento de la gestión remota mediante SSH.
- Configuración de autenticación en los dispositivos de red.
- Bloqueo de tráfico no autorizado mediante ACLs:
    - Bloqueo de tráfico entre dispositivos de áreas administrativas con dispositivos de áreas médicas o UCI.
    - Bloqueo de tráfico entre dispositivos de áreas administrativas con dispositivos IoMT.

- Bloqueo de tráfico entre dispositivos de la red de invitados con dispositivos de la red interna o IoMT.
- Bloqueo de tráfico entre dispositivos no autorizados con el servidor de archivos de otro hospital.

- Permiso de tráfico mediante ACLs:
  - Conectividad entre dispositivos de áreas médicas con dispositivos de la UCI.
  - Conectividad entre dispositivos de áreas médicas con dispositivos IoMT tipo 1.
  - Conectividad entre dispositivos de la UCI con dispositivos IoMT tipo 2.
  - Conectividad entre el dispositivo autorizado de la UCI con dispositivos IoMT tipo 3.
  - Conectividad entre el dispositivo autorizado de un hospital con el servidor de archivos de otro hospital.

7.2.1. VPN IPSec

Para comprobar que la VPN está bien configurada y que se encriptan todos los paquetes que pasan por la red, basta con insertar el comando "show crypto ipsec saz fijarse en la interfaz que conecta con el router con el cual se han intercambiado paquetes, habiendo realizado previamente una comunicación entre dos dispositivos de dos hospitales.

Para ver la salida por consola del comando aplicado, ver el anexo A.28. En este caso, se ha realizado un par de pings desde el PC de IT del hospital de Manacor hasta el servidor de archivos del hospital Son Espases, y se ha insertado el comando anterior en el router del hospital de Manacor.

7.2.2. DHCP Snooping

Para comprobar que DHCP Snooping está bien configurado, hay que ver que todas las interfaces del switch, excepto la que comunica con el servidor DHCP autorizado, no están en modo "Trustedz además hay que ver que las IPs y MACs de los dispositivos que han solicitado una IP dinámica están registradas en una tabla propia del switch.

Para ver la salida por consola de la comprobación del modo de las interfaces, ver el anexo A.29.1. Y para ver la salida por consola de la comprobación de las IPs de la tabla del switch, ver el anexo A.29.2.

7.2.3. SSH

Para garantizar que la gestión remota mediante SSH está bien configurada, se ha intentado acceder mediante SSH a cualquier dispositivo de red del hospital y ha habido que autenticarse para poder acceder a él.

Para ver una imagen que corrobore la autenticación anteriormente mencionada, ver el anexo A.26. En esa imagen, se puede ver cómo se ha iniciado una petición de acceso remoto al switch de distribución 1, usando el usuario .ªdminz la contraseña çisco".

7.2.4. Autenticación en Dispositivos de Red

Para comprobar que hay un sistema de autenticación configurado en los dispositivos de red, se ha intentado acceder a cada dispositivo de red. Para poder acceder al CLI del dispositivo se ha tenido que poner una primera contraseña, en este caso çisco", y para poder acceder con privilegios de administrador, se ha tenido que utilizar la contraseña çisco". Para ver la secuencia de comandos y la salida resultante, ver el anexo A.27.

7.2.5. ACLs

Bloqueos

Para probar que el tráfico entre los dispositivos de áreas administrativas y dispositivos de la UCI o IoMT de tipo 1 está correctamente bloqueado, basta con hacer un ping desde un PC del departamento de Recursos Humanos a un dispositivo de esas áreas. La salida por consola al hacer un ping debería ser "Destination host unreachable".

También se puede acceder a las listas de control de acceso y ver qué reglas se han aplicado.

Para ver la salida por consola del ping desde un PC de Recursos Humanos a un dispositivo IoMT, ver el anexo A.31.1.

Para ver la salida por consola del ping desde un PC de Recursos Humanos a un PC del área médica, ver el anexo A.31.2.

Para ver la salida por consola del ping desde un PC de Recursos Humanos a un PC de la UCI, ver el anexo A.31.3.

Para ver la salida por consola del ping desde un PC de la red de invitados a un PC de la red interna, ver el anexo A.31.4.

Para ver la salida por consola del ping desde un PC de la red de invitados a un dispositivo IoMT, ver el anexo A.31.5.

Para ver la salida por consola del ping desde un PC no autorizado de la red interna de Son Espases al servidor de archivos del hospital de Manacor, ver el anexo A.31.5.

Permisos

Para probar que hay conectividad o que se permite la comunicación entre dos dispositivos, basta con hacer un ping desde un dispositivo hasta otro y de esa forma

comprobar que los paquetes llegan al destinatario. A veces puede que los primeros paquetes Internet Control Message Protocol (ICMP) no den conectividad, ya que primero se tienen que enviar mensajes ARP para conocer la dirección MAC del dispositivo de destino. Una vez conocida la dirección MAC, los switches ya pueden enrutar el paquete ICMP en modo unicast hacia el dispositivo de destino.

Para ver la salida por consola del ping desde un PC de las áreas médicas a un PC de la UCI, ver el anexo A.32.1.

Para ver la salida por consola del ping desde un PC de las áreas médicas a un dispositivo IoMT tipo 1, ver el anexo A.32.2.

Para ver la salida por consola del ping desde un dispositivo de la UCI a un dispositivo IoMT tipo 2, ver el anexo A.32.3.

Para ver la salida por consola del ping desde el PC autorizado de la UCI a un dispositivo IoMT tipo 3, ver el anexo A.32.4.

Para ver la salida por consola del ping desde un PC de IT de un hospital a un servidor de archivos de otro hospital, ver el anexo A.32.5.

7.3. Pruebas de Disponibilidad

A continuación se muestran las pruebas de disponibilidad realizadas:

- Tolerancia a fallos de HSRP en los routers.
- Tolerancia a fallos de HSRP en los switches L3.
- Tolerancia a fallos de EtherChannel.

7.3.1. Tolerancia a fallos de HSRP en Routers

Para comprobar que hay tolerancia a fallos a nivel de hardware en cuanto a los routers, hay que simular una caída de un router y probar que el router auxiliar coge el relevo y se convierte en el router que gestiona las comunicaciones.

Para ver la salida por consola que debería salir al simular la caída del router, ver el anexo A.33.1.

7.3.2. Tolerancia a fallos de HSRP en Switches L3

Para comprobar que hay tolerancia a fallos a nivel de hardware en cuanto a los switches, hay que simular una caída de un switch y probar que el switch auxiliar coge el relevo y se convierte en el switch que gestiona las comunicaciones.

Para ver la salida por consola que debería salir al simular la caída del switch, ver el anexo A.33.2.

7.3.3. Tolerancia a fallos de EtherChannel

Para comprobar que hay tolerancia a fallos a nivel de enlace en las conexiones entre los switches de acceso y los switches de distribución, hay que simular la caída de uno de estos enlaces redundantes y probar que las comunicaciones siguen funcionando.

Para ver la salida por consola que debería salir al simular la caída de un enlace redundante, ver el anexo A.34.

7.4. Pruebas de Protocolos de Red

A continuación se muestran las pruebas de protocolos de red realizadas:

- Correcto funcionamiento de OSPF.
- Correcto funcionamiento de DHCP.
- Correcto funcionamiento de NAT.

7.4.1. OSPF

Para garantizar que el protocolo OSPF funciona correctamente en la red, se ha comprobado que todos los dispositivos de red tengan visibilidad del resto de redes del hospital. En caso de que se muestren todas las redes del hospital, se puede afirmar que el protocolo OSPF ha hecho su función. Para ver la salida por consola de las rutas que salen en todos los dispositivos de red del hospital, ver el anexo A.23.

En el caso de la red de interconexión entre hospitales, también deberían salir las redes de los otros hospitales.

7.4.2. DHCP

Para comprobar que el protocolo DHCP se ha configurado correctamente, se ha comprobado que todos los dispositivos de todas las VLANs tengan direcciones IP dinámicas propias de cada subred.

Para ver alguna de las IPs asignadas por el servidor DHCP interno, ver el anexo A.24.

7.4.3. NAT

Para comprobar que el servicio NAT está bien implementado y configurado, se ha probado tanto que desde Internet se pueda acceder al servidor web, como que desde la red interna o la de invitados se pueda acceder a Internet. Mirando en la consola del router las traducciones de direcciones IP y comprobando la conectividad entre los dispositivos correspondientes (comprobada en las secciones 7.1.1 y 7.1.3), se puede afirmar que el servicio NAT funciona correctamente.

Para ver las imágenes de la traducción de IPs en el router para las comunicaciones desde el interior hacia Internet, ver el anexo A.25.1. Y para ver las imágenes de la traducción

de IPs en el router para las comunicaciones desde Internet hacia el servidor web, ver el anexo A.25.2.

CAPÍTULO 8

CONCLUSIÓN

Tras completar el proceso de análisis, diseño, implementación y validación de la infraestructura de red hospitalaria simulada, resulta necesario realizar una reflexión final sobre los resultados obtenidos, las dificultades encontradas y las oportunidades de mejora detectadas a lo largo del proyecto.

Este capítulo recoge las conclusiones generales derivadas del desarrollo del trabajo, valorando el grado de cumplimiento de los objetivos planteados inicialmente y la eficacia de las soluciones implementadas. Se analiza, además, el impacto de las decisiones técnicas adoptadas en términos de seguridad, disponibilidad, segmentación y gestión de la red hospitalaria simulada.

Asimismo, se identifican posibles líneas de mejora y ampliación futura del proyecto, considerando aspectos que no se han abordado debido a las limitaciones del entorno de simulación o del alcance definido, y que podrían implementarse en un entorno real o en futuras versiones de esta infraestructura.

El objetivo de este capítulo es, por tanto, evaluar de forma crítica el trabajo realizado y sentar las bases para futuras evoluciones del diseño planteado, consolidando los conocimientos adquiridos durante el desarrollo del proyecto.

8.1. Logros Alcanzados

A lo largo del desarrollo de este proyecto se han obtenido una serie de logros relevantes, tanto en términos técnicos como académicos, que permiten valorar de forma positiva los resultados alcanzados. A continuación, se enumeran los principales hitos conseguidos:

- **Diseño completo de una infraestructura de red hospitalaria segmentada** mediante VLANs y subredes diferenciadas para invitados, dispositivos IoMT y servi-

cios hospitalarios, adaptada a los requisitos de seguridad propios de un entorno sanitario.

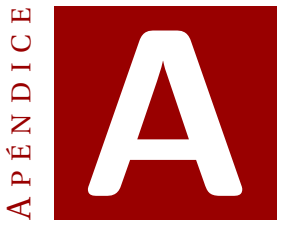
- **Implementación de una red simulada de interconexión entre cuatro hospitales**, garantizando la comunicación segura entre ellos mediante la implementación de VPN IPSec, y asegurando la continuidad del servicio mediante mecanismos de redundancia de enlaces y gateways.
- **Integración de dispositivos médicos conectados (IoMT)** en una subred específica, aplicando restricciones de seguridad reforzadas, gestión independiente de direcciones IP y control de accesos selectivo.
- **Configuración eficaz de servicios de red críticos**, como DHCP, DNS, NAT y SSH, que permiten gestionar de forma automatizada y segura las comunicaciones internas y externas de la red.

8.2. Mejoras y Ampliaciones Futuras

Si bien los resultados han sido satisfactorios, se identifican algunas líneas de mejora y ampliación para desarrollos futuros:

- Añadir servicios de monitorización de red en tiempo real y sistemas IDS/IPS para la detección proactiva de amenazas.
- Incorporar mecanismos de seguridad adicionales para la subred dedicada a los invitados.
- Simular escenarios de ataque más avanzados para evaluar la robustez de la infraestructura ante ciberamenazas complejas.
- Implementar el diseño en una herramienta de virtualización profesional (como GNS3 o Cisco VIRL) que permita un mayor realismo y compatibilidad con tecnologías actuales no disponibles en Cisco Packet Tracer.

Nota: *Cabe recordar que las limitaciones y el alcance del proyecto fueron definidos previamente en la fase de análisis (sección 1.3.2), de manera que las conclusiones aquí presentadas se extraen dentro del marco establecido en aquel apartado.*



ANEXOS

A.1. Configuración Básica Dispositivos de Red

A continuación se muestra el fragmento de código bash utilizado para la configuración básica de los dispositivos de red:

Listing A.1: Configuración Básica de los Dispositivos de Red

```
%Passwords
enable
config t
hostname nombre_dispositivo
enable password cisco
no ip domain lookup
banner motd #Solo Acceso Autorizado!!#
line console 0
password cisco
login
exit
service password-encryption

%SSH
ip domain name cisco.net
username admin password cisco
crypto key generate rsa
1024
line vty 0 15
login local
transport input ssh
```

A.2. Configuración VLANs en Switches de Acceso

A continuación se muestra el fragmento de código bash utilizado para la configuración de las VLANs en los switches de acceso:

Listing A.2: Configuración VLANs en Switches de Acceso

```
%Create VLAN
vlan xx
name nombre_VLAN
exit

%Ports Configuration
interface range Fa0/1-2
switchport mode trunk
switchport trunk allowed vlan xx
exit

interface range Fa0/3-24
switchport mode access
switchport access vlan xx
exit
```

A.3. Configuración VLANs en Switches de Distribución

A continuación se muestra el fragmento de código bash utilizado para la configuración de las VLANs en los switches de distribución:

Listing A.3: Configuración VLANs en Switches de Distribución

```
%Create VLANs
vlan xx
name nombre_VLAN1
exit

vlan yy
name nombre_VLAN2
exit

vlan zz
name nombre_VLAN_interconexion_Core
exit

vlan nn
name nombre_VLAN_interconexion_Distribuidores
exit

%Ports Configuration
interface GigabitEthernet1/0/3 %Enlace con Switch Acceso 1
switchport mode trunk
switchport trunk allowed vlan xx
exit

interface GigabitEthernet1/0/4 %Enlace con Switch Acceso 2
```

```
switchport mode trunk
switchport trunk allowed vlan yy
exit

interface GigabitEthernet1/0/1 %Enlace con Switch Core 1
switchport mode trunk
switchport trunk allowed vlan xx,yy,zz
exit

interface GigabitEthernet1/0/6 %Enlace con Switch Core 2
switchport mode trunk
switchport trunk allowed vlan xx,yy,zz
exit

interface GigabitEthernet1/0/2 %Enlace con Switch Distribucion 1
switchport mode trunk
switchport trunk allowed vlan xx,yy,nn
exit

interface GigabitEthernet1/0/7 %Enlace con Switch Distribucion 2
switchport mode trunk
switchport trunk allowed vlan xx,yy,nn
exit
```

A.4. Configuración VLANs en Switches Core

A continuación se muestra el fragmento de código bash utilizado para la configuración de las VLANs en los switches core:

Listing A.4: Configuración VLANs en Switches Core

```
%Create VLANs
vlan xx
name nombre_VLAN1
exit

vlan yy
name nombre_VLAN2
exit

vlan nn
name nombre_VLAN3
exit

vlan zz
name nombre_VLAN_interconexion_Core
exit

%Ports Configuration
interface GigabitEthernet1/0/3 %Enlace con Switch Distribucion 1
switchport mode trunk
switchport trunk allowed vlan xx,zz
exit
```

```
interface GigabitEthernet1/0/4 %Enlace con Switch Distribucion 2
switchport mode trunk
switchport trunk allowed vlan yy,zz
exit

interface GigabitEthernet1/0/1 %Enlace con Switch Core
switchport mode trunk
switchport trunk allowed vlan xx,yy,nn,zz
exit
```

A.5. Configuración EtherChannel

A continuación se muestra el fragmento de código bash utilizado para la configuración del EtherChannel.

Listing A.5: Configuración EtherChannel

```
interface range fa0/1-2 %Enlaces al switch de acceso/distribucion
switchport mode trunk
switchport trunk allowed vlan xx
channel-group 1 mode active
no shutdown
exit

interface port-channel 1
switchport mode trunk
switchport trunk allowed vlan xx
no shutdown
```

A.6. Configuración Medidas Seguridad DMZ

A continuación se muestra el fragmento de código bash utilizado para la configuración de las medidas de seguridad básicas en las DMZ.

Listing A.6: Configuración Medidas Seguridad DMZ

```
int range fa0/2-24 %Enlaces a dispositivos finales
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation shutdown
```

A.7. Configuración HSRP en Switches L3

A continuación se muestra el fragmento de código bash utilizado para la configuración de la configuración de HSRP en los switches L3.

Listing A.7: Configuración HSRP en Switches L3

```
interface vlan xx
ip address 192.168.10.2 255.255.255.0
standby xx ip 192.168.10.1
```

```
standby xx priority 120
standby xx preempt %Permite recuperar el control del servicio
no shutdown
```

A.8. Configuración HSRP en Routers

A continuación se muestra el fragmento de código bash utilizado para la configuración de la configuración de HSRP en los routers.

Listing A.8: Configuración HSRP en Routers

```
int range fa0/2-24 %Enlaces a dispositivos finales
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation shutdown
```

A.9. Configuración Direccionamiento IP Estático

A continuación se muestra el fragmento de código bash utilizado para el direccionamiento IP estático.

Listing A.9: Configuración Direccionamiento IP Estático

```
int gig1/0/1
ip address 192.168.0.1 255.255.255.0
```

A.10. Configuración DHCP Relay

A continuación se muestra el fragmento de código bash utilizado para la configuración de DHCP Relay en switches L3.

Listing A.10: Configuración Direccionamiento IP Estático

```
int vlan xx
ip helper-address 10.0.3.6
```

A.11. Configuración OSPF

A continuación se muestra el fragmento de código bash utilizado para la configuración de OSPF.

Listing A.11: Configuración OSPF

```
ip routing
router ospf 10
#Poner todas las redes a las que esta conectado cada switch/router
network 10.2.1.0 0.0.0.7 area 0
network 10.1.0.0 0.0.0.31 area 0
```

A.12. Configuración RSTP

A continuación se muestra el fragmento de código bash utilizado para la configuración de RSTP.

Listing A.12: Configuración RSTP

```
spanning-tree mode rapid-pvst
```

A.13. Configuración NAT para Comunicaciones Internas

A continuación se muestra el fragmento de código bash utilizado para la configuración de NAT para Comunicaciones Internas.

Listing A.13: Configuración NAT para Comunicaciones Internas

```
%Outside Interfaces
interface serial1/0
ip nat outside

%Inside Interfaces
interface gig1/0.150
ip nat inside

%Define ACLs
access-list 1 permit subred1 mascara_de_red1
access-list 1 permit subred2 mascara_de_red2
access-list 1 permit subred3 mascara_de_red3

%Create NAT
ip nat inside source list 1 interface se0/0 overload
```

A.14. Configuración NAT para Comunicaciones Externas

A continuación se muestra el fragmento de código bash utilizado para la configuración de NAT para Comunicaciones Externas.

Listing A.14: Configuración NAT para Comunicaciones Externas

```
%Create NAT
ip nat inside source static IP_Servidor_Web IP_Publica
```

A.15. Configuración DHCP Snooping

A continuación se muestra el fragmento de código bash utilizado para la configuración de DHCP Snooping en los switches de acceso.

Listing A.15: Configuración DHCP Snooping

```
%Active DHCP Snooping
ip dhcp snooping
ip dhcp snooping vlan xx
```

```
%Packets Rate Limitation
int range fa0/1-24
ip dhcp snooping limit rate 5

%Trust Interfaces
int range fa0/1-2
ip dhcp snooping trust
```

A.16. Configuración ACLs Switch IoMt Planta 3

A continuación se muestra el fragmento de código bash utilizado para la configuración de ACLs en el switch IoMT de la planta 3.

Listing A.16: Configuración ACLs Switch IoMt Planta 3

```
%Declare ACL
access-list 101 permit udp any any eq 67
access-list 101 permit udp any any eq 68
access-list 101 permit ip 10.0.2.64 0.0.0.63 172.16.64.0 0.0.15.255
access-list 101 deny ip any any

access-list 102 permit udp any any eq 67
access-list 102 permit udp any any eq 68
access-list 102 permit ip 172.16.64.0 0.0.15.255 10.0.2.64 0.0.0.63
access-list 102 deny ip any any

%Apply ACL on Interface
int vlan220
ip access-group 101 out
ip access-group 102 in

%Declare ACL
access-list 103 permit udp any any eq 67
access-list 103 permit udp any any eq 68
access-list 103 permit ip host 10.0.2.70 172.16.128.0 0.0.15.255
access-list 103 deny ip any any

access-list 104 permit udp any any eq 67
access-list 104 permit udp any any eq 68
access-list 104 permit ip 172.16.128.0 0.0.15.255 host 10.0.2.70
access-list 104 deny ip any any

%Apply ACL on Interface
int vlan230
ip access-group 104 in
ip access-group 103 out
```

A.17. Configuración ACLs Switch IoMt Plantas 0, 1 y 2

A continuación se muestra el fragmento de código bash utilizado para la configuración de ACLs en el switch IoMT de las plantas 0, 1 y 2.

Listing A.17: Configuración ACLs Switch IoMt Plantas 0, 1 y 2

```
%Declare ACL
access-list 120 permit udp any any eq 67
access-list 120 permit udp any any eq 68
access-list 120 permit ospf any any
access-list 120 permit ip 10.0.2.64 0.0.0.63 172.16.48.0 0.0.15.255
access-list 120 permit ip 10.0.0.128 0.0.0.63 172.16.48.0 0.0.15.255
access-list 120 permit ip 10.0.0.192 0.0.0.63 172.16.48.0 0.0.15.255
access-list 120 permit ip 10.0.1.0 0.0.0.63 172.16.48.0 0.0.15.255
access-list 120 permit ip 10.0.1.64 0.0.0.63 172.16.48.0 0.0.15.255
access-list 120 permit ip 10.0.1.128 0.0.0.63 172.16.48.0 0.0.15.255
access-list 120 permit ip 10.0.1.192 0.0.0.63 172.16.48.0 0.0.15.255
access-list 120 deny ip any any


access-list 121 permit udp any any eq 67
access-list 121 permit udp any any eq 68
access-list 121 permit ospf any any
access-list 121 permit ip 172.16.48.0 0.0.15.255 10.0.2.64 0.0.0.63
access-list 121 permit ip 172.16.48.0 0.0.15.255 10.0.0.128 0.0.0.63
access-list 121 permit ip 172.16.48.0 0.0.15.255 10.0.0.192 0.0.0.63
access-list 121 permit ip 172.16.48.0 0.0.15.255 10.0.1.0 0.0.0.63
access-list 121 permit ip 172.16.48.0 0.0.15.255 10.0.1.64 0.0.0.63
access-list 121 permit ip 172.16.48.0 0.0.15.255 10.0.1.128 0.0.0.63
access-list 121 permit ip 172.16.48.0 0.0.15.255 10.0.1.192 0.0.0.63
access-list 121 deny ip any any

%Apply ACL on Interface
int vlan 210
ip access-group 120 out
ip access-group 121 in
```

A.18. Configuración ACLs Routers

A continuación se muestra el fragmento de código bash utilizado para la configuración de ACLs en los routers.

Listing A.18: Configuración ACLs Routers

```
%Declare ACL
access-list 110 permit udp any any eq 67
access-list 110 permit udp any any eq 68
access-list 110 permit ospf any any
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.0 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.8 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.16 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.4 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.12 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.20 0.0.0.3
access-list 110 deny ip any any

access-list 111 permit udp any any eq 67
```

```
access-list 111 permit udp any any eq 68
access-list 111 permit ospf any any
access-list 111 permit ip 195.136.17.0 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.8 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.16 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.4 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.12 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.20 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 deny ip any any

%Apply ACL on Interface
int g4/0.190
ip access-group 110 in
ip access-group 111 out
```

A.19. Configuración ACLs Switches Distribución

A continuación se muestra el fragmento de código bash utilizado para la configuración de ACLs en los switches de distribución.

Listing A.19: Configuración ACLs Switches Distribución

```
%Declare ACL
access-list 130 deny ip 10.0.0.0 0.0.0.63 10.0.0.128 0.0.0.63
access-list 130 deny ip 10.0.0.0 0.0.0.63 10.0.0.192 0.0.0.63
access-list 130 deny ip 10.0.0.0 0.0.0.63 10.0.1.0 0.0.0.63
access-list 130 deny ip 10.0.0.0 0.0.0.63 10.0.1.64 0.0.0.63
access-list 130 deny ip 10.0.0.0 0.0.0.63 10.0.1.128 0.0.0.63
access-list 130 deny ip 10.0.0.0 0.0.0.63 10.0.1.192 0.0.0.63
access-list 130 permit ip any any

%Apply ACL on Interface
int vlan10
ip access-group 130 in

%Declare ACL
access-list 131 deny ip 10.0.0.64 0.0.0.63 10.0.0.128 0.0.0.63
access-list 131 deny ip 10.0.0.64 0.0.0.63 10.0.0.192 0.0.0.63
access-list 131 deny ip 10.0.0.64 0.0.0.63 10.0.1.0 0.0.0.63
access-list 131 deny ip 10.0.0.64 0.0.0.63 10.0.1.64 0.0.0.63
access-list 131 deny ip 10.0.0.64 0.0.0.63 10.0.1.128 0.0.0.63
access-list 131 deny ip 10.0.0.64 0.0.0.63 10.0.1.192 0.0.0.63
access-list 131 permit ip any any

%Apply ACL on Interface
int vlan20
ip access-group 131 in

%Declare ACL
access-list 132 deny ip 10.0.2.0 0.0.0.63 10.0.0.128 0.0.0.63
access-list 132 deny ip 10.0.2.0 0.0.0.63 10.0.0.192 0.0.0.63
access-list 132 deny ip 10.0.2.0 0.0.0.63 10.0.1.0 0.0.0.63
access-list 132 deny ip 10.0.2.0 0.0.0.63 10.0.1.64 0.0.0.63
```

```
access-list 132 deny ip 10.0.2.0 0.0.0.63 10.0.1.128 0.0.0.63
access-list 132 deny ip 10.0.2.0 0.0.0.63 10.0.1.192 0.0.0.63
access-list 132 permit ip any any

%Apply ACL on Interface
int vlan90
ip access-group 132 in

%Declare ACL
access-list 133 deny ip 10.0.2.64 0.0.0.63 10.0.0.128 0.0.0.63
access-list 133 deny ip 10.0.2.64 0.0.0.63 10.0.0.192 0.0.0.63
access-list 133 deny ip 10.0.2.64 0.0.0.63 10.0.1.0 0.0.0.63
access-list 133 deny ip 10.0.2.64 0.0.0.63 10.0.1.64 0.0.0.63
access-list 133 deny ip 10.0.2.64 0.0.0.63 10.0.1.128 0.0.0.63
access-list 133 deny ip 10.0.2.64 0.0.0.63 10.0.1.192 0.0.0.63
access-list 133 permit ip any any

%Apply ACL on Interface
int vlan100
ip access-group 133 in

%Declare ACL
access-list 134 deny ip 10.0.2.128 0.0.0.63 10.0.0.128 0.0.0.63
access-list 134 deny ip 10.0.2.128 0.0.0.63 10.0.0.192 0.0.0.63
access-list 134 deny ip 10.0.2.128 0.0.0.63 10.0.1.0 0.0.0.63
access-list 134 deny ip 10.0.2.128 0.0.0.63 10.0.1.64 0.0.0.63
access-list 134 deny ip 10.0.2.128 0.0.0.63 10.0.1.128 0.0.0.63
access-list 134 deny ip 10.0.2.128 0.0.0.63 10.0.1.192 0.0.0.63
access-list 134 permit ip any any

%Apply ACL on Interface
int vlan110
ip access-group 134 in

%Declare ACL
access-list 135 deny ip 10.0.2.192 0.0.0.63 10.0.0.128 0.0.0.63
access-list 135 deny ip 10.0.2.192 0.0.0.63 10.0.0.192 0.0.0.63
access-list 135 deny ip 10.0.2.192 0.0.0.63 10.0.1.0 0.0.0.63
access-list 135 deny ip 10.0.2.192 0.0.0.63 10.0.1.64 0.0.0.63
access-list 135 deny ip 10.0.2.192 0.0.0.63 10.0.1.128 0.0.0.63
access-list 135 deny ip 10.0.2.192 0.0.0.63 10.0.1.192 0.0.0.63
access-list 135 permit ip any any

%Apply ACL on Interface
int vlan120
ip access-group 135 in
```

A.20. Configuración ACLs Routers Interconexión

A continuación se muestra el fragmento de código bash utilizado para la configuración de ACLs en los routers de interconexión.

Listing A.20: Configuración ACLs Routers Interconexión

```
%R-SonEspases-Man
access-list 110 permit ip 192.168.100.0 0.0.3.255 192.168.104.0 0.0.1.255
access-list 110 permit ip 192.168.100.0 0.0.3.255 192.168.106.0 0.0.0.127
access-list 110 permit ip 192.168.100.0 0.0.3.255 192.168.106.128 0.0.0.63

%SE-Inca
access-list 120 permit ip 192.168.100.0 0.0.3.255 192.168.108.0 0.0.1.255
access-list 120 permit ip 192.168.100.0 0.0.3.255 192.168.110.0 0.0.0.255
access-list 120 permit ip 192.168.100.0 0.0.3.255 192.168.111.0 0.0.0.63

%Inca-SE
access-list 120 permit ip 192.168.108.0 0.0.1.255 192.168.100.0 0.0.3.255
access-list 120 permit ip 192.168.110.0 0.0.0.255 192.168.100.0 0.0.3.255
access-list 120 permit ip 192.168.111.0 0.0.0.63 192.168.100.0 0.0.3.255

%SE-SL
access-list 130 permit ip 192.168.100.0 0.0.3.255 192.168.112.0 0.0.1.255
access-list 130 permit ip 192.168.100.0 0.0.3.255 192.168.114.0 0.0.0.255
access-list 130 permit ip 192.168.100.0 0.0.3.255 192.168.115.0 0.0.0.127

%SL-SE
access-list 130 permit ip 192.168.112.0 0.0.1.255 192.168.100.0 0.0.3.255
access-list 130 permit ip 192.168.114.0 0.0.0.255 192.168.100.0 0.0.3.255
access-list 130 permit ip 192.168.115.0 0.0.0.127 192.168.100.0 0.0.3.255

%Man-Inca
access-list 140 permit ip 192.168.104.0 0.0.1.255 192.168.108.0 0.0.1.255
access-list 140 permit ip 192.168.104.0 0.0.1.255 192.168.110.0 0.0.0.255
access-list 140 permit ip 192.168.104.0 0.0.1.255 192.168.111.0 0.0.0.63
access-list 140 permit ip 192.168.106.0 0.0.0.127 192.168.108.0 0.0.1.255
access-list 140 permit ip 192.168.106.0 0.0.0.127 192.168.110.0 0.0.0.255
access-list 140 permit ip 192.168.106.0 0.0.0.127 192.168.111.0 0.0.0.63
access-list 140 permit ip 192.168.106.128 0.0.0.63 192.168.108.0 0.0.1.255
access-list 140 permit ip 192.168.106.128 0.0.0.63 192.168.110.0 0.0.0.255
access-list 140 permit ip 192.168.106.128 0.0.0.63 192.168.111.0 0.0.0.63

%Inca-Man
access-list 140 permit ip 192.168.108.0 0.0.1.255 192.168.104.0 0.0.1.255
access-list 140 permit ip 192.168.110.0 0.0.0.255 192.168.104.0 0.0.1.255
access-list 140 permit ip 192.168.111.0 0.0.0.63 192.168.104.0 0.0.1.255
access-list 140 permit ip 192.168.108.0 0.0.1.255 192.168.106.0 0.0.0.127
access-list 140 permit ip 192.168.110.0 0.0.0.255 192.168.106.0 0.0.0.127
access-list 140 permit ip 192.168.111.0 0.0.0.63 192.168.106.0 0.0.0.127
access-list 140 permit ip 192.168.108.0 0.0.1.255 192.168.106.128 0.0.0.63
access-list 140 permit ip 192.168.110.0 0.0.0.255 192.168.106.128 0.0.0.63
access-list 140 permit ip 192.168.111.0 0.0.0.63 192.168.106.128 0.0.0.63

%Inca-SL
access-list 150 permit ip 192.168.108.0 0.0.1.255 192.168.112.0 0.0.1.255
access-list 150 permit ip 192.168.108.0 0.0.1.255 192.168.114.0 0.0.0.255
access-list 150 permit ip 192.168.108.0 0.0.1.255 192.168.115.0 0.0.0.127
```

```
access-list 150 permit ip 192.168.110.0 0.0.0.255 192.168.112.0 0.0.1.255
access-list 150 permit ip 192.168.110.0 0.0.0.255 192.168.114.0 0.0.0.255
access-list 150 permit ip 192.168.110.0 0.0.0.255 192.168.115.0 0.0.0.127
access-list 150 permit ip 192.168.111.0 0.0.0.63 192.168.112.0 0.0.1.255
access-list 150 permit ip 192.168.111.0 0.0.0.63 192.168.114.0 0.0.0.255
access-list 150 permit ip 192.168.111.0 0.0.0.63 192.168.115.0 0.0.0.127

%SL-Inca
access-list 150 permit ip 192.168.112.0 0.0.1.255 192.168.108.0 0.0.1.255
access-list 150 permit ip 192.168.114.0 0.0.0.255 192.168.108.0 0.0.1.255
access-list 150 permit ip 192.168.115.0 0.0.0.127 192.168.108.0 0.0.1.255
access-list 150 permit ip 192.168.112.0 0.0.1.255 192.168.110.0 0.0.0.255
access-list 150 permit ip 192.168.114.0 0.0.0.255 192.168.110.0 0.0.0.255
access-list 150 permit ip 192.168.115.0 0.0.0.127 192.168.110.0 0.0.0.255
access-list 150 permit ip 192.168.112.0 0.0.1.255 192.168.111.0 0.0.0.63
access-list 150 permit ip 192.168.114.0 0.0.0.255 192.168.111.0 0.0.0.63
access-list 150 permit ip 192.168.115.0 0.0.0.127 192.168.111.0 0.0.0.63

%Man-SL
access-list 160 permit ip 192.168.104.0 0.0.1.255 192.168.112.0 0.0.1.255
access-list 160 permit ip 192.168.104.0 0.0.1.255 192.168.114.0 0.0.0.255
access-list 160 permit ip 192.168.104.0 0.0.1.255 192.168.115.0 0.0.0.127
access-list 160 permit ip 192.168.106.0 0.0.0.127 192.168.112.0 0.0.1.255
access-list 160 permit ip 192.168.106.0 0.0.0.127 192.168.114.0 0.0.0.255
access-list 160 permit ip 192.168.106.0 0.0.0.127 192.168.115.0 0.0.0.127
access-list 160 permit ip 192.168.106.128 0.0.0.63 192.168.112.0 0.0.1.255
access-list 160 permit ip 192.168.106.128 0.0.0.63 192.168.114.0 0.0.0.255
access-list 160 permit ip 192.168.106.128 0.0.0.63 192.168.115.0 0.0.0.127

%SL-Man
access-list 160 permit ip 192.168.112.0 0.0.1.255 192.168.104.0 0.0.1.255
access-list 160 permit ip 192.168.114.0 0.0.0.255 192.168.104.0 0.0.1.255
access-list 160 permit ip 192.168.115.0 0.0.0.127 192.168.104.0 0.0.1.255
access-list 160 permit ip 192.168.112.0 0.0.1.255 192.168.106.0 0.0.0.127
access-list 160 permit ip 192.168.114.0 0.0.0.255 192.168.106.0 0.0.0.127
access-list 160 permit ip 192.168.115.0 0.0.0.127 192.168.106.0 0.0.0.127
access-list 160 permit ip 192.168.112.0 0.0.1.255 192.168.106.128 0.0.0.63
access-list 160 permit ip 192.168.114.0 0.0.0.255 192.168.106.128 0.0.0.63
access-list 160 permit ip 192.168.115.0 0.0.0.127 192.168.106.128 0.0.0.63

%Declare ACL to Block Access to File Server
access-list 105 permit ip host 192.168.100.133 host 192.168.103.134
access-list 105 permit ip host 192.168.104.133 host 192.168.103.134
access-list 105 permit ip host 192.168.108.133 host 192.168.103.134
access-list 105 permit ip host 192.168.112.133 host 192.168.103.134
access-list 105 deny ip any any

%Apply ACL on Interface
int g0/1.200
ip access-group 105 out
```

A.21. Configuración VPN entre Son Espases y Manacor

A continuación se muestra el fragmento de código bash utilizado para la configuración de la VPN entre Son Espases y Manacor.

Listing A.21: Configuración VPN entre Son Espases y Manacor

```
%R-Son_Espases
crypto isakmp policy 60
encryption aes 256
authentication pre-share
group 5
exit
crypto isakmp key vpnpa55 address 192.168.103.178
crypto ipsec transform-set VPN-SET6 esp-aes esp-sha-hmac
crypto map VPN-MAP6 60 ipsec-isakmp
description VPN connection to Son Llatzer.
set peer 192.168.103.178
set transform-set VPN-SET6
match address 160

%Apply VPN Config on Interface
interface S0/3/1
crypto map VPN-MAP6

%R-Manacor
crypto isakmp policy 60
encryption aes 256
authentication pre-share
group 5
exit
crypto isakmp key vpnpa55 address 192.168.103.177
crypto ipsec transform-set VPN-SET6 esp-aes esp-sha-hmac
crypto map VPN-MAP6 60 ipsec-isakmp
description VPN connection to Manacor.
set peer 192.168.103.177
set transform-set VPN-SET6
match address 160
exit

%Apply VPN Config on Interface
interface S0/3/0
crypto map VPN-MAP6
```

A.22. Configuraciones Completas

A.22.1. Switch RRHH

A continuación se muestra la configuración completa del dispositivo de red Switch RRHH.

Listing A.22: Configuración Completa Switch RRHH

```
!
version 15.0
```

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname RRHH
!
enable password 7 0822455D0A16
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
username admin privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Port-channel1
 switchport trunk allowed vlan 10
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk allowed vlan 10
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/2
 switchport trunk allowed vlan 10
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 10
 switchport mode trunk
!
interface FastEthernet0/7
 switchport access vlan 10
 switchport mode access
```

```
!
interface FastEthernet0/8
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 10
 switchport mode access
!
```

```
interface FastEthernet0/21
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
ip default-gateway 10.0.0.1
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.2. Switch FyC

A continuación se muestra la configuración completa del dispositivo de red Switch FyC.

Listing A.23: Configuración Completa Switch FyC

```
!
```

```
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname FyC
!
enable password 7 0822455D0A16
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
username admin privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Port-channel2
 switchport trunk allowed vlan 20
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk allowed vlan 20
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/2
 switchport trunk allowed vlan 20
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 20
 switchport mode trunk
!
interface FastEthernet0/7
 switchport access vlan 20
```

```
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 20
 switchport mode access
```

```
!
interface FastEthernet0/21
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
ip default-gateway 10.0.0.65
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.3. Switch Oftalmologia

A continuación se muestra la configuración completa del dispositivo de red Switch Oftalmologia.

Listing A.24: Configuración Completa Switch Oftalmologia

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Oftalmologia
!
enable password 7 0822455D0A16
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
username admin privilege 1 password 7 0822455D0A16
!
!
ip dhcp snooping vlan 30
ip dhcp snooping
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping trust
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode trunk
!
interface FastEthernet0/3
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
```

```
!
interface FastEthernet0/6
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping trust
 ip dhcp snooping limit rate 5
 switchport mode trunk
!
interface FastEthernet0/7
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
```

```
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 30
```

```
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 30
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.4. Switch Urologia

A continuación se muestra la configuración completa del dispositivo de red Switch Urologia.

Listing A.25: Configuración Completa Switch Urologia

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Urologia
!
enable password 7 0822455D0A16
```

```
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
username admin privilege 1 password 7 0822455D0A16
!
!
ip dhcp snooping vlan 40
ip dhcp snooping
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping trust
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode trunk
!
interface FastEthernet0/3
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping trust
 ip dhcp snooping limit rate 5
 switchport mode trunk
!
interface FastEthernet0/7
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
```

```
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 40
```

```
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 40
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface GigabitEthernet0/1
```

```
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.5. Switch Cardiologia

A continuación se muestra la configuración completa del dispositivo de red Switch Cardiologia.

Listing A.26: Configuración Completa Switch Cardiologia

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Cardiologia
!
enable password 7 0822455D0A16
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
username admin privilege 1 password 7 0822455D0A16
!
!
ip dhcp snooping vlan 50
```

```
ip dhcp snooping
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping trust
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode trunk
!
interface FastEthernet0/3
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping trust
 ip dhcp snooping limit rate 5
 switchport mode trunk
!
interface FastEthernet0/7
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/9
```

```
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
```

```
interface FastEthernet0/18
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 50
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
banner motd #Solo Acceso Autorizado!!#
!
!
```

```
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.6. Switch Dermatologia

A continuación se muestra la configuración completa del dispositivo de red Switch Dermatologia.

Listing A.27: Configuración Completa Switch Dermatologia

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Dermatologia
!
enable password 7 0822455D0A16
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
username admin privilege 1 password 7 0822455D0A16
!
!
ip dhcp snooping vlan 60
ip dhcp snooping
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode trunk
!
```

```
interface FastEthernet0/2
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping trust
 ip dhcp snooping limit rate 5
 switchport mode trunk
!
interface FastEthernet0/3
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping trust
 ip dhcp snooping limit rate 5
 switchport mode trunk
!
interface FastEthernet0/7
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
```

```
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
```

```
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 60
 switchport trunk allowed vlan 2-1001
 ip dhcp snooping limit rate 5
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
```

```
 login local
 transport input ssh
!
!
!
!
end
```

A.22.7. Switch Radiologia

A continuación se muestra la configuración completa del dispositivo de red Switch Radiologia.

Listing A.28: Configuración Completa Switch Radiologia

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Radiologia
!
enable password 7 0822455D0A16
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
username admin privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Port-channel1
 switchport trunk allowed vlan 70
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk allowed vlan 70
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/2
 switchport trunk allowed vlan 70
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/3
 switchport access vlan 70
```

```
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode trunk
!
interface FastEthernet0/7
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
```

```
interface FastEthernet0/14
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 70
 switchport trunk allowed vlan 2-1001
```

```
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.8. Switch Inmunologia

A continuación se muestra la configuración completa del dispositivo de red Switch Inmunologia.

Listing A.29: Configuración Completa Switch Inmunologia

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Inmunologia
!
enable password 7 0822455D0A16
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
username admin privilege 1 password 7 0822455D0A16
```

```
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Port-channel2
 switchport trunk allowed vlan 80
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk allowed vlan 80
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/2
 switchport trunk allowed vlan 80
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/3
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode trunk
!
interface FastEthernet0/7
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
```

```
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/20
```

```
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 80
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.9. Switch Admisión

A continuación se muestra la configuración completa del dispositivo de red Switch Admisión.

Listing A.30: Configuración Completa Switch Admisión

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Admision
!
enable password 7 0822455D0A16
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
username admin privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Port-channel1
 switchport trunk allowed vlan 90
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk allowed vlan 90
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/2
 switchport trunk allowed vlan 90
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/3
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/5
```

```
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode trunk
!
interface FastEthernet0/7
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
```

```
!
interface FastEthernet0/16
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 90
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
```

```
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.10. Switch UCI

A continuación se muestra la configuración completa del dispositivo de red Switch UCI.

Listing A.31: Configuración Completa Switch UCI

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname UCI
!
enable password 7 0822455D0A16
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
username admin privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Port-channel2
 switchport trunk allowed vlan 100
 switchport mode trunk
!
```

```
interface FastEthernet0/1
 switchport trunk allowed vlan 100
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/2
 switchport trunk allowed vlan 100
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/3
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode trunk
!
interface FastEthernet0/7
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
```

```
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/22
```

```
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 100
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.11. Switch Atención Pacientes

A continuación se muestra la configuración completa del dispositivo de red Switch Atención Pacientes.

Listing A.32: Configuración Completa Switch Atención Pacientes

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

```
service password-encryption
!
hostname At.Paciente
!
enable password 7 0822455D0A16
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
username admin privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Port-channel1
 switchport trunk allowed vlan 110
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk allowed vlan 110
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/2
 switchport trunk allowed vlan 110
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/3
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode trunk
!
interface FastEthernet0/7
```

```
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
```

```
!
interface FastEthernet0/18
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 110
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
```

```
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.12. Switch Asesoría Jurídica

A continuación se muestra la configuración completa del dispositivo de red Switch Asesoría Jurídica.

Listing A.33: Configuración Completa Switch Asesoría Jurídica

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Ases.Juridica
!
enable password 7 0822455D0A16
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
username admin privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Port-channel2
 switchport trunk allowed vlan 120
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk allowed vlan 120
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/2
 switchport trunk allowed vlan 120
 switchport mode trunk
 channel-group 2 mode active
```

```
!
interface FastEthernet0/3
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode trunk
!
interface FastEthernet0/7
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 120
```

```
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
```

```
interface FastEthernet0/24
 switchport access vlan 120
 switchport trunk allowed vlan 2-1001
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.13. Switch Distribución 1

A continuación se muestra la configuración completa del dispositivo de red Switch Distribución 1.

Listing A.34: Configuración Completa Switch Distribución 1

```
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sw.Distribucion1
!
!
enable password 7 0822455D0A16
!
!
!
```

```
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
spanning-tree mode rapid-pvst
!
!
!
!
!
!
interface Port-channel1
 switchport trunk allowed vlan 10
 switchport mode trunk
!
interface Port-channel2
 switchport trunk allowed vlan 20
 switchport mode trunk
!
interface GigabitEthernet1/0/1
 switchport trunk allowed vlan 10
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet1/0/2
 switchport trunk allowed vlan 10
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet1/0/3
 switchport trunk allowed vlan 20
 switchport mode trunk
```

```
 channel-group 2 mode active
!
interface GigabitEthernet1/0/4
 switchport trunk allowed vlan 20
 switchport mode trunk
 channel-group 2 mode active
!
interface GigabitEthernet1/0/5
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/6
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/7
 switchport trunk allowed vlan 110
 switchport mode trunk
!
interface GigabitEthernet1/0/8
 switchport trunk allowed vlan 120
 switchport mode trunk
!
interface GigabitEthernet1/0/9
 switchport trunk allowed vlan 2-9,11-19,21-119,121-1001
 switchport mode trunk
!
interface GigabitEthernet1/0/10
 switchport trunk allowed vlan 2-9,11-19,21-109,111-1001
 switchport mode trunk
!
interface GigabitEthernet1/0/11
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/12
 switchport trunk allowed vlan 10,20,110,120,200
 switchport mode trunk
!
interface GigabitEthernet1/0/13
 switchport trunk allowed vlan 10,20,110,120,200
 switchport mode trunk
!
interface GigabitEthernet1/0/14
 switchport trunk allowed vlan 10,20,110,120,205
 switchport mode trunk
!
interface GigabitEthernet1/0/15
 switchport trunk allowed vlan 10,20,110,120
!
interface GigabitEthernet1/0/16
 switchport trunk allowed vlan 10,20,110,120
!
interface GigabitEthernet1/0/17
 switchport trunk allowed vlan 10,20,110,120,205
 switchport mode trunk
```

```
!
interface GigabitEthernet1/0/18
 switchport trunk allowed vlan 10,20,110,120
!
interface GigabitEthernet1/0/19
 switchport trunk allowed vlan 10,20,110,120
!
interface GigabitEthernet1/0/20
 switchport trunk allowed vlan 10,20,110,120
!
interface GigabitEthernet1/0/21
 switchport trunk allowed vlan 10,20,110,120
!
interface GigabitEthernet1/0/22
 switchport trunk allowed vlan 10,20,110,120
!
interface GigabitEthernet1/0/23
 switchport trunk allowed vlan 10,20,110,120
!
interface GigabitEthernet1/0/24
 switchport trunk allowed vlan 10,20,110,120
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 mac-address 0000.0cb3.2c01
 ip address 10.0.0.2 255.255.255.192
 ip helper-address 10.0.3.6
 ip access-group 130 in
 standby 10 ip 10.0.0.1
 standby 10 priority 110
 standby 10 preempt
!
interface Vlan20
 mac-address 0000.0cb3.2c02
 ip address 10.0.0.66 255.255.255.192
 ip helper-address 10.0.3.6
 ip access-group 131 in
 standby 20 ip 10.0.0.65
 standby 20 priority 110
 standby 20 preempt
!
interface Vlan110
```

```
 mac-address 0000.0cb3.2c03
 ip address 10.0.2.131 255.255.255.192
 ip helper-address 10.0.3.6
 standby 110 ip 10.0.2.129
 standby 110 preempt
!
interface Vlan120
 mac-address 0000.0cb3.2c04
 ip address 10.0.2.195 255.255.255.192
 ip helper-address 10.0.3.6
 standby 120 ip 10.0.2.193
 standby 120 preempt
!
interface Vlan200
 mac-address 0000.0cb3.2c05
 ip address 10.1.0.1 255.255.255.224
 ip ospf cost 10
!
interface Vlan205
 mac-address 0000.0cb3.2c06
 ip address 10.1.1.1 255.255.255.224
 ip ospf cost 100
!
router ospf 10
 log-adjacency-changes
 network 10.0.0.0 0.0.0.63 area 0
 network 10.0.0.64 0.0.0.63 area 0
 network 10.0.2.128 0.0.0.63 area 0
 network 10.0.2.192 0.0.0.63 area 0
 network 10.1.0.0 0.0.0.31 area 0
 network 10.1.1.0 0.0.0.31 area 0
!
ip classless
!
ip flow-export version 9
!
!
access-list 130 deny ip 10.0.0.0 0.0.0.63 10.0.0.128 0.0.0.63
access-list 130 deny ip 10.0.0.0 0.0.0.63 10.0.0.192 0.0.0.63
access-list 130 deny ip 10.0.0.0 0.0.0.63 10.0.1.0 0.0.0.63
access-list 130 deny ip 10.0.0.0 0.0.0.63 10.0.1.64 0.0.0.63
access-list 130 deny ip 10.0.0.0 0.0.0.63 10.0.1.128 0.0.0.63
access-list 130 deny ip 10.0.0.0 0.0.0.63 10.0.1.192 0.0.0.63
access-list 130 deny ip 10.0.0.0 0.0.0.63 10.0.2.64 0.0.0.63
access-list 130 permit ip any any
access-list 131 deny ip 10.0.0.64 0.0.0.63 10.0.0.128 0.0.0.63
access-list 131 deny ip 10.0.0.64 0.0.0.63 10.0.0.192 0.0.0.63
access-list 131 deny ip 10.0.0.64 0.0.0.63 10.0.1.0 0.0.0.63
access-list 131 deny ip 10.0.0.64 0.0.0.63 10.0.1.64 0.0.0.63
access-list 131 deny ip 10.0.0.64 0.0.0.63 10.0.1.128 0.0.0.63
access-list 131 deny ip 10.0.0.64 0.0.0.63 10.0.1.192 0.0.0.63
access-list 131 deny ip 10.0.0.64 0.0.0.63 10.0.2.64 0.0.0.63
access-list 131 permit ip any any
```

```
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.14. Switch Distribución 2

A continuación se muestra la configuración completa del dispositivo de red Switch Distribución 2.

Listing A.35: Configuración Completa Switch Distribución 2

```
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sw.Distribucion2
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
```

```
!
username admin password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
spanning-tree mode rapid-pvst
!
!
!
!
!
!
interface GigabitEthernet1/0/1
 switchport trunk allowed vlan 2-9,11-19,21-39,41-199,201-1001
 switchport mode trunk
!
interface GigabitEthernet1/0/2
 switchport trunk allowed vlan 2-199,201-1001
 switchport mode trunk
!
interface GigabitEthernet1/0/3
 switchport trunk allowed vlan 40
 switchport mode trunk
!
interface GigabitEthernet1/0/4
 switchport trunk allowed vlan 40
 switchport mode trunk
!
interface GigabitEthernet1/0/5
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/6
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/7
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/8
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/9
 switchport trunk allowed vlan 2-1001
```

```
!
interface GigabitEthernet1/0/10
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/11
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/12
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/13
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/14
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/15
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/16
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/17
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/18
 switchport trunk allowed vlan 2-199,201-1001
!
interface GigabitEthernet1/0/19
 switchport trunk allowed vlan 2-19,21-29,31-39,41-199,201-1001
 switchport mode trunk
!
interface GigabitEthernet1/0/20
 switchport trunk allowed vlan 2-9,11-29,31-39,41-199,201-1001
 switchport mode trunk
!
interface GigabitEthernet1/0/21
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/22
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/23
 switchport trunk allowed vlan 2-204,206-1001
!
interface GigabitEthernet1/0/24
 switchport trunk allowed vlan 2-204,206-1001
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
```

```
!
interface GigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 mac-address 0002.1749.2801
 ip address 10.0.0.3 255.255.255.192
 ip helper-address 10.0.3.6
 standby 10 ip 10.0.0.1
 standby 10 preempt
!
interface Vlan20
 mac-address 0002.1749.2802
 ip address 10.0.0.67 255.255.255.192
 ip helper-address 10.0.3.6
 standby 20 ip 10.0.0.65
 standby 20 preempt
!
interface Vlan30
 mac-address 0002.1749.2803
 ip address 10.0.0.130 255.255.255.192
 ip helper-address 10.0.3.6
 standby 30 ip 10.0.0.129
 standby 30 priority 110
 standby 30 preempt
!
interface Vlan40
 mac-address 0002.1749.2804
 ip address 10.0.0.194 255.255.255.192
 ip helper-address 10.0.3.6
 standby 40 ip 10.0.0.193
 standby 40 priority 110
 standby 40 preempt
!
interface Vlan200
 mac-address 0002.1749.2805
 ip address 10.1.0.2 255.255.255.224
 ip ospf cost 10
!
interface Vlan205
 mac-address 0002.1749.2806
 ip address 10.1.1.2 255.255.255.224
 ip ospf cost 100
!
router ospf 10
 log-adjacency-changes
 network 10.0.0.0 0.0.0.63 area 0
 network 10.0.0.64 0.0.0.63 area 0
 network 10.0.0.128 0.0.0.63 area 0
 network 10.0.0.192 0.0.0.63 area 0
```

```
 network 10.1.0.0 0.0.0.31 area 0
 network 10.1.1.0 0.0.0.31 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.15. Switch Distribución 3

A continuación se muestra la configuración completa del dispositivo de red Switch Distribución 3.

Listing A.36: Configuración Completa Switch Distribución 3

```
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sw.Distribucion3
!
!
enable password 7 0822455D0A16
!
!
!
!
```

```
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
spanning-tree mode rapid-pvst
!
!
!
!
!
!
interface GigabitEthernet1/0/1
 switchport trunk allowed vlan 2-29,31-39,41-59,61-1001
!
interface GigabitEthernet1/0/2
 switchport trunk allowed vlan 2-204,206-1001
!
interface GigabitEthernet1/0/3
 switchport trunk allowed vlan 30,40,50,60,200
 switchport mode trunk
!
interface GigabitEthernet1/0/4
 switchport trunk allowed vlan 60
 switchport mode trunk
!
interface GigabitEthernet1/0/5
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/6
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/7
 switchport trunk allowed vlan 2-1001
```

```
!
interface GigabitEthernet1/0/8
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/9
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/10
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/11
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/12
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/13
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/14
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/15
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/16
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/17
 switchport trunk allowed vlan 2-39,41-49,51-59,61-1001
 switchport mode trunk
!
interface GigabitEthernet1/0/18
 switchport trunk allowed vlan 2-29,31-49,51-59,61-1001
 switchport mode trunk
!
interface GigabitEthernet1/0/19
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/20
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/21
 switchport trunk allowed vlan 2-199,201-1001
!
interface GigabitEthernet1/0/22
 switchport trunk allowed vlan 2-199,201-1001
 switchport mode trunk
!
interface GigabitEthernet1/0/23
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/24
```

```
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan30
 mac-address 0001.9619.ac01
 ip address 10.0.0.131 255.255.255.192
 ip helper-address 10.0.3.6
 standby 30 ip 10.0.0.129
 standby 30 preempt
!
interface Vlan40
 mac-address 0001.9619.ac02
 ip address 10.0.0.195 255.255.255.192
 ip helper-address 10.0.3.6
 standby 40 ip 10.0.0.193
 standby 40 preempt
!
interface Vlan50
 mac-address 0001.9619.ac03
 ip address 10.0.1.2 255.255.255.192
 ip helper-address 10.0.3.6
 standby 50 ip 10.0.1.1
 standby 50 priority 110
 standby 50 preempt
!
interface Vlan60
 mac-address 0001.9619.ac04
 ip address 10.0.1.66 255.255.255.192
 ip helper-address 10.0.3.6
 standby 60 ip 10.0.1.65
 standby 60 priority 110
 standby 60 preempt
!
interface Vlan200
 mac-address 0001.9619.ac05
 ip address 10.1.0.3 255.255.255.224
 ip ospf cost 10
!
interface Vlan205
 mac-address 0001.9619.ac06
 ip address 10.1.1.3 255.255.255.224
 ip ospf cost 100
```

```
!
router ospf 10
 log-adjacency-changes
 network 10.0.1.0 0.0.0.63 area 0
 network 10.0.1.64 0.0.0.63 area 0
 network 10.0.0.128 0.0.0.63 area 0
 network 10.0.0.192 0.0.0.63 area 0
 network 10.1.0.0 0.0.0.31 area 0
 network 10.1.1.0 0.0.0.31 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.16. Switch Distribución 4

A continuación se muestra la configuración completa del dispositivo de red Switch Distribución 4.

Listing A.37: Configuración Completa Switch Distribución 4

```
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sw.Distribucion4
```

```
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
spanning-tree mode rapid-pvst
!
!
!
!
!
!
interface Port-channel1
 switchport trunk allowed vlan 70
 switchport mode trunk
!
interface Port-channel2
 switchport trunk allowed vlan 80
 switchport mode trunk
!
interface GigabitEthernet1/0/1
 switchport trunk allowed vlan 70
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet1/0/2
 switchport trunk allowed vlan 70
```

```
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet1/0/3
 switchport trunk allowed vlan 80
 switchport mode trunk
 channel-group 2 mode active
!
interface GigabitEthernet1/0/4
 switchport trunk allowed vlan 80
 switchport mode trunk
 channel-group 2 mode active
!
interface GigabitEthernet1/0/5
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/6
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/7
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/8
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/9
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/10
 switchport trunk allowed vlan 2-204,206-1001
!
interface GigabitEthernet1/0/11
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/12
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/13
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/14
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/15
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/16
 switchport trunk allowed vlan 2-59,61-69,71-79,81-1001
 switchport mode trunk
!
interface GigabitEthernet1/0/17
 switchport trunk allowed vlan 2-49,51-69,71-79,81-1001
 switchport mode trunk
```

```
!
interface GigabitEthernet1/0/18
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/19
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/20
 switchport trunk allowed vlan 2-204,206-1001
!
interface GigabitEthernet1/0/21
 switchport trunk allowed vlan 2-199,201-1001
!
interface GigabitEthernet1/0/22
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/23
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/24
 switchport trunk allowed vlan 2-199,201-1001
 switchport mode trunk
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan50
 mac-address 0001.9720.ea01
 ip address 10.0.1.3 255.255.255.192
 ip helper-address 10.0.3.6
 standby 50 ip 10.0.1.1
 standby 50 preempt
!
interface Vlan60
 mac-address 0001.9720.ea02
 ip address 10.0.1.67 255.255.255.192
 ip helper-address 10.0.3.6
 standby 60 ip 10.0.1.65
 standby 60 preempt
!
interface Vlan70
 mac-address 0001.9720.ea03
 ip address 10.0.1.130 255.255.255.192
 ip helper-address 10.0.3.6
```

```
 standby 70 ip 10.0.1.129
 standby 70 priority 110
 standby 70 preempt
!
interface Vlan80
 mac-address 0001.9720.ea04
 ip address 10.0.1.194 255.255.255.192
 ip helper-address 10.0.3.6
 standby 80 ip 10.0.1.193
 standby 80 priority 110
 standby 80 preempt
!
interface Vlan200
 mac-address 0001.9720.ea05
 ip address 10.1.0.4 255.255.255.224
 ip ospf cost 10
!
interface Vlan205
 mac-address 0001.9720.ea06
 ip address 10.1.1.4 255.255.255.224
 ip ospf cost 100
!
router ospf 10
 log-adjacency-changes
 network 10.0.1.0 0.0.0.63 area 0
 network 10.0.1.64 0.0.0.63 area 0
 network 10.0.1.128 0.0.0.63 area 0
 network 10.0.1.192 0.0.0.63 area 0
 network 10.1.0.0 0.0.0.31 area 0
 network 10.1.1.0 0.0.0.31 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
```

```
 transport input ssh
!
!
!
!
end
```

A.22.17. Switch Distribución 5

A continuación se muestra la configuración completa del dispositivo de red Switch Distribución 5.

Listing A.38: Configuración Completa Switch Distribución 5

```
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sw.Distribucion5
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
spanning-tree mode rapid-pvst
```

```
!
!
!
!
!
!
interface Port-channel1
 switchport trunk allowed vlan 90
 switchport mode trunk
!
interface Port-channel2
 switchport trunk allowed vlan 100
 switchport mode trunk
!
interface GigabitEthernet1/0/1
 switchport trunk allowed vlan 90
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet1/0/2
 switchport trunk allowed vlan 90
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet1/0/3
 switchport trunk allowed vlan 100
 switchport mode trunk
 channel-group 2 mode active
!
interface GigabitEthernet1/0/4
 switchport trunk allowed vlan 100
 switchport mode trunk
 channel-group 2 mode active
!
interface GigabitEthernet1/0/5
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/6
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/7
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/8
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/9
 switchport trunk allowed vlan 30,40
 switchport mode trunk
!
interface GigabitEthernet1/0/10
 switchport trunk allowed vlan 30,40
 switchport mode trunk
```

```
!
interface GigabitEthernet1/0/11
 switchport trunk allowed vlan 50,60
 switchport mode trunk
!
interface GigabitEthernet1/0/12
 switchport trunk allowed vlan 50,60
 switchport mode trunk
!
interface GigabitEthernet1/0/13
 switchport trunk allowed vlan 70,80
 switchport mode trunk
!
interface GigabitEthernet1/0/14
 switchport trunk allowed vlan 70,80
 switchport mode trunk
!
interface GigabitEthernet1/0/15
 switchport trunk allowed vlan 2-29,31-39,41-49,51-59,61-199,201-1001
 switchport mode trunk
!
interface GigabitEthernet1/0/16
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/17
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/18
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/19
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/20
 switchport trunk allowed vlan 2-29,31-39,41-49,51-59,61-204,206-1001
!
interface GigabitEthernet1/0/21
 switchport trunk allowed vlan 2-29,31-39,41-49,51-59,61-204,206-1001
!
interface GigabitEthernet1/0/22
 switchport trunk allowed vlan 2-29,31-39,41-49,51-59,61-1001
!
interface GigabitEthernet1/0/23
 switchport trunk allowed vlan 2-29,31-39,41-49,51-59,61-1001
!
interface GigabitEthernet1/0/24
 switchport trunk allowed vlan 2-29,31-39,41-49,51-59,61-199,201-1001
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
```

```
!
interface GigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan70
 mac-address 00d0.ba85.e601
 ip address 10.0.1.131 255.255.255.192
 ip helper-address 10.0.3.6
 standby 70 ip 10.0.1.129
 standby 70 preempt
!
interface Vlan80
 mac-address 00d0.ba85.e602
 ip address 10.0.1.195 255.255.255.192
 ip helper-address 10.0.3.6
 standby 80 ip 10.0.1.193
 standby 80 preempt
!
interface Vlan90
 mac-address 00d0.ba85.e603
 ip address 10.0.2.2 255.255.255.192
 ip helper-address 10.0.3.6
 ip access-group 132 in
 standby 90 ip 10.0.2.1
 standby 90 priority 110
 standby 90 preempt
!
interface Vlan100
 mac-address 00d0.ba85.e604
 ip address 10.0.2.66 255.255.255.192
 ip helper-address 10.0.3.6
 ip access-group 133 in
 standby 100 ip 10.0.2.65
 standby 100 priority 110
 standby 100 preempt
!
interface Vlan200
 mac-address 00d0.ba85.e605
 ip address 10.1.0.5 255.255.255.224
 ip ospf cost 10
!
interface Vlan205
 mac-address 00d0.ba85.e606
 ip address 10.1.1.5 255.255.255.224
 ip ospf cost 100
!
router ospf 10
 log-adjacency-changes
 network 10.0.2.0 0.0.0.63 area 0
 network 10.0.2.64 0.0.0.63 area 0
```

```
 network 10.0.1.128 0.0.0.63 area 0
 network 10.0.1.192 0.0.0.63 area 0
 network 10.1.0.0 0.0.0.31 area 0
 network 10.1.1.0 0.0.0.31 area 0
!
ip classless
!
ip flow-export version 9
!
!
access-list 132 deny ip 10.0.2.0 0.0.0.63 10.0.0.128 0.0.0.63
access-list 132 deny ip 10.0.2.0 0.0.0.63 10.0.0.192 0.0.0.63
access-list 132 deny ip 10.0.2.0 0.0.0.63 10.0.1.0 0.0.0.63
access-list 132 deny ip 10.0.2.0 0.0.0.63 10.0.1.64 0.0.0.63
access-list 132 deny ip 10.0.2.0 0.0.0.63 10.0.1.128 0.0.0.63
access-list 132 deny ip 10.0.2.0 0.0.0.63 10.0.1.192 0.0.0.63
access-list 132 deny ip 10.0.2.0 0.0.0.63 10.0.2.64 0.0.0.63
access-list 132 permit ip any any
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.18. Switch Distribución 6

A continuación se muestra la configuración completa del dispositivo de red Switch Distribución 6.

Listing A.39: Configuración Completa Switch Distribución 6

```
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
```

```
service password-encryption
!
hostname Sw.Distribucion6
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
spanning-tree mode rapid-pvst
!
!
!
!
!
!
interface Port-channel1
 switchport trunk allowed vlan 110
 switchport mode trunk
!
interface Port-channel2
 switchport trunk allowed vlan 120
 switchport mode trunk
!
interface GigabitEthernet1/0/1
 switchport trunk allowed vlan 110
 switchport mode trunk
 channel-group 1 mode active
```

```
!
interface GigabitEthernet1/0/2
 switchport trunk allowed vlan 110
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet1/0/3
 switchport trunk allowed vlan 120
 switchport mode trunk
 channel-group 2 mode active
!
interface GigabitEthernet1/0/4
 switchport trunk allowed vlan 120
 switchport mode trunk
 channel-group 2 mode active
!
interface GigabitEthernet1/0/5
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/6
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/7
 switchport trunk allowed vlan 90
 switchport mode trunk
!
interface GigabitEthernet1/0/8
 switchport trunk allowed vlan 100
 switchport mode trunk
!
interface GigabitEthernet1/0/9
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/10
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/11
 switchport trunk allowed vlan 2-199,201-1001
 switchport mode trunk
!
interface GigabitEthernet1/0/12
 switchport trunk allowed vlan 2-204,206-1001
!
interface GigabitEthernet1/0/13
 switchport trunk allowed vlan 2-204,206-1001
!
interface GigabitEthernet1/0/14
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/15
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/16
```

```
 switchport trunk allowed vlan 2-199,201-1001
!
interface GigabitEthernet1/0/17
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/18
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/19
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/20
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/21
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/22
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/23
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/24
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan90
 mac-address 0001.631b.c001
 ip address 10.0.2.3 255.255.255.192
 ip helper-address 10.0.3.6
 standby 90 ip 10.0.2.1
 standby 90 preempt
!
interface Vlan100
 mac-address 0001.631b.c002
 ip address 10.0.2.67 255.255.255.192
 ip helper-address 10.0.3.6
 standby 100 ip 10.0.2.65
 standby 100 preempt
!
interface Vlan110
```

```
 mac-address 0001.631b.c003
 ip address 10.0.2.130 255.255.255.192
 ip helper-address 10.0.3.6
 ip access-group 134 in
 standby 110 ip 10.0.2.129
 standby 110 priority 110
 standby 110 preempt
!
interface Vlan120
 mac-address 0001.631b.c004
 ip address 10.0.2.194 255.255.255.192
 ip helper-address 10.0.3.6
 ip access-group 135 in
 standby 120 ip 10.0.2.193
 standby 120 priority 110
 standby 120 preempt
!
interface Vlan200
 mac-address 0001.631b.c005
 ip address 10.1.0.6 255.255.255.224
 ip ospf cost 10
!
interface Vlan205
 mac-address 0001.631b.c006
 ip address 10.1.1.6 255.255.255.224
 ip ospf cost 100
!
router ospf 10
 log-adjacency-changes
 network 10.0.2.0 0.0.0.63 area 0
 network 10.0.2.64 0.0.0.63 area 0
 network 10.0.2.128 0.0.0.63 area 0
 network 10.0.2.192 0.0.0.63 area 0
 network 10.1.0.0 0.0.0.31 area 0
 network 10.1.1.0 0.0.0.31 area 0
!
ip classless
!
ip flow-export version 9
!
!
access-list 134 deny ip 10.0.2.128 0.0.0.63 10.0.0.128 0.0.0.63
access-list 134 deny ip 10.0.2.128 0.0.0.63 10.0.0.192 0.0.0.63
access-list 134 deny ip 10.0.2.128 0.0.0.63 10.0.1.0 0.0.0.63
access-list 134 deny ip 10.0.2.128 0.0.0.63 10.0.1.64 0.0.0.63
access-list 134 deny ip 10.0.2.128 0.0.0.63 10.0.1.128 0.0.0.63
access-list 134 deny ip 10.0.2.128 0.0.0.63 10.0.1.192 0.0.0.63
access-list 134 permit ip any any
access-list 133 deny ip 10.0.2.128 0.0.0.63 10.0.2.64 0.0.0.63
access-list 135 deny ip 10.0.2.192 0.0.0.63 10.0.0.128 0.0.0.63
access-list 135 deny ip 10.0.2.192 0.0.0.63 10.0.0.192 0.0.0.63
access-list 135 deny ip 10.0.2.192 0.0.0.63 10.0.1.0 0.0.0.63
access-list 135 deny ip 10.0.2.192 0.0.0.63 10.0.1.64 0.0.0.63
```

```
access-list 135 deny ip 10.0.2.192 0.0.0.63 10.0.1.128 0.0.0.63
access-list 135 deny ip 10.0.2.192 0.0.0.63 10.0.1.192 0.0.0.63
access-list 135 deny ip 10.0.2.192 0.0.0.63 10.0.2.64 0.0.0.63
access-list 135 permit ip any any
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.19. Switch Core 1

A continuación se muestra la configuración completa del dispositivo de red Switch Core 1.

Listing A.40: Configuración Completa Switch Core 1

```
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sw.Core1
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
ip routing
!
```

```
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
spanning-tree mode rapid-pvst
!
!
!
!
!
!
interface GigabitEthernet1/0/1
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120,250
 switchport mode trunk
!
interface GigabitEthernet1/0/2
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120,250
 switchport mode trunk
!
interface GigabitEthernet1/0/3
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120,250
 switchport mode trunk
!
interface GigabitEthernet1/0/4
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120,200
 switchport mode trunk
!
interface GigabitEthernet1/0/5
 switchport trunk allowed vlan 10,20,110,120,200
 switchport mode trunk
!
interface GigabitEthernet1/0/6
 switchport trunk allowed vlan 10,20,30,40,200
 switchport mode trunk
!
interface GigabitEthernet1/0/7
 switchport trunk allowed vlan 30,40,50,60,200
 switchport mode trunk
```

```
!
interface GigabitEthernet1/0/8
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
interface GigabitEthernet1/0/9
 switchport trunk allowed vlan 30,40,50,60,70,80,100,200,210
 switchport mode trunk
!
interface GigabitEthernet1/0/10
 switchport trunk allowed vlan 30,40,50,60,70,80,100,200,212
 switchport mode trunk
!
interface GigabitEthernet1/0/11
 switchport trunk allowed vlan 30,40,50,60,70,80,100,200,211
 switchport mode trunk
!
interface GigabitEthernet1/0/12
 switchport trunk allowed vlan 30,40,50,60,70,80,100,200,213,220,230
 switchport mode trunk
!
interface GigabitEthernet1/0/13
 switchport trunk allowed vlan 50,60,70,80,200
 switchport mode trunk
!
interface GigabitEthernet1/0/14
 switchport trunk allowed vlan 70,80,90,100,200
 switchport mode trunk
!
interface GigabitEthernet1/0/15
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
interface GigabitEthernet1/0/16
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
interface GigabitEthernet1/0/17
 switchport trunk allowed vlan 90,100,110,120,200
 switchport mode trunk
!
interface GigabitEthernet1/0/18
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
interface GigabitEthernet1/0/19
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
interface GigabitEthernet1/0/20
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
```

```
interface GigabitEthernet1/0/21
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
interface GigabitEthernet1/0/22
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
interface GigabitEthernet1/0/23
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
interface GigabitEthernet1/0/24
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan200
 mac-address 00e0.b09b.0a01
 ip address 10.1.0.7 255.255.255.224
 ip ospf cost 10
!
interface Vlan250
 mac-address 00e0.b09b.0a02
 ip address 10.2.0.5 255.255.255.248
!
router ospf 10
 log-adjacency-changes
 network 10.2.0.0 0.0.0.7 area 0
 network 10.1.0.0 0.0.0.31 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
```

```
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.20. Switch Core 2

A continuación se muestra la configuración completa del dispositivo de red Switch Core 2.

Listing A.41: Configuración Completa Switch Core 2

```
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sw.Core2
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
!
!
!
```

```
!
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
spanning-tree mode rapid-pvst
!
!
!
!
!
!
interface GigabitEthernet1/0/1
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120,255
 switchport mode trunk
!
interface GigabitEthernet1/0/2
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120,255
 switchport mode trunk
!
interface GigabitEthernet1/0/3
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120,255
 switchport mode trunk
!
interface GigabitEthernet1/0/4
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120,200
 switchport mode trunk
!
interface GigabitEthernet1/0/5
 switchport trunk allowed vlan 10,20,110,120,200
 switchport mode trunk
!
interface GigabitEthernet1/0/6
 switchport trunk allowed vlan 10,20,30,40,200
 switchport mode trunk
!
interface GigabitEthernet1/0/7
 switchport trunk allowed vlan 30,40,50,60,200
 switchport mode trunk
!
interface GigabitEthernet1/0/8
 switchport trunk allowed vlan 90,100,110,120,200
 switchport mode trunk
!
interface GigabitEthernet1/0/9
 switchport trunk allowed vlan 30,40,50,60,70,80,100,200,210
 switchport mode trunk
!
interface GigabitEthernet1/0/10
```

```
 switchport trunk allowed vlan 30,40,50,60,70,80,100,200,212
 switchport mode trunk
!
interface GigabitEthernet1/0/11
 switchport trunk allowed vlan 30,40,50,60,70,80,100,200,211
 switchport mode trunk
!
interface GigabitEthernet1/0/12
 switchport trunk allowed vlan 30,40,50,60,70,80,100,200,213,220,230
 switchport mode trunk
!
interface GigabitEthernet1/0/13
 switchport trunk allowed vlan 50,60,70,80,200
 switchport mode trunk
!
interface GigabitEthernet1/0/14
 switchport trunk allowed vlan 70,80,90,100,200
 switchport mode trunk
!
interface GigabitEthernet1/0/15
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
interface GigabitEthernet1/0/16
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
interface GigabitEthernet1/0/17
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
interface GigabitEthernet1/0/18
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
interface GigabitEthernet1/0/19
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
interface GigabitEthernet1/0/20
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
interface GigabitEthernet1/0/21
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
interface GigabitEthernet1/0/22
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
interface GigabitEthernet1/0/23
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
```

```
 switchport mode trunk
!
interface GigabitEthernet1/0/24
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,100,110,120
 switchport mode trunk
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan200
 mac-address 0006.2abc.9a01
 ip address 10.1.0.8 255.255.255.224
 ip ospf cost 10
!
interface Vlan255
 mac-address 0006.2abc.9a02
 ip address 10.2.1.5 255.255.255.248
!
router ospf 10
 log-adjacency-changes
 network 10.2.1.0 0.0.0.7 area 0
 network 10.1.0.0 0.0.0.31 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
```

```
 login local
 transport input ssh
!
!
!
!
end
```

A.22.21. Switch IoMT Planta 0

A continuación se muestra la configuración completa del dispositivo de red Switch IoMT Planta 0.

Listing A.42: Configuración Completa Switch IoMT Planta 0

```
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sw.IoMT-P0
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
```

```
spanning-tree mode rapid-pvst
!
!
!
!
!
!
interface GigabitEthernet1/0/1
 switchport access vlan 210
!
interface GigabitEthernet1/0/2
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/3
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/4
 switchport access vlan 210
!
interface GigabitEthernet1/0/5
 switchport access vlan 210
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
```

```
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan200
 mac-address 0001.64e1.1201
 ip address 10.1.0.9 255.255.255.224
!
interface Vlan210
 mac-address 0001.64e1.1202
 ip address 172.16.0.1 255.255.240.0
 ip helper-address 172.16.192.5
 ip access-group 121 in
 ip access-group 120 out
!
router ospf 10
 log-adjacency-changes
 network 172.16.0.0 0.0.15.255 area 0
 network 10.1.0.0 0.0.0.31 area 0
!
ip classless
!
ip flow-export version 9
!
!
access-list 120 permit udp any any eq bootps
access-list 120 permit udp any any eq bootpc
access-list 120 permit ospf any any
access-list 120 permit ip 10.0.2.64 0.0.0.63 172.16.0.0 0.0.15.255
access-list 120 permit ip 10.0.0.128 0.0.0.63 172.16.0.0 0.0.15.255
access-list 120 permit ip 10.0.0.192 0.0.0.63 172.16.0.0 0.0.15.255
access-list 120 permit ip 10.0.1.0 0.0.0.63 172.16.0.0 0.0.15.255
access-list 120 permit ip 10.0.1.64 0.0.0.63 172.16.0.0 0.0.15.255
access-list 120 permit ip 10.0.1.128 0.0.0.63 172.16.0.0 0.0.15.255
access-list 120 permit ip 10.0.1.192 0.0.0.63 172.16.0.0 0.0.15.255
access-list 120 deny ip any any
access-list 121 permit udp any any eq bootps
access-list 121 permit udp any any eq bootpc
```

```
access-list 121 permit ospf any any
access-list 121 permit ip 172.16.0.0 0.0.15.255 10.0.2.64 0.0.0.63
access-list 121 permit ip 172.16.0.0 0.0.15.255 10.0.0.128 0.0.0.63
access-list 121 permit ip 172.16.0.0 0.0.15.255 10.0.0.192 0.0.0.63
access-list 121 permit ip 172.16.0.0 0.0.15.255 10.0.1.0 0.0.0.63
access-list 121 permit ip 172.16.0.0 0.0.15.255 10.0.1.64 0.0.0.63
access-list 121 permit ip 172.16.0.0 0.0.15.255 10.0.1.128 0.0.0.63
access-list 121 permit ip 172.16.0.0 0.0.15.255 10.0.1.192 0.0.0.63
access-list 121 deny ip any any
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.22. Switch IoMT Planta 1

A continuación se muestra la configuración completa del dispositivo de red Switch IoMT Planta 1.

Listing A.43: Configuración Completa Switch IoMT Planta 1

```
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sw.IoMT-P1
!
!
enable password 7 0822455D0A16
!
!
!
```

```
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
spanning-tree mode rapid-pvst
!
!
!
!
!
!
interface GigabitEthernet1/0/1
 switchport access vlan 211
!
interface GigabitEthernet1/0/2
 switchport access vlan 211
!
interface GigabitEthernet1/0/3
 switchport access vlan 211
!
interface GigabitEthernet1/0/4
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/5
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
```

```
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan200
 mac-address 0001.c79a.3701
 ip address 10.1.0.10 255.255.255.224
!
interface Vlan211
 mac-address 0001.c79a.3702
 ip address 172.16.16.1 255.255.240.0
 ip helper-address 172.16.192.5
 ip access-group 121 in
```

```
 ip access-group 120 out
!
router ospf 10
 log-adjacency-changes
 network 172.16.16.0 0.0.15.255 area 0
 network 10.1.0.0 0.0.0.31 area 0
!
ip classless
!
ip flow-export version 9
!
!
access-list 120 permit udp any any eq bootps
access-list 120 permit udp any any eq bootpc
access-list 120 permit ospf any any
access-list 120 permit ip 10.0.2.64 0.0.0.63 172.16.16.0 0.0.15.255
access-list 120 permit ip 10.0.0.128 0.0.0.63 172.16.16.0 0.0.15.255
access-list 120 permit ip 10.0.0.192 0.0.0.63 172.16.16.0 0.0.15.255
access-list 120 permit ip 10.0.1.0 0.0.0.63 172.16.16.0 0.0.15.255
access-list 120 permit ip 10.0.1.64 0.0.0.63 172.16.16.0 0.0.15.255
access-list 120 permit ip 10.0.1.128 0.0.0.63 172.16.16.0 0.0.15.255
access-list 120 permit ip 10.0.1.192 0.0.0.63 172.16.16.0 0.0.15.255
access-list 120 deny ip any any
access-list 121 permit udp any any eq bootps
access-list 121 permit udp any any eq bootpc
access-list 121 permit ospf any any
access-list 121 permit ip 172.16.16.0 0.0.15.255 10.0.2.64 0.0.0.63
access-list 121 permit ip 172.16.16.0 0.0.15.255 10.0.0.128 0.0.0.63
access-list 121 permit ip 172.16.16.0 0.0.15.255 10.0.0.192 0.0.0.63
access-list 121 permit ip 172.16.16.0 0.0.15.255 10.0.1.0 0.0.0.63
access-list 121 permit ip 172.16.16.0 0.0.15.255 10.0.1.64 0.0.0.63
access-list 121 permit ip 172.16.16.0 0.0.15.255 10.0.1.128 0.0.0.63
access-list 121 permit ip 172.16.16.0 0.0.15.255 10.0.1.192 0.0.0.63
access-list 121 deny ip any any
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
```

```
!
!
!
end
```

A.22.23. Switch IoMT Planta 2

A continuación se muestra la configuración completa del dispositivo de red Switch IoMT Planta 2.

Listing A.44: Configuración Completa Switch IoMT Planta 2

```
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sw.IoMT-P2
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
spanning-tree mode rapid-pvst
!
!
```

```
!
!
!
!
interface GigabitEthernet1/0/1
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/2
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/3
 switchport access vlan 212
!
interface GigabitEthernet1/0/4
 switchport access vlan 212
!
interface GigabitEthernet1/0/5
 switchport access vlan 212
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
```

```
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan200
 mac-address 0005.5ed1.1701
 ip address 10.1.0.11 255.255.255.224
!
interface Vlan212
 mac-address 0005.5ed1.1702
 ip address 172.16.32.1 255.255.240.0
 ip helper-address 172.16.192.5
 ip access-group 121 in
 ip access-group 120 out
!
router ospf 10
 log-adjacency-changes
 network 172.16.32.0 0.0.15.255 area 0
 network 10.1.0.0 0.0.0.31 area 0
!
ip classless
!
ip flow-export version 9
!
!
access-list 120 permit udp any any eq bootps
access-list 120 permit udp any any eq bootpc
access-list 120 permit ospf any any
access-list 120 permit ip 10.0.2.64 0.0.0.63 172.16.32.0 0.0.15.255
access-list 120 permit ip 10.0.0.128 0.0.0.63 172.16.32.0 0.0.15.255
access-list 120 permit ip 10.0.0.192 0.0.0.63 172.16.32.0 0.0.15.255
access-list 120 permit ip 10.0.1.0 0.0.0.63 172.16.32.0 0.0.15.255
access-list 120 permit ip 10.0.1.64 0.0.0.63 172.16.32.0 0.0.15.255
access-list 120 permit ip 10.0.1.128 0.0.0.63 172.16.32.0 0.0.15.255
access-list 120 permit ip 10.0.1.192 0.0.0.63 172.16.32.0 0.0.15.255
access-list 120 deny ip any any
access-list 121 permit udp any any eq bootps
access-list 121 permit udp any any eq bootpc
access-list 121 permit ospf any any
access-list 121 permit ip 172.16.32.0 0.0.15.255 10.0.2.64 0.0.0.63
access-list 121 permit ip 172.16.32.0 0.0.15.255 10.0.0.128 0.0.0.63
```

```
access-list 121 permit ip 172.16.32.0 0.0.15.255 10.0.0.192 0.0.0.63
access-list 121 permit ip 172.16.32.0 0.0.15.255 10.0.1.0 0.0.0.63
access-list 121 permit ip 172.16.32.0 0.0.15.255 10.0.1.64 0.0.0.63
access-list 121 permit ip 172.16.32.0 0.0.15.255 10.0.1.128 0.0.0.63
access-list 121 permit ip 172.16.32.0 0.0.15.255 10.0.1.192 0.0.0.63
access-list 121 deny ip any any
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.24. Switch IoMT Planta 3

A continuación se muestra la configuración completa del dispositivo de red Switch IoMT Planta 3.

Listing A.45: Configuración Completa Switch IoMT Planta 3

```
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sw.IoMT-P3
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
```

```
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
spanning-tree mode rapid-pvst
!
!
!
!
!
!
interface GigabitEthernet1/0/1
 switchport access vlan 213
!
interface GigabitEthernet1/0/2
 switchport access vlan 220
!
interface GigabitEthernet1/0/3
 switchport access vlan 213
!
interface GigabitEthernet1/0/4
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/5
 switchport trunk allowed vlan 2-1001
!
interface GigabitEthernet1/0/6
 switchport access vlan 230
!
interface GigabitEthernet1/0/7
 switchport access vlan 230
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
```

```
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan200
 mac-address 0001.c9c5.8601
 ip address 10.1.0.12 255.255.255.224
!
interface Vlan212
 mac-address 0001.c9c5.8602
 no ip address
!
interface Vlan213
 mac-address 0001.c9c5.8603
```

```
 ip address 172.16.48.1 255.255.240.0
 ip helper-address 172.16.192.5
 ip access-group 121 in
 ip access-group 120 out
!
interface Vlan220
 mac-address 0001.c9c5.8604
 ip address 172.16.64.1 255.255.192.0
 ip helper-address 172.16.192.5
 ip access-group 102 in
 ip access-group 101 out
!
interface Vlan230
 mac-address 0001.c9c5.8605
 ip address 172.16.128.1 255.255.192.0
 ip helper-address 172.16.192.5
 ip access-group 104 in
 ip access-group 103 out
!
router ospf 10
 log-adjacency-changes
 network 172.16.48.0 0.0.15.255 area 0
 network 10.1.0.0 0.0.0.31 area 0
 network 172.16.64.0 0.0.31.255 area 0
 network 172.16.128.0 0.0.31.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
access-list 120 permit udp any any eq bootps
access-list 120 permit udp any any eq bootpc
access-list 120 permit ospf any any
access-list 120 permit ip 10.0.2.64 0.0.0.63 172.16.48.0 0.0.15.255
access-list 120 permit ip 10.0.0.128 0.0.0.63 172.16.48.0 0.0.15.255
access-list 120 permit ip 10.0.0.192 0.0.0.63 172.16.48.0 0.0.15.255
access-list 120 permit ip 10.0.1.0 0.0.0.63 172.16.48.0 0.0.15.255
access-list 120 permit ip 10.0.1.64 0.0.0.63 172.16.48.0 0.0.15.255
access-list 120 permit ip 10.0.1.128 0.0.0.63 172.16.48.0 0.0.15.255
access-list 120 permit ip 10.0.1.192 0.0.0.63 172.16.48.0 0.0.15.255
access-list 120 deny ip any any
access-list 121 permit udp any any eq bootps
access-list 121 permit udp any any eq bootpc
access-list 121 permit ospf any any
access-list 121 permit ip 172.16.48.0 0.0.15.255 10.0.2.64 0.0.0.63
access-list 121 permit ip 172.16.48.0 0.0.15.255 10.0.0.128 0.0.0.63
access-list 121 permit ip 172.16.48.0 0.0.15.255 10.0.0.192 0.0.0.63
access-list 121 permit ip 172.16.48.0 0.0.15.255 10.0.1.0 0.0.0.63
access-list 121 permit ip 172.16.48.0 0.0.15.255 10.0.1.64 0.0.0.63
access-list 121 permit ip 172.16.48.0 0.0.15.255 10.0.1.128 0.0.0.63
access-list 121 permit ip 172.16.48.0 0.0.15.255 10.0.1.192 0.0.0.63
access-list 121 deny ip any any
```

```
access-list 101 permit udp any any eq bootps
access-list 101 permit udp any any eq bootpc
access-list 101 permit ip 10.0.2.64 0.0.0.63 172.16.64.0 0.0.15.255
access-list 101 deny ip any any
access-list 102 permit udp any any eq bootps
access-list 102 permit udp any any eq bootpc
access-list 102 permit ip 172.16.64.0 0.0.15.255 10.0.2.64 0.0.0.63
access-list 102 deny ip any any
access-list 103 permit udp any any eq bootps
access-list 103 permit udp any any eq bootpc
access-list 103 permit ip host 10.0.2.70 172.16.128.0 0.0.15.255
access-list 103 deny ip any any
access-list 104 permit udp any any eq bootps
access-list 104 permit udp any any eq bootpc
access-list 104 permit ip 172.16.128.0 0.0.15.255 host 10.0.2.70
access-list 104 deny ip any any
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.25. Switch L3 Invitados

A continuación se muestra la configuración completa del dispositivo de red Switch L3 Invitados.

Listing A.46: Configuración Completa Switch L3 Invitados

```
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
```

```
hostname Sw.Guest
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
spanning-tree mode rapid-pvst
!
!
!
!
!
!
interface GigabitEthernet1/0/1
 switchport mode trunk
!
interface GigabitEthernet1/0/2
 switchport mode trunk
!
interface GigabitEthernet1/0/3
 switchport mode trunk
!
interface GigabitEthernet1/0/4
 switchport trunk allowed vlan 1-189,191-1005
 switchport mode trunk
!
interface GigabitEthernet1/0/5
```

```
 switchport trunk allowed vlan 1-189,191-1005
 switchport mode trunk
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
```

```
interface Vlan180
 mac-address 00d0.ba38.bc01
 ip address 192.168.0.1 255.255.128.0
 ip helper-address 192.168.128.5
!
interface Vlan190
 mac-address 00d0.ba38.bc02
 ip address 192.168.130.5 255.255.255.248
!
router ospf 10
 log-adjacency-changes
 network 192.168.0.0 0.0.127.255 area 0
 network 192.168.130.0 0.0.0.7 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.26. Switch L2 Invitados 1

A continuación se muestra la configuración completa del dispositivo de red Switch L2 Invitados 1.

Listing A.47: Configuración Completa Switch L2 Invitados 1

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

```
no service timestamps debug datetime msec
service password-encryption
!
hostname SW.Guest1
!
enable password 7 0822455D0A16
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
username admin privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 180
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport access vlan 180
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
```

```
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.27. Switch L2 Invitados 2

A continuación se muestra la configuración completa del dispositivo de red Switch L2 Invitados 2.

Listing A.48: Configuración Completa Switch L2 Invitados 2

```
!
```

```
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname SW.Guest2
!
enable password 7 0822455D0A16
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
username admin privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 180
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
```

```
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.28. Switch DMZ Interna

A continuación se muestra la configuración completa del dispositivo de red Switch DMZ Interna.

Listing A.49: Configuración Completa Switch DMZ Interna

```
!
```

```
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname DMZ-Interno
!
enable password 7 0822455D0A16
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
username admin privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport access vlan 150
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/5
 switchport access vlan 150
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/6
 switchport access vlan 150
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/7
 switchport access vlan 150
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/8
 switchport access vlan 150
 switchport mode access
```

```
!
interface FastEthernet0/9
 switchport access vlan 150
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 150
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 150
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 150
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 150
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 150
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 150
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 150
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 150
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 150
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 150
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 150
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 150
 switchport mode access
!
```

```
interface FastEthernet0/22
 switchport access vlan 150
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 150
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 150
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.29. Switch DMZ IoMT

A continuación se muestra la configuración completa del dispositivo de red Switch DMZ IoMT.

Listing A.50: Configuración Completa Switch DMZ IoMT

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
```

```
hostname DMZ-IoMT
!
enable password 7 0822455D0A16
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
username admin privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 160
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/2
 switchport access vlan 160
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/3
 switchport trunk allowed vlan 2-1001
 switchport mode trunk
!
interface FastEthernet0/4
 switchport access vlan 150
 switchport trunk allowed vlan 2-1001
 switchport mode trunk
!
interface FastEthernet0/5
 switchport access vlan 150
 switchport trunk allowed vlan 2-1001
 switchport mode trunk
!
interface FastEthernet0/6
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/7
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/8
```

```
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/9
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/10
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/11
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/12
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/13
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/14
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/15
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/16
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
```

```
interface FastEthernet0/17
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/18
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/19
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/20
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/21
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/22
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/23
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/24
 switchport access vlan 160
 switchport trunk allowed vlan 2-1001
 switchport mode access
 switchport port-security mac-address sticky
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
```

```
 no ip address
 shutdown
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.30. Switch DMZ Invitados

A continuación se muestra la configuración completa del dispositivo de red Switch DMZ Invitados.

Listing A.51: Configuración Completa Switch DMZ Invitados

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname DMZ-Web
!
enable password 7 0822455D0A16
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
username admin privilege 1 password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
```

```
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/5
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/6
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/7
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/8
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/9
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/10
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/11
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/12
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
```

```
interface FastEthernet0/13
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/14
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/15
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/16
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/17
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/18
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/19
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/20
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/21
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/22
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface FastEthernet0/23
 switchport access vlan 170
 switchport mode access
```

```
 switchport port-security mac-address sticky
!
interface FastEthernet0/24
 switchport access vlan 170
 switchport mode access
 switchport port-security mac-address sticky
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end
```

A.22.31. Router Principal

A continuación se muestra la configuración completa del dispositivo de red Router Principal.

Listing A.52: Configuración Completa Router Principal

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router_Principal
!
!
!
enable password 7 0822455D0A16
```

```
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
!
!
!
!
!
!
interface Serial0/0
 ip address 195.136.17.2 255.255.255.252
 ip nat outside
 clock rate 2000000
!
interface Serial1/0
 ip address 195.136.17.6 255.255.255.252
 ip nat outside
 clock rate 2000000
!
interface Serial2/0
 no ip address
 clock rate 2000000
!
interface GigabitEthernet3/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet3/0.160
 encapsulation dot1Q 160
 ip address 172.16.192.2 255.255.255.248
```

```
 ip nat inside
 standby 160 ip 172.16.192.1
 standby 160 priority 120
 standby 160 preempt
!
interface GigabitEthernet4/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet4/0.190
 encapsulation dot1Q 190
 ip address 192.168.130.2 255.255.255.248
 ip access-group 110 in
 ip access-group 111 out
 ip nat inside
 standby 190 ip 192.168.130.1
 standby 190 priority 120
 standby 190 preempt
!
interface GigabitEthernet5/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet6/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet6/0.250
 encapsulation dot1Q 250
 ip address 10.2.0.2 255.255.255.248
 ip nat inside
 standby 250 ip 10.2.0.1
 standby 250 priority 120
 standby 250 preempt
!
interface GigabitEthernet7/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet7/0.255
 encapsulation dot1Q 255
 ip address 10.2.1.2 255.255.255.248
 ip nat inside
 standby 255 ip 10.2.1.1
 standby 255 priority 120
 standby 255 preempt
```

```
!
interface GigabitEthernet8/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet8/0.170
 encapsulation dot1Q 170
 ip address 192.168.128.2 255.255.255.248
 ip access-group 110 in
 ip nat inside
 standby 170 ip 192.168.128.1
 standby 170 priority 120
 standby 170 preempt
!
interface GigabitEthernet9/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet9/0.150
 encapsulation dot1Q 150
 ip address 10.0.3.2 255.255.255.240
 standby 150 ip 10.0.3.1
 standby 150 priority 120
 standby 150 preempt
!
router ospf 10
 log-adjacency-changes
 network 10.2.0.0 0.0.0.7 area 0
 network 10.2.1.0 0.0.0.7 area 0
 network 10.0.3.0 0.0.0.15 area 0
 network 195.136.17.0 0.0.0.3 area 0
 network 195.136.17.4 0.0.0.3 area 0
 network 192.168.130.0 0.0.0.7 area 0
 network 192.168.128.0 0.0.0.7 area 0
 network 172.16.192.0 0.0.0.7 area 0
!
ip nat inside source list 1 interface Serial0/0 overload
ip nat inside source static 192.168.128.6 195.136.17.6
ip classless
!
ip flow-export version 9
!
!
access-list 1 permit 10.0.0.0 0.0.0.63
access-list 1 permit 10.0.0.64 0.0.0.63
access-list 1 permit 10.0.0.128 0.0.0.63
access-list 1 permit 10.0.0.192 0.0.0.63
access-list 1 permit 10.0.1.0 0.0.0.63
access-list 1 permit 10.0.1.64 0.0.0.63
```

```
access-list 1 permit 10.0.1.128 0.0.0.63
access-list 1 permit 10.0.1.192 0.0.0.63
access-list 1 permit 10.0.2.0 0.0.0.63
access-list 1 permit 10.0.2.64 0.0.0.63
access-list 1 permit 10.0.2.128 0.0.0.63
access-list 1 permit 10.0.2.192 0.0.0.63
access-list 1 permit 192.168.0.0 0.0.127.255
access-list 111 permit udp any any eq bootps
access-list 111 permit udp any any eq bootpc
access-list 111 permit ospf any any
access-list 111 permit udp any any eq 1985
access-list 111 permit udp any host 224.0.0.2
access-list 111 permit ip 195.136.17.0 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.8 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.16 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.4 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.12 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.20 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 deny ip any any
access-list 110 permit udp any any eq bootps
access-list 110 permit udp any any eq bootpc
access-list 110 permit ospf any any
access-list 110 permit udp any any eq 1985
access-list 110 permit udp any host 224.0.0.2
access-list 110 permit ip host 192.168.128.6 host 195.136.17.5
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.0 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.8 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.16 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.4 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.12 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.20 0.0.0.3
access-list 110 deny ip any any
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
```

```
!
end
```

A.22.32. Router Auxiliar 1

A continuación se muestra la configuración completa del dispositivo de red Router Auxiliar 1.

Listing A.53: Configuración Completa Router Auxiliar 1

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router_Auxiliar1
!
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
!
!
!
!
!
!
interface Serial0/0
 ip address 195.136.17.10 255.255.255.252
```

```
 ip nat outside
!
interface Serial1/0
 ip address 195.136.17.14 255.255.255.252
 ip nat outside
 clock rate 2000000
!
interface Serial2/0
 no ip address
 clock rate 2000000
!
interface GigabitEthernet3/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet3/0.160
 encapsulation dot1Q 160
 ip address 172.16.192.3 255.255.255.248
 ip nat inside
 standby 160 ip 172.16.192.1
 standby 160 priority 110
 standby 160 preempt
!
interface GigabitEthernet4/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet4/0.190
 encapsulation dot1Q 190
 ip address 192.168.130.3 255.255.255.248
 ip access-group 110 in
 ip access-group 111 out
 ip nat inside
 standby 190 ip 192.168.130.1
 standby 190 priority 110
 standby 190 preempt
!
interface GigabitEthernet5/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet6/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet6/0.150
```

```
 encapsulation dot1Q 150
 ip address 10.0.3.3 255.255.255.240
 standby 150 ip 10.0.3.1
 standby 150 priority 110
 standby 150 preempt
!
interface GigabitEthernet7/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet7/0.170
 encapsulation dot1Q 170
 ip address 192.168.128.3 255.255.255.248
 ip access-group 110 in
 ip nat inside
 standby 170 ip 192.168.128.1
 standby 170 priority 110
 standby 170 preempt
!
interface GigabitEthernet8/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet8/0.255
 encapsulation dot1Q 255
 ip address 10.2.1.3 255.255.255.248
 ip nat inside
 standby 255 ip 10.2.1.1
 standby 255 priority 110
 standby 255 preempt
!
interface GigabitEthernet9/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet9/0.250
 encapsulation dot1Q 250
 ip address 10.2.0.3 255.255.255.248
 ip nat inside
 standby 250 ip 10.2.0.1
 standby 250 priority 110
 standby 250 preempt
!
router ospf 10
 log-adjacency-changes
 network 10.2.0.0 0.0.0.7 area 0
 network 10.2.1.0 0.0.0.7 area 0
```

```
 network 10.0.3.0 0.0.0.15 area 0
 network 195.136.17.8 0.0.0.3 area 0
 network 195.136.17.12 0.0.0.3 area 0
 network 192.168.130.0 0.0.0.7 area 0
 network 192.168.128.0 0.0.0.7 area 0
 network 172.16.192.0 0.0.0.7 area 0
!
ip nat inside source list 1 interface Serial0/0 overload
ip nat inside source static 192.168.128.6 195.136.17.14
ip classless
!
ip flow-export version 9
!
!
access-list 1 permit 10.0.0.0 0.0.0.63
access-list 1 permit 10.0.0.64 0.0.0.63
access-list 1 permit 10.0.0.128 0.0.0.63
access-list 1 permit 10.0.0.192 0.0.0.63
access-list 1 permit 10.0.1.0 0.0.0.63
access-list 1 permit 10.0.1.64 0.0.0.63
access-list 1 permit 10.0.1.128 0.0.0.63
access-list 1 permit 10.0.1.192 0.0.0.63
access-list 1 permit 10.0.2.0 0.0.0.63
access-list 1 permit 10.0.2.64 0.0.0.63
access-list 1 permit 10.0.2.128 0.0.0.63
access-list 1 permit 10.0.2.192 0.0.0.63
access-list 1 permit 192.168.0.0 0.0.127.255
access-list 111 permit udp any any eq bootps
access-list 111 permit udp any any eq bootpc
access-list 111 permit ospf any any
access-list 111 permit udp any any eq 1985
access-list 111 permit udp any host 224.0.0.2
access-list 111 permit ip 195.136.17.0 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.8 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.16 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.4 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.12 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.20 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 deny ip any any
access-list 110 permit udp any any eq bootps
access-list 110 permit udp any any eq bootpc
access-list 110 permit ospf any any
access-list 110 permit udp any any eq 1985
access-list 110 permit udp any host 224.0.0.2
access-list 110 permit ip host 192.168.128.6 host 195.136.17.5
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.0 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.8 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.16 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.4 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.12 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.20 0.0.0.3
access-list 110 deny ip any any
!
```

```
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
end
```

A.22.33. Router Auxiliar 2

A continuación se muestra la configuración completa del dispositivo de red Router Auxiliar 2.

Listing A.54: Configuración Completa Router Auxiliar 2

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router_Auxiliar2
!
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
```

```
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
!
!
!
!
!
!
interface Serial0/0
 ip address 195.136.17.18 255.255.255.252
 ip nat outside
!
interface Serial1/0
 ip address 195.136.17.22 255.255.255.252
 ip nat outside
 clock rate 2000000
!
interface Serial2/0
 no ip address
 clock rate 2000000
!
interface GigabitEthernet3/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet3/0.160
 encapsulation dot1Q 160
 ip address 172.16.192.4 255.255.255.248
 standby 160 ip 172.16.192.1
 standby 160 preempt
!
interface GigabitEthernet4/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet4/0.190
 encapsulation dot1Q 190
 ip address 192.168.130.4 255.255.255.248
 ip access-group 110 in
```

```
 ip access-group 111 out
 standby 190 ip 192.168.130.1
 standby 190 preempt
!
interface GigabitEthernet5/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet6/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet6/0.250
 encapsulation dot1Q 250
 ip address 10.2.0.4 255.255.255.248
 standby 250 ip 10.2.0.1
 standby 250 preempt
!
interface GigabitEthernet7/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet7/0.255
 encapsulation dot1Q 255
 ip address 10.2.1.4 255.255.255.248
 standby 255 ip 10.2.1.1
 standby 255 preempt
!
interface GigabitEthernet8/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet8/0.150
 encapsulation dot1Q 150
 ip address 10.0.3.4 255.255.255.240
 standby 150 ip 10.0.3.1
 standby 150 preempt
!
interface GigabitEthernet9/0
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet9/0.170
 encapsulation dot1Q 170
```

```
 ip address 192.168.128.4 255.255.255.248
 ip access-group 110 in
 standby 170 ip 192.168.128.1
 standby 170 preempt
!
router ospf 10
 log-adjacency-changes
 network 10.2.0.0 0.0.0.7 area 0
 network 10.2.1.0 0.0.0.7 area 0
 network 10.0.3.0 0.0.0.15 area 0
 network 195.136.17.16 0.0.0.3 area 0
 network 195.136.17.20 0.0.0.3 area 0
 network 192.168.130.0 0.0.0.7 area 0
 network 192.168.128.0 0.0.0.7 area 0
 network 172.16.192.0 0.0.0.7 area 0
!
ip nat inside source list 1 interface Serial0/0 overload
ip nat inside source static 192.168.128.6 195.136.17.22
ip classless
!
ip flow-export version 9
!
!
access-list 1 permit 10.0.0.0 0.0.0.63
access-list 1 permit 10.0.0.64 0.0.0.63
access-list 1 permit 10.0.0.128 0.0.0.63
access-list 1 permit 10.0.0.192 0.0.0.63
access-list 1 permit 10.0.1.0 0.0.0.63
access-list 1 permit 10.0.1.64 0.0.0.63
access-list 1 permit 10.0.1.128 0.0.0.63
access-list 1 permit 10.0.1.192 0.0.0.63
access-list 1 permit 10.0.2.0 0.0.0.63
access-list 1 permit 10.0.2.64 0.0.0.63
access-list 1 permit 10.0.2.128 0.0.0.63
access-list 1 permit 10.0.2.192 0.0.0.63
access-list 1 permit 192.168.0.0 0.0.127.255
access-list 111 permit udp any any eq bootps
access-list 111 permit udp any any eq bootpc
access-list 111 permit ospf any any
access-list 111 permit udp any any eq 1985
access-list 111 permit udp any host 224.0.0.2
access-list 111 permit ip 195.136.17.0 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.8 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.16 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.4 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.12 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 permit ip 195.136.17.20 0.0.0.3 192.168.0.0 0.0.127.255
access-list 111 deny ip any any
access-list 110 permit udp any any eq bootps
access-list 110 permit udp any any eq bootpc
access-list 110 permit ospf any any
access-list 110 permit udp any any eq 1985
access-list 110 permit udp any host 224.0.0.2
```

```
access-list 110 permit ip host 192.168.128.6 host 195.136.17.5
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.0 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.8 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.16 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.4 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.12 0.0.0.3
access-list 110 permit ip 192.168.0.0 0.0.127.255 195.136.17.20 0.0.0.3
access-list 110 deny ip any any
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
end
```

A.22.34. Router Son Espases

A continuación se muestra la configuración completa del dispositivo de red Router Son Espases, de la red de interconexión entre hospitales.

Listing A.55: Configuración Completa Router Son Espases

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R-SonEspases
!
!
!
enable password 7 0822455D0A16
!
!
!
```

```
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
license udi pid CISCO2911/K9 sn FTX1524E75B-
license boot module c2900 technology-package securityk9
!
!
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp policy 20
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp policy 30
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp key vpnpa55 address 192.168.103.162
crypto isakmp key vpnpa55 address 192.168.103.166
crypto isakmp key vpnpa55 address 192.168.103.169
crypto isakmp key vpnpa55 address 192.168.103.170
!
!
!
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
crypto ipsec transform-set VPN-SET2 esp-aes esp-sha-hmac
crypto ipsec transform-set VPN-SET3 esp-aes esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
 description This VPN connects to Manacor.
 set peer 192.168.103.162
 set transform-set VPN-SET
 match address 110
!
!
crypto map VPN-MAP2 20 ipsec-isakmp
 description VPN connection to Inca.
 set peer 192.168.103.166
 set transform-set VPN-SET2
```

```
 match address 120
!
!
crypto map VPN-MAP3 30 ipsec-isakmp
 description VPN connection to Son Llatzer.
 set peer 192.168.103.169
 set peer 192.168.103.170
 set transform-set VPN-SET3
 match address 130
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 192.168.103.198 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.200
 encapsulation dot1Q 200
 ip address 192.168.103.129 255.255.255.240
 ip access-group 105 out
!
interface GigabitEthernet0/2
 ip address 192.168.103.202 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/1/0
 ip address 195.136.17.1 255.255.255.252
 ip nat outside
 clock rate 64000
!
interface Serial0/1/1
```

```
 ip address 195.136.17.5 255.255.255.252
 ip nat outside
 clock rate 64000
!
interface Serial0/2/0
 ip address 192.168.103.161 255.255.255.252
 clock rate 2000000
 crypto map VPN-MAP
!
interface Serial0/2/1
 ip address 192.168.103.165 255.255.255.252
 clock rate 2000000
 crypto map VPN-MAP2
!
interface Serial0/3/0
 ip address 192.168.103.169 255.255.255.252
 clock rate 2000000
 crypto map VPN-MAP3
!
interface Serial0/3/1
 no ip address
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 10
 log-adjacency-changes
 network 192.168.103.196 0.0.0.3 area 0
 network 192.168.103.200 0.0.0.3 area 0
 network 195.136.17.0 0.0.0.3 area 0
 network 195.136.17.4 0.0.0.3 area 0
 network 192.168.103.128 0.0.0.15 area 0
 network 192.168.103.160 0.0.0.3 area 0
 network 192.168.103.164 0.0.0.3 area 0
 network 192.168.103.168 0.0.0.3 area 0
!
router rip
!
ip nat inside source list 1 interface Serial0/1/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 195.136.17.2
ip route 0.0.0.0 0.0.0.0 195.136.17.6 70
!
ip flow-export version 9
!
!
access-list 1 permit 192.168.100.0 0.0.0.63
access-list 1 permit 192.168.100.64 0.0.0.63
access-list 1 permit 192.168.100.128 0.0.0.63
access-list 1 permit 192.168.100.192 0.0.0.63
access-list 1 permit 192.168.101.0 0.0.0.63
```

```
access-list 1 permit 192.168.101.64 0.0.0.63
access-list 1 permit 192.168.101.128 0.0.0.63
access-list 1 permit 192.168.101.192 0.0.0.63
access-list 1 permit 192.168.102.0 0.0.0.63
access-list 1 permit 192.168.102.64 0.0.0.63
access-list 1 permit 192.168.102.128 0.0.0.63
access-list 1 permit 192.168.102.192 0.0.0.63
access-list 1 permit 192.168.103.0 0.0.0.63
access-list 1 permit 192.168.103.64 0.0.0.63
access-list 110 permit ip 192.168.100.0 0.0.3.255 192.168.104.0 0.0.1.255
access-list 110 permit ip 192.168.100.0 0.0.3.255 192.168.106.0 0.0.0.127
access-list 110 permit ip 192.168.100.0 0.0.3.255 192.168.106.128 0.0.0.63
access-list 120 permit ip 192.168.100.0 0.0.3.255 192.168.108.0 0.0.1.255
access-list 120 permit ip 192.168.100.0 0.0.3.255 192.168.110.0 0.0.0.255
access-list 120 permit ip 192.168.100.0 0.0.3.255 192.168.111.0 0.0.0.63
access-list 130 permit ip 192.168.100.0 0.0.3.255 192.168.112.0 0.0.1.255
access-list 130 permit ip 192.168.100.0 0.0.3.255 192.168.114.0 0.0.0.255
access-list 130 permit ip 192.168.100.0 0.0.3.255 192.168.115.0 0.0.0.127
access-list 105 permit ip host 192.168.100.133 host 192.168.103.134
access-list 105 permit ip host 192.168.104.133 host 192.168.103.134
access-list 105 permit ip host 192.168.108.133 host 192.168.103.134
access-list 105 permit ip host 192.168.112.133 host 192.168.103.134
access-list 105 deny ip any any
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
end
```

A.22.35. Router Manacor

A continuación se muestra la configuración completa del dispositivo de red Router Manacor, de la red de interconexión entre hospitales.

Listing A.56: Configuración Completa Router Manacor

```
!
```

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R-Manacor
!
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
license udi pid CISCO2911/K9 sn FTX15241WUA-
license boot module c2900 technology-package securityk9
!
!
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp policy 40
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp policy 60
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp key vpnpa55 address 192.168.103.161
crypto isakmp key vpnpa55 address 192.168.103.174
crypto isakmp key vpnpa55 address 192.168.103.178
!
!
!
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
crypto ipsec transform-set VPN-SET4 esp-aes esp-sha-hmac
crypto ipsec transform-set VPN-SET6 esp-aes esp-sha-hmac
```

```
!
crypto map VPN-MAP 10 ipsec-isakmp
 description VPN connection to Son Espases.
 set peer 192.168.103.161
 set transform-set VPN-SET
 match address 110
!
!
crypto map VPN-MAP4 40 ipsec-isakmp
 description VPN connection to Inca.
 set peer 192.168.103.174
 set transform-set VPN-SET4
 match address 140
!
!
crypto map VPN-MAP6 60 ipsec-isakmp
 description VPN connection to Son Llatzer.
 set peer 192.168.103.178
 set transform-set VPN-SET6
 match address 160
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 192.168.107.198 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.400
 encapsulation dot1Q 400
 ip address 192.168.107.1 255.255.255.240
 ip access-group 105 out
!
interface GigabitEthernet0/2
```

```
 ip address 192.168.107.202 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/2/0
 ip address 195.136.17.9 255.255.255.252
 ip nat outside
 clock rate 64000
!
interface Serial0/2/1
 ip address 192.168.103.162 255.255.255.252
 crypto map VPN-MAP
!
interface Serial0/3/0
 ip address 192.168.103.173 255.255.255.252
 clock rate 2000000
 crypto map VPN-MAP4
!
interface Serial0/3/1
 ip address 192.168.103.177 255.255.255.252
 clock rate 2000000
 crypto map VPN-MAP6
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 10
 log-adjacency-changes
 network 192.168.107.196 0.0.0.3 area 0
 network 192.168.107.200 0.0.0.3 area 0
 network 192.168.103.160 0.0.0.3 area 0
 network 192.168.107.0 0.0.0.15 area 0
 network 195.136.17.8 0.0.0.3 area 0
 network 192.168.103.172 0.0.0.3 area 0
 network 192.168.103.176 0.0.0.3 area 0
!
ip nat inside source list 1 interface Serial0/2/0 overload
ip classless
!
ip flow-export version 9
!
!
access-list 1 permit 192.168.104.0 0.0.0.63
access-list 1 permit 192.168.104.64 0.0.0.63
access-list 1 permit 192.168.104.128 0.0.0.63
access-list 1 permit 192.168.104.192 0.0.0.63
access-list 1 permit 192.168.105.0 0.0.0.63
access-list 1 permit 192.168.105.64 0.0.0.63
access-list 1 permit 192.168.105.128 0.0.0.63
access-list 1 permit 192.168.105.192 0.0.0.63
access-list 1 permit 192.168.106.0 0.0.0.63
```

```
access-list 1 permit 192.168.106.64 0.0.0.63
access-list 1 permit 192.168.106.128 0.0.0.63
access-list 1 permit 192.168.106.192 0.0.0.63
access-list 1 permit 192.168.107.144 0.0.0.7
access-list 110 permit ip 192.168.104.0 0.0.1.255 192.168.100.0 0.0.3.255
access-list 110 permit ip 192.168.106.0 0.0.0.127 192.168.100.0 0.0.3.255
access-list 110 permit ip 192.168.106.128 0.0.0.63 192.168.100.0 0.0.3.255
access-list 140 permit ip 192.168.104.0 0.0.1.255 192.168.108.0 0.0.1.255
access-list 140 permit ip 192.168.104.0 0.0.1.255 192.168.110.0 0.0.0.255
access-list 140 permit ip 192.168.104.0 0.0.1.255 192.168.111.0 0.0.0.63
access-list 140 permit ip 192.168.106.0 0.0.0.127 192.168.108.0 0.0.1.255
access-list 140 permit ip 192.168.106.0 0.0.0.127 192.168.110.0 0.0.0.255
access-list 140 permit ip 192.168.106.0 0.0.0.127 192.168.111.0 0.0.0.63
access-list 140 permit ip 192.168.106.128 0.0.0.63 192.168.108.0 0.0.1.255
access-list 140 permit ip 192.168.106.128 0.0.0.63 192.168.110.0 0.0.0.255
access-list 140 permit ip 192.168.106.128 0.0.0.63 192.168.111.0 0.0.0.63
access-list 160 permit ip 192.168.104.0 0.0.1.255 192.168.112.0 0.0.1.255
access-list 160 permit ip 192.168.104.0 0.0.1.255 192.168.114.0 0.0.0.255
access-list 160 permit ip 192.168.104.0 0.0.1.255 192.168.115.0 0.0.0.127
access-list 160 permit ip 192.168.106.0 0.0.0.127 192.168.112.0 0.0.1.255
access-list 160 permit ip 192.168.106.0 0.0.0.127 192.168.114.0 0.0.0.255
access-list 160 permit ip 192.168.106.0 0.0.0.127 192.168.115.0 0.0.0.127
access-list 160 permit ip 192.168.106.128 0.0.0.63 192.168.112.0 0.0.1.255
access-list 160 permit ip 192.168.106.128 0.0.0.63 192.168.114.0 0.0.0.255
access-list 160 permit ip 192.168.106.128 0.0.0.63 192.168.115.0 0.0.0.127
access-list 105 permit ip host 192.168.100.133 host 192.168.107.6
access-list 105 permit ip host 192.168.104.133 host 192.168.107.6
access-list 105 permit ip host 192.168.108.133 host 192.168.107.6
access-list 105 permit ip host 192.168.112.133 host 192.168.107.6
access-list 105 deny ip any any
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
end
```

A.22.36. Router Inca

A continuación se muestra la configuración completa del dispositivo de red Router Inca, de la red de interconexión entre hospitales.

Listing A.57: Configuración Completa Router Inca

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R-Inca
!
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
license udi pid CISCO2911/K9 sn FTX1524CM13-
license boot module c2900 technology-package securityk9
!
!
!
crypto isakmp policy 20
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp policy 40
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp policy 50
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp key vpnpa55 address 192.168.103.165
crypto isakmp key vpnpa55 address 192.168.103.173
```

```
crypto isakmp key vpnpa55 address 192.168.103.182
!
!
!
crypto ipsec transform-set VPN-SET2 esp-aes esp-sha-hmac
crypto ipsec transform-set VPN-SET4 esp-aes esp-sha-hmac
crypto ipsec transform-set VPN-SET5 esp-aes esp-sha-hmac
!
crypto map VPN-MAP2 20 ipsec-isakmp
 description VPN connection to Son Espases.
 set peer 192.168.103.165
 set transform-set VPN-SET2
 match address 120
!
!
crypto map VPN-MAP4 40 ipsec-isakmp
 description VPN connection to Manacor.
 set peer 192.168.103.173
 set transform-set VPN-SET4
 match address 140
!
!
crypto map VPN-MAP5 50 ipsec-isakmp
 description VPN connection to Son Llatzer.
 set peer 192.168.103.182
 set transform-set VPN-SET5
 match address 150
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 192.168.111.198 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 ip nat inside
 duplex auto
 speed auto
```

```
!
interface GigabitEthernet0/1.600
 encapsulation dot1Q 600
 ip address 192.168.111.65 255.255.255.240
 ip access-group 105 out
 ip nat inside
!
interface GigabitEthernet0/2
 ip address 192.168.111.202 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/2/0
 ip address 195.136.17.13 255.255.255.252
 ip nat outside
 clock rate 2000000
!
interface Serial0/2/1
 ip address 192.168.103.166 255.255.255.252
 crypto map VPN-MAP2
!
interface Serial0/3/0
 ip address 192.168.103.174 255.255.255.252
 crypto map VPN-MAP4
!
interface Serial0/3/1
 ip address 192.168.103.181 255.255.255.252
 clock rate 2000000
 crypto map VPN-MAP5
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 10
 log-adjacency-changes
 network 192.168.111.64 0.0.0.15 area 0
 network 195.136.17.12 0.0.0.3 area 0
 network 192.168.111.196 0.0.0.3 area 0
 network 192.168.111.200 0.0.0.3 area 0
 network 192.168.103.164 0.0.0.3 area 0
 network 192.168.103.172 0.0.0.3 area 0
 network 192.168.103.180 0.0.0.3 area 0
!
ip nat inside source list 1 interface Serial0/2/0 overload
ip classless
!
ip flow-export version 9
!
!
access-list 1 permit 192.168.108.0 0.0.0.63
access-list 1 permit 192.168.108.64 0.0.0.63
access-list 1 permit 192.168.108.128 0.0.0.63
```

```
access-list 1 permit 192.168.108.192 0.0.0.63
access-list 1 permit 192.168.109.0 0.0.0.63
access-list 1 permit 192.168.109.64 0.0.0.63
access-list 1 permit 192.168.109.128 0.0.0.63
access-list 1 permit 192.168.109.192 0.0.0.63
access-list 1 permit 192.168.110.0 0.0.0.63
access-list 1 permit 192.168.110.64 0.0.0.63
access-list 1 permit 192.168.110.128 0.0.0.63
access-list 1 permit 192.168.110.192 0.0.0.63
access-list 1 permit 192.168.111.0 0.0.0.63
access-list 120 permit ip 192.168.108.0 0.0.1.255 192.168.100.0 0.0.3.255
access-list 120 permit ip 192.168.110.0 0.0.0.255 192.168.100.0 0.0.3.255
access-list 120 permit ip 192.168.111.0 0.0.0.63 192.168.100.0 0.0.3.255
access-list 140 permit ip 192.168.108.0 0.0.1.255 192.168.104.0 0.0.1.255
access-list 140 permit ip 192.168.110.0 0.0.0.255 192.168.104.0 0.0.1.255
access-list 140 permit ip 192.168.111.0 0.0.0.63 192.168.104.0 0.0.1.255
access-list 140 permit ip 192.168.108.0 0.0.1.255 192.168.106.0 0.0.0.127
access-list 140 permit ip 192.168.110.0 0.0.0.255 192.168.106.0 0.0.0.127
access-list 140 permit ip 192.168.111.0 0.0.0.63 192.168.106.0 0.0.0.127
access-list 140 permit ip 192.168.108.0 0.0.1.255 192.168.106.128 0.0.0.63
access-list 140 permit ip 192.168.110.0 0.0.0.255 192.168.106.128 0.0.0.63
access-list 140 permit ip 192.168.111.0 0.0.0.63 192.168.106.128 0.0.0.63
access-list 150 permit ip 192.168.108.0 0.0.1.255 192.168.112.0 0.0.1.255
access-list 150 permit ip 192.168.108.0 0.0.1.255 192.168.114.0 0.0.0.255
access-list 150 permit ip 192.168.108.0 0.0.1.255 192.168.115.0 0.0.0.127
access-list 150 permit ip 192.168.110.0 0.0.0.255 192.168.112.0 0.0.1.255
access-list 150 permit ip 192.168.110.0 0.0.0.255 192.168.114.0 0.0.0.255
access-list 150 permit ip 192.168.110.0 0.0.0.255 192.168.115.0 0.0.0.127
access-list 150 permit ip 192.168.111.0 0.0.0.63 192.168.112.0 0.0.1.255
access-list 150 permit ip 192.168.111.0 0.0.0.63 192.168.114.0 0.0.0.255
access-list 150 permit ip 192.168.111.0 0.0.0.63 192.168.115.0 0.0.0.127
access-list 105 permit ip host 192.168.100.133 host 192.168.111.73
access-list 105 permit ip host 192.168.104.133 host 192.168.111.73
access-list 105 permit ip host 192.168.108.133 host 192.168.111.73
access-list 105 permit ip host 192.168.112.133 host 192.168.111.73
access-list 105 deny ip any any
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
```

```
 transport input ssh
!
!
!
end
```

A.22.37. Router Son Llàtzer

A continuación se muestra la configuración completa del dispositivo de red Router Son Llàtzer, de la red de interconexión entre hospitales.

Listing A.58: Configuración Completa Router Son Llàtzer

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R-SonLlatzer
!
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
license udi pid CISCO2911/K9 sn FTX152417OG-
license boot module c2900 technology-package securityk9
!
!
!
crypto isakmp policy 30
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp policy 50
 encr aes 256
 authentication pre-share
 group 5
!
```

```
crypto isakmp policy 60
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp key vpnpa55 address 192.168.103.169
crypto isakmp key vpnpa55 address 192.168.103.177
crypto isakmp key vpnpa55 address 192.168.103.181
!
!
!
crypto ipsec transform-set VPN-SET3 esp-aes esp-sha-hmac
crypto ipsec transform-set VPN-SET5 esp-aes esp-sha-hmac
crypto ipsec transform-set VPN-SET6 esp-aes esp-sha-hmac
!
crypto map VPN-MAP3 30 ipsec-isakmp
 description VPN connection to Son Espases.
 set peer 192.168.103.169
 set transform-set VPN-SET3
 match address 130
!
!
crypto map VPN-MAP5 50 ipsec-isakmp
 description VPN connection to Inca.
 set peer 192.168.103.181
 set transform-set VPN-SET5
 match address 150
!
!
crypto map VPN-MAP6 60 ipsec-isakmp
 description VPN connection to Manacor.
 set peer 192.168.103.177
 set transform-set VPN-SET6
 match address 160
!
!
!
!
no ip domain-lookup
ip domain-name cisco.net
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 192.168.115.202 255.255.255.252
 ip nat inside
 duplex auto
```

```
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.800
 encapsulation dot1Q 800
 ip address 192.168.115.129 255.255.255.240
 ip access-group 105 out
!
interface GigabitEthernet0/2
 ip address 192.168.115.198 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/2/0
 ip address 195.136.17.17 255.255.255.252
 ip nat outside
 clock rate 2000000
!
interface Serial0/2/1
 ip address 192.168.103.170 255.255.255.252
 crypto map VPN-MAP3
!
interface Serial0/3/0
 ip address 192.168.103.178 255.255.255.252
 crypto map VPN-MAP6
!
interface Serial0/3/1
 ip address 192.168.103.182 255.255.255.252
 crypto map VPN-MAP5
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 10
 log-adjacency-changes
 network 192.168.103.168 0.0.0.3 area 0
 network 192.168.103.176 0.0.0.3 area 0
 network 192.168.103.180 0.0.0.3 area 0
 network 195.136.17.16 0.0.0.3 area 0
 network 192.168.115.128 0.0.0.15 area 0
 network 192.168.115.196 0.0.0.3 area 0
 network 192.168.115.200 0.0.0.3 area 0
!
router rip
!
ip nat inside source list 1 interface Serial0/2/0 overload
ip classless
```

```
!
ip flow-export version 9
!
!
access-list 1 permit 192.168.112.0 0.0.0.63
access-list 1 permit 192.168.112.64 0.0.0.63
access-list 1 permit 192.168.112.128 0.0.0.63
access-list 1 permit 192.168.112.192 0.0.0.63
access-list 1 permit 192.168.113.0 0.0.0.63
access-list 1 permit 192.168.113.64 0.0.0.63
access-list 1 permit 192.168.113.128 0.0.0.63
access-list 1 permit 192.168.113.192 0.0.0.63
access-list 1 permit 192.168.114.0 0.0.0.63
access-list 1 permit 192.168.114.64 0.0.0.63
access-list 1 permit 192.168.114.128 0.0.0.63
access-list 1 permit 192.168.114.192 0.0.0.63
access-list 1 permit 192.168.115.0 0.0.0.63
access-list 1 permit 192.168.115.64 0.0.0.63
access-list 130 permit ip 192.168.112.0 0.0.1.255 192.168.100.0 0.0.3.255
access-list 130 permit ip 192.168.114.0 0.0.0.255 192.168.100.0 0.0.3.255
access-list 130 permit ip 192.168.115.0 0.0.0.127 192.168.100.0 0.0.3.255
access-list 150 permit ip 192.168.112.0 0.0.1.255 192.168.108.0 0.0.1.255
access-list 150 permit ip 192.168.114.0 0.0.0.255 192.168.108.0 0.0.1.255
access-list 150 permit ip 192.168.115.0 0.0.0.127 192.168.108.0 0.0.1.255
access-list 150 permit ip 192.168.112.0 0.0.1.255 192.168.110.0 0.0.0.255
access-list 150 permit ip 192.168.114.0 0.0.0.255 192.168.110.0 0.0.0.255
access-list 150 permit ip 192.168.115.0 0.0.0.127 192.168.110.0 0.0.0.255
access-list 150 permit ip 192.168.112.0 0.0.1.255 192.168.111.0 0.0.0.63
access-list 150 permit ip 192.168.114.0 0.0.0.255 192.168.111.0 0.0.0.63
access-list 150 permit ip 192.168.115.0 0.0.0.127 192.168.111.0 0.0.0.63
access-list 160 permit ip 192.168.112.0 0.0.1.255 192.168.104.0 0.0.1.255
access-list 160 permit ip 192.168.114.0 0.0.0.255 192.168.104.0 0.0.1.255
access-list 160 permit ip 192.168.115.0 0.0.0.127 192.168.104.0 0.0.1.255
access-list 160 permit ip 192.168.112.0 0.0.1.255 192.168.106.0 0.0.0.127
access-list 160 permit ip 192.168.114.0 0.0.0.255 192.168.106.0 0.0.0.127
access-list 160 permit ip 192.168.115.0 0.0.0.127 192.168.106.0 0.0.0.127
access-list 160 permit ip 192.168.112.0 0.0.1.255 192.168.106.128 0.0.0.63
access-list 160 permit ip 192.168.114.0 0.0.0.255 192.168.106.128 0.0.0.63
access-list 160 permit ip 192.168.115.0 0.0.0.127 192.168.106.128 0.0.0.63
access-list 105 permit ip host 192.168.100.133 host 192.168.115.136
access-list 105 permit ip host 192.168.104.133 host 192.168.115.136
access-list 105 permit ip host 192.168.108.133 host 192.168.115.136
access-list 105 permit ip host 192.168.112.133 host 192.168.115.136
access-list 105 deny ip any any
!
banner motd #Solo Acceso Autorizado!!#
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
```

```
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
end
```

A.23. Validación OSPF

A continuación se muestra una imágen de las rutas IP posibles en un switch de distribución.

```
10.0.0.0/8 is variably subnetted, 17 subnets, 4 masks
   10.0.0.0/26 is directly connected, Vlan10
   10.0.0.64/26 is directly connected, Vlan20
   10.0.0.128/26 [110/2] via 10.0.0.3, 00:16:59, Vlan10
                 [110/2] via 10.0.0.67, 00:16:59, Vlan20
   10.0.0.192/26 [110/2] via 10.0.0.3, 00:16:59, Vlan10
                 [110/2] via 10.0.0.67, 00:16:59, Vlan20
   10.0.1.0/26 [110/3] via 10.0.0.3, 00:16:59, Vlan10
               [110/3] via 10.0.0.67, 00:16:59, Vlan20
   10.0.1.64/26 [110/3] via 10.0.0.3, 00:16:59, Vlan10
                [110/3] via 10.0.0.67, 00:16:59, Vlan20
   10.0.1.128/26 [110/3] via 10.0.2.130, 00:16:59, Vlan110
                 [110/3] via 10.0.2.194, 00:16:59, Vlan120
   10.0.1.192/26 [110/3] via 10.0.2.130, 00:16:59, Vlan110
                 [110/3] via 10.0.2.194, 00:16:59, Vlan120
   10.0.2.0/26 [110/2] via 10.0.2.130, 00:16:59, Vlan110
               [110/2] via 10.0.2.194, 00:16:59, Vlan120
   10.0.2.64/26 [110/2] via 10.0.2.130, 00:16:59, Vlan110
                [110/2] via 10.0.2.194, 00:16:59, Vlan120
   10.0.2.128/26 is directly connected, Vlan110
   10.0.2.192/26 is directly connected, Vlan120
   10.0.3.0/28 [110/12] via 10.1.0.7, 00:01:23, Vlan200
               [110/12] via 10.1.0.8, 00:01:23, Vlan200
   10.1.0.0/27 is directly connected, Vlan200
   10.1.1.0/27 is directly connected, Vlan205
   10.2.0.0/29 [110/11] via 10.1.0.7, 00:03:22, Vlan200
   10.2.1.0/29 [110/11] via 10.1.0.8, 00:01:23, Vlan200
172.16.0.0/16 is variably subnetted, 7 subnets, 3 masks
   172.16.0.0/20 [110/11] via 10.1.0.9, 00:16:21, Vlan200
   172.16.16.0/20 [110/11] via 10.1.0.10, 00:06:04, Vlan200
   172.16.32.0/20 [110/11] via 10.1.0.11, 00:00:39, Vlan200
   172.16.48.0/20 [110/11] via 10.1.0.12, 00:16:21, Vlan200
   172.16.64.0/18 [110/11] via 10.1.0.12, 00:16:21, Vlan200
   172.16.128.0/18 [110/11] via 10.1.0.12, 00:16:21, Vlan200
   172.16.192.0/29 [110/12] via 10.1.0.7, 00:01:23, Vlan200
                   [110/12] via 10.1.0.8, 00:01:23, Vlan200
192.168.0.0/17 [110/13] via 10.1.0.7, 00:01:23, Vlan200
               [110/13] via 10.1.0.8, 00:01:23, Vlan200
192.168.128.0/29 is subnetted, 1 subnets
   192.168.128.0 [110/12] via 10.1.0.7, 00:01:23, Vlan200
                 [110/12] via 10.1.0.8, 00:01:23, Vlan200
192.168.130.0/29 is subnetted, 1 subnets
   192.168.130.0 [110/12] via 10.1.0.7, 00:01:23, Vlan200
                 [110/12] via 10.1.0.8, 00:01:23, Vlan200
195.136.17.0/30 is subnetted, 6 subnets
   195.136.17.0 [110/75] via 10.1.0.7, 00:01:23, Vlan200
                [110/75] via 10.1.0.8, 00:01:23, Vlan200
   195.136.17.4 [110/75] via 10.1.0.7, 00:01:23, Vlan200
                [110/75] via 10.1.0.8, 00:01:23, Vlan200
   195.136.17.8 [110/75] via 10.1.0.7, 00:01:23, Vlan200
                [110/75] via 10.1.0.8, 00:01:23, Vlan200
   195.136.17.12 [110/75] via 10.1.0.7, 00:01:23, Vlan200
                 [110/75] via 10.1.0.8, 00:01:23, Vlan200
   195.136.17.16 [110/75] via 10.1.0.7, 00:01:23, Vlan200
                 [110/75] via 10.1.0.8, 00:01:23, Vlan200
   195.136.17.20 [110/75] via 10.1.0.7, 00:01:23, Vlan200
                 [110/75] via 10.1.0.8, 00:01:23, Vlan200
```

Figura A.1: OSPF en Switches de Distribución en Hospital Son Espases

A.24. Validación DHCP

A continuación se muestran algunas imágenes que corroboran que el protocolo DHCP está correctamente configurado y asigna direcciones IPs dinámicas a los dispositivos de la red.

A.24.1. Dirección IP Dinámica en PC de Recursos Humanos

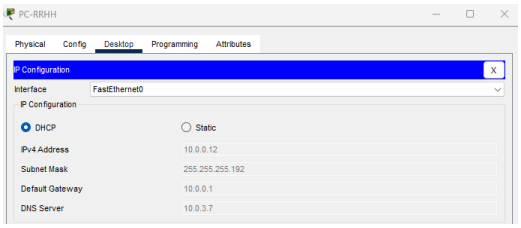


Figura A.2: Dirección IP Dinámica en PC de Recursos Humanos

A.24.2. Dirección IP Dinámica en PC de Admisión

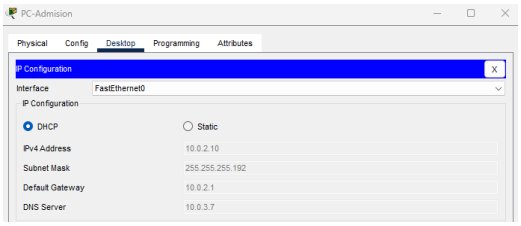


Figura A.3: Dirección IP Dinámica en PC de Admisión

A.25. Validación NAT

A continuación se muestran las traducciones de direcciones IPs hechas por el servicio NAT, que permiten la conectividad entre los dispositivos internos con Internet y viceversa.

A.25.1. Traducción IPs hacia Internet

```
Router_Principal#sh ip nat trans
Pro  Inside global     Inside local       Outside local      Outside global
icmp 195.136.17.2:5    192.168.0.7:5      195.136.17.1:5     195.136.17.1:5
icmp 195.136.17.2:6    192.168.0.7:6      195.136.17.1:6     195.136.17.1:6
icmp 195.136.17.2:7    192.168.0.7:7      195.136.17.1:7     195.136.17.1:7
icmp 195.136.17.2:8    192.168.0.7:8      195.136.17.1:8     195.136.17.1:8
```

Figura A.4: Traducción IPs hacia Internet

A.25.2. Traducción IPs desde Internet

```
icmp 195.136.17.6:1    192.168.128.6:1    195.136.17.5:1     195.136.17.5:1
icmp 195.136.17.6:2    192.168.128.6:2    195.136.17.5:2     195.136.17.5:2
icmp 195.136.17.6:3    192.168.128.6:3    195.136.17.5:3     195.136.17.5:3
icmp 195.136.17.6:4    192.168.128.6:4    195.136.17.5:4     195.136.17.5:4
```

Figura A.5: Traducción IPs desde Internet

A.26. Validación SSH

A continuación se muestra la imágen de la consola, donde se ve la conexión realizada mediante SSH a un dispositivo de red del hospital.

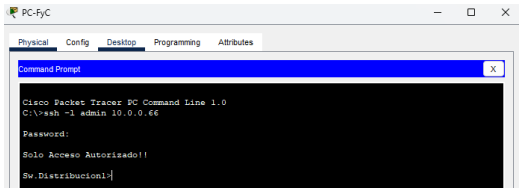


Figura A.6: Conexión Remota mediante SSH a Switch de Distribución 1

A.27. Validación Autenticación en Dispositivos de Red

A continuación se muestra la imágen de la consola, donde se ve la autenticación realizada para poder acceder al switch de distribución 2.

```
Solo Acceso Autorizado!!

User Access Verification

Password:

Sw.Distribucion2>enable
Password:
Sw.Distribucion2#
```

Figura A.7: Autenticación en Switch de Distribución 2

A.28. Validación VPN IPSec

A continuación se muestra la imágen de la consola, donde se ve la salida dada al insertar el comando "show crypto ipsec sa".

```
R-Manacor#show crypto ipsec sa

interface: Serial0/2/1
    Crypto map tag: VPN-MAP, local addr 192.168.103.162

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.104.0/255.255.254.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.100.0/255.255.252.0/0/0)
   current_peer 192.168.103.161 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
   #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 192.168.103.162, remote crypto endpt.:192.168.103.161
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/2/1
     current outbound spi: 0x1CD9CCB3(484035763)

     inbound esp sas:
      spi: 0xC0557F23(3226828579)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2003, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3566)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
```

Figura A.8: Salida por consola de show crypto ipsec sa

A.29. Validación DHCP Snooping

A.29.1. Interfaces en Modo Trusted

A continuación se muestra la imágen de la consola, donde se ve la salida dada al insertar el comando "show ip dhcp snooping".

```
Oftalmologia#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
30
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                    Trusted    Rate limit (pps)
-----------------------      -------    ----------------
FastEthernet0/2              no         5
FastEthernet0/1              yes        unlimited
FastEthernet0/6              yes        5
FastEthernet0/3              no         5
FastEthernet0/9              no         5
FastEthernet0/5              no         5
FastEthernet0/4              no         5
FastEthernet0/8              no         5
FastEthernet0/7              no         5
FastEthernet0/12             no         5
FastEthernet0/15             no         5
FastEthernet0/10             no         5
FastEthernet0/13             no         5
FastEthernet0/11             no         5
FastEthernet0/14             no         5
FastEthernet0/18             no         5
FastEthernet0/20             no         5
FastEthernet0/17             no         5
FastEthernet0/16             no         5
FastEthernet0/19             no         5
FastEthernet0/22             no         5
FastEthernet0/24             no         5
FastEthernet0/21             no         5
FastEthernet0/23             no         5
```

Figura A.9: Salida por consola de show ip dhcp snooping

A.29.2. Tabla de IPs

A continuación se muestra la imágen de la consola, donde se ve la salida dada al insertar el comando "show ip dhcp snooping binding".

```
Oftalmologia#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----
------------------
00:01:96:61:41:AA   10.0.0.134       86400       dhcp-snooping  30    FastEthernet0/4
00:0B:BE:64:5D:50   10.0.0.136       86400       dhcp-snooping  30    FastEthernet0/3
00:01:64:89:7E:92   10.0.0.140       86400       dhcp-snooping  30    FastEthernet0/3
Total number of bindings: 3
```

Figura A.10: Salida por consola de show ip dhcp snooping binding

A.30. Validación Conectividad

A.30.1. Conectividad Dispositivos Internos con Internet

A continuación se muestra la imágen de la consola, donde se ve la salida dada al realizar el ping desde un PC de la red interna a la puerta de enlace del ISP 1 (Internet).

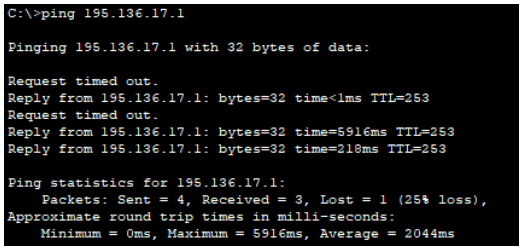


Figura A.11: Conectividad Dispositivos Internos con Internet

A.30.2. Conectividad Dispositivos Invitados con Internet

A continuación se muestra la imágen de la consola, donde se ve la salida dada al realizar el ping desde el portátil de la red de invitados a la puerta de enlace del ISP 1 (Internet).

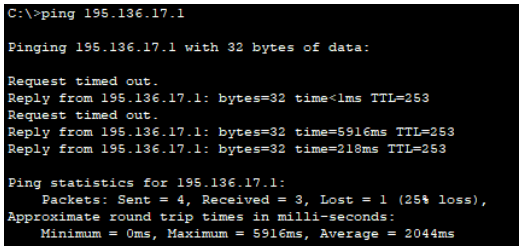


Figura A.12: Conectividad Dispositivos Invitados con Internet

A.30.3. Conectividad Internet con Servidor Web

A continuación se muestra la imágen de la consola, donde se ve la salida dada al realizar el ping desde la peurta de enlace del ISP 1 (Internet) al servidor web del hospital.

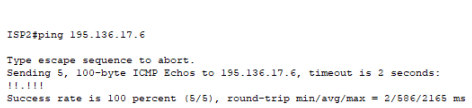


Figura A.13: Conectividad Internet con Servidor Web

A.31. Validación ACLs Bloqueantes

A.31.1. Bloqueo entre Dispositivo Administrativo con Dispositivo IoMT

A continuación se muestra la imágen de la consola, donde se ve la salida dada al realizar el ping entre un dispositivo administrativo con un dispositivo IoMT.

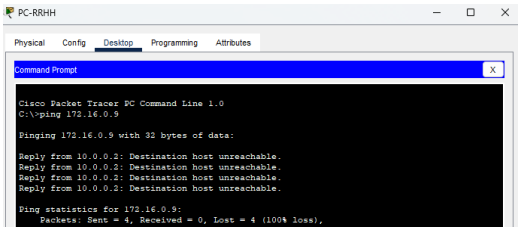


Figura A.14: Bloqueo entre Dispositivo Administrativo con Dispositivo IoMT

A.31.2. Bloqueo entre Dispositivo Administrativo con Dispositivo Médico

A continuación se muestra la imágen de la consola, donde se ve la salida dada al realizar el ping entre un dispositivo administrativo con un dispositivo médico.

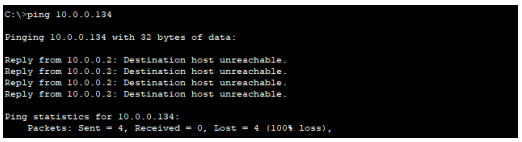


Figura A.15: Bloqueo entre Dispositivo Administrativo con Dispositivo Médico

A.31.3. Bloqueo entre Dispositivo Administrativo con Dispositivo de la UCI

A continuación se muestra la imágen de la consola, donde se ve la salida dada al realizar el ping entre un dispositivo administrativo con un dispositivo de la UCI.

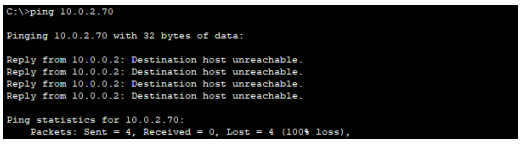


Figura A.16: Bloqueo entre Dispositivo Administrativo con Dispositivo de la UCI

A.31.4. Bloqueo entre Dispositivo Invitado con Dispositivo Interno

A continuación se muestra la imágen de la consola, donde se ve la salida dada al realizar el ping entre un dispositivo invitado con un dispositivo interno.

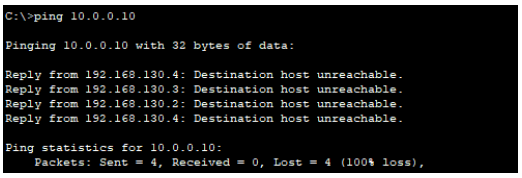


Figura A.17: Bloqueo entre Dispositivo Invitado con Dispositivo Interno

A.31.5. Bloqueo entre Dispositivo Invitado con Dispositivo IoMT

A continuación se muestra la imágen de la consola, donde se ve la salida dada al realizar el ping entre un dispositivo invitado con un dispositivo IoMT.

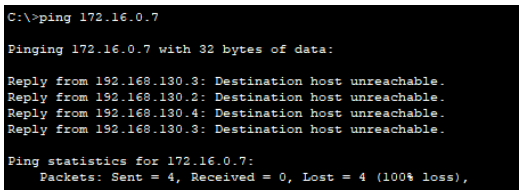


Figura A.18: Bloqueo entre Dispositivo Invitado con Dispositivo IoMT

A.31.6. Bloqueo entre Dispositivo No Autorizado con Servidor de Archivos

A continuación se muestra la imágen de la consola, donde se ve la salida dada al realizar el ping entre un dispositivo invitado con un dispositivo IoMT.

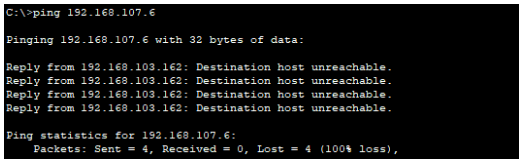


Figura A.19: Bloqueo entre Dispositivo No Autorizado con Servidor de Archivos

A.32. Validación ACLs Permisivas

A.32.1. Conectividad entre Dispositivo Médico con Dispositivo UCI

A continuación se muestra la imágen de la consola, donde se ve la salida dada al realizar el ping entre un dispositivo médico con un dispositivo de la UCI.

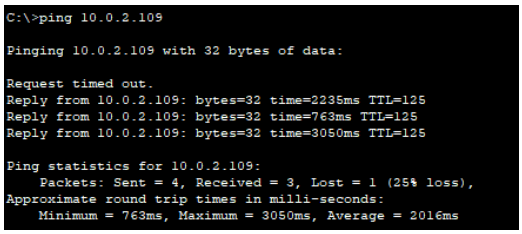


Figura A.20: Conectividad entre Dispositivo Médico con Dispositivo UCI

A.32.2. Conectividad entre Dispositivo Médico con Dispositivo IoMT Tipo 1

A continuación se muestra la imágen de la consola, donde se ve la salida dada al realizar el ping entre un dispositivo médico con un dispositivo IoMT tipo 1.

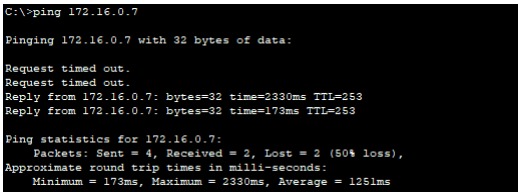


Figura A.21: Conectividad entre Dispositivo Médico con Dispositivo IoMT Tipo 1

A.32.3. Conectividad entre Dispositivo de la UCI con Dispositivo IoMT Tipo 2

A continuación se muestra la imágen de la consola, donde se ve la salida dada al realizar el ping entre un dispositivo de la UCI con un dispositivo IoMT tipo 2.

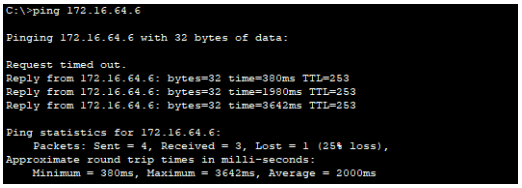


Figura A.22: Conectividad entre Dispositivo de la UCI con Dispositivo IoMT Tipo 2

A.32.4. Conectividad entre Dispositivo Autorizado de la UCI con Dispositivo IoMT Tipo 3

A continuación se muestra la imágen de la consola, donde se ve la salida dada al realizar el ping entre el dispositivo autorizado de la UCI con un dispositivo IoMT tipo 3.

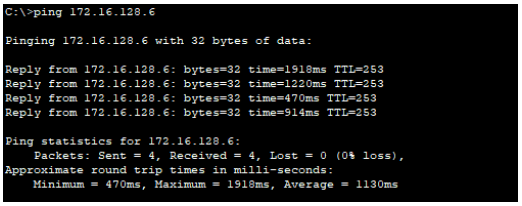


Figura A.23: Conectividad entre Dispositivo Autorizado de la UCI con Dispositivo IoMT Tipo 3

A.32.5. Conectividad PC Autorizado de IT con Servidor de Archivos

A continuación se muestra la imágen de la consola, donde se ve la salida dada al realizar el ping entre el PC de IT de Son Espases con el servidor de archivos del hospital de Manacor.

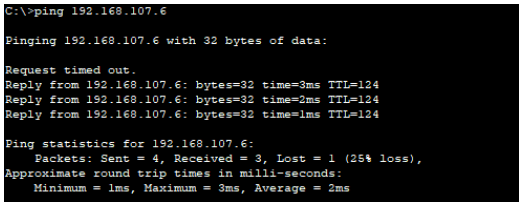


Figura A.24: Conectividad PC Autorizado de IT con Servidor de Archivos

A.33. Validación HSRP

A.33.1. HSRP en Routers

A continuación se muestran las imágenes del estado del HSRP de los tres routers, antes de la caída del router principal y después de la caída del router principal.

```
Router_Principal$show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig         160  120 P Active   local           172.16.192.3    172.16.192.1
Gig         190  120 P Active   local           192.168.130.3   192.168.130.1
Gig         250  120 P Active   local           10.2.0.3        10.2.0.1
Gig         255  120 P Active   local           10.2.1.3        10.2.1.1
Gig         170  120 P Active   local           192.168.128.3   192.168.128.1
Gig         150  120 P Active   local           10.0.3.3        10.0.3.1
```

Figura A.25: Router Principal Antes

```
Router_Auxiliar1$show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig         160  110 P Standby  172.16.192.2    local           172.16.192.1
Gig         190  110 P Standby  192.168.130.2   local           192.168.130.1
Gig         150  110 P Standby  10.0.3.2        local           10.0.3.1
Gig         170  110 P Standby  192.168.128.2   local           192.168.128.1
Gig         255  110 P Standby  10.2.1.2        local           10.2.1.1
Gig         250  110 P Standby  10.2.0.2        local           10.2.0.1
```

Figura A.26: Router Auxiliar 1 Antes

```
Router_Auxiliar2$ show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig         160  100 P Listen   172.16.192.2    unknown         172.16.192.1
Gig         190  100 P Listen   192.168.130.2   unknown         192.168.130.1
Gig         250  100 P Listen   10.2.0.2        10.2.0.4        10.2.0.1
Gig         255  100 P Listen   10.2.1.2        unknown         10.2.1.1
Gig         150  100 P Listen   10.0.3.2        unknown         10.0.3.1
Gig         170  100 P Listen   192.168.128.2   unknown         192.168.128.1
```

Figura A.27: Router Auxiliar 2 Antes

```
Router_Auxiliar1$show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig         160  110 P Active   local           172.16.192.4    172.16.192.1
Gig         190  110 P Active   local           192.168.130.4   192.168.130.1
Gig         150  110 P Active   local           10.0.3.4        10.0.3.1
Gig         170  110 P Active   local           192.168.128.4   192.168.128.1
Gig         255  110 P Active   local           10.2.1.4        10.2.1.1
Gig         250  110 P Active   local           10.2.0.4        10.2.0.1
```

Figura A.28: Router Auxiliar 1 Después

```
Router_Auxiliar2# show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig         160  100 P Standby  172.16.192.3    local           172.16.192.1
Gig         190  100 P Standby  192.168.130.3   local           192.168.130.1
Gig         250  100 P Standby  10.2.0.3        local           10.2.0.1
Gig         255  100 P Standby  10.2.1.3        local           10.2.1.1
Gig         150  100 P Standby  10.0.3.3        local           10.0.3.1
Gig         170  100 P Standby  192.168.128.3   local           192.168.128.1
```

Figura A.29: Router Auxiliar 2 Después

A.33.2. HSRP en Switches

A continuación se muestra las imágenes del estado del HSRP de los dos switches, antes de la caída del switch principal y después de la caída del switch principal.

```
Sw.Distribucion1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   110 P Active   local           10.0.0.3        10.0.0.1
Vl20        20   110 P Active   local           10.0.0.67       10.0.0.65
Vl1110      110  100 P Standby  10.0.2.130      local           10.0.2.129
Vl1120      120  100 P Standby  10.0.2.194      local           10.0.2.193
```

Figura A.30: Switch Principal Antes

```
Sw.Distribucion2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   100 P Standby  10.0.0.2        local           10.0.0.1
Vl20        20   100 P Standby  10.0.0.66       local           10.0.0.65
Vl30        30   110 P Active   local           10.0.0.131      10.0.0.129
Vl40        40   110 P Active   local           10.0.0.195      10.0.0.193
```

Figura A.31: Switch Auxiliar Antes

```
Sw.Distribucion2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   100 P Active   local           unknown         10.0.0.1
Vl20        20   100 P Active   local           unknown         10.0.0.65
Vl30        30   110 P Active   local           10.0.0.131      10.0.0.129
Vl40        40   110 P Active   local           10.0.0.195      10.0.0.193
```

Figura A.32: Switch Auxiliar Después

A.34. Validación EtherChannel

A continuación se muestra las imágenes del estado del EtherChannel de los dos switches, antes de la caída de un enlace redundante y después de la caída de un enlace redundante.

```
At.Paciente#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)          LACP    Fa0/1(P) Fa0/2(P)
```

Figura A.33: Switch Acceso Antes

```
Sw.Distribucion6#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)          LACP   Gig1/0/1(P) Gig1/0/2(P)
2      Po2(SU)          LACP   Gig1/0/3(P) Gig1/0/4(P)
```

Figura A.34: Switch Distribución Antes

```
At.Paciente#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)          LACP   Fa0/1(D) Fa0/2(P)
```

Figura A.35: Switch Acceso Después

```
Sw.Distribucion6#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)          LACP   Gig1/0/1(D) Gig1/0/2(P)
2      Po2(SU)          LACP   Gig1/0/3(P) Gig1/0/4(P)
```

Figura A.36: Switch Distribución Después

A.35. Validación Subred Interconexión

A.36. Red Completa del Hospital Son Espases

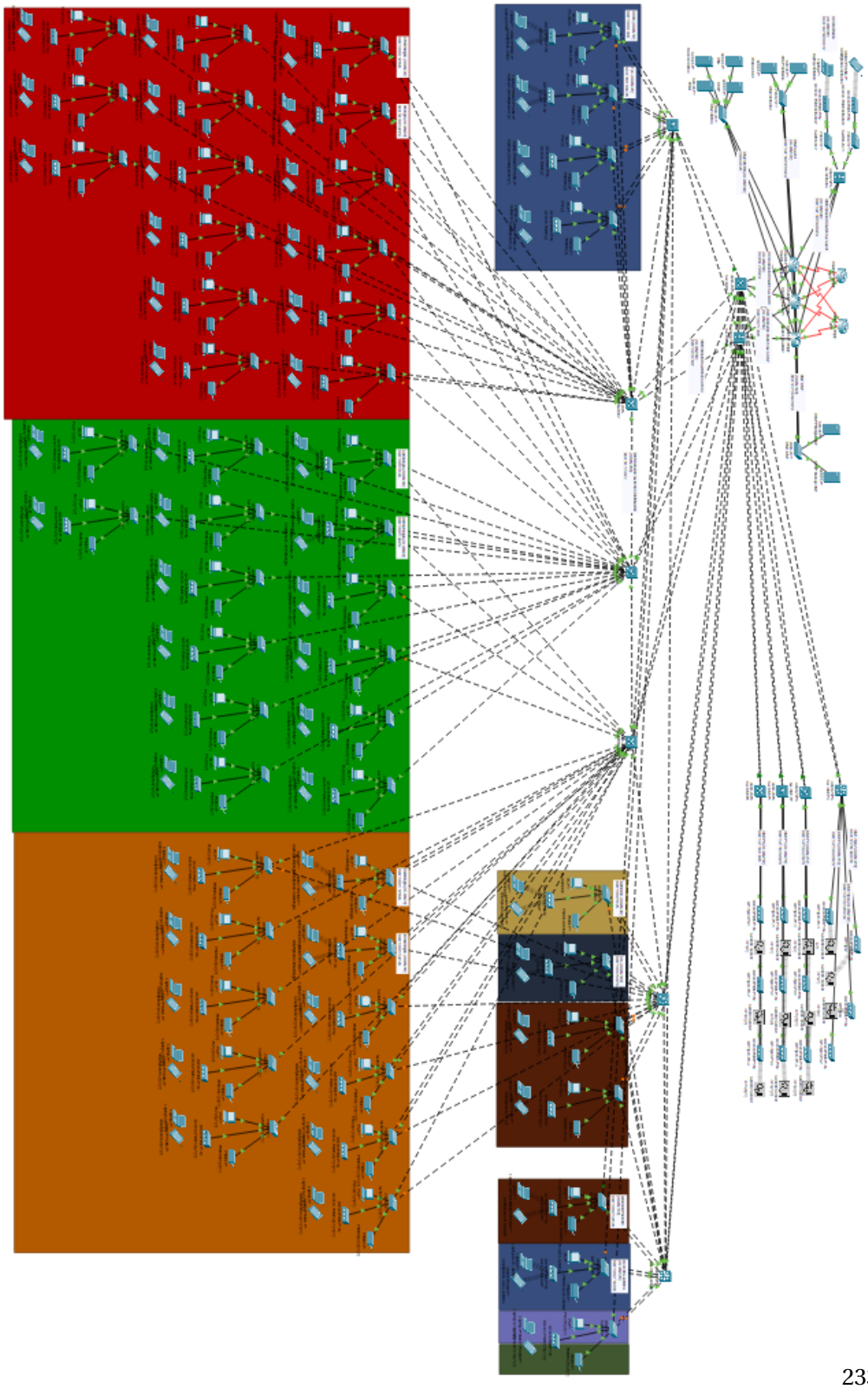


Figura A.37: Red Completa del Hospital Son Espases

A.37. Red Completa de Interconexión entre Hospitales

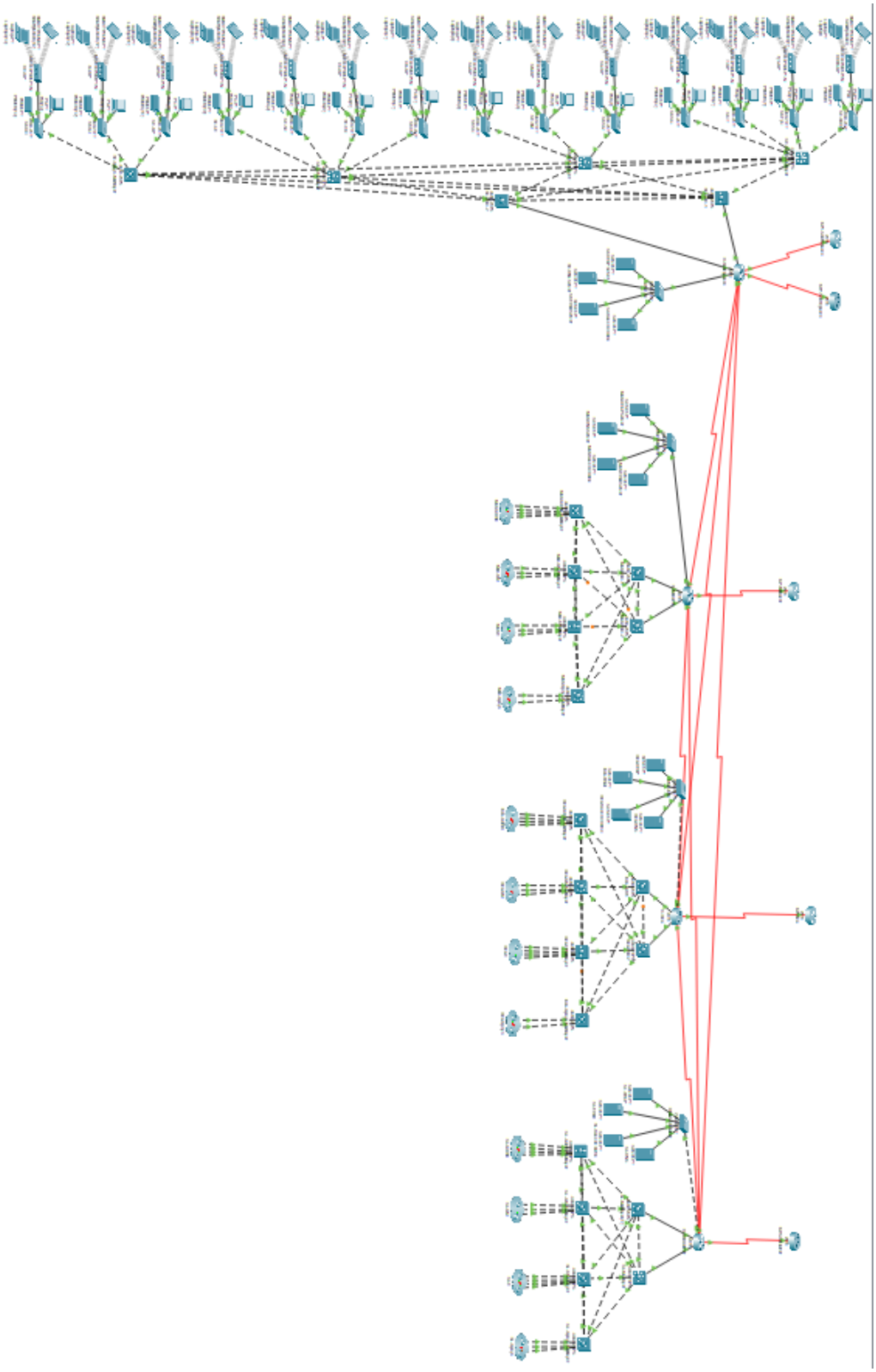


Figura A.38: Red Completa de Interconexión entre Hospitales

BIBLIOGRAFÍA

[1] I. Cisco Systems, *IP Routing: OSPF Configuration Guide*, 2024. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book/iro-cfg.html 2.2.1

[2] ——, *Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00*, 2024. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/software/17_4/b_redundancy_17-4_iot_switch_cg/m-ip-hsrp-cg.html 2.3.1

[3] NetworkLessons.com. (2024) Etherchannel on cisco ios catalyst switch. [Online]. Available: https://networklessons.com/switching/etherchannel-cisco-ios-catalyst-switch 2.3.2

[4] I. Cisco Systems, "Cisco hospital network design," Cisco, Tech. Rep., 2023. [Online]. Available: https://es.scribd.com/document/723946102/Report-CISCO-Hospital-Network-Design 2.4.2, 2.5.1, 2.5.2, 2.5.3

[5] C. Systems, *Configuring DHCP Snooping*, 2019. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/security/502_n2_1m/b_Cisco_n5k_security_config_gd_rel_502_n2_1/Cisco_n5k_security_config_gd_rel_502_n2_1_chapter8.pdf 2.5.4, 5.6.2

[6] AWS. (2024) ¿qué es ipsec? [Online]. Available: https://networklessons.com/switching/etherchannel-cisco-ios-catalyst-switch 2.5.5, 2.5.5, 2.5.5, 2.5.5

[7] B. Kim, S. Kim, M. Lee, H. Chang, E. Park, and T. Han, "Application of an internet of medical things (iomt) to communications in a hospital environment," *Applied Sciences*, vol. 12, no. 23, 2022. [Online]. Available: https://www.mdpi.com/2076-3417/12/23/12042 2.6

[8] A. A. El-Saleh, A. M. Sheikh, M. A. M. Albreem, and M. S. Honnurvali, "The internet of medical things (iomt): opportunities and challenges," in *Wireless Networks*, 2025, pp. 327–344. [Online]. Available: https://doi.org/10.1007/s11276-024-03764-8 2.6

[9] U. A. Patil, M. Venkatesan, and S. Prasad, "An improved wireless network architecture for iot in hospital healthcare," in *2021 IEEE Bombay Section Signature Conference (IBSSC)*, Nov 2021, pp. 1–6. 2.6

[10] E. HOSPITAL. (2023) ¿qué equipos son esenciales en la unidad de cuidados intensivos de un hospital? [Online]. Available: https://www.elhospital.com/es/noticias/que-equipos-son-esenciales-en-la-unidad-de-cuidados-intensivos-de-un-hospital 3.2.5

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

[12] IBSALUT. Hospital universitario son espases - ponent. [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

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

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

[15] C. Systems. (2011) Configuring access and trunk interfaces. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/503_n1_1/Cisco_n5k_layer2_config_gd_rel_503_N1_1_chapter6.html 6.2.1

[16] ——, *Configuring the Cisco IOS DHCP Relay Agent*, 2014. [Online]. Available: http://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htdhcpre.html 6.5.3

[17] ——. (2023) Understand rapid spanning tree protocol (802.1w). [Online]. Available: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html 6.7