Universitat de les Illes Balears

TRABAJO DE FIN DE GRADO

RED INTELIGENTE SEGURA DE LOS GRANDES HOSPITALES DE MALLORCA

Victor Canelo Galera

Grau d'Enginyeria Informàtica

Escola Politècnica Superior

Año académico 2024-25

RED INTELIGENTE SEGURA DE LOS GRANDES HOSPITALES DE MALLORCA

Victor Canelo Galera

Trabajo de Fin de Grado

Escola Politècnica Superior

Universitat de les Illes Balears

Año académico 2024-25

Paraules clau del treball: TFG, memoria, LaTeX

Tutor: Sebastià Galmes

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

ÍNDICE GENERAL

ACRÓNIMOS

RESUMEN

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

En este proyecto se presenta el diseño y simulación de una red hospitalaria utilizando Cisco Packet Tracer, 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) y protocolos de enrutamiento adecuados, además de incluir redundancia tanto a nivel de hardware como a nivel de enlace. 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

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, tecnologías y normativas implicadas. Este marco teórico tiene como finalidad proporcionar una visión general sobre las infraestructuras de red en entornos hospitalarios, su organización, los criterios de seguridad aplicables y las particularidades derivadas de la incorporación de tecnologías emergentes como el Internet of Medical Things (IoMT).

A lo largo de este capítulo se describirán los fundamentos de las redes LAN y VLAN, las características específicas de las redes hospitalarias, los requisitos de seguridad y segmentación, así como los retos que supone la gestión de dispositivos médicos conectados.

2.1 Redes de Computadores en Entornos Hospitalarios

El uso de redes de computadores en entornos hospitalarios constituye un pilar fundamental para el funcionamiento eficiente y seguro de los servicios sanitarios modernos. Los hospitales dependen en gran medida de infraestructuras de red que permitan la transmisión de información clínica, administrativa y de soporte, garantizando la disponibilidad, integridad y confidencialidad de los datos en todo momento. La correcta gestión de estas redes resulta esencial, ya que cualquier interrupción o fallo de seguridad puede afectar de forma directa a la calidad asistencial y, en casos críticos, incluso a la vida de los pacientes.

Dado el carácter crítico de estos entornos, una red hospitalaria debe ser diseñada y planificada cuidadosamente, considerando desde el inicio las necesidades presentes y futuras del centro, los riesgos potenciales y las medidas de seguridad necesarias. Una infraestructura bien segmentada y protegida no solo garantiza el correcto funciona-

miento de los servicios asistenciales, sino que también contribuye a la confidencialidad de los datos clínicos y a la seguridad de los pacientes.

Además, la irrupción de tecnologías emergentes como el Internet of Medical Things (IoMT) ha supuesto un nuevo desafío para estas redes, aumentando la cantidad de dispositivos conectados y ampliando la superficie de exposición a posibles ciberamenazas, lo que ha obligado a reforzar las políticas de seguridad y segmentación en las infraestructuras hospitalarias modernas.

2.2 Redes LAN y VLAN

2.2.1 Redes LAN en Entornos Hospitalarios

Una Local Area Network (LAN) es una red de área local que permite la interconexión de dispositivos dentro de un ámbito geográfico limitado, como puede ser un edificio, planta hospitalaria o campus sanitario. Su finalidad es compartir recursos de red, dispositivos y servicios de manera rápida y segura, permitiendo la comunicación entre estaciones de trabajo, servidores, dispositivos médicos y sistemas de almacenamiento centralizados.

En entornos hospitalarios, las redes LAN constituyen la infraestructura básica sobre la que se sustentan tanto los sistemas administrativos como los servicios asistenciales. Gracias a la conectividad que proporcionan, se facilita el acceso a sistemas de información hospitalaria, historiales médicos electrónicos, servicios de radiología digital y monitorización médica en tiempo real. Además, la llegada de nuevas tecnologías como el Internet of Medical Things (IoMT) ha incrementado notablemente la densidad de dispositivos conectados a las redes LAN hospitalarias, exigiendo una mayor capacidad de gestión, segmentación y seguridad en estas infraestructuras.

2.2.2 VLANs en Entornos Hospitalarios

Para mejorar la eficiencia, la seguridad y la organización de las redes LAN, se recurre a la creación de Virtual LANs (VLANs). Una VLAN permite agrupar lógicamente dispositivos dentro de una misma red física, segmentando el tráfico de datos aunque se encuentren conectados al mismo switch o infraestructura física.

Esta segmentación se basa en criterios funcionales, organizativos o de seguridad, de manera que cada grupo de usuarios o dispositivos que comparte necesidades similares de comunicación se integra en una VLAN específica. Esto evita el tráfico innecesario entre áreas que no requieren comunicación directa, mejora la seguridad al aislar departamentos sensibles y optimiza el rendimiento de la red al reducir las colisiones y la congestión de tráfico.

En entornos hospitalarios, las VLAN se utilizan habitualmente para separar el tráfico de los distintos departamentos (Urgencias, Administración, Laboratorio, Consultas Externas, etc.) y también para aislar segmentos críticos como la red de dispositivos médicos o la subred específica de IoMT. Esta segmentación lógica permite, además,

aplicar políticas de seguridad específicas mediante listas de control de acceso (ACLs), limitando la visibilidad y comunicación entre VLANs cuando sea necesario.

El uso de VLANs en entornos sanitarios aporta numerosos beneficios:

- **Mejora de la seguridad:** al separar físicamente el tráfico sensible, como datos clínicos o monitorización de pacientes, del resto de la red.
- **Optimización del rendimiento:** al reducir la cantidad de tráfico broadcast y minimizar las colisiones de red.
- **Flexibilidad en la gestión:** al permitir reasignar dispositivos o usuarios a diferentes VLANs sin necesidad de modificar la infraestructura física.
- **Facilidad de escalado:** favoreciendo la incorporación de nuevos servicios o dispositivos, como los IoMT, sin comprometer la seguridad ni el rendimiento de la red existente.
- **Aplicación de políticas de control de acceso más específicas y eficientes.**

Gracias a esta capacidad de segmentación y control, las VLAN se han convertido en un componente imprescindible para garantizar la seguridad, el buen funcionamiento y la disponibilidad de los servicios hospitalarios.

2.3 Seguridad en Redes Hospitalarias

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.

2.3.1 Principales Amenazas en Redes Hospitalarias

Las redes hospitalarias, por su naturaleza, presentan una serie de vulnerabilidades que pueden ser explotadas si no se implementan las medidas adecuadas. Entre las amenazas más frecuentes se encuentran:

- **Intercepción de datos sensibles:** accesos no autorizados a historiales médicos y datos clínicos personales.
- **Intrusiones externas e internas:** ataques desde el exterior o desde dentro de la propia red, aprovechando errores de configuración o dispositivos desprotegidos.
- **Ataques de denegación de servicio (DoS/DDoS):** que pueden dejar inoperativos servicios críticos.

- **Malware y ransomware:** capaces de bloquear el acceso a sistemas de información hospitalaria o alterar el funcionamiento de dispositivos clínicos.
- **Vulnerabilidades en dispositivos IoMT:** por sus recursos limitados y configuraciones menos robustas.

2.4 Introducción a IoMT (Internet of Medical Things)

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

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

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

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

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

En definitiva, la implantación del IoMT en entronos hospitalrios representa una oportunidad estratégica para transformar la asistencia sanitaria, dotándola de mayor flexibilidad, capacidad predictiva y resiliencia frente a sistuaciones de crisis como la

vivida durante la pandemia de COVID-19, donde estas tecnologías demostraron su potencial para mejorar la monitorización, la toma de decisiones y la gestión de recursos clínicos en tiempo real.

CAPÍTULO 3

ANÁLISIS

3.1 Requisitos del Sistema

3.1.1 Requisitos Funcionales

3.1.2 Requisitos No Funcionales

3.1.3 Requisitos de Seguridad

En terminos generales y requisitos especficos de la subred IoMT.

3.1.4 Requisitos de Conectividad

3.2 Interesados

xxx

CAPÍTULO 4

METODOLOGÍA DE TRABAJO

4.1 Enfoque y Planificación del Proyecto

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

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

4.1.1 Enfoque de Trabajo Adoptado

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

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

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

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

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

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

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

4.1.2 Planificación y Seguimiento

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

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

4.2 Herramientas y Tecnologías Utilizadas

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

4.2.1 Cisco Packet Tracer

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

4.2.2 Git y GitHub

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

4.2.3 Google Calendar

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

4.2.4 SketchUp

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

CAPÍTULO 5

DISEÑO

5.1 Criterios de Diseño

5.1.1 Segmentación por Departamentos y Servicios

5.1.2 Consideraciones Específicas para Dispositivos IoMT

5.2 Topología de Red Propuesta

5.2.1 Topología Física

5.2.2 Topología Lógica

5.2.3 Descripción de Dispositivos Utilizados

5.3 Direccionamiento IP y Subnetting

5.3.1 Planificación de Subredes

5.3.2 Asignación de Direcciones IP

5.3.3 Asignación de Direcciones IP Estáticas

5.4 Configuración de VLANs y Segmentación de Red

5.4.1 Definición de VLANs por Departamento

5.4.2 Asignación de Puertos a VLANs

5.4.3 Configuración de Troncales y Acceso a VLANs

5.5 Seguridad de la Red

5.5.1 Seguridad a Nivel Físico

5.5.2 Seguridad a Nivel Lógico

5.6 Subred IoMT: Diseño y Seguridad

5.6.1 Justificación de la Subred IoMT

5.6.2 Diseño y Direccionamiento de la Subred IoMT

5.6.3 Políticas de Seguridad para la Subred IoMT

5.6.4 COntrol de Accesos y Monitorización

5.7 Protocolos y Servicios de Red

5.7.1 Configuración de DHCP

5.7.2 Configuración de DNS

5.7.3 Configuración de NAT y Acceso a Internet

5.7.4 Configuración de Protocolos de Enrutamiento

5.7.5 Configuración de HSRP

CAPÍTULO 6

IMPLEMENTACIÓN

6.1 Configuración de Dispositivos

6.2 Creación de VLANs y Asignación de Puertos

6.3 Configuración de Direccionamiento IP

6.4 Configuración de Seguridad

6.5 Configuración de la Subred IoMT

CAPÍTULO 7

PRUEBAS Y VALIDACIÓN

7.1 Pruebas de Conectividad

7.2 Pruebas de Seguridad

7.3 Resultados y Análisis

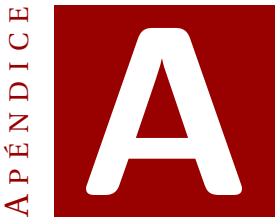
CAPÍTULO 8

CONCLUSIÓN

8.1 Logros Alcanzados

8.2 Dificultades Encontradas

8.3 Mejoras y Ampliaciones Futuras



ANEXO

BIBLIOGRAFÍA